MODELLING AND ANALYSIS OF DIGITAL GOVERNMENT TRANSFORMATION

(DİJİTAL DEVLET DÖNÜŞÜMÜNÜN MODELLENMESİ VE ANALİZİ)

by

Merve GÜLER KESMEZ, M.S.

Thesis

Submitted in Partial Fulfillment

of the Requirements

for the Degree of

DOCTOR OF PHILOSOPHY

in

INDUSTRIAL ENGINEERING

in the

GRADUATE SCHOOL OF SCIENCE AND ENGINEERING

of

GALATASARAY UNIVERSITY

Dec 2023

ACKNOWLEDGEMENTS

I would like to express my gratitude to my advisor, Prof. Dr. Gülçin BÜYÜKÖZKAN FEYZİOĞLU, for providing her unique guidance, knowledge, patience, and precious support throughout this thesis. I am grateful to her for offering help when I needed it. I would also like to thank committee members Prof. Dr. Orhan FEYZİOĞLU and Prof. Dr. Şule ÖNSEL EKİCİ for their help, support, encouragement, and guidance.

This thesis would not be possible without the contributions of the experts. I thank all of the experts who contributed to this thesis with their instrumental insights that were effective in getting case study results. Especially, I would like to thank Prof. Dr. Orhan FEYZİOĞLU for his precious contributions, support, and invaluable insights, and I would like to thank Dr. Cüneyt KALPAKOĞLU for his helpful approach, sharing his important experiences, and contributions.

I wouldn't have imagined this thesis journey without the support of my loved ones. I would like to thank to;

- My mother, Emine GÜLER, and my father, Orhan GÜLER, for their encouragement, confidence in me, and limitless support,
- My love of life, Halil KESMEZ, for his endless help during my Ph.D. thesis and for being the one who shares every moment of this journey with me,
- My best friend Esin MUKUL, for her precious friendship and for being the sister I needed.

I want to thank TÜBİTAK for providing financial support to realize my thesis with the project number 2211-A.

Dec 2023
Merve GÜLER KESMEZ

TABLE OF CONTENTS

LIST OF SYMBOLS

AHP	Analytic Hierarchy Process
AI	Artificial Intelligence
BM	Bonferroni Mean
BWM	Best Worst Method
C2M2	Cybersecurity Capability Maturity Model
CART	Classification and Regression Tree
CM	Cognitive Map
CMM	Cybersecurity Maturity Model
CMMI	Capability Maturity Model Integration
COBRA	Cost, Benefit, Risk, Opportunity
COPRAS	Complex Proportional Assessment
CR	Consistency Ratio
DCI	Digital Citizenship Improvement
DD	Dijital Devlet
DEA	Data Envelopment Analysis
DEMATEL	Decision-Making Trial and Evaluation Laboratory
DESI	Digital Economy and Society Index
DG	Digital Government
DGT	Digital Government Transformation
DM	Decision Maker
DSI	Digital Service Improvement
DTI	Digital Technology Improvement
FCM	Fuzzy Cognitive Map
FPR	Fuzzy Preference Relations
G2B	Government-to-Business
G2C	Government-to-Citizens
G2E	Government-to-Employee
G2G	Government-to-Government
GaaP	Government as a Platform
GDM	Group Decision-Making
GDPR	General Data Protection Regulation
HFBM	Hesitant Fuzzy Bonferroni Mean
HFL	Hesitant Fuzzy Linguistic
HFLBM	Hesitant Fuzzy Linguistic Bonferroni Mean
HFLCM	Hesitant Fuzzy Linguistic Cognitive Map
HFLHM	Hesitant Fuzzy Linguistic Heronian Mean
HFLPA	Hesitant Fuzzy Linguistic Power Average
HFLTS	Hesitant Fuzzy Linguistic Term Set
HFLOWA	Hesitant Fuzzy Linguistic Ordered Weighted Averaging

HFLOWG	Hesitant Fuzzy Linguistic Ordered Weighted Geometric
HFPR	Hesitant Fuzzy Preference Relations
HFPR-AHP	Hesitant Fuzzy Preference Relations Analytic Hierarchy Process
HFS	Hesitant Fuzzy Sets
HFLWA	Hesitant Fuzzy Linguistic Weighted Averaging
HFLWG	Hesitant Fuzzy Linguistic Weighted Geometric
HM	Heronian Mean
HMPM	Hesitant Multiplicative Programming Method
ICT	Information and Communication Technologies
IoT	Internet of Things
IS	Information Systems
ISO	International Organization for Standardization
IT	Information Technology
MCDM	Multi-Criteria Decision-Making
N/A	Not Applicable
NIST	National Institute of Standards and Technology
OGD	Open Government Data
OWA	Ordered Weight Average
PA	Power Average
PRISMA	Preferred Reporting Items for Systematic Reviews and Meta-Analyses
QFD	Quality Function Deployment
RI	Random Index
RQ	Research Question
SDG	Sustainable Development Goal
TOPSIS	The Technique for Order of Preference by Similarity to Ideal Solution
U.K.	United Kingdom
U.S.	United States
VIKOR	VIseKriterijumska Optimizacija I Kompromisno Resenje
WoS	Web of Science

LIST OF FIGURES

LIST OF TABLES

ABSTRACT

With the rapid development of digital technologies, digital transformation reshapes the functioning of governments. Digital Government (DG) aims to leverage technology to enhance the delivery of public services, improve efficiency, and foster transparency. Embracing DG is a strategic imperative for governments looking to provide practical, transparent, and citizen-centric services in the 21st century. Therefore, many government organizations intensified their DG efforts in response to its necessity.

The comprehensive literature review on the DG field revealed that research focusing on a holistic DG approach for reducing failures and increasing the success of DG transformation initiatives is very limited, and generally, these studies focus on a single point of view considering benefits and employ qualitative approaches. This thesis aims to address the aforementioned literature gaps by modelling and analysing DG framework with integrated methodologies to obtain an accessible, effective, and accountable DG.

Therefore, the main stages of the thesis are: Modelling and analysis of the DG framework for a better understanding of the success and risk factors of the DG transformation by using the Cognitive Map approach; Proposing a Cybersecurity Maturity Model and analysing cybersecurity maturity levels of public institutions using the Multi-Criteria Decision-Making methods; Proposing a cybersecurity roadmap for providing secure DG transformation to public institutions by using gap analysis. The Hesitant Fuzzy Linguistic Term Set technique is integrated with the Cognitive Map approach, and the incomplete Hesitant Fuzzy Preference Relations technique is integrated with Multi-Criteria Decision-Making methods.

In the first stage, the Digital Government Transformation (DGT) is investigated into how governments shall transform themselves to take advantage of the potential of emerging

and future digital technologies, enhance DG adoption through the implications of digital transformation on its structures, and extend the relationships with all stakeholders.

The modelling and analysis of success and risk factors of DGT provides a holistic framework by considering multiple factors and provides valuable insights for public institutions. Focusing on cybersecurity for secure DGT in the second stage helps public institutions assess cybersecurity maturity levels. Finally, the cybersecurity action plans and roadmap can be used as a guide for providing secure DGT.

Case studies are realized with the help of experts to show the robustness of the proposed approaches. At the end of case studies, the results are discussed. The concluding remarks are provided to build an effective DG framework in the DG transformation journey.

ÖZET

Dijital teknolojilerin hızla gelişmesiyle birlikte dijital dönüşüm, devletlerin işleyişini yeniden şekillendirmektedir. Dijital Devlet (DD), kamu hizmetlerinin işleyişini geliştirmek, verimliliği artırmak ve şeffaflığı teşvik etmek için teknolojiden yararlanmayı amaçlamaktadır. DD'yi benimsemek, 21. yüzyılda pratik, şeffaf ve vatandaş odaklı hizmetler sunmak isteyen devletler için stratejik bir zorunluluktur. Bu nedenle birçok devlet kurumu, bu gerekliliğe yanıt olarak DD çalışmalarını yoğunlaştırmıştır.

DD konusuna ilişkin kapsamlı literatür taraması, DD dönüşümü girişimlerinin başarısızlıklarını azaltmak ve başarısını artırmak için bütünsel bir yaklaşıma odaklanan araştırmaların oldukça sınırlı olduğunu, genellikle bu çalışmaların faydaları dikkate alarak tek bir bakış açısına odaklandığını ve niteliksel yaklaşımlar kullandığını ortaya koymuştur. Bu tez, erişilebilir, etkili ve hesap verebilir bir DD elde etmek için DD yapısını entegre metodolojilerle modelleyerek ve analiz ederek yukarıda belirtilen literatürdeki boşlukları gidermeyi amaçlamaktadır.

Tezin temel adımları şu şekildedir: DD dönüşümünün başarı ve risk faktörlerinin daha iyi anlaşılması için Bilişsel Haritalama yaklaşımı kullanılarak DD yapısının modellenmesi ve analizi; Sibergüvenlik Olgunluk Modeli'nin önerilmesi ve kamu kurumlarının sibergüvenlik olgunluk düzeylerinin Çok Kriterli Karar Verme yöntemleri kullanılarak analiz edilmesi; kamu kurumlarında güvenli DD dönüşümünün sağlanmasına yönelik sibergüvenlik yol haritasının boşluk analizi kullanılarak önerilmesi. Sezgisel Bulanık Dilsel Terim Seti tekniği Bilişsel Haritalama yaklaşımıyla, tamamlanmamış Sezgisel Bulanık Tercih İlişkileri tekniği ise Çok Kriterli Karar Verme yöntemleriyle entegre edilmiştir.

Tezin ilk aşamasında, DD dönüşümünde, devletlerin yeni ortaya çıkan ve gelecekteki dijital teknolojilerin potansiyelinden yararlanmak için kendilerini nasıl dönüştürecekleri, dijital dönüşümün etkileri neticesinde DD'in benimsenmesini nasıl geliştirecekleri ve tüm paydaşlarla ilişkileri nasıl geliştirecekleri araştırılmaktadır. Bu doğrultuda, DD dönüşümünde başarı ve risk faktörlerinin modellenmesi ve analizi, birden fazla faktörü göz önünde bulundurarak bütünsel bir çerçeve sağlamakta ve kamu kurumları için değerli bilgiler sunmaktadır. İkinci aşamada, güvenli DD dönüşümü gerçekleştirmek için sibergüvenliğe odaklanılarak, kamu kurumlarının sibergüvenlik olgunluk seviyelerini değerlendirmesi sağlanmaktadır. Son olarak sunulan sibergüvenlik eylem planları ve yol haritası ise DD dönüşümünün sağlanmasında bir referans olarak kullanılmaktadır.

Önerilen yaklaşımların sağlamlığını göstermek için uzmanların yardımıyla vaka çalışmaları gerçekleştirilmektedir. Vaka çalışmalarının sonunda bulgular tartışılmaktadır. Çalışmanın sonuçları DD dönüşümü yolculuğunda etkin bir DD yapısı oluşturmak için sunulmaktadır.

1. INTRODUCTION

1.1 Digital Government (DG)

Digital technologies are no doubt transforming societies. The McKinsey Global Institute highlighted digital technology adoption as the most critical factor for future economic growth, accounting for about sixty percent of potential productivity growth by 2030. Digital technologies support governments in engaging with their stakeholders (e.g., citizens, businesses, and government agencies) and improve government legitimacy by operating more transparently, giving governments win-win opportunities through technology and automation (McKinsey & Company, 2020). Electronic government (e-government) initiatives are also getting increasingly popular (Ashaye & Irani, 2019). The "e-Government" concept is evolving into the idea of "digital government" (DG) over time with the utilization of new technologies (e.g., mobile applications, data analytics, social media, open data, Internet of Things (IoT)) (Ramon Gil-Garcia et al., 2007).

The four types of DG interactions are studied in the related literature: (1) Government-to-Citizens (G2C): the government intends to interact with citizens; (2) Government-to-Business (G2B): the government intends to interact with business enterprises; (3) Government-to-Government (G2G): the government intends to make services more friendly, transparent, convenient, and inexpensive; (4) Government-to-Employee (G2E): the government intends to empower employees to help citizens in the most appropriate and fastest way, speed up administrative processes, and optimize governmental solutions (ElKheshin, 2016). Despite considerable investments in the last three decades, there is still a need to transform governments. While this transformation is on the agenda of the public sector itself, government employees, policymakers, citizens, and businesses, not all actors understand the same under a DG. People's and businesses' expectations and interactions with governments change continuously. Meeting such new expectations constitutes a great challenge for governments (Zou et al., 2023).

1.2 Characteristics of DG

In the related literature, there is no proper agreement on the definition of DG, and different conceptualizations contain and focus on various aspects (Gil-Garcia & Flores-Zúñiga, 2020). In this section, different meanings of "digital government,"; "e-government,"; "government 4.0,"; "m-government," "t-government," and "GaaP" from different sources are presented. Figure 1.1 illustrates these definitions (ElKheshin, 2016; Hussain, 2017; Institute for Government, 2021; Janowski, 2015; Y. Liu et al., 2014; Margetts & Naumann, 2017; Weerakkody et al., 2019).

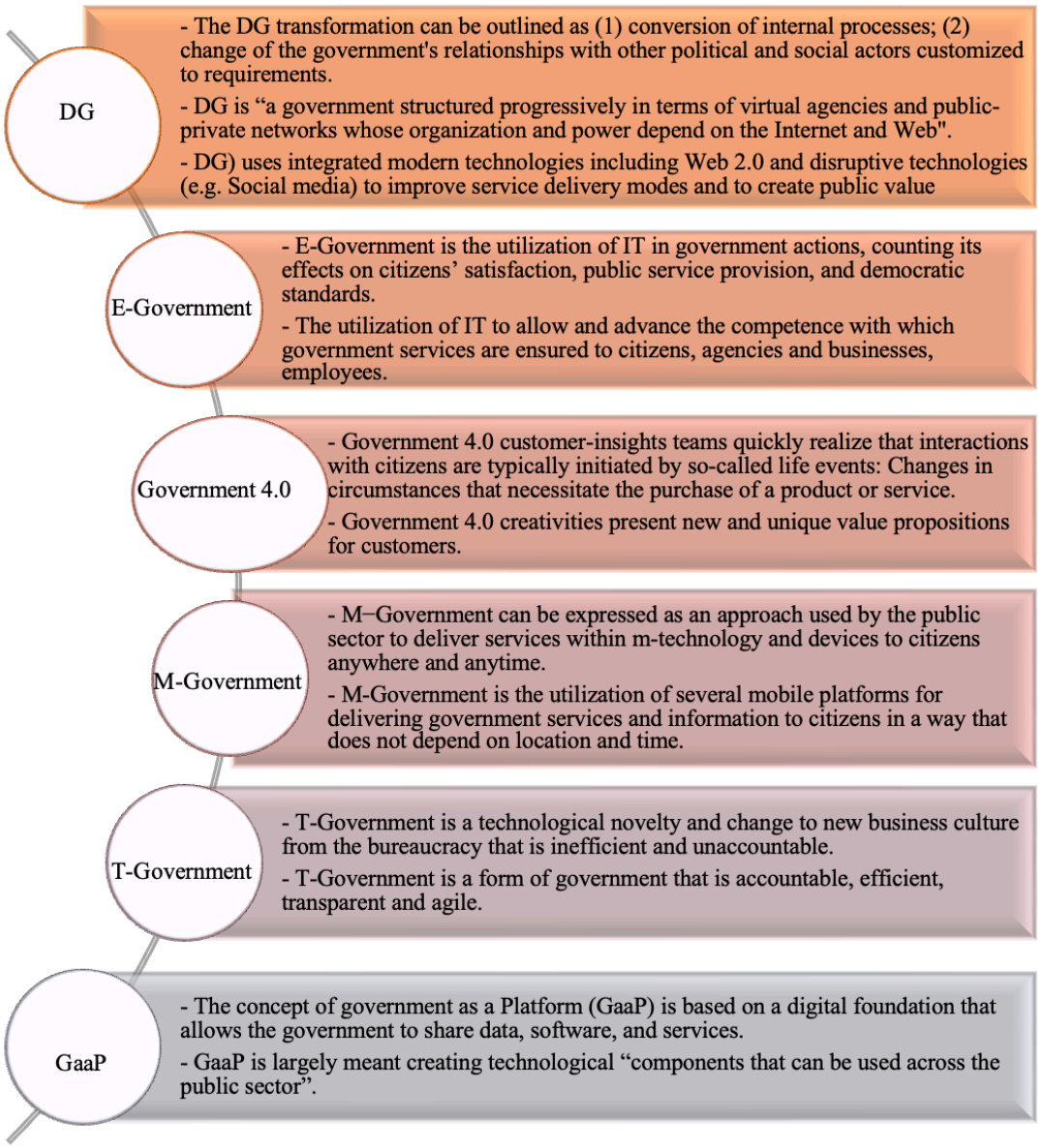

Figure 1.1: Definitions of concepts

Based on existing research (M. Hasan et al., 2018; Janowski, 2015), we define DG as follows (Güler & Büyüközkan, 2023): "A government that is organized progressively in terms of virtual agencies, cross-agency, and public-private networks to deliver improved public services and advance its relationships with citizens, the private sector, and civil society by improving service delivery modes and creating public value."

Figure 1.2 illustrates the evolution of DG. In the late 1990s-early 2000s, DG operated by one-way government-oriented operations at a national level, paper transactions were replaced by worldwide web (i.e., www) technologies, and key Information and Communication Technologies (ICT) areas were infrastructure management. In the late 2000s-early 2010s, DG operations focused on citizen-oriented operations, collaborative governance was aimed, Web 2.0 technologies and open-source computing power were driving technologies, and key ICT areas were people and data.

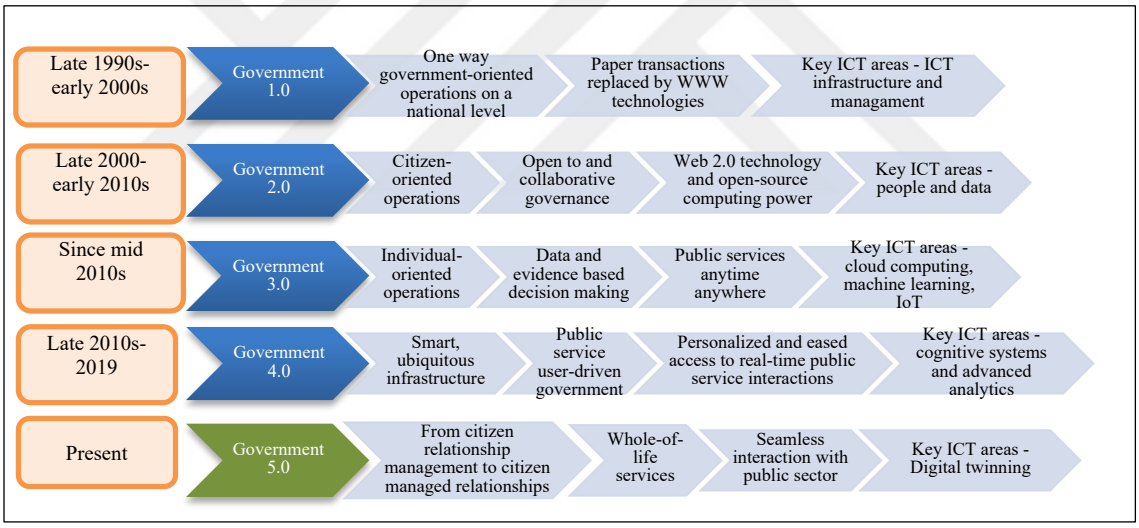

Figure 1.2: The evolution of DG (Barcevičius et al., 2019)

Since the mid-2010s, DG has focused on individual-oriented operations, data, and evidence-based decision-making as a management tool; providing public services anytime and anywhere was achievable. Key ICT areas were cloud computing, machine learning, and IoT. In late 2010-2019, smart ubiquitous infrastructure was implemented where user-driven public services with personalized access to real-time interactions were employed. Key ICT areas were cognitive systems and advanced analytics. From 2020 to the present, citizen-managed relationships were achieved by implementing whole-of-life

services with seamless interaction with the public sector, and key ICT areas were digital twinning (Barcevičius et al., 2019).

DG should not be isolated from the overall context of effective governance. DG does not exist in a vacuum and should be seen as a means to enhance citizen orientation and public service delivery within a given government. Based on the OECD report (OECD, 2020), the main dimensions of DG are illustrated in Figure 1.3. They are designed in the DG policy instrument of OECD to ensure adequate public sector digital transformation.

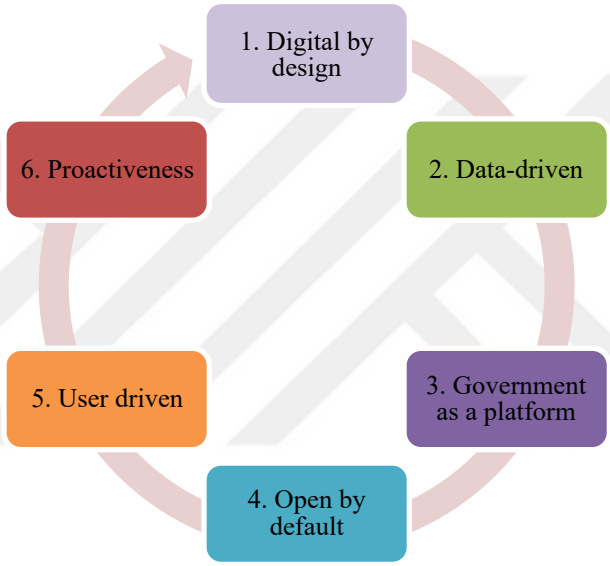

Figure 1.3: Dimensions of DG (Source: OECD (2020))

McKinsey & Company (2020) highlights three challenges for the digital technologies' utilization in governments' operations;

- Workers' skills are usually insufficient;
- Future works are less inclusive and more unequal without reforms;
- Resistance to automation.

According to WEF (2023), collaboration is more essential than ever to achieve the successful digital transformation goal for governments.

Based on the UN Committee of Experts on Public Administration (CEPA) report (ESCAP, 2021), there are three pillars for DG; these pillars are:

- Effectiveness,

- Accountability,
- Inclusiveness.

These pillars serve the UN's sixteenth Sustainable Development Goal (SDG): peace, justice, and strong institutions. The main principles under these three pillars for DG are illustrated in Figure 1.4.

Figure 1.4: Principles of DG (Source: ESCAP (2021))

The drivers of DG can be summarized as:

- **Political and Social Drivers**

Governments usually try to find ways to meet their citizens' expectations to sustain or increase their legitimacy and approval. Citizens' demands can represent a strong driver for governments to adopt them since they realize these technologies can drastically improve the democratic processes. Citizens are willing to obtain political outcomes and want transparency in decision-making. Therefore, they are developing a more incredible culture of interacting and participating in policy-making.

- **Economic Drivers**

The cost savings are direct and indirect. It can be related to lesser expenditure on administrative processes from the public budget or enabling citizens, businesses, and

managers to complete their tasks faster and more successfully. Cognitive automation can realize tasks at impractical scales, speeds, and volumes. Besides service delivery, many significant economic and social benefits are achieved through advanced technology utilization to inform decision-making across government, providing an excellent opportunity for governments.

- **Technological Drivers**

It stems from significant recent advancements in ICTs. The ubiquity of ICTs, their increasing ability to make connections and process, analyze, and store data, as well as increasing ICT literacy and accessibility, are also primary drivers for open and digital government. For instance, the development of mobile technology and the decreasing costs have acted as significant drivers for developing open e-government services to be mobile-compatible. The smartphones' fast-increasing technological capacity and constant connection have allowed citizens to access public services 'on the go. Moreover, it has driven a surge in public authority mobile application development for open government services.

The challenges for DG can be summarized as:

- **Technological Challenges**

The first technological challenge is the outdated IT infrastructure of the public sector. The lack of interoperability can be considered as the second technological barrier. Another relevant technical barrier is determined as access to data in the literature. This is a fundamental precondition for producing the potential benefits of governments. Because the more government data is available as open data, the greater the capacity to contribute to policy innovation through big data analysis.

- **Organizational Challenges**

The lack of strategy aimed at a fundamental digital transformation of governments has been identified as the leading barrier impeding early-stage organizations from taking full advantage of digital trends. Government agencies are trying to redesign their human resource strategy because of increased work and processes. The public-sector workforce transformation has not been easy for most governments, but this will become one of the critical enablers for a successful digital transformation. The diffusion of digital government is highly related to the digital skills of government employees.

- **Legal Challenges**

The lack of legal frameworks appropriate to the new technologies is another barrier governments face since new privacy and regulatory issues are developing. Personal information disclosure is threatened by occurrences of making government datasets publicly available. This situation may result in open profiling or data mining for private purposes. The issue of cybersecurity is the other challenge that governments face. Therefore, new legal frameworks should address privacy issues and broader accountability challenges.

- **Ethical Challenges**

There is an increasing need to develop new ethical frameworks around algorithms that support decision-making since transparency and ethical use of data have also become critical issues. AI and other technologies affect ethical issues very significantly.

- **Social and Cultural Challenges**

One of the most relevant barriers in the e-government evolution is the low level of citizens' adoption of e-government services by many authors; governments are now focusing on the citizens' side. However, it varies across countries since the social and behavioral factors explain the low level of adoption of government services.

- **Economic and Financial Challenges**

At the idea generation and idea selection phase, financial issues are sometimes considered an obstacle to innovation. For instance, many ideas have been developed for public sector improvement, and a few can be developed further.

1.3 Research Framework and Directions

The main objective is to model and analyze the DG framework. Research on the DG subject in academic papers, industry reports, and theses revealed research gaps. Several findings are developed to address these research gaps and progress in the potential research directions. The chapters of this thesis support the DG by addressing the following statements.

- **Lack of frameworks (roadmaps) for successful DG implementations**

There is a need for frameworks to further guide DG implementations by considering the interrelationships among variables from all perspectives with analytical techniques. This thesis proposes the cognitive map approach to address this gap. Examining the DG implementation framework by using cognitive maps can shed light on four important properties of the framework's causal structure: the levels of complexity, focus, and clustering that characterize the causal structure and the mechanisms underlying the causal links featured in that structure.

- **Lack of comprehensive research on the success/ failure factors of DGT**

Insufficient attention is paid to the issues of government digitalization risks, and more comprehensive and balanced perspectives on the influential factors on DGT are practically absent. This thesis proposes a comprehensive DGT success/risk factors framework to address this gap.

- **Lack of efficient practices to address security and trust issues among stakeholders**

There is a lack of studies providing practices for governments to increase citizens' trust and confidence. Cybersecurity can enhance citizens' trust by protecting against unauthorized access to data centers and other computerized systems. Thus, cybersecurity can help governments adopt DG services by preventing mistrust. This thesis addresses this research gap by proposing a cybersecurity maturity model, presenting a research methodology for cybersecurity maturity assessment, and proposing a cybersecurity roadmap for providing secure DGT.

- **Lack of analytical techniques**

The DG literature is mainly based on qualitative research. Although the implementation of analytical techniques is appropriate, little study combines the subject with analytical techniques. The research integrating the subject with those techniques certainly gains different perspectives and becomes closer to real-life problems. For this reason, in this thesis, integrating the DG subject with the cognitive map approach and MCDM methods provides a robust methodology.

- **Lack of fuzzy extensions and GDM**

The fuzzy extensions (i.e., type-1 fuzzy sets, type-2 fuzzy sets, intuitionistic fuzzy sets) and GDM approach are restricted in DG and cybersecurity literature. This thesis proposes an HFLCM methodology, an incomplete HFPR AHP method, and GDM with HFL Bonferroni means operator to address this gap.

The main stages of this thesis can be summarized:

- Modelling and analysis of the DG framework for a better understanding of the success and risk factors of the DG transformation using the CM approach under HFLTS and GDM environment.
- Proposing a Cybersecurity Maturity Model (CMM) and analyzing cybersecurity maturity levels of public institutions using the MCDM methods under incomplete HFPRs GDM environment.
- Proposing a cybersecurity roadmap for providing secure DG transformation to public institutions by using gap analysis.

The research framework of the thesis is provided in Figure 1.5, where the goals, the research questions, the methodology, and the findings of the chapters are included. The thesis consists of six chapters. A detailed literature review of DG is provided in Chapter 2. The technical background of the techniques used is provided in Chapter 3. In Chapter 4, the success/risk factors of the DGT framework are modeled and analyzed with the HFLCM approach. Chapter 5 provides a detailed review of cybersecurity, and CMM, then proposes a CMM, a methodology for maturity assessment, and a cybersecurity roadmap for providing secure DG. Finally, Chapter 6 summarizes the conclusion, contributions, limitations, and recommendations for future research.

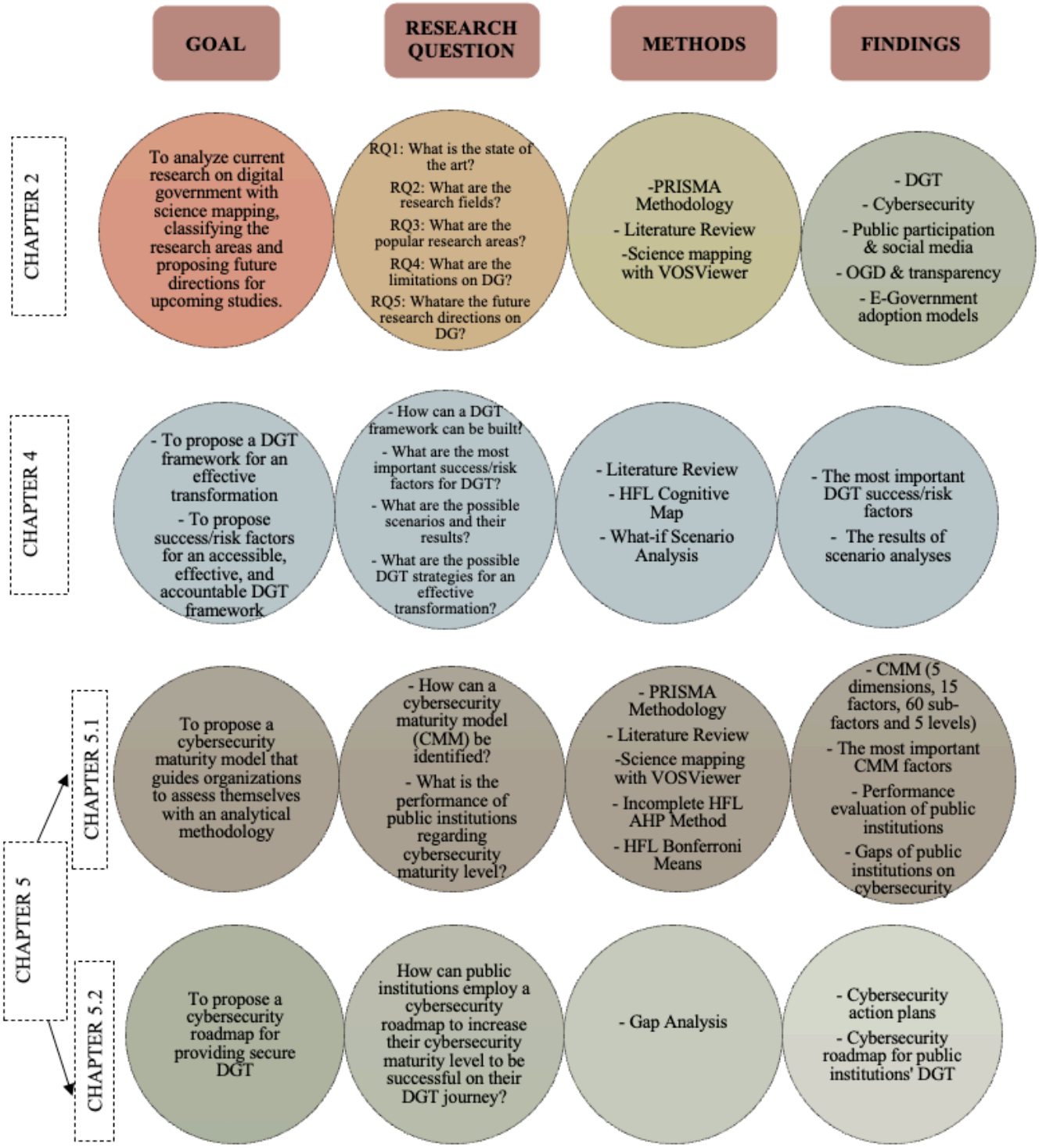

Figure 1.5: The research framework

2. LITERATURE REVIEW ON DG

Many recently published studies are discussing DG. Some reviews examined local governments in specific regions or countries (Erzhenin, 2018; E. Li et al., 2023). Some others studied the DG architecture by examining the challenges and problems to investigate the research agenda (Baheer et al., 2020; Clarke, 2020; Wilson & Mergel, 2022). Other review papers focused on knowledge management in the public sector and Open Government Data (OGD) (Alvarenga et al., 2020; Matheus & Janssen, 2020). So far, none of these studies about DG has applied science mapping to capture the literature by examining their key terms. Science mapping applies visualization methods to ensure a novel approach to dynamically discover new frontiers (Alcaide–Muñoz et al., 2017).

The complex structure of these studies indicates a need to progress the research in the DG field by classifying the existing studies. This study presents a systematic literature review with science mapping about DG. Our literature review aims to answer the following research problem about future studies' construction on the concept of DG based on existing research. We have further developed the following RQs for this research problem:

- RQ1: What is the state of the art of DG?
- RQ2: What are the research fields (i.e., article type, applied methods, technology, country) of the research on DG?
- RQ3: What are the popular research areas of DG?
- RQ4: What are the limitations of the existing research on DG?
- RQ5: What are the future research directions of DG?

The main contributions of this review can be listed as follows:
(1) We present the preliminaries of DG, such as the definitions and the research fields, and summarize the existing research on DG.

(2) Based on the existing literature, we utilize VOSviewer (van Eck & Waltman, 2014), an instrument for text mining, to perform bibliometric analysis to follow the latest developments and illustrate the main areas of DG.
(3) According to the analysis of existing research, we point out the limitations of present research concerning DG and present the potential future research directions.

Constructing the co-occurrence, bibliographic coupling, and co-citation networks can allow us to find proximate research areas, authors collaborating, sources with the most citations, and the most examined countries. At the very least, such a map can help trace the relationships' change as discoveries are made over time (Alcaide–Muñoz et al., 2017). This study uses bibliometric maps to handle the limitations of subjective human judgments. Though the interpretation of the bibliometric maps is based on subjective reviews, this technique can significantly decrease the impact of human factors. In other words, this technique offers an objective perspective for analyzing DG research. Therefore, integrating subjective and objective analyses improves the quality of our literature review. This paper may inspire other academics, practitioners, policymakers, and public employees to comprehend the subject better, set up a theoretical framework, discover research gaps, and identify future directions in the field of DG.

2.1 Review Methodology

This study presents a systematic review using the PRISMA (Preferred Reporting Items for Systematic Reviews and Meta-Analyses) guidelines for searching activities, as illustrated in Figure 2.2 (Moher et al., 1996). At the very start, we collect data from the WoS and Scopus databases. Then, we pre-process data to remove duplications.

In the literature review (i.e., the left side of Figure 2.2), the abstracts and full texts are first screened to identify those articles that will be included in the detailed analysis. Only publications in the related areas are included. Dissertation theses and industry papers about DG are added to the selected articles. In science mapping (i.e., the right side of Figure 2.2), the pre-processed data (n=11,917) are transferred to VOSViewer. Then, the keyword co-occurrence analysis, bibliographic coupling, and co-citation analysis are

applied to create bibliometric networks. The clusters are determined, and the research on the DG subject is visualized through maps.

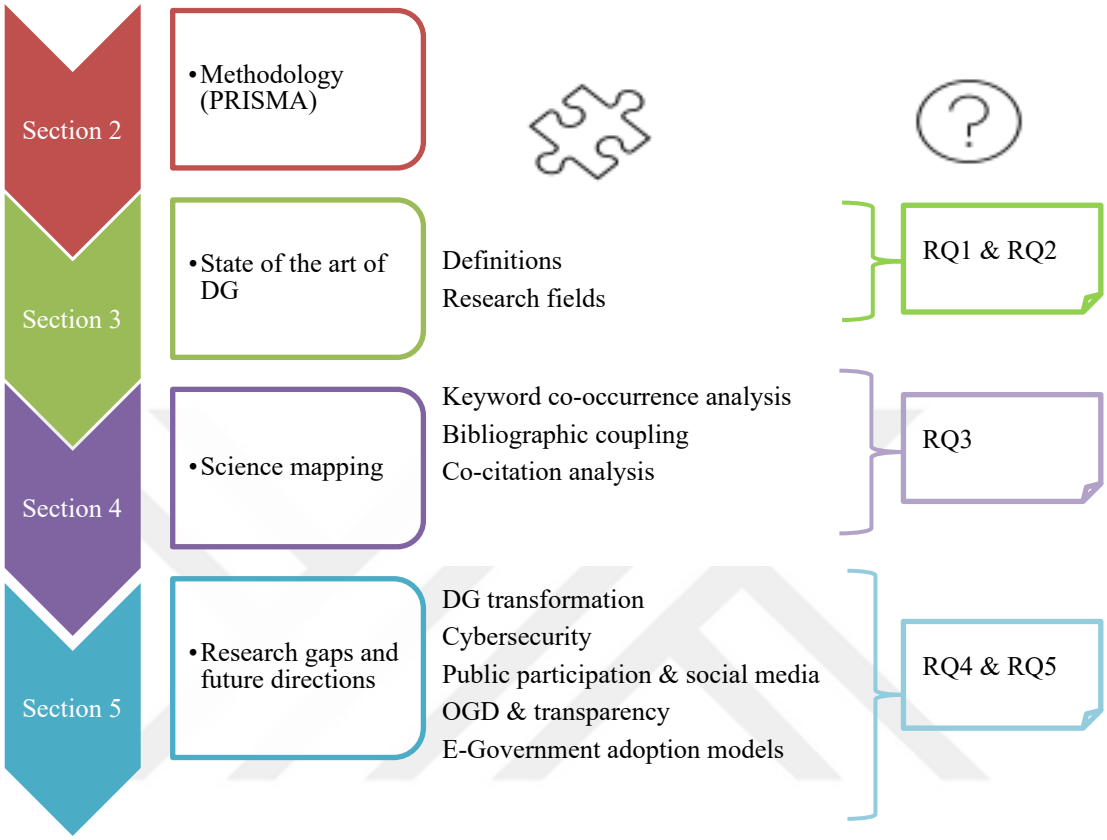

Figure 2.1: The overall survey framework

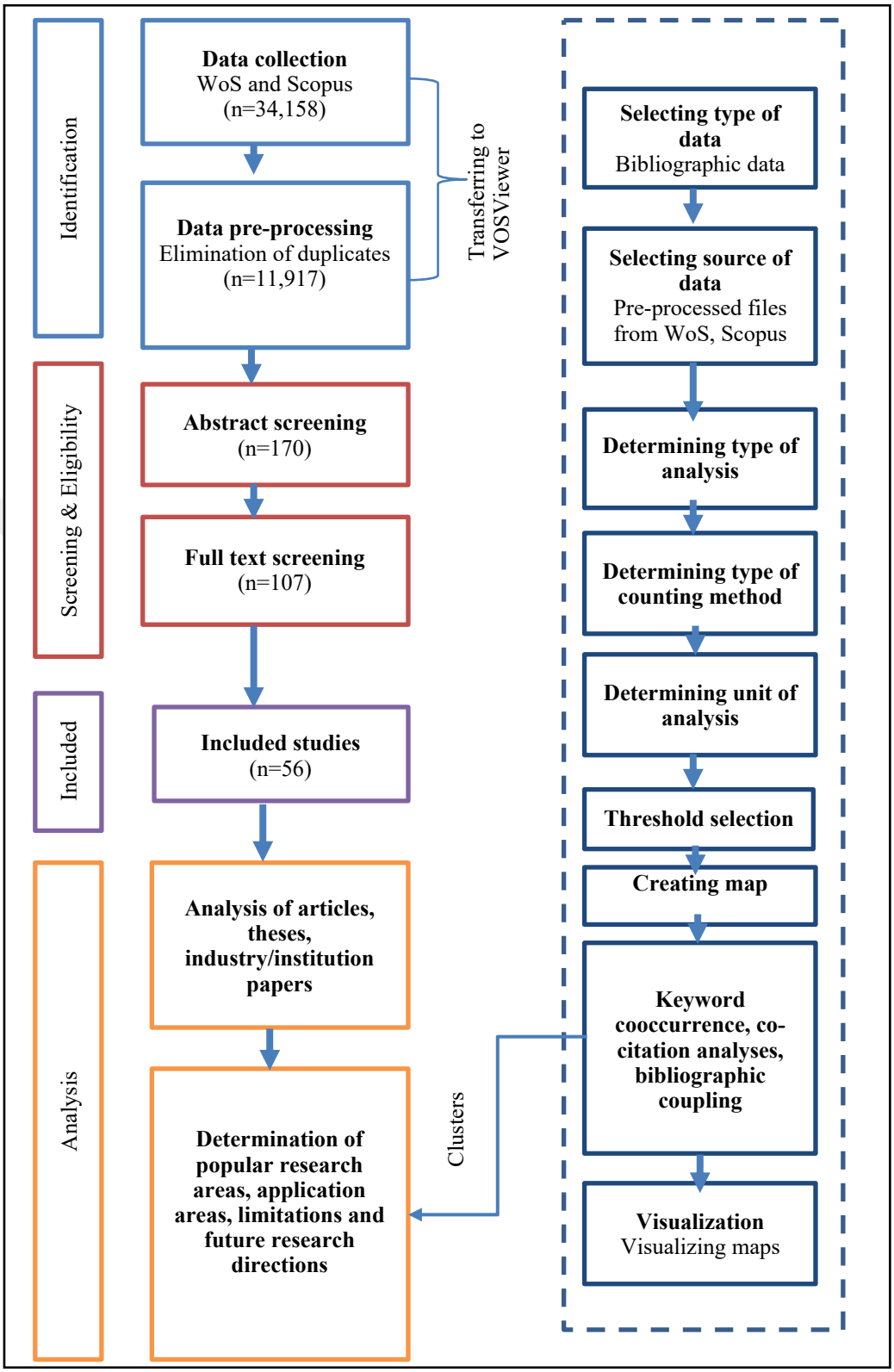

Figure 2.2: The PRISMA flow guiding the review methodology

2.1.1 Data Collection and Data Extraction

The first step of bibliometric analysis is to gather the required metadata (e.g., references, authors, citations, countries, etc.). The two largest databases are Scopus from Elsevier and the Web of Science (WoS) from Clarivate Analytics. In this paper, data is collected from these two databases. The search strings are used for the "topic" field in the WoS core collection. This ensures that the results include the selected keyword in the documents' title, abstract, and author keywords. In Scopus, the search strings are used for the "article title, abstract, keywords" field. The databases are searched with the following keywords with six queries:

> "digital government"; "e-Government"; "digital technology" AND "government"; "digital transformation" AND "government"; "platform" AND "government"; "ICT" AND "government".

The search is restricted to the criteria given in Table 2.1. Then, restraints are applied to the year (documents published after 2000), language (English), and document type (articles) (Merigó et al., 2016).

Table 2.1: The number of papers on data extraction phases (Source: Authors' own elaboration)

Search Keywords	1. Initial Search		2.Year (2000-2023)		3.Language (English)		4.Document type (Article)	
	WoS	Scopus	WoS	Scopus	WoS	Scopus	WoS	Scopus
1. "digital government"	687	1184	686	1183	657	1145	387	404
2. "e-Government"	10,724	17766	10,717	17,761	10,289	16,570	5514	5237
3. "digital technology" AND "government"	555	2110	550	2087	532	1997	407	972
4. "digital transformation" AND "government"	782	1298	782	1298	722	1226	466	497
5. "platform" AND "government"	17,727	14,834	11,009	17,202	10,388	16,261	6661	7928
6. "ICT" AND "government"	5032	7420	5021	7393	4755	7190	2732	2953
Total	35,507	44,612	28,765	46,924	27,343	44,389	16,167	17,991

Following this, duplicates within and between WoS and Scopus search results, first within the same database and then between both databases, were eliminated by removing articles with identical DOIs, ending up with 11,917 records.

After duplications are eliminated, 170 abstracts are screened, and examined based on their aims, methods, and findings. Then, 107 full texts are examined regarding their contents, originality, methods, and findings. To analyze the DG subject, 56 articles are included, and these articles are examined in detail.

2.1.2 Data Analysis with Science Mapping

Science mapping aims to build bibliometric maps defining how research areas, scientific fields, or disciplines are socially, conceptually, and intellectually formed (Cobo et al., 2011). In this study, we have selected VOSViewer version 1.6.15., since it is a powerful and efficient tool for illustrating bibliometric maps. It is compelling to introduce large bibliometric maps in an efficiently interpretable way (van Eck & Waltman, 2014). VOSviewer provides the main functions for generating, visualizing, and discovering bibliometric networks.

The terminology should be clear to better make sense of the maps created by the software. Items are the objects of interest (e.g., researchers, publications, or terms), and a link is a relationship or a connection between two items. A network is a set of items with links between the items. A cluster is a set of items grouped in a map. In VOSViewer, clusters are non-overlapping (van Eck & Waltman, 2014). Natural language processing algorithms determine the terms in the text data. Bibliographic data can be used in VOSviewer for WoS, Scopus, PubMed, RIS, or Crossref JSON files.

2.2 State-of-the-art DG

2.2.1 Analysis of the Academic Papers

The number of publications with the “digital government” keyword published from 2000 to 2023 November is illustrated in Figure 2.3. In the first 17 years, the number of journal articles grew steadily. Our research has shown a solid increasing trend from 2018 to 2020.

The number of journal articles increased from 28 in 2018 to 55 in 2020. In 2021, 53 articles were published. In 2022, 83 publications showed the growing attention to studies related to the DG subject. Until November 2023, there were 101 studies, and the increasing trend is expected to continue till the end of 2023.

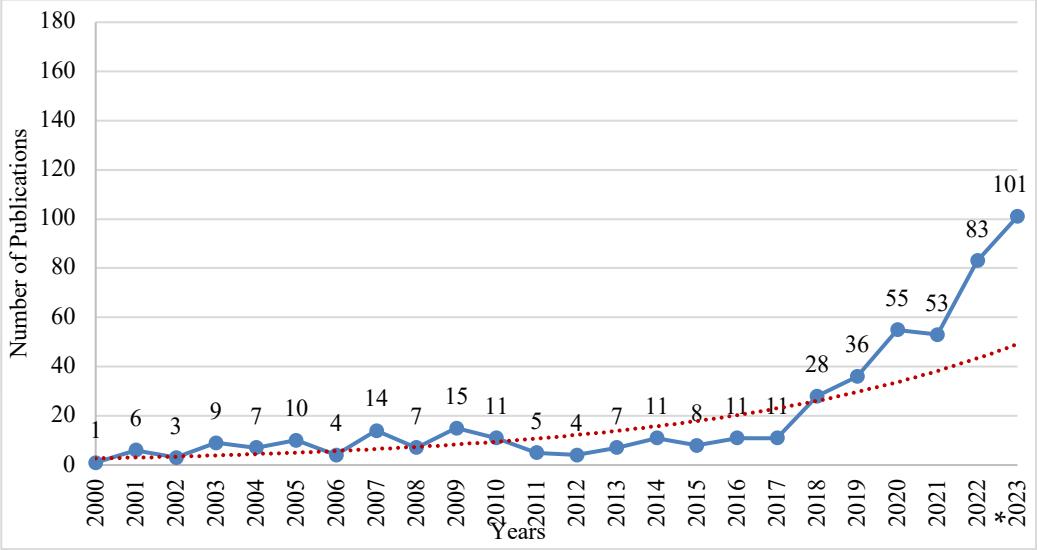

Figure 2.3: The number of publications published in 2000-2023 (Source: Scopus, November, 2023)

* This number indicates the publications until November, 2023.

The selected 56 articles are examined according to year, author(s), article type, system, applied methods, technology, and country in Table 2.2. Our examination by the article type aims to distinguish research articles from review articles. The distribution of the articles regarding article type is illustrated in Figure 2.4.

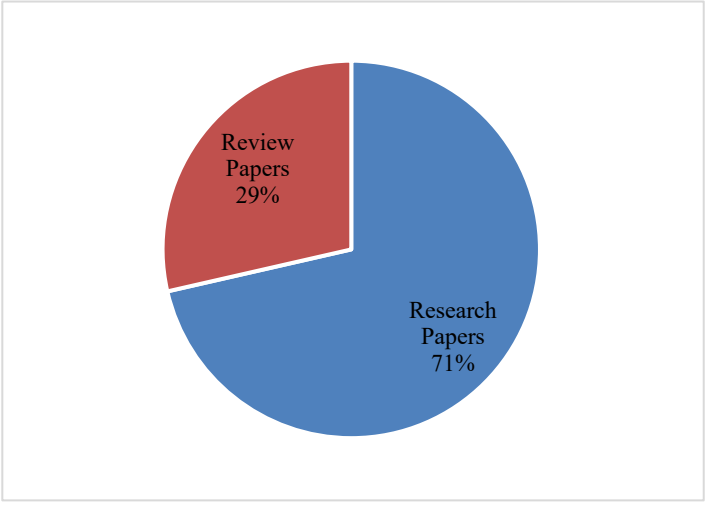

Figure 2.4: The percentages of article types in examined articles

Table 2.2: Articles concerning DG subject

Author (s)	Type	System	Applied Methods	Technology	Country
(Gil-García, 2004)	Review Article	IT policies and standards	Comparative Review	Information technology (IT)	-
(Kim et al., 2008)	Research Article	Web information system	Data mining	Information systems (IS)	South Korea
(Magoutas & Mentzas, 2010)	Research Article	e-Government services	Case Study	e-services	Austria
(Andersen et al., 2011)	Research Article	e-Government	Case Study	IS	Denmark
(Osman, Anouze, Irani, Al-Ayoubi, Lee, Balcı, et al., 2014)	Research Article	e-Government services	The Proposed COBRA (Cost, Benefit, Risk, Opportunity) Model	e-services	Türkiye
(Weerakkody et al., 2014)	Review Article	e-Government	Weight Analysis, Meta-Analysis	-	-
(Bright et al., 2015)	Research Article	OGD	Hypothesis Testing	Websites	U.K.
(Weerakkody et al., 2015)	Review Article	e-Government	Systematic Review	-	-
(Dawes et al., 2016)	Research Article	OGD	Case Study	OGD programs	U.S. and Russia
(Weerakkody et al., 2016)	Research Article	e-Government	Hypothesis Testing, Descriptive Analysis, Structural Model Testing	-	U.K.
(Alcaide–Muñoz et al., 2017)	Review Article	e-Government	Science Mapping Approach	-	-
(Margetts & Naumann, 2017)	Research Article	Government as a Platform (GaaP)	Comparative Analysis	-	Estonia and U.K.
(Al-Muftah et al., 2018)	Research Article	e-diplomacy	Interpretative Structural Modelling (ISM)	ICT	U.S., U.K., and Qatar
(Choi et al., 2018)	Research Article	Public sector IT service procurement	Fuzzy Cognitive Map, Simulation	IT services	Russia

Table 2.2: Articles concerning DG subject (*continue*)

Author (s)	Type	System	Applied Methods	Technology	Country
(Gil-Garcia et al., 2018)	Review Article	DG, public management	Systematic Review	-	-
(Guenduez et al., 2018)	Review Article	Smart government	Qualitative Analysis	-	Switzerland
(M. Hasan et al., 2018)	Research Article	Citizen-centric DG	Frequency Analysis	Digital technologies	Malaysia
(Srimuang et al., 2018)	Research Article	OGD	Survey, Online Assessment	OGD web-based application	Thailand
(Akram et al., 2019)	Research Article	e-tax filing	Hypothesis testing, ANOVA	Online tax filing	Pakistan
(Ashaye & Irani, 2019)	Research Article	e-Government implementation	Qualitative Analysis	-	-
(Khatib et al., 2019)	Research Article	Government-to-citizen (G2C) transactions	Hypothetic-Deductive Approach	-	Kuwait
(Mahmood et al., 2019)	Research Article	Government transformation	Hypothesis Testing	-	Bahrain
(Osman et al., 2019)	Research Article	e-Government services	Data Envelopment Analysis (DEA), Classification and Regression Tree (CART)	e-services	Türkiye
(Weerakkody et al., 2019)	Research Article	e-Government services	Case Study	e- services	U.K.
(L. Chen & Aklikokou, 2020)	Research Article	e-Government	Hypothesis Testing	-	-
(Clarke, 2020)	Review Article	DG units	Interviews, Document Analysis	-	-
(Gil-Garcia, Pardo, et al., 2020)	Review Article	Public sector	Conceptual Analysis	IoT	-
(Gil-Garcia, Gasco-Hernandez, et al., 2020)	Research Article	Open government	Randomized Survey Experiment, ANOVA	-	U.S.

Table 2.2: Articles concerning DG subject (*continue*)

Author (s)	Type	System	Applied Methods	Technology	Country
(Gil-Garcia & Flores-Zúñiga, 2020)	Review Article	DG	Hypothesis Testing	-	Mexico
(Gjaltema et al., 2020)	Review Article	Meta-governance	Systematic Review	-	-
(Gong et al., 2020)	Review Article	DG	Case Study	-	China
(Kaya, Sağsan, Medeni, et al., 2020)	Research Article	e-Government	Qualitative Analysis	e-voting	Türkiye
(Kaya, Sağsan, Yıldız, et al., 2020)	Research Article	e-Government	Descriptive Analysis	e-voting	Cyprus
(Long & Gil-Garcia, 2020)	Research Article	e-Government	Online Survey	Online services, Websites	China
(Matheus & Janssen, 2020)	Review Article	OGD	Content Analysis Method	-	-
(Omar et al., 2020)	Review Article	t-Government	Descriptive Analysis, Thematic Analysis	-	-
(Porumbescu et al., 2020)	Review Article	Open government	Randomized Survey Experiment	IT	-
(Luna-Reyes et al., 2021)	Research Article	DG	Case Study, System Dynamics	-	U.S.
(Matheus et al., 2021)	Research Article	Digital transparency	Design Science Research	-	-
(Alshallaqi, 2022)	Research Article	e-Government	Case Study	Digital technologies, AI-enabled solutions	-
(Y. Chen et al., 2022)	Research Article	Local government	Survey, Hypothesis Testing	e-procurement	-
(H. Choi et al., 2022)	Research Article	DG	Comparative Analysis	ICT, portal-based platform, OGD	South Korea and Denmark

Table 2.2: Articles concerning DG subject (*continue*)

Author (s)	Type	System	Applied Methods	Technology	Country
(Makki & Alqahtani, 2022)	Research Article	DG	ISM	-	Saudi Arabia
(Ndlovu et al., 2022)	Research Article	DG	Hypothesis Testing	DG platform	South Africa
(Newman et al., 2022)	Review Article	DG	Systematic Review	Digital technologies, AI	-
(Puron-Cid et al., 2022)	Research Article	DG	Principal Component Analysis	Digital technologies, ICT, government web-sites	Mexico
(Shen et al., 2022)	Research Article	DG	Case Study	DG platform	China
(Simonofski et al., 2022)	Research Article	OGD	Design Science Research	OGD portals	Belgium
(Wilson & Mergel, 2022)	Review Article	DG	Literature Review, Interviews	-	U.S.
(Young, 2022)	Research Article	Digital services	Survival Analysis	ICT, social media, smartphone	-
(Castilla et al., 2023)	Research Article	DG	Application Development	Digital technologies	Peru
(E. Li et al., 2023)	Research Article	DG	Hypothesis Testing	Websites	China
(Patergiannaki & Pollalis, 2023)	Research Article	e-Government	Regression	-	Greece
(Sterrenberg & L'Espoir Decosta, 2023)	Research Article	e-Government	Case Study	-	Australia

Table 2.3: Theses concerning DG subject

Author	Subject	System	Country
(AL-Shehry, 2008)	E-Government Adoption Model	e-Government	Saudi Arabia
(Re, 2010)	Quality of Digital Services in e-Government	e-Government	-
(Ashaye, 2014)	E-Government Implementation	e-Government	Nigeria
(Mahundu, 2015)	Higher Education Institutions' Service Provision and Quality Assurance	e-Governance	Tanzania
(Almamari, 2016)	DG Implementation	DG	Oman
(ElKheshin, 2016)	E-Government Service Adoption Model	e-Government	Egypt
(Hussain, 2017)	Mobile-based government (m-Government) Implementation	m-Government	Bangladesh and Australia
(Nikaj, 2017)	Technology-Enabled State-Building	e-Government	Kosovo
(Meijer, 2019)	E-Government Innovation Platform	e-Government	Netherlands
(Ekinci, 2021)	Smart Government Transformation	Smart Government	Estonia and Singapore
(McDaniel, 2022)	E-Governance in Urban Planning	e-Government	U.S.
(Sapraz, 2023)	E-Government and Environmental Sustainability	e-Government	Sri Lanka

Table 2.4: Industry reports on DG subject

Author(s)	Source	System	Country
(CLC, 2018)	CLC	Smart Nation	Singapore
(Microsoft, 2018)	Microsoft	DG Transformation	-
(OPDC, 2018)	OPDC	Government Innovation Lab	Thailand
(Deloitte, 2019)	Deloitte	DG Transformation	-
(Barcevičius et al., 2019)	European Commission	DG Transformation	Belgium, Italy, Poland, Spain, and U.K.
(Shi-Kupfer & Ohlberg, 2019)	Merics	DG	China
(McKinsey & Company, 2020)	McKinsey	Future of Work	-
(OECD, 2020)	OECD	DG Policy Framework	-
(United Nations, 2022a)	United Nations	E-Government	Several countries
(Deloitte, 2021)	Deloitte	DG Transformation	-

Table 2.4: Industry reports on DG subject (*continue*)

Author(s)	Source	System	Country
(Institute for Government, 2021)	Institute for Government	DG	U.K.
(PwC, 2021)	PwC	DG	Canada
(Deloitte, 2022)	Deloitte	DG Trends	-
(European Commission, 2022b)	European Commission	e-Government Benchmark	EU27+
(European Commission, 2022a)	European Commission	Digital Economy and Society Index (DESI)	EU27+
(The World Bank, 2022)	The World Bank	DG Transformation-GovTech	Several countries
(McKinsey &Company, 2022)	McKinsey	DG Transformation	Several countries
(PwC, 2022)	PwC	DG 5.0	-
(WEF, 2023)	WEF	Digital Transition Framework	-

As seen in Figure 2.4, 71.43% of the examined documents are research articles, while 28.57% are review articles. The applied methods are examined to find the literature gaps from an analytical perspective. Technologies and countries are examined to see which country is studied for which technology in the related literature.

The chronological evolution of the examined technologies in DG research between 2004 and 2023 is respectively IT, IS, ICT, government websites, e-services, e-voting, e-procurement, online tax filing, OGD, e-Government, social media, DG platform, digital technologies, and (i.e., IoT, machine learning, blockchain, artificial intelligence). Table 2.5 provides the percentage of technologies used in examined articles. ICT is the most examined technology with 26.68%; digital technologies are the second with 16.66%; OGD is the third with 13.33%; websites and e-services have an equal percentage (10%).

Table 2.5: The percentages of the examined technologies in academic articles

Technology	Percentage
IT, IS, and ICT	26.68%
Digital technologies	16.66%
OGD	13.33%
Websites	10%
e-services	10%
e-voting	6.67%
DG platform	6.67%
e-procurement	3.33%
Online tax filing	3.33%
IoT	3.33%

Our findings reveal that DG, e-Government, e-Government services, OGD, and GaaP are the most frequently examined systems, as seen in Figure 2.5. The countries investigated in the articles provided in Table 2.2 can be listed according to their frequency in descending order: U.K., U.S., China, Türkiye, Denmark, Mexico, South Korea, Australia, Austria, Bahrain, Belgium, Cyprus, Estonia, Greece, Kuwait, Malaysia, Pakistan, Peru, Russia, Saudi Arabia, South Africa, Switzerland, and Thailand. The methods in research articles provided in Table 2.2 can be listed according to their frequency in descending order as case study, hypothesis testing, descriptive analysis, qualitative analysis, comparative analysis, design science research, Interpretative Structural Modelling (ISM), Application Development, ANOVA, Classification and Regression Tree (CART), Data

Envelopment Analysis (DEA), frequency Analysis, fuzzy cognitive map, online survey, and simulation. Review articles applied analysis methods such as systematic review, interviews, conceptual analysis, content analysis method, meta-analysis, science mapping approach, thematic analysis, and weight analysis.

Figure 2.5: The word cloud based on systems in examined articles

2.2.2 Analysis of the Theses

Table 2.3 categorizes the selected 12 theses according to their subject, system, and country. Their subject and system are included to discover the DG terminology and research fields within the theses. Generally, the theses realized in the DG concept are based on implementation and adoption models. Developing countries (i.e., Nigeria, Tanzania, Egypt, Bangladesh, Kosovo) are examined in an essential part of the thesis with case studies about e-Government, smart government, DG, and m-Government systems.

2.2.3 Analysis of the Industry Reports

The selected 19 reports from international organizations (e.g., WEF, OECD, European Commission) and top-tier advisory companies (e.g., Deloitte, McKinsey, PwC) are provided in Table 2.4. The source, system, and country of these reports are analyzed. The systems examined in those reports include smart nation, DG, DG transformation, future of work, e-Government, digital economy and society index, DG 5.0, and digital transition framework. The countries examined in those reports are Canada, China, EU27+, Singapore, Spain, Italy, the U.K., Belgium, Poland, and Thailand.

2.3 Science Mapping

2.3.1 Keyword Co-Occurrence Analysis

VOSviewer is used for a keyword co-occurrence analysis to create a visualization based on clustering. Keywords characterize the focused topics of a scientific field. Keyword networks can show how a knowledge body is constructed by studying the interrelationships of research fields (van Eck & Waltman, 2014).

The different clusters of the most common keywords in the articles (n=11,917) are displayed in Figure 2.6, and the keywords in each of the clusters are listed in Table 2.6. Different colors make the most featured topics in the literature more visible. The sizes of the circles in Figure 2.6 represent the occurrences of the keywords. The larger the size of the circles, the higher the frequency of occurrence of keywords in the articles.

This analysis found 101 items, 7 clusters, and 942 links, with a total length strength of 1596. Full counting is used as the counting method. The author keyword is selected as the unit of analysis, and the threshold value is determined as 10, and 101 keywords have met the threshold. The keyword “E-Government” is found as the most frequent one with 330 occurrences with a total link strength of 354.

Table 2.6: Keywords for co-occurrence analysis

Clusters (colors)	# of items	Items and their occurrences
Cluster 1 (red)	17	1. Cloud computing (21) 2. Crowdsourcing (16) 3. European union (10) 4. Facebook (11) 5. Indonesia (10) 6. Local government (27) 7. Machine learning (12) 8. Open data (35) 9. Open government (36) 10. Participation (23) 11. Public value (19) 12. Satisfaction (13) **13. Social media (85)*** 14. Survey (10) 15. Trust (20) 16. Twitter (21) 17. Web 2.0 (12)

Table 2.6: Keywords for co-occurrence analysis (*continue*)

Clusters (colors)	# of items	Items and their occurrences
Cluster 2 (green)	16	1. Accessibility (13) 2. Benchmarking (11) **3. China (60)*** 4. Covid-19 (52) 5. Development (20) 6. Egovernment (15) 7. Evaluation (17) 8. Health care (12) 9. Innovation (25) 10. Internet (10) 11. Knowledge (13) 12. Management (11) 13. Measurement (12) 14. Public health (13) 15. Strategy (10) 16. Technology (22) 17. Telemedicine (10)
Cluster 3 (blue)	16	1. Accountability (23) 2. Barriers (10) 3. Collaboration (16) 4. Corruption (10) 5. Democracy (17) 6. E-democracy (27) 7. E-governance (30) 8. E-participation (31) **9. Governance (43)*** 10. ICTs (10) 11. Information and communication technology (17) 12. Internet (41) 13. Municipalities (12) 14. Nigeria (16) 15. Stakeholders (10) 16. Transparency (40)
Cluster 4 (yellow)	14	1. Artificial intelligence (12) 2. Big data (21) 3. Blockchain (10) 4. Case study (16) 5. Citizen participation (21) 6. Gender (12) 7. Information technology (16) 8. Privacy (15) 9. Public services (17) 10. Security (31) 11. Smart cities (31) **12. Smart city (37)*** 13. Sustainability (33) 14. Sustainable development (21)

Table 2.6: Keywords for co-occurrence analysis (*continue*)

Clusters (colors)	# of items	Items and their occurrences
Cluster 5 (purple)	14	1. Adoption (24) 2. Developing countries (28) 3. E-commerce (15) **4. E-government (330)*** 5. E-learning (13) 6. E-procurement (13) 7. E-services (11) 8. GIS (10) 9. ICT (108) 10. India (29) 11. Innovation (23) 12. Public participation (14) 13. Technology adoption (14) 14. Utaut (14)
Cluster 6 (light blue)	12	1. Africa (14) 2. Australia (10) 3. Digital divide (34) 4. Digital inclusion (10) 5. Digital technology (11) 6. Economic growth (16) 7. Education (26) **8. Government (37)*** 9. Information society (13) 10. Information technologies (10) 11. Policy (17) 12. Public policy (12)
Cluster 7 (orange)	11	1. Digital economy (20) **2. Digital government (56)*** 3. Digital transformation (22) 4. Digitalization (22) 5. Digitization (11) 6. Electronic government (35) 7. Information and communication technologies (12) 8. Institutional theory (11) 9. Public administration (34) 10. Public sector (35) 11. Social networks (10)

* The keywords with the highest occurrences within clusters are highlighted in bold characters.

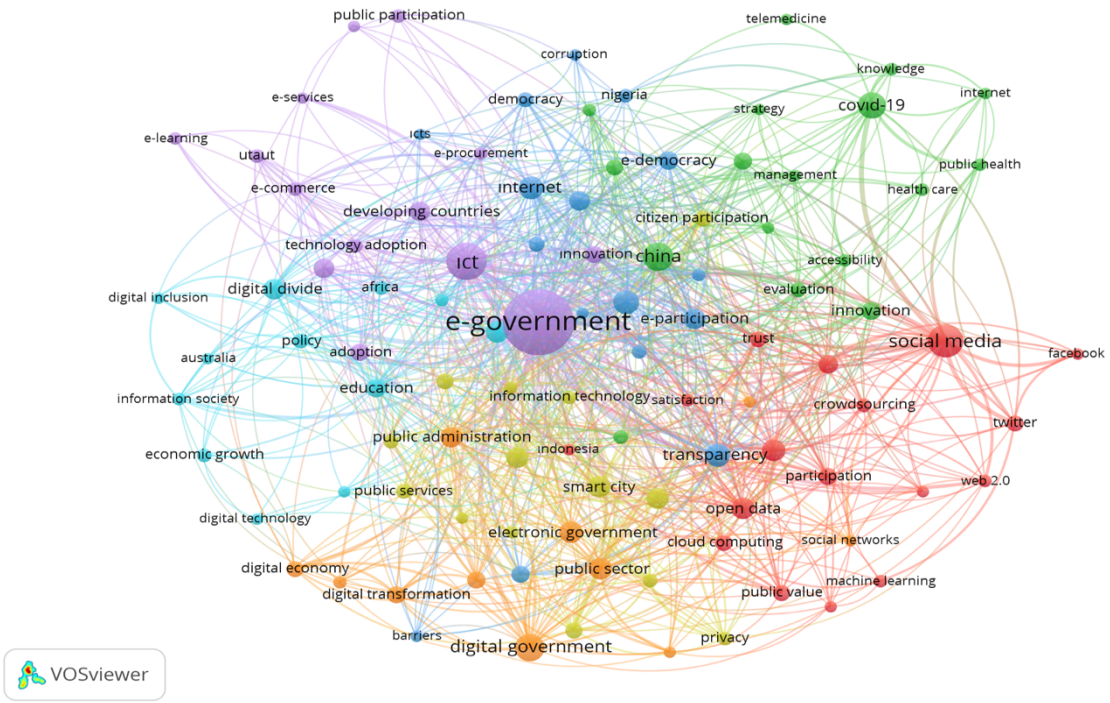

Figure 2.6: Network visualization of keyword co-occurrence analysis

From the keyword co-occurrence analysis, we can group clusters into five research areas:

- **Research Area 1- DG transformation from Cluster 4&6&7**

"Digital government," "digital transformation," and "digitalization" are the most frequently studied keywords from cluster 7. Other key research topics from clusters 4, 6, and 7 involve "government," "smart city," and "smart cities." Besides, "sustainability," "sustainable development," "security," "digital divide," and "education" concepts have also been frequently studied in DG literature. In the acceleration of DG transformation, data exchange across the "public sector" should be expanded by technologies to construct an integrated and sustainable system (Makki & Alqahtani, 2022). The most promising "digital technologies" for governments are found as "artificial intelligence," "blockchain," and "big data."

- **Research Area 2-Cybersecurity from Clusters 1&4**

Cybersecurity as a general concept has been gaining relevance because of its strategic importance for society, citizens, companies, and the country. To solve "trust," "privacy," and "security" issues on "information technologies" and "information and communication technologies," cybersecurity practices are implied. Moreover, the

utilization of digital technologies such as “blockchain” and “artificial intelligence” in government applications necessitates secure and efficient end-to-end processing capabilities, avoiding fraud and raising “transparency” and “trust” between stakeholders.

- **Research Area 3- Public participation & social media from Cluster 1**

“Social media,” especially “Twitter” and “Facebook,” has a vital utilization rate for the public sector. These technologies can be used for (1) information transmission from the government to the public, (2) information transmission from the public to the government, and (3) building and supporting networks between the government and the public and within the public at large (Young, 2022). In the studies about public participation and social media, “participation,” “public value,” “local government,” “trust,” “satisfaction,” and “e-democracy” are the most frequently used keywords.

- **Research Area 4- OGD & transparency from Cluster 1&3**

OGD programs have been applied in several countries, political systems, cultures, and sub-national and municipal levels. The social and political benefits of “open government” comprise greater “transparency” and “accountability” (Dawes et al., 2016). Generally, the absence of transparency in government actions and decision-making practices causes “corruption” scandals (Matheus et al., 2021). The success of OGD programs necessitates an integrated use of complementary tools for “collaboration” with citizens and “stakeholders” (Porumbescu et al., 2020).

- **Research Area 5- E-Government adoption models from Clusters 2&3&5**

In this analysis, “E-Government” is the most frequently studied keyword which has been an evolving trend in recent years, attracting the interest of policymakers, citizens, bureaucrats, and “public administration” researchers. In the “adoption” of “e-services,” “e-democracy,” “e-governance,” and “e-participation,” their “accountability” should be considered (ElKheshin, 2016; M. Hasan et al., 2018; Matheus et al., 2021). “Governance” is the key to government systems, and “e-governance” defines the responsibility of an organization’s online presence and who has the power to make decisions (Makki & Alqahtani, 2022). In “China,” e-government research focuses on “public health.” In this context, the “Covid-19” keyword is included in a majority of the studies since it has an

accelerating effect using “digital technologies” such as “telemedicine” (Deloitte, 2021; WEF, 2023).

2.3.2 Bibliographic Coupling

Bibliographic coupling can group thematically parallel documents into clusters. Two documents have a citation link between them if one document comprises a cited reference that has a matching key consistent with one of the match keys representing the other document. In the bibliography, the number of bibliographic coupling links between two publications equals the number of pairs of cited references in the two publications (van Eck & Waltman, 2014).

In this analysis, the counting method is selected as full counting, the unit of analysis is selected as countries, and the maximum country number for each document is selected as 25 to ignore those publications that are co-authored by many countries. The minimum number of documents in a country is set to 5. Out of the 134 countries, 78 countries have met the thresholds. Table 2.7 provides the top 10 countries; Figure 2.7 displays the bibliographic coupling.

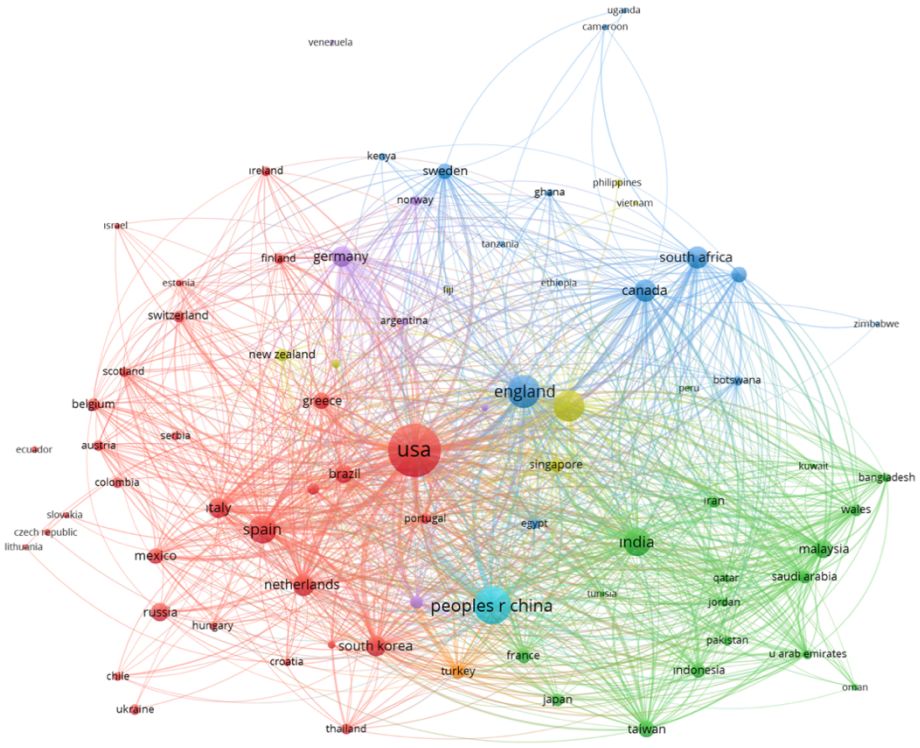

Figure 2.7: Overlay visualization of bibliographic coupling regarding countries

Table 2.7: Top 10 countries resulted by bibliographic coupling

Rank	Countries	Total link strength
1	United States	154,856
2	United Kingdom	60,938
3	China	60,193
4	Spain	52,452
5	Australia	49,109
6	India	44,454
7	Netherlands	35,359
8	Canada	34,610
9	South Korea	34,031
10	Malaysia	30,097

The bibliographic coupling analysis shown in Figure 2.7 and Table 2.7 indicates that the United States has the highest total link strength. The United Kingdom and China are ranked as the second and the third-ranked countries, respectively. Therefore, this bibliographic coupling analysis showed that the themes of the documents published in the United States, the United Kingdom, and China show great similarities.

2.3.3 Co-Citation Analysis

The connection between the journals in terms of co-citation links are represented by the distance between them in the visualization. The citations attribute shows the number of citations made to a cited source, a cited reference, or a cited author (van Eck & Waltman, 2014).

In the analysis, the counting method is selected as full counting, the unit of analysis is selected as cited sources, the minimum number of citations of a source is selected as 50, and 263 sources have met the threshold. Figure 2.8 displays the document co-citation analysis regarding sources. Figure 2.8 illustrates the clusters' colors that indicate the similar types of journals having common co-citation links.

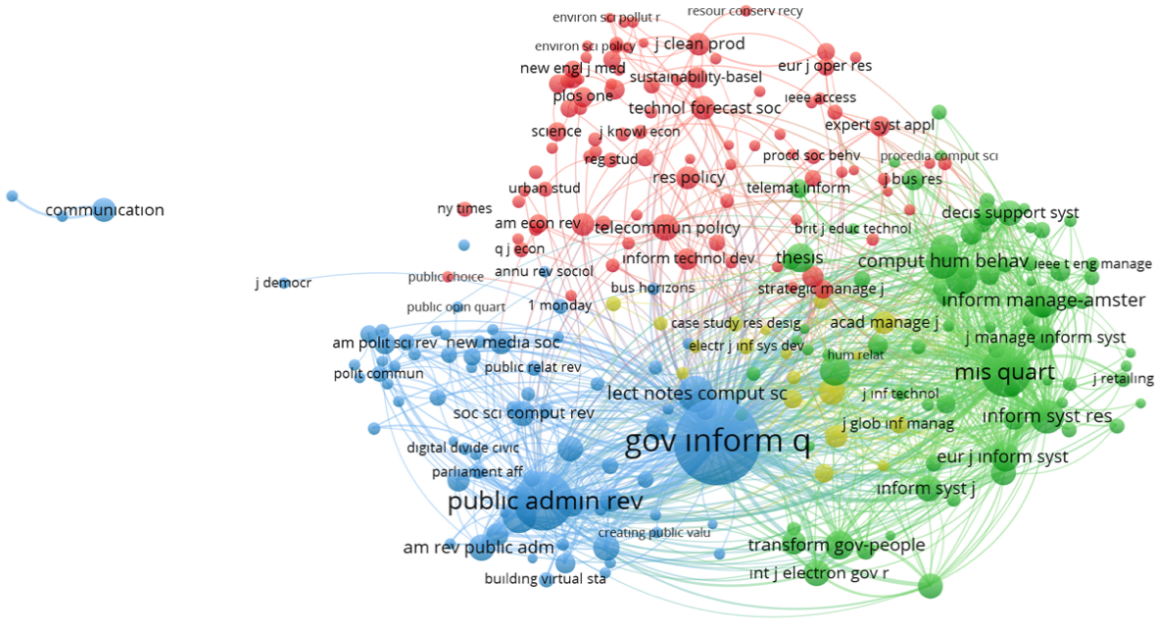

Figure 2.8: Document co-citation analysis (sources)

The analysis shows that the most-cited journal is Government Information Quarterly followed by Public Administration Review and Management Information Systems Quarterly.

2.4 Findings and Limitations of DG Literature

Since DG transformation plays a vital role in the public sector's agenda, this study aimed to analyze current DG research by applying a science mapping approach. The selected publications are grouped into five distinct research areas to support scholars in discussing new literature-related findings as a theoretical contribution of this research. As a practical contribution, the practitioners, academics, policymakers, and public employees can be inspired and guided by this paper to comprehend the subject better, set up a theoretical framework, discover research gaps, and identify future directions in the field of DG.

Government employees, policymakers, citizens, and businesses, not all actors understand the same under a DG. Therefore, the DG terminology is clarified in the RQ1. The literature is analyzed by examining the articles, industry reports, and theses in the RQ2 to identify the research fields in DG. VOSViewer software is utilized for creating

bibliometric maps based on clustering, and the research areas are determined in RQ3. The limitations of the existing research are identified in RQ4, and the future research directions are proposed in RQ5. The findings of the RQs are detailed in the following sections.

- **RQ1: What is the state of the art of DG?**

The terminology of DG is divided into six concepts. “digital government”; “e-Government”; “government 4.0”; “mobile government”; “t-government” and “GaaP”. These concepts have distinguishing features; however, they can be used interchangeably.

To summarize, DG is a government structured progressively in terms of virtual agencies whose organization and power depend on the Internet. E-Government is IT utilization in government services, counting its effects on citizens’ satisfaction, public service provision, and democratic standards. Government 4.0 focuses on whole-of-government alignment for citizens. Several mobile platforms are used in m-Government to deliver government services and information to citizens. T-Government concept aims to achieve an accountable, efficient, transparent, and agile government. The main objective of GaaP concept is to create technological components that can be used across the public sector (ElKheshin, 2016; Hussain, 2017; Institute for Government, 2021; Janowski, 2015; Y. Liu et al., 2014; Weerakkody et al., 2019).

- **RQ2: What are the research fields (i.e., article type, applied methods, technology, country) of the research on DG?**

Our findings from academic literature reveal the research fields of DG literature as follows:

  - **Article type:** 71.43% of the examined articles are research articles, while 28.57% are review articles.
  - **Applied methods:** In research articles; case study, hypothesis testing, descriptive analysis, qualitative analysis, comparative analysis, design science research, Interpretative Structural Modelling (ISM), Application Development, ANOVA, Classification and Regression Tree (CART), Data Envelopment Analysis (DEA), frequency Analysis, fuzzy cognitive map, online survey, and simulation are used. In review articles, analysis methods such as systematic review, interviews, conceptual analysis, content analysis

method, meta-analysis, science mapping approach, thematic analysis, and weight analysis are used.

- **Technology:** ICT is the most examined technology; digital technologies are the second. Other technologies include IT, IS, government websites, e-services, e-voting, e-procurement, online tax filing, OGD, e-Government, social media, DG platform, and digital technologies (i.e., IoT, machine learning, blockchain, artificial intelligence).
- **Country:** The countries investigated in the articles are U.K., U.S., China, Türkiye, Denmark, Mexico, South Korea, Australia, Austria, Bahrain, Belgium, Cyprus, Estonia, Greece, Kuwait, Malaysia, Pakistan, Peru, Russia, Saudi Arabia, South Africa, Switzerland, and Thailand.

Our findings from industry reports reveal the research fields of DG literature as follows:

- **System:** The systems examined in those reports include smart nation, DG, DG transformation, future of work, e-Government, digital economy and society index, DG 5.0, and digital transition framework.
- **Country:** The countries examined in the reports are Canada, China, EU27+, Singapore, Spain, Italy, the U.K., Belgium, Poland, and Thailand.

- **RQ3: What are the popular research areas of DG?**

The science mapping approach is used to determine DG's popular research areas. Keyword co-occurrence analysis is conducted on VOSviewer. A bibliometric map based on clustering is achieved at the end of the analysis. Five popular research areas of DG are determined as follows:

- *Research Area 1* - DG transformation,
- *Research Area 2* - Cybersecurity,
- *Research Area 3* - Public participation & social media,
- *Research Area 4* - OGD & transparency,
- *Research Area 5* - E-Government adoption models.

The keywords in the clusters provided in Figure 2.6 are examined based on these sub-periods in Figure 2.9.

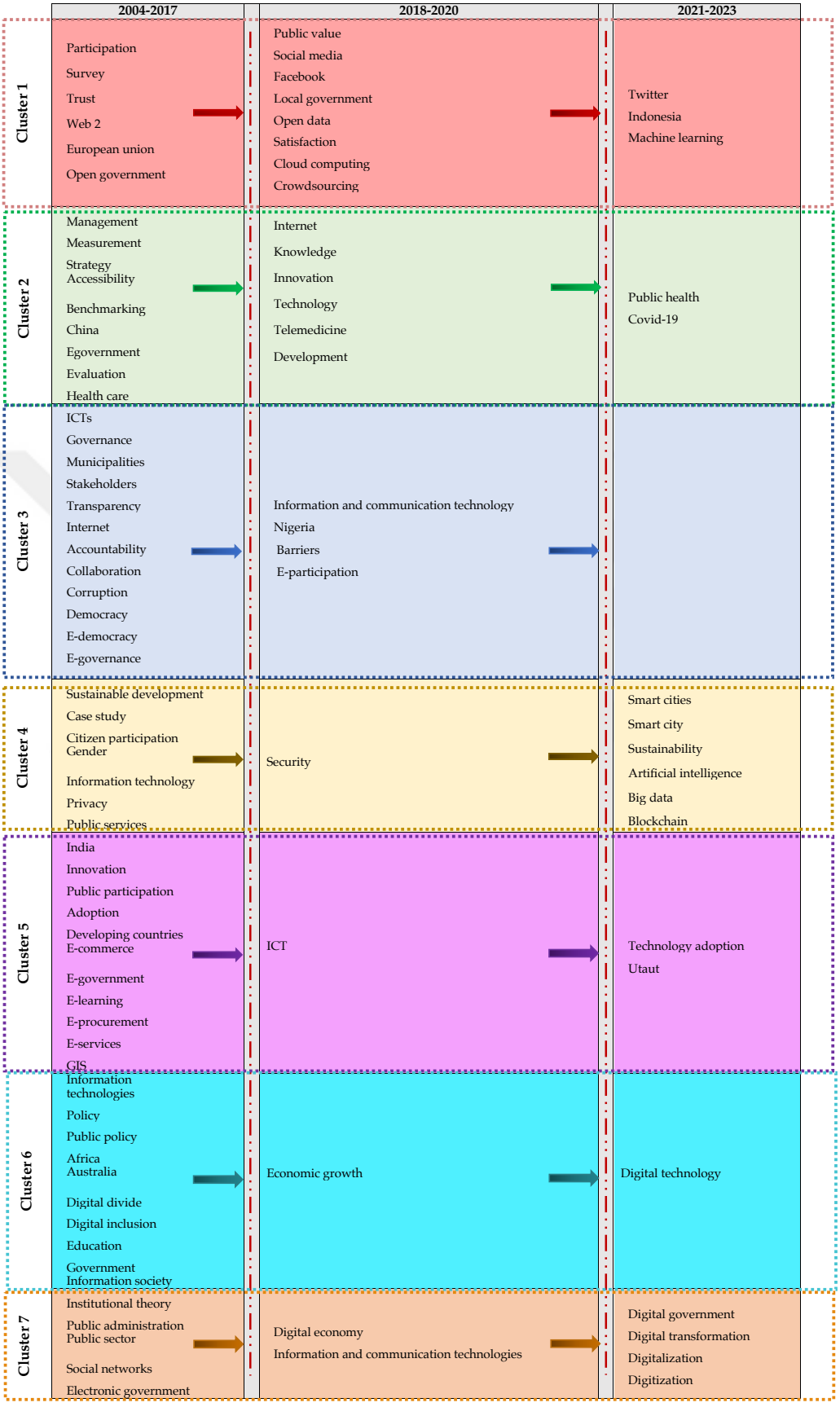

Figure 2.9: Thematic evolution of DG based on the keywords

Due to the increase in the number of articles in 2018, the time horizon was divided into three sub-periods: 2004-2017, 2018-2020, and 2021-2023. According to Figure 2.9, research area 1 was mainly extended in 2021-2023 with keywords such as DG, digital transformation, digitalization, and digital technology. Research area 2 was mainly discussed in the 2018-2020 time period with security keywords, while trust and privacy were popular research trends between 2004 and 2017. Research area 3 was popular in the 2018-2020 period with social media keywords; while some social media platform keywords (i.e., Facebook) were popular in those years, others (i.e., Twitter) were popular in 2021-2023. The keywords open government and transparency in research area 4 were popular in 2004-2017, while open data was popular in 2018-2020. Research area 5 was mainly popular in the 2004-2017 time period.

- **RQ4: What are the limitations of the existing research on DG?**

The limitations of the existing research on DG according to five research areas can be summarized as follows:

- DG transformation: The DG literature is mainly based on qualitative research; quantitative research can be developed. One of the most significant research gaps in DG transformation literature is frameworks examining seamless service delivery and adaptive workplaces in government (Al-Muftah et al., 2018; Osman, Anouze, Irani, Al-Ayoubi, Lee, Balc, et al., 2014; Shen et al., 2022).
- Cybersecurity: Our findings reveal a lack of studies developing practices for governments to enhance citizens' security. Therefore, government cybersecurity systems and sustaining trust in public services are the major research gaps in the literature (Deloitte, 2022; Kam et al., 2022; Z. Wang et al., 2023).
- Public participation & social media: The literature lacks in discussing e-participation in comprehending the citizens' expectations of public participation (Alarabiat et al., 2021; Alcaide–Muñoz et al., 2017; Castilla et al., 2023; Coelho et al., 2022; H. Li & Kostka, 2022). The security, privacy, and nepotism problems should be addressed in the literature to implement social media utilization and e-voting systems successfully (Kaya, Sağsan, Medeni, et al., 2020; Kaya, Sağsan, Yıldız, et al., 2020; Z. Wang et al., 2023).

- OGD & transparency: The factors that influence the performance of OGD programs should be analyzed. The analysis of data generation at local, national, and regional levels is essential for the body of research on OGD & transparency (De Blasio & Selva, 2016; Piscopo et al., 2017).
- E-Government adoption models: In the adoption of e-government, citizens' perceptions of trust should be analyzed. The literature lacks studies about blockchain technology utilization in e-government for effective and safe processing capabilities (Akram et al., 2019; Ashok et al., 2022; Y. C. Chen & Lee, 2018; Osman, Anouze, Irani, Al-Ayoubi, Lee, Balc, et al., 2014; Weerakkody et al., 2016).

- **RQ5: What are the future research directions of DG?**

According to the results of our study, the future research directions of DG are identified as follows:

- Integrating DG field with operation research, data mining, and multi-criteria decision-making techniques,
- Proposing cybersecurity frameworks to analyze governments' cybersecurity capabilities,
- Examining the citizens' incentives in e-participation,
- Analyzing e-voting systems increasing public trust,
- Examining factors that influence the performance of OGD programs,
- Developing an ecosystem approach for OGD planning,
- Implementing blockchain technology to enhance transparency and trust in the DG ecosystem,
- Comparing citizens' perception of trust for similar public services in traditional means and their e-government versions.

2.5 Research Gaps and Research Areas

Our literature review and science mapping analysis show that the most prevalent topics in the field of DG can be grouped into five research areas: public participation & social media, OGD & transparency, e-Government adoption models, cybersecurity, and DG transformation. The recommendations for future research according to gaps in the research areas are discussed in the following sections.

- **DG transformation**

One key focus of research has been the successful DG transformation. For example, Ashaye and Irani (2019) examined the influencing factors and the relationships with stakeholders on successful DG implementation. Mahundu (2015) studied the socio-technical effects of DG implementation. Almamari (2016) investigated the organizational culture's role in DG transformation. Hussain (2017) constructed a mobile-based DG implementation framework and applied this model to two countries.

Seamless service delivery, personalized, frictionless, and anticipatory; adaptive workplaces in government; and generating more excellent public value from government and agile government present the biggest research gaps on DG transformation (Addo, 2022). The DG literature is mainly based on qualitative research. Although quantitative research is appropriate for evaluating DG, few studies have combined the subject with analytical techniques. For this reason, integrating the study of DG with operational research, data mining, and multi-criteria decision-making techniques can prove helpful. The research integrating the subject with those techniques will certainly gain from further diverse perspectives and be closer to real-life problems (Al-Muftah et al., 2018; Osman, Anouze, Irani, Al-Ayoubi, Lee, Balc, et al., 2014; Shen et al., 2022).

- **Cybersecurity**

In the related literature, security and trust issues among different stakeholders are investigated. Weerakkody et al. (2014) found that trust is one of DG's most widely explored keywords. Weerakkody et al. (2016) investigated the impact of trust on user satisfaction with e-Government services, where it was identified as a significant factor. Hasan et al. (2018) aimed to determine critical success factors for citizen-centric DG, and the authors have found trust to be one of the determinants of success. Mahmood et al. (2019) examined the influence of government transformation on citizen trust and confidence. Kam et al. (2022) analyzed the effect of self-motivation of public employees on cybersecurity training.

Our review shows a lack of studies providing practices for governments to increase citizens' trust and security. Government cybersecurity systems and sustaining public trust in government are the major research gaps in the literature (Deloitte, 2022). Cybersecurity

can potentially enhance the trust and security of citizens by protecting against unauthorized access to data centers and other computerized systems. Thus, cybersecurity can help governments adopt DG services by preventing mistrust. In future studies, different cybersecurity frameworks can be constructed to analyze governments' cybersecurity capabilities in different dimensions.

- **Public participation & social media**

Alarabiat et al. (2021) searched citizens' motivations for e-participation through Facebook and found that e-participation via social media platforms is not necessarily beneficial without citizens' awareness. Another study by Weerakkody et al. (2019) revealed that the exchange and collaboration between stakeholders is an important barrier for government systems.

The Internet can help construct a democratic and inclusive framework. Further research is necessary to shed light on the context essential to facilitate citizens' participation in public affairs and the e-participation actions mobilized by citizens in various social media contexts (Coelho et al., 2022). The issues of security, privacy, and nepotism are to be addressed in successful e-voting systems to increase public trust (Kaya et al., 2020; Z. Wang et al., 2023). However, the literature fails to sufficiently discuss e-participation in comprehending the citizens' expectations from such participation (Alarabiat et al., 2021; Alcaide–Muñoz et al., 2017; Castilla et al., 2023; Coelho et al., 2022; H. Li & Kostka, 2022).

- **OGD & transparency**

Generating value from OGD implies a rise in data quantity and enhancement of the capacity to detect high-value data geared to increasing use. Governments have a key role in data publishing to provide open data and spur collaboration (OECD, 2020). Bright et al. (2015) described usage patterns in OGD with hypothesis testing. Dawes et al. (2016) developed an OGD ecosystem model for planning and design, while Srimuang et al. (2018) presented an assessment model for OGD by conducting an online survey. Matheus and Janssen (2020) constructed a comprehensive model for OGD, and Porumbescu et al. (2020) proposed a framework for open government in their literature review article.

OGD literature can be further expanded by examining those factors that influence the performance of OGD programs, as well as by investigating data generation at local, national, and regional levels (De Blasio & Selva, 2016; Piscopo et al., 2017). An ecosystem approach, system quality, data quality, and organizational characteristics, can be used for OGD planning (Ahuja et al., 2023; Dawes et al., 2016). Individual characteristics have a crucial impact on OGD (Matheus & Janssen, 2020), which can benefit from more attention from government managers, policymakers, and researchers.

- **E-Government adoption models**

In the e-Government concept, people trust the government and its ability to deliver services, solve problems as promised, and safeguard personal information. Therefore, e-services will require the assurance that citizens' privacy and security are protected. Weerakkody et al. (2016) examined the impact of trust on user satisfaction of e-Government services, where it was identified as a significant factor. Hasan et al. (2018) aimed to determine critical success factors of citizen-centric DG, with trust being one of the determinants of success. Pérez-Morote et al. (2020) analyzed e-Government usage in European countries, and the authors found that communication and promotion strategies are essential in the citizen-centric e-government policy. Y. Li and Shang (2020) revealed that service quality, satisfaction, and service value are the main reasons for continuously utilizing e-Government platforms. Patergiannaki and Pollalis (2023) assessed the e-Government maturity of Greek municipalities where population, ideology, and budget have been found to have a limited influence.

In future studies, it would be possible to compare citizens' perceptions of trust for similar public services in traditional means and their digital versions. In addition, researchers will be implored to examine blockchain technology for more effective and safe processing capabilities, such as fraud prevention, transparency, and confidence enhancing the DG (Akram et al., 2019; Ashok et al., 2022; Y. C. Chen & Lee, 2018; Osman et al., 2014; Weerakkody et al., 2016). The opinions of government employees against citizens' perceptions, habits, trust, self-efficacy, and social influences can be examined in future studies. Besides, citizens can be sampled randomly for potential users and non-users to investigate their opinions (Akram et al., 2019; Kaya et al., 2020; E. Li et al., 2023; Weerakkody et al., 2016).

2.6 Concluding Remarks on Literature Review on DG

Governments implement various projects to promote DG. The subject has caught the attention of academics, industrial practitioners, government agencies, and advisory companies. A significant number of papers have been committed to the study of DG since 2000. This study introduced a structured literature review for DG leveraged by the science mapping approach, especially for 2000-2023. In this context, the state of the art of DG, the research fields and the popular research areas of DG, the limitations in the existing research on DG, and potential future research directions are determined. Our findings show that an evolutionary trend exists in the DG field.

Articles, theses, and reports are examined to investigate the research fields of DG. We utilized the VOSviewer software for advanced bibliometric analysis with a visual presentation of the results. Raw bibliographic records collected from Scopus and WoS databases are pre-processed to eliminate duplicates. The maps are created using keyword co-occurrence, bibliographic coupling, and co-citation networks. The keyword co-occurrence analysis determines and clusters the articles' most important keywords. Then, the following five main popular research areas are identified: (1) DG transformation, (2) Cybersecurity, (3) Public participation & social media, (4) OGD & transparency, and (5) E-Government adoption models.

DG transformation and cybersecurity are examined in the following chapters, and the DG subject is analyzed with integrated analytical approaches. The factors that influence the performance and success of DG transformation are modeled and analyzed. A cybersecurity framework is proposed to analyze public institutions' cybersecurity maturity levels and to guide them with cybersecurity action plans.

3. THEORETICAL BACKGROUND

This chapter provides the theoretical background for the techniques used in this thesis. The used techniques in the following chapters of the thesis are illustrated in Figure 3.1.

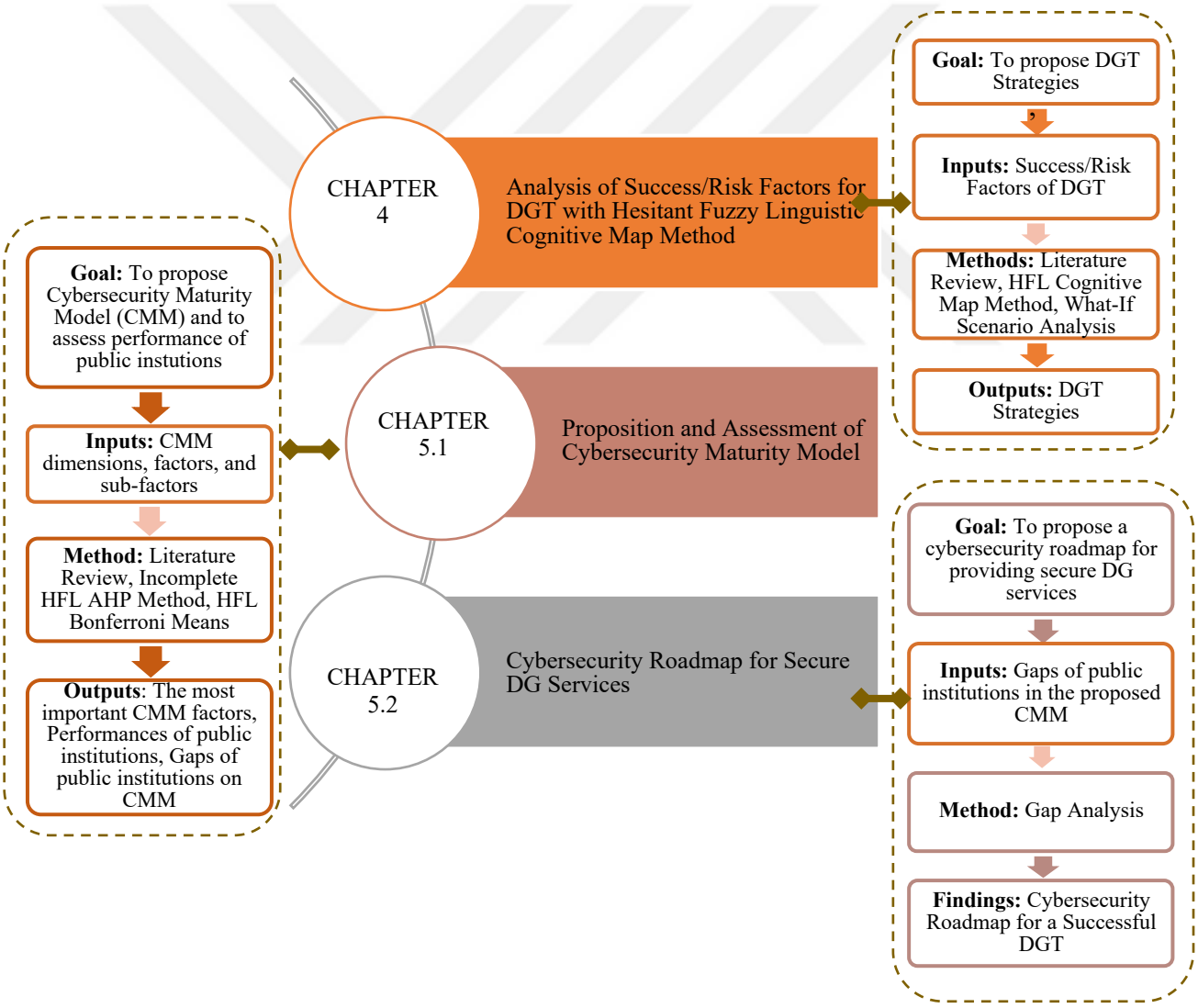

Figure 3.1: The flowchart of the thesis

3.1 Overview of Hesitant Fuzzy Sets

The uncertainty in human judgments can be better represented by fuzzy set theory (Zadeh, 1965), where a degree of membership is assigned to each element. The fuzzy set theory uses a membership function that generates a value between zero and one that allows the assessment of elements' membership values in a set. In many cases, however, even fuzzy numbers can prove insufficient. Decision Makers (DMs) may have difficulties correctly expressing their thoughts and hesitate at specific points. Hesitant Fuzzy Sets (HFS) were introduced by Torra (2010). HFS describes a component's membership level as one of the possible values between zero and one. Rodríguez et al. (2011) extended HFS to the Hesitant Fuzzy Linguistic Term Sets (HFLTS) by integrating the concept of a fuzzy linguistic approach into HFSs. The HFLTS approach allows the utilization of comparative linguistic term sets. The combination of this HFLTS technique and Multi-Criteria Decision-Making (MCDM) methods makes the decision-making process resemble real life. Since HFLTS brings flexibility by eliciting linguistic options, it facilitates the expression of DMs' opinions in the evaluation phases. The advantage of the introduced method lies in its capacity to reflect and consider both the hesitation and vagueness of DMs' judgments in the evaluation phases.

3.1.1 Hesitant Fuzzy Sets

The preliminaries of HFS are summarized next (Torra, 2010).

Definition 3.1 Let X be a reference set. The function of HFS, where HFS is membership functions' union over X, is provided as:

$$E = \{\langle x, h_E(x) \rangle \mid x \in X\} \tag{3.1}$$

Here, $h_E(x)$ is named a Hesitant Fuzzy Element (HFE), and H is the set of all HFE.

Definition 3.2 h is a function that renders values between [0, 1]:

$$h: X \rightarrow \{[0, 1]\} \tag{3.2}$$

Definition 3.3 The boundaries of *h* are denoted as:

$$h^{-}(x) = \min h(x) \tag{3.3}$$

$$h^{+}(x) = \max h(x) \tag{3.4}$$

The preliminaries of HFS are summarized next (Rodríguez et al., 2011):

Definition 3.4 $S = \{s_0, \ldots, s_g\}$ is a set of linguistic terms. HFLTS, H_s, is a subset of the elements of S. Sometimes, S is expressed by subscript-symmetric term set, $S=\{si \mid i=-\tau,\ldots,-1,0,1,\ldots,\tau\}$.

Definition 3.5 The boundaries of HFLTS (H_s), H_{s+}, and H_{s-} are defined as:

$$H_{s+} = \max(s_i)=s_j \text{ , } s_i \in H_s \text{ and } s_i \leq s_j \quad \forall i; \tag{3.5}$$

$$H_{s-} = \min(s_i)=s_j \text{ , } s_i \in H_s \text{ and } s_i \leq s_j \quad \forall i; \tag{3.6}$$

Definition 3.6 Let E_{GH} be a function that transforms phrases into HFLTS, H_S. Let G_H be a grammar that uses the term set in S. S_{ll} is the domain of expressions created by G_H. This relationship is given as:

$$E_{GH}: S_{II} \rightarrow H_s \tag{3.7}$$

Conditional expressions are transformed into HFLTS with the following functions:

$$E_{GH}(s_i) = \{s_i | s_i \in S\} \quad (3.8)$$

$$E_{GH}(\text{at most } s_i) = \{s_j | s_j \in S \text{ and } s_j \leq s_i\} \quad (3.9)$$

$$E_{GH}(\text{lower than } s_i) = \{s_j | s_j \in S \text{ and } s_j < s_i\} \quad (3.10)$$

$$E_{GH}(\text{at least } s_i) = \{s_j | s_j \in S \text{ and } s_j \geq s_i\} \quad (3.11)$$

$$E_{GH}(\text{greater than } s_i) = \{s_j | s_j \in S \text{ and } s_j > s_i\} \quad (3.12)$$

$$E_{GH}(\text{between } s_i \text{ and } s_j) = \{s_k | s_k \in S \text{ and } s_i \leq s_k \leq s_j\} \quad (3.13)$$

3.1.2 Incomplete Hesitant Fuzzy Preference Relations and Literature Review on Incomplete HFPR

In Hesitant Fuzzy Preference Relations (HFPR) approach, several possible values can be considered as the preference information when decision-making team is not sure about a value. HFPR is based on Fuzzy Preference Relations (FPR) proposed by Orlovsky (1978). However, in decision-making, DMs may not have sufficient knowledge and/or experience of the decision-making problem. Besides, DMs may be unwilling to express their opinions. In such cases, DMs generally construct an incomplete HFPR, in which some elements are missing. Then, the missing elements in an incomplete HFPR are estimated. To deal with incomplete HFPRs, Zhang et al. (2015) proposed additive consistent HFPRs concept.

The preliminaries of FPR are summarized next (Orlovsky, 1978).

Definition 3.7 Let $X = \{x_1, x_2, \dots, x_n\}$ indicate a set of alternatives, where the ith alternative is represented by x_i. $R = (r_{ij})_{nxn}$ represents a FPR on X x X by the following conditions:

$$r_{ij} \geq 0, r_{ij} + r_{ji} = 1, i, j = 1,2, \dots, n. \quad (3.14)$$

Where r_{ij} indicates the degree provided from DM that alternative x_i is preferred to x_j.

Definition 3.8 Let $R = (r_{ij})_{nxn}$ be a FPR, then $R = (r_{ij})_{nxn}$ is called an additive consistent FPR if it satisfies the following condition:

$$r_{ij} = r_{ik} + r_{jk} + 0.5 \; for \; all \; i, j, k = 1,2, \dots, n. \tag{3.15}$$

The preliminaries of HFPR are summarized next (Xia & Xu, 2013); (Zhu & Xu, 2013); (Xia & Xu, 2013); (Zhu et al., 2014).

Definition 3.9 Let $X = \{x_1, x_2, \dots, x_n\}$ be a fixed set.

$H = (h_{ij})_{nxn} \subset XxX$ indicates a HFPR H on X where $h_{ij} = \left\{h_{ij}^{\sigma(s)} | s = 1,2, \dots, l_{h_{ij}}\right\}$ is a HFE. For all $i, j = 1,2, \dots, n$, h_{ij} should satisfy the following conditions:

$$\begin{cases} h_{ij}^{\sigma(s)} + h_{ji}^{\sigma(l_{h_{ij}} - s + 1)} = 1, \\ h_{ii} = \{0.5\}, \\ l_{h_{ij}} = l_{h_{ji}}. \end{cases} \tag{3.16}$$

Where $h_{ij}^{\sigma(s)}$ is the smallest element in h_{ij}.

Definition 3.10 Let $H = (h_{ij})_{nxn}$ be a HFPR, h_{ij}^{+} and h_{ij}^{-} be the maximum and minimum elements in h_{ij} respectively, $i, j = 1,2, \dots, n$, and let $\varsigma (0 \leq \varsigma \leq 1)$ be an optimized parameter. If we add some elements to h_{ij}(i<j) as $\bar{h}_{ij} = \varsigma h_{ij}^{+} + (1 - \varsigma) h_{ij}^{-}$; and if we add some elements to h_{ji}(i<j) as $\bar{h}_{ji} = (1 - \varsigma) h_{ij}^{+} + \varsigma h_{ij}^{-}$; , then we find a HFPR $\bar{H} = (\bar{h}_{ij})_{nxn}$.

For all $i, j = 1,2, \dots, n$, $\bar{h}_{ij}$ should satisfy the following conditions:

$$\begin{cases} l = l_{\bar{h}_{ij}} = max\left\{l_{h_{ij}} | i, j = 1,2, \dots, n, i \neq j\right\}, \\ \bar{h}_{ij}^{\sigma(s)} + \bar{h}_{ji}^{\sigma(l_{h_{ij}} - s + 1)} = 1 \\ \bar{h}_{ii} = \{0.5\}, \end{cases} \tag{3.17}$$

Where $\bar{h}_{ij}^{\sigma(s)}$ and $\bar{h}_{ji}^{\sigma(s)}$ are the sth smallest elements in $\bar{h}_{ij}$ and $\bar{h}_{ji}$, respectively. Then, $\bar{H} = (\bar{h}_{ij})_{nxn}$ is called as a normalized HFPR with the optimized parameter ς.

The preliminaries of HFPR are summarized next (Zhang et al., 2015).

Definition 3.11 Let $H = (h_{ij})_{nxn}$ be a HFPR, where $h_{ij} = \left\{h_{ij}^{\sigma(s)} | s = 1,2, \dots, l_{h_{ij}}\right\} (i, j = 1,2, \dots, n)$, then H is called an incomplete HFPR, if some of its elements cannot be given by the decision maker, that is denoted by the unknown variable "x", and the others can be provided by the DM which satisfy the following conditions:

$$\begin{cases} h_{ij}^{\sigma(s)} + h_{ji}^{\sigma(l_{h_{ij}} - s + 1)} = 1, \\ h_{ii} = \{0.5\}, \\ l_{h_{ij}} = l_{h_{ji}}. \end{cases} \tag{3.18}$$

For all $h_{ij} \in \Omega$, where Ω is the set of all the known elements in H.

Definition 3.12 Let $H = (h_{ij})_{nxn}$ be an incomplete HFPR, and let $\varsigma (0 \leq \varsigma \leq 1)$ be an optimized parameter where ς is used to add elements to $h_{ij} \in \Omega$(i<j),and 1- ς is used to add some elements to $h_{ji} \in \Omega$ $(i < j)$, to obtain an incomplete HFPR $\bar{H} = (\bar{h}_{ij})_{nxn}$.

For any $i, j = 1,2, \dots, n$, $\bar{h}_{ij} \in \Omega$, this preference relation should satisfy the following conditions:

$$\begin{cases} l = l_{\bar{h}_{ij}} = max\left\{l_{h_{ij}} | i, j = 1,2, \dots, n, i \neq j, h_{ij} \in \Omega\right\}, \\ \bar{h}_{ij}^{\sigma(s)} + \bar{h}_{ji}^{\sigma(l_{h_{ij}} - s + 1)} = 1 \\ \bar{h}_{ii} = \{0.5\}, \end{cases} \tag{3.19}$$

Then, $\bar{H} = (\bar{h}_{ij})_{nxn}$ is called as a normalized HFPR with the optimized parameter ς.

Definition 3.13 Let $H = (h_{ij})_{nxn}$ be an incomplete HFPR, if $(i, j) \cap (k, l) \neq \emptyset$, then the elements h_{ij} and h_{kl} are called adjacent. For a missing element h_{ij}, it can be determined indirectly if there exists a series of known elements $h_{ij_1}, h_{j_1 j_2}, \dots, h_{j_t j}$.

Definition 3.14 Let $H = (h_{ij})_{nxn}$ be an incomplete HFPR. If all missing element of H can be derived from its known elements, it is called an acceptable incomplete HFPR.

Theorem 3.1 For an acceptable incomplete HFPR H, there exists at least one known element (except diagonal elements) in each line or each column of H, i.e. at least $n - 1$ judgments should be provided by the experts. In other words, each alternative should be compared at least once.

Definition 3.15 Let $H = (h_{ij})_{nxn}$ be an incomplete HFPR, and $\bar{H} = (\bar{h}_{ij})_{nxn}$ be its normalized HFPR with the optimized parameter ς, if the known elements of $\bar{H}$ satisfy

$$\bar{h}_{ij_1}^{\sigma(s)} + \bar{h}_{j_1 j_2}^{\sigma(s)} + \cdots + \bar{h}_{j_{t-1} t}^{\sigma(s)} + \bar{h}_{j_t i}^{\sigma(l-s+1)} = \frac{t+1}{2}, \forall i < j_1 < j_2 < \cdots < j_t, s = 1,2, \dots, l \tag{3.20}$$

Then H is called an additive consistent incomplete HFPR with ς.

In the related literature, to test the acceptably additive consistency of HFPRs, Meng et al. (2021) proposed an optimization model-based technique. To measure the consistency level of an HFPR, Zhang et al. (2018) developed the best additive consistency index, the

worst additive consistency index, and the average additive consistency index. Li et al. (2021) proposed an algorithm for normalized HFPRs to improve the individual consistency and group consensus simultaneously. J. Li et al. (2022) considered the satisfaction degrees of DMs in incomplete HFPRs.

J. Li et al. (2021) integrated HFPRs with a MCDM technique (i.e. Best Worst Method (BWM)). J. Liu et al. (2021) integrated probabilistic HFPRs and Data Envelope Analysis (DEA) as a GDM method. Jin et al. (2022) evaluated sustainable development of small and medium-sized enterprises by using Charnes-Cooper-Rhodes DEA (CCR-DEA) method and HFPRs. Gao et al. (2021) integrated social network MCDM and satisfaction-driven consensus model for incomplete information. Lu et al. (2022) studied large-scale GDM in social networks with incomplete HFPRs.

To the authors' knowledge, incomplete hesitant fuzzy AHP technique and HFL Bonferroni means have not been used together before. This review indicates limited research on incomplete hesitant fuzzy MCDM approach studies. Incomplete HFPRs and MCDM methods have not been combined so far for assessing the cybersecurity maturity levels of institutions. A few papers realized case studies evaluating cybersecurity subjects with the MCDM approach.

3.1.3 HFL Aggregation Operators and Literature Review on HFL Aggregation Operators

Aggregation is essential in the decision-making problem because it derives a collective decision by representing individual opinions. In addition, aggregation of individual judgments or preferences is used to transform experts' judgment knowledge and decision-making problems because it is used to derive a collective decision made by the decision-makers by representing e in relative weight.

As many different types of criteria relationships exist in the real world, there is a need for many types of formal aggregation operations to model these numerous types of relationships. Different types of aggregation operators are illustrated in Figure 3.2.

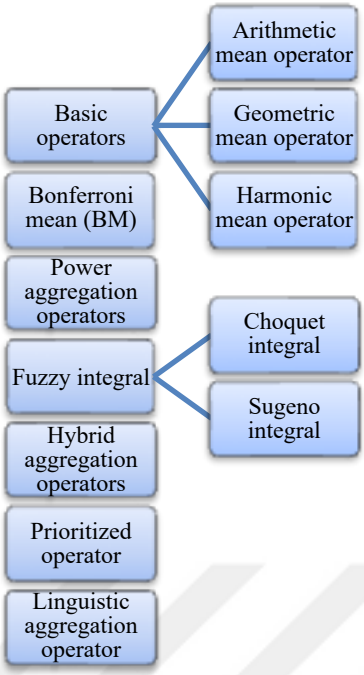

Figure 3.2: Aggregation operators

The HFL aggregation operators are examined in Table 3.1. The main characteristics of the aggregation operators are displayed to determine aggregation operators based on necessity in GDM.

Table 3.1: Papers applying HFL aggregation operators

The aggregation operator	Main characteristic	Reference
• Hesitant fuzzy linguistic weighted averaging (HFLWA) operator • Hesitant fuzzy linguistic weighted geometric (HFLWG) operator	• HFLWA and HFLWG weigh the hesitant fuzzy argument itself but ignore the importance of the ordered position of the argument. • The values obtained by the HFLWG operator are not bigger than the ones obtained by the HFLWA operator.	(Xia and Xu, 2011)
• Hesitant fuzzy linguistic ordered weighted averaging (HFLOWA) operator • Hesitant fuzzy linguistic ordered weighted geometric (HFLOWG) operator	• HFLOWA and HFLOWG operators are developed based on the idea of the OWA operator. • They weight the ordered position of each given argument, but ignore the importance of the argument.	(Xia and Xu, 2011)

Table 3.1: Papers applying HFL aggregation operators (*continue*)

The aggregation operator	Main characteristic	Reference
• Power Average (PA) operator • HFLPA operator	• PA operator allows for aggregations in which a subset of data clustered around a common value can combine in a nonlinear fashion to act in concert in determining the aggregated value. • HFLPA enables aggregations which can capture both the features of mode-like methods, with their focus on finding the most common or typical value, and the averaging-type operator with its focus on a fusing of the data.	(Yager, 2009); (Jiang et al., 2020)
• Heronian Mean (HM) operator • HFLHM operator	• HM operator has the peculiarity of catching the correlations of the aggregated arguments. • The operators based on HM describes the interrelationships between different variables, explain the interrelationship between a decision criterion and itself and also differ the interrelationship between $Cj$and Ci from the interrelationship between criteria Ci and Cj.	(Beliakov et al., 2007); (Jiang et al., 2020)
• Bonferroni Mean (BM) • HFLBM operator	• BM operator can capture the interrelationships among arguments, it has been applied widely in MCDM under different circumstances. • HFLBM operator not only considers the significance of the weights of all criteria, but also considers the interrelationships among the criteria.	(Yager, 2009); (Beliakov et al., 2010); (Xia et al., 2013); Xu and Yager 2011); (Gou, et al., 2017)

The BM and the HM operators require the inputs of the p, q values. A series of examples have shown that the p, q values of the BM- and the HM-based operators influence the interaction degrees of the variables so as to influence the ranking results of the alternatives, where the increase of the values of p and q enhances the interaction degrees between the variables (Sun, 2018).

The HFLWA operator proposed by Xia and Xu (2011) is used in this study in Chapter 4 to aggregate DMs' opinions in GDM. Yager (2009) proposed the Bonferroni mean operator. Zhu & Xu (2013) developed the Hesitant Fuzzy Bonferroni Mean (HFBM) operator that provides the desired properties and the modeling capability of the Bonferroni mean. Particularly, the Bonferroni mean (BM) has desirable properties capturing the interrelationships among arguments. To aggregate the DMs' opinions, the HFL Bonferroni Mean (HFLBM) operator proposed by Gou et al. (2017) is used in this study in Chapter 5. The advantage of the HFLBM is that it can capture the interrelationship between HFEs.

3.1.4 HFL AHP Approach and Literature Review on HFL AHP Approach

The AHP method was proposed by Saaty (1980), and the hesitant fuzzy extension of the AHP method was developed by Mousavi et al. (2014). AHP is widely used for calculating the criteria weights (Avanzi et al., 2017; Zandieh & Aslani, 2019). The benefits of AHP are:

- Utilization of the people's constrained capability that people could give precise information when making a comparison of two objectives (Ren et al., 2019),
- Building the hierarchy of the relative problem visibly and dividing the original problem into sub-problems could be resolved more easily (Çevik Onar et al., 2016; Liao et al., 2019; Ren et al., 2019; S. Wang et al., 2019),
- The weight of each object from the bottom to the top could be computed by the relative comparison matrix (Liao et al., 2019),
- Flexibility in handling complex and comprehensive decision-making problems (Mi et al., 2019).

The drawbacks of the AHP method are:

- There is a paradox in the consistency test in the pairwise comparison method (K. Xu & Xu, 2019).

As illustrated in Table 3.2, HFL AHP has been used in different application fields such as environment, mining, technology, logistics, energy, manufacturing, healthcare, management, tourism, supply chain, and finance.

This paper uses an incomplete HFL AHP method to calculate the cybersecurity maturity factors' weights. Since the nature of the problem is appropriate for pairwise comparison, one of the aforementioned drawbacks is handled. Since the paradox of consistency is a subjective drawback of this method, it is not considered. As seen in Table 3.2, many of the papers removed the partiality in decision-making by using GDM approach.

An incomplete HFPR-AHP method is employed for dealing with incomplete preferences provided by experts for the first time. A research methodology based on an incomplete HFPR-AHP method with a GDM approach with Bonferroni means operator is presented, which calculates the importance degrees of the maturity factors.

Table 3.2: Papers applying of HFL AHP method

Author(s)	Aim of the Study	Application Area	Applied HFL MCDM methods	Type	GDM
(Mousavi et al., 2014)	Propose HFS for AHP method	Construction	**AHP**	Case Study	+
(Zhu & Xu, 2014)	Propose hesitant multiplicative programming method (HMPM)	Environment	**AHP** and HMPM	Case Study	+
(Zhu et al., 2016)	Develop a new prioritizing method to derive priorities	Mining	**AHP**	Case Study	+
(Çevik Onar et al., 2016)	Develop new QFD method grounded on HFLTS	Technology	**AHP**, TOPSIS, and QFD	Case Study	+
(Boltürk et al., 2016)	Select warehouse location	Logistics	**AHP**	Case Study	+
(Başar, 2016)	Software cost estimation	Technology	**AHP**	Case Study	+
(Çolak & Kaya, 2017)	Prioritization of renewable energy alternatives	Energy	**AHP**, TOPSIS	Case Study	+
(Tüysüz & Şimşek, 2017)	Examination of the factors affecting the performance	Logistics	**AHP**		+
(Acar et al., 2018)	Investigate the sustainability of hydrogen systems	Energy	**AHP**	Case Study	+
(Büyüközkan et al., 2018)	Select renewable energy sources	Energy	**AHP,** COPRAS	Case Study	+
(Camci et al., 2018)	Select the CNC router	Manufacturing	**AHP**	Case Study	+
(Aktas & Kabak, 2018)	Assess the solar power plant location sites	Energy	**AHP,** TOPSIS	Case Study	+
(Liao et al., 2019)	Evaluate the performances of hospitals	Healthcare	**AHP,** BWM	Illustrative Example	+
(Mi et al., 2019)	Advance HFL AHP method by realizing consistency check	-	**AHP**	Case Study	-
(Öztayşi et al., 2019)	Choose the most suitable water treatment technology	Environment	**AHP**	Case Study	+
(Srdjevic et al., 2019)	Rank the urban ecosystems services	Environment	**AHP**	Case Study	+
(Ren et al., 2019)	Choose the most appropriate artificial intelligence strategy	Technology	**AHP, VIKOR**	Case Study	+
(S. Wang et al., 2019)	Evaluate renewable energy investments	Energy	**AHP,** DEMATEL, TOPSIS, VIKOR	Illustrative Example	+

Table 3.2: Papers applying of HFL AHP method (*continue*)

Author(s)	Aim of the Study	Application Area	Applied HFL MCDM methods	Type	GDM
(K. Xu & Xu, 2019)	Improve probability HFL AHP process	-	**AHP**	Illustrative Example	-
(Yıldız & Tüysüz, 2019)	Select strategic retail location	Management	**AHP**, GRA	Case Study	+
(Ayağ & Samanlioglu, 2020)	Rank ERP software packages	Technology	**AHP**, TOPSIS	Case Study	+
(Büyüközkan & Güler, 2020)	Rank companies according to their digital maturity	Technology	**AHP**, ARAS	Case Study	+
(Çolak et al., 2020)	Evaluate blockchain technology for different sectors	Supply Chain	**AHP,** TOPSIS	Illustrative Example	+
(Wu et al., 2020)	Build a decision model for incineration power plant performance evaluation	Environment	**AHP,** Entropy	Case Study	+
(Tüysüz & Yıldız, 2020)	Evaluate the performance of banks	Finance	**AHP**, GRA	Case Study	+
(Batur Sir & Sir, 2021)	Evaluate COVID19 treatment alternatives	Healthcare	**AHP,** VIKOR	Case Study	+
(Büyüközkan et al., 2020)	Evaluate the health tourism strategies	Tourism	**AHP**, MABAC	Case Study	+
(Sahu et al., 2021)	Assess reliability prediction models for software	Technology	**AHP,** TOPSIS	Case Study	+
(K. Wang et al., 2021)	Analyze aircraft structural parts	Transportation	**AHP,** fuzzy synthetic evaluation	Case Study	+
(Y. Xu et al., 2022)	Develop consensus checking for AHP with dual hesitant fuzzy sets	Healthcare	**AHP**	Illustrative Example	+

3.2 Overview of the Cognitive Map Approach

Cognitive Map (CM) deals with mapping humans' mental activities in the problem-solving (Tolman, 1948). The topic is introduced in the 70s as a type of directed graphs used to capture and understand cause and effect relationships in complex causal systems and to facilitate the understanding of the interconnections within the elements of the concepts (Axelrod, 1976). At first, a political scientist Axelrod (1976) introduced cognitive maps for representing social scientific knowledge and describing the methods that are used for decision-making in social and political systems.

3.2.1 Cognitive Map Approach

CM has two elements: concepts and causal belief. Concepts are the variables that represent the belief system of a person, and the causal belief consists of the causal decencies between these variables. The elements of CM are shown in Figure 3.3. An example of CM is illustrated in Figure 3.4.

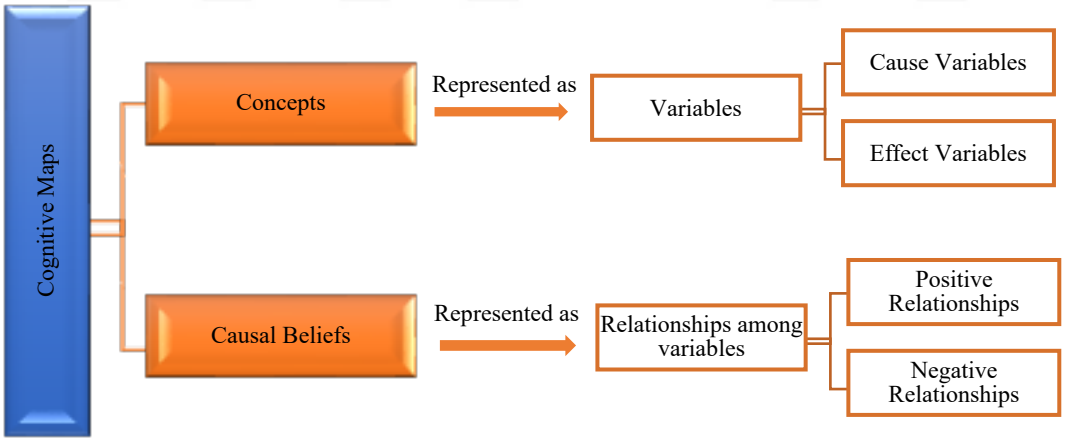

Figure 3.3: The elements of CM (Rodriguez-Repiso et al., 2007)

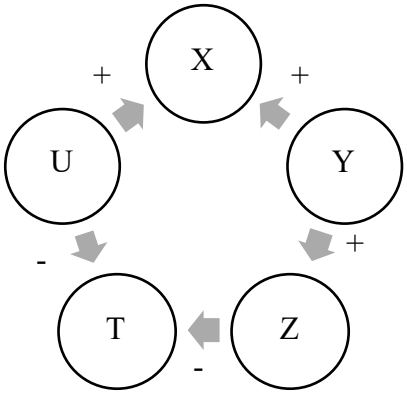

Figure 3.4: An example of part of CM

Fuzzy Cognitive Map (FCM) methodology is a symbolic representation for the description and modeling of complex systems. Some studies (Kosko, 1986; Kosko & Burgess, 1998) enhanced the power of cognitive maps, considering fuzzy values for the concepts of the cognitive map and fuzzy degrees of interrelationships between concepts. After this pioneering work, FCMs attracted the attention of scientists from many fields and have been used in a variety of different scientific problems (Stylios & Groumpos, 1999).

FCMs describe different aspects of the behavior of a complex system in terms of concepts; each concept represents a state or a characteristic of the system, and these concepts interact with each other, showing the dynamics of the system. FCMs illustrate the whole system by a graph showing the cause and effect along concepts and are a simple way to symbolically describe the system's model and behavior, exploiting the accumulated knowledge of the system. An FCM integrates the accumulated experience and knowledge on the operation of the system as a result of the method by which it is constructed, i.e., using human experts who know the operation of the system and its behavior in different circumstances. Moreover, FCM utilizes learning techniques, which have been implemented in Neural Network Theory, to train FCM and choose appropriate weights for its interconnections. FCMs represent knowledge in a symbolic manner and relate states, processes, events, values and inputs. The knowledge which accumulated for years on the operation and behavior of a system can be adequately explained using FCMs. Figure 3.5 illustrates a graphical representation of a FCM consisting of five concepts (C1

to C5) and related weights, w_{ji} (cause-effect relationships among the concepts) (Markinos et al., 2007).

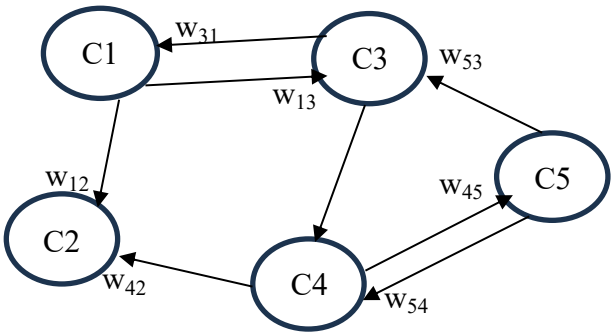

Figure 3.5: An example of part of FCM

The cause and effect interconnection between two concepts C_j and C_i is described with the weight w_{ji}, taking a value in the range –1 to 1. Three possible types of causal relationships exist:

- $\boldsymbol{w_{ji}} > 0$ which indicates positive causality between concepts C_j and C_i,
- $\boldsymbol{w_{ji}} < 0$ which indicates negative causality between concepts C_j and C_i, and
- $\boldsymbol{w_{ji}} = 0$ which indicates no relationship between C_j and C_i.

The value A_i of the concept C_i expresses the degree of its corresponding physical value. At each simulation step, the value A_i of the concept C_i is calculated by computing the influence of other concepts C_i's on the specific concept C_j following the calculation rule (Markinos et al., 2007):

$$A_i^{(k+1)} = f(A_i^{(k)} + \sum_{j \neq i}^{N} A_j^{(k)} \cdot w_{ji}) \tag{3.21}$$

where $A_i^{(k+1)}$ is the value of concept C_i at simulation step $k+1$, where $A_j^{(k)}$ is the value of concept C_j at simulation step k, w_{ji} is the weight of the interconnection from concept C_j to concept C_i and f is a sigmoid threshold function (Markinos et al., 2007):

$$f = \frac{1}{1+e^{-\lambda x}} \tag{3.22}$$

where $\lambda > 0$ is a parameter that determines its steepness. The procedure for constructing fuzzy cognitive maps is as follows: experts define the main concepts that represent the model of the system; they describe the structure and the interconnections of the network using fuzzy conditional statements.

FCMs have proven particularly useful for solving problems in which a number of decision variable and uncontrollable variables are causality interrelated. FCMs are capable of modeling scenarios described in terms of significant events (or concepts) in the scenario and their cause-effect relationships. One of the most useful aspects of the FCM is its potential for use in decision support as a prediction tool (Kosko, 1986). Given an initial state of a system, represented by a set of values of its constituent concepts, a FCM can simulate its evolution over time to predict its future behavior. These features make FCM a very attractive tool for analyzing factors. Moreover, FCM has successfully applied in a lot of areas such as strategic planning, information technology, electronic business and commerce, decision making, project management, investment analysis, medicine, environmental, ecological topics, airline service (Büyüközkan & Vardaloglu, 2012).

FCMs often require decision-makers to deliver evaluations on the relationships between factors, which is time-consuming and involves dealing with many uncertainties from a number of different sources. Thus, obtaining exact evaluations in FCMs is usually unrealistic when the available data for the assessments is ambiguous, insufficient, hesitant, etc. To deal with the uncertainties, some kinds of extensions of FCMs have been presented. Salmeron (2010) proposed fuzzy grey cognitive maps (FGCMs) based on grey systems theory. Iakovidis & Papageorgiou (2011) proposed intuitionistic fuzzy cognitive maps (IFCMs), which combine intuitionistic fuzzy sets (IFSs) and FCMs. Through reviewing the literature, we can find that most of the above extensions are utilized to model the uncertainties inherent in the evaluation process. It is essential to model this kind of uncertainty when a group of experts is invited to take part in the assessment process, which is typically the case in FCM. Therefore, X. Liu et al. (2019) presented a novel approach to FCM based on HFSs for dealing with these issues. Authors have combined the hesitant fuzzy set (HFS) theory with FCM to address a certain kind of uncertainty, that is, hesitancy.

3.2.2 Literature Review on Cognitive Map Approach

In this literature review section, the research on CM and the government's digital transformation are investigated. The two largest databases are Scopus from Elsevier and the Web of Science (WoS) from Clarivate Analytics. In this paper, data is collected from these two databases. The search strings are used for the "topic" field in the WoS core collection. This makes sure that the results include the selected keyword in the documents' title, abstract, and author keywords. In Scopus, the search strings are used for the "article title, abstract, keywords" field.

The databases are searched with the following keywords: "government" AND "cognitive map"; "e-Government" AND "cognitive map"; "digital government" AND "cognitive map".

The examined studies are presented in Table 3.3. It aims to display the related categories of CM publications and is structured into five sections to summarize the main concept of each paper to convey their relevance. The application area is presented to display the involvement of the government in each paper. Its application environment is displayed in the next section. The integrated method illustrates which methodology is integrated with CM in the paper. The type of its application is presented in the fourth section. Following this, the publications are identified as GDM or not.

According to the literature review of CM in Table 3.3, there is research on several government subjects, such as international cooperation, open government, open innovation, national economic system, local government decision-making, education, transportation, insurance, and public service procurement. In most of these studies, type-1 fuzzy sets are preferred as extensions. Besides, some studies use HFSs, intuitionistic fuzzy sets, and neutrosophic fuzzy sets. Simulation is the most frequently used method with CM. Moreover, PESTEL analysis, design science research, and statistical methods are used. A case study is preferred in the majority of this research, while the GDM approach is highly preferred.

Table 3.3: Literature review on CM studies on DG

Author(s)	Application Area	Fuzzy Extension	Integrated Method(s)	Application Type	GDM
(Durman et al., 2021)	International Cooperation	-	-	Case Study	+
(Gómez et al., 2022)	Open Government	Neutrosophic Fuzzy Sets	PESTEL	Case Study	+
(Greco et al., 2017)	Open Innovation in Power and Energy Sector	Type-1 Fuzzy Sets	-	Case Study	+
(Gupta & Gupta, 2017)	National Economic System	Type-1 Fuzzy Sets	-	Illustrative Example	-
(Oe et al., 2016)	Decision-Making in Local Government	-	Text Mining	Case Study	+
(Salustri, 2022)	Public Policy-Making in Municipalities	-	-	Case Study	-
(Sonje et al., 2023)	Government-Aided Basic Education System	Type-1 Fuzzy Sets	Value-Focused Thinking	Case Study	-
(Shiaua and Liu, 2013)	Local Governments' Transportattion	Type-1 Fuzzy Sets	-	Illustrative Example	-
(Tiller et al., 2016)	Climate Change in Local Communities	Type-1 Fuzzy Sets	-	Case Study	+
(Yun & Jung, 2021)	Public Medical Insurance Reforms	Type-1 Fuzzy Sets	Simulation	Case Study	+
(Y. Zhang et al., 2022)	Government Procurement of Public Services	Type-1 Fuzzy Sets	-	Case Study	+

3.2.3 Literature Review on Hesitant Fuzzy Linguistic Fuzzy Cognitive Map Approach

In this literature review section, the research on HFLCM are investigated. The two largest. The search strings are used for the "topic" field in the WoS core collection In Scopus, the search strings are used for the "article title, abstract, keywords" field.

The databases are searched with the following keywords: "hesitant" AND "fuzzy cognitive map". The examined studies are presented in Table 3.4.

To the authors' knowledge, a HFLCM methodology with the fuzzy envelope technique is not been proposed. There also exists no study in the literature analyzing the structure of the DG framework with CMs. Thus, the originality of our thesis stems from offering a

novel framework for analyzing the DG framework by integrating the CM approach with the HFLCM technique under the GDM environment for the first time.

Table 3.4: Literature review on HFLCM

Author(s)	Application Area	Fuzzy Extension	Integrated Method(s)	Application Type	GDM
(Budak & Onar, 2021)	Online Shopping	Hesitant Fuzzy Sets	-	Case Study	+
(Budak & Çoban, 2021)	Blockchain Technology on Supply Chain	Hesitant Fuzzy Sets	-	Illustrative Example	+
(Çoban & Onar, 2017)	Renewable Energy Investment in Public Sector	Hesitant Fuzzy Sets	-	Illustrative Example	-
(Gündoğdu, 2022)	Smart Energy	Hesitant Fuzzy Z-Numbers	DEMATEL	Illustrative Example	-
(Liu et al., 2019)	Electric Power System	Hesitant Fuzzy Sets	-	Illustrative Example	-
(Wang et al., 2021)	Emergency Management	Dual Hesitant Fuzzy Sets	-	Case Study	-

In this study, an HFLCM with a fuzzy envelope technique is constructed, in which the concepts are evaluated by using comparative linguistic terms and Hesitant Fuzzy Linguistic Elements (HFEs), and transformed into trapezoidal fuzzy numbers. Therefore, HFLCM is a novel study to be proposed by the authors in which generalization of Fuzzy CM is proposed in the hesitant fuzzy environment to cope with complex links among concepts for the DG framework.

4. MODELLING AND ANALYSIS OF THE DGT FRAMEWORK

The future of government has arrived. Over the past two decades, many governments have undergone significant digital advancement, from the early e-government efforts during the dotcom era to the user-experience–fueled launch of government digital service units and the adoption of commercial IT practices. While they made progress, governments became wired but not transformed. Too many still focused chiefly on digitizing front-end services while postponing the stricter issues of fundamentally reengineering underlying government operations, processes, and systems (William D. Eggers, Jason Manstof, Pankaj Kamleshkumar Kishnani, 2021). Only 20% of public sector transformations meet their goals, compared to the cross-industry private sector average of 30% (Mourtada et al., 2022). While the global pandemic magnified cracks in the workings of government, such as IT, supply chain, and back office limitations, it has also been a springboard for advancements in remote working, agile policy-making, and rapid service design. Successfully navigating the debt journey ahead will require governments to abandon traditional thinking. They should wisely replace the typical reliance on program cuts and funding restraints by pursuing new opportunities for programs, investments, and innovations that underpin sustained economic growth and advancement (KPMG International, 2021).

Digital Government Transformation (DGT) is the use of digital technologies to transform government by enhancing the ability of citizens, businesses, and government to engage in transactions with the public sector to make it more accessible, effective, and accountable. Recently, many studies have developed models on DGT. Despite the well-founded efforts towards DGT, public organizations need help to realize their full potential. One of the reasons for this is that public organizations are not always properly prepared to face this challenge. Therefore, the study's originality comes from proposing a DGT framework and introducing a new research methodology based on the Hesitant

Fuzzy Linguistic Term Sets (HFLTS) technique, fuzzy envelope technique, and the Hesitant Fuzzy Linguistic Cognitive Map (HFLCM). Academicians, researchers, organizations, executives, and policy-makers can use this study to guide their studies. This study has the following contributions:

- a DGT framework with three main areas for public institutions is analyzed,
- an HFLCM with the fuzzy envelope technique is presented as the research methodology,
- and various simulations for efficient DGT employment are conducted with what-if scenario analyses.

Governments may understandably be tempted to offset the pandemic's overwhelming price tag with strict new fiscal restraints that limit inevitable future investment in technology, new talent, 21st-century digital services, and economic growth. As governments move quickly to manage the looming debt burden, civil services will be under new pressure to do more with less (KPMG International, 2021).

Many government organizations intensified their digital transformation efforts in response to the needs and external drivers that surfaced or intensified during COVID-19. Indeed, they've found that they can drive more change faster than they had thought possible. Governments should build on this experience to commit to a faster pace of digital transformation (William D. Eggers, Jason Manstof, Pankaj Kamleshkumar Kishnani, 2021).

In Figure 4.1, the characteristics of the new DG are illustrated (Lee et al., 2018). DGT aims to leverage advancements in technologies. It is expected to:

- Improve mission effectiveness and efficiency,
- Optimize outcomes, such as transparency and openness,
- Long-range cost savings,
- Better governance,
- Better quality of life for citizens.

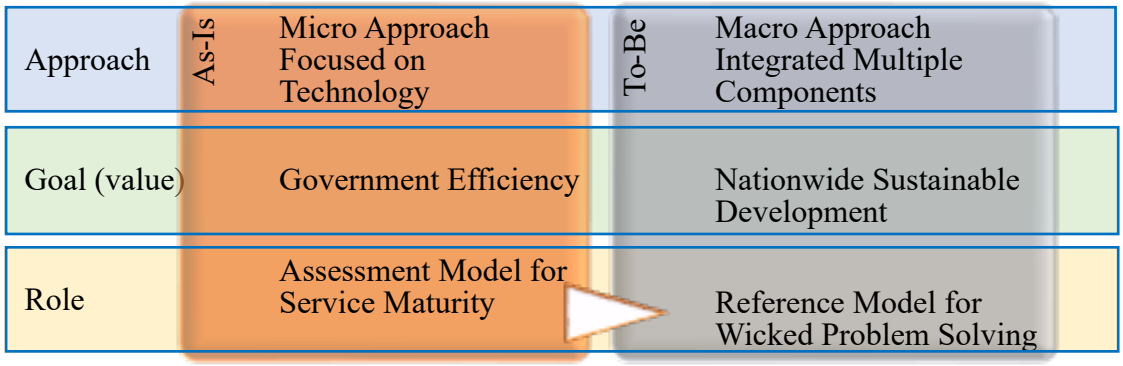

Figure 4.1: Characteristics of new DG (Lee et al., 2018)

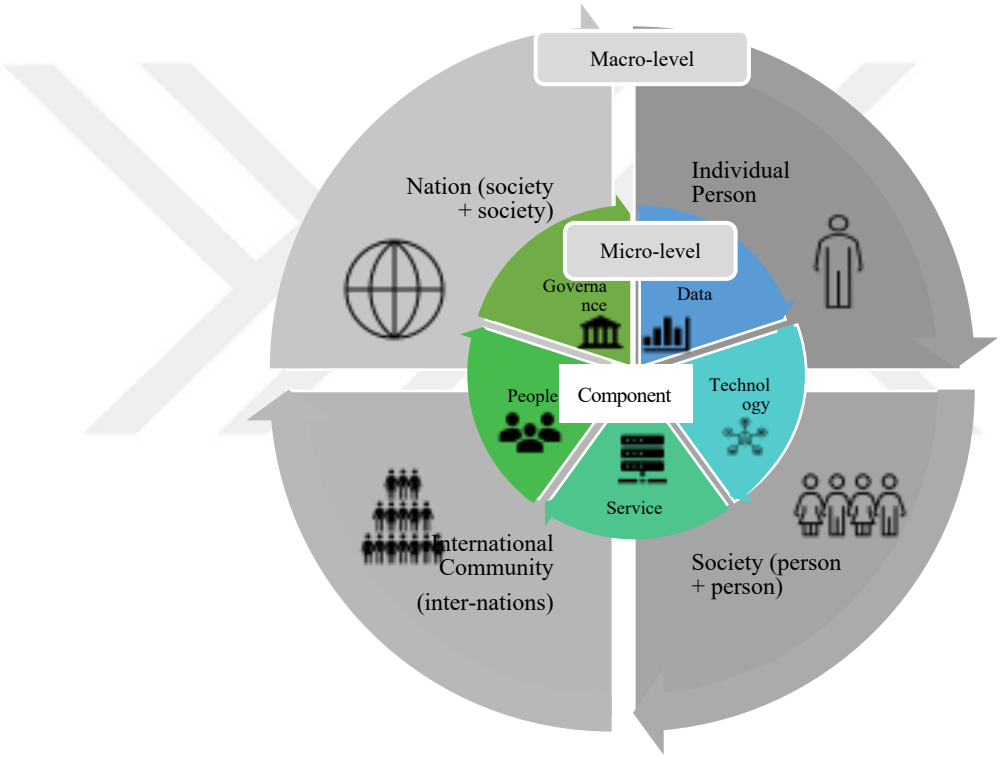

Figure 4.2: Four target areas (macro-level) and five critical elements (micro-level) (Lee et al., 2018)

In Figure 4.2., the components of DG for the micro-level and macro-level are illustrated. At the macro level, individuals, society, the international community, and the nation are the main components of the DG system. When we look at the micro-level, people, governance, data, technology, and service are the main components of the DG system.

4.1 Success and Risk Factors of the DGT Framework

The success and risk factors for an accessible, effective, and accountable DGT framework are proposed based on literature review, industry reports, and experts' views. To evaluate holistically the DGT subject from different stakeholders' perspectives, an HFLCM is proposed as a novel study. The success and risk factors are categorized into three main groups: Digital Citizenship Improvement, Digital Technology Improvement, and Digital Service Improvement. Figure 4.3 illustrates the proposed DGT framework.

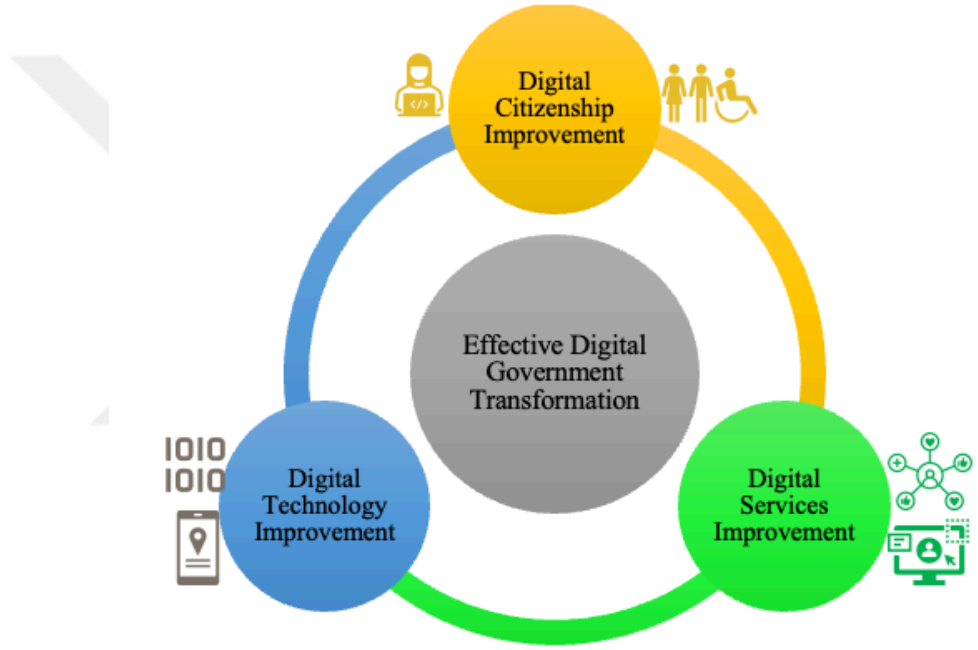

Figure 4.3: The proposed DGT framework

4.1.1 Digital Citizenship Improvement

- **Digital Training and Education (DCI1):** Digital education is a learning approach that allows users to master new skills on their own time over the Internet. Digital training and education allow the acquisition of basic digital skills by university research centers. Digital education utilizes online platforms, multimedia resources, educational software, and social media to enhance teaching and learning (Economic Commission for Latin America and

the Caribbean (ECLAC), 2021; European Commission, 2021).

- **Citizen Engagement (DCI_2):** Citizen engagement is an activity that fosters information flow between members of the public and policymakers. This interchange contains information concerning facts as well as values, opinions, and impressions. An effective DGT implementation should re-conceptualize the interactions with citizens and enable citizen engagement (European Commission, 2021; United Nations, 2022b; Wilson & Mergel, 2022).
- **Citizen Satisfaction (DCI_3):** Citizens evaluate government services based on prior expectations. The fulfillment of expected benefits from DGT increases citizen satisfaction. Obtaining information easily and quickly, no need for citizens to visit government offices physically, and cost and time saving for citizens can be listed as some benefits of DGT (Malodia et al., 2021; Tangi et al., 2021; Vaccari et al., 2021).
- **Efficient Use of Feedback Mechanism (DCI_4):** Feedback mechanisms give institutions data and perceptions from primary users about the quality and efficacy of their efforts. Respecting national and cross-border user needs and receiving feedback from citizens and stakeholders are critical in designing and implementing the DGT (Ionescu et al., 2022; Wilson & Mergel, 2022). Citizen feedback is essential as it helps to inform and guide the county government on what is working, what is not, and areas that require attention or improvement. These mechanisms can be meaningful only if they are easily accessible, affordable, and appreciated by the government (Country Tool Kit, 2020).
- **Digital Literacy (DCI_5):** Digital literacy is the ability to access, manage, understand, integrate, communicate, evaluate, and create information safely and appropriately through digital technologies for employment, decent jobs, and entrepreneurship. It includes various competencies called computer literacy, ICT literacy, information literacy, and media literacy (Law et al., 2018). In other words, the lack of this factor is explained in terms of a lack of technological familiarity (European Commission, 2021; United Nations, 2022b; Wilson & Mergel, 2022).
- **Public Awareness (DCI_6):** Public awareness refers to the general public's comprehension of the significance and repercussions of a particular program or activity. Raising public awareness does not imply instructing people what

to do. It is the process of clarifying issues and spreading knowledge to people so they can make their judgments. Lack of public awareness of DGT constitutes a barrier to accepting and adopting DG Services (Mujali Al-rawahna et al., 2018; Wilson & Mergel, 2022).

- **Ethical Concerns (DCI_7):** Ethical concerns are circumstances arising from a moral dilemma and must be resolved. As a result, ethical issues frequently clash with the principles of a community (Makki & Alqahtani, 2022; Ndlovu et al., 2022; Wilson & Mergel, 2022). The societal demand for ethical practices to supplement data protection and legislation has grown, reflecting a growing interest in ensuring that data is utilized in ways that respect the public interest and produce reliable results (OECD, 2022).
- **Digital Trust in Government (DCI_8):** The level of trust citizens and organizations have in the security, privacy, and dependability of digital transactions and interactions is called digital trust. The development of political, economic, cultural, and social activities in the digital society is influenced by digital trust. Therefore, DGT implementation should provide increased transparency, enhanced accountability, ease of tracking applications, and reduced corruption (Elsheikh et al., 2022; Malodia et al., 2021).
- **Motivation to Learn Advanced Technologies (DCI_9):** Advanced technologies are the key to unlocking unprecedented opportunities by seamlessly integrating physical and digital systems while harnessing the power of enabling technologies. This factor represents citizens' learning motivation about utilizing new digital technologies and DG services (Al Sulaimani, 2022).
- **Well-orchestrated Citizen Journeys (DCI_{10}):** Citizen journey orchestration is a more advanced form of citizen journey management, which maximizes the citizen experience via technology to create one-of-a-kind interactions. Well-orchestrated user journeys result in more robust collaboration with citizens (Ionescu et al., 2022).
- **Citizen Involvement (DCI_{11}):** Transforming DG service delivery begins with understanding citizens' needs and priorities. Identifying which services citizens find most problematic and measuring the extent of that dissatisfaction

is one way governments can prioritize areas for improvement via citizen involvement. This way, government leaders can focus improvement initiatives on what matters most to citizens (Dudley et al., 2015). Citizen involvement stimulates the fertilization of ideas, solutions, and knowledge (Hassan & Lee, 2019).

- **Digital Divide (DCI_{12}):** The digital divide refers to the difference between demographics and regions with access to contemporary information and communications technologies and those without limited access. The digital divide indicates the digital gap in society. For developing countries, it can cause social inequality and hinder the DGT implementation (Elsheikh et al., 2022; Hassan & Lee, 2019; Mujali Al-rawahna et al., 2018).
- **Perceived Privacy Concerns (DCI_{13}):** The level of control citizens have over personally identifiable information is measured by the privacy concern. Citizens are concerned with the privacy of their personal information during digital transactions. Thus, privacy and security issues such as online theft and fraud should be prevented by governments (Mujali Al-rawahna et al., 2018; Ndlovu et al., 2022).
- **Public Participation (DCI_{14}):** Public participation is about actions a person or group can take to get interested in government or community issues that concern them. It ensures that citizens are heard and can actively participate in decisions that impact their needs. Individuals' interaction with the various structures and institutions of democracy, such as voting, contacting a political representative, campaigning and lobbying, and participating in consultations and demonstrations, is called public participation (Country Tool Kit, 2020). Participation is a crucial element in transforming governments. Government websites, applications, and portals are central to realizing public participation. The implication is that all aspects of DGs should organize their entities for interacting with the citizens (Ndlovu et al., 2022).

4.1.2 Digital Technology Improvement

- **Sustainable Digital Infrastructure (DTI_1):** Digitalization in governments brings associated environmental risks such as increased energy consumption

and carbon footprint due to the use of digital technologies, increased generation of hazardous waste related to the production and disposal of electronic devices, increased demand for natural resources in the manufacture of electronic devices and technology, and excessive dependence on technologies that may be vulnerable to extreme weather events, such as floods, earthquakes or storms. Applying social, economic, and environmental stewardship principles to digital products, services, and data given via the Internet is known as digital sustainability. Therefore, it is critical to make DGT sustainable (European Commission, 2021; IDB, 2020).

- **Data Ownership Rules (DTI_2):** Data ownership encompasses control and information responsibility. Data owners can access, generate, edit, package, benefit from, sell, or remove data and delegate these rights to others. The data ownership rules and procedures reduce the risk by advocating the end users to protect their information against illegitimate disclosure, and the mechanism protects the sensitive information through encryption techniques (Hassan & Lee, 2019). Upon being informed about how and with whom personal and collectively owned data is shared, individuals (including citizens and residents) and communities should be given decision-making power to exercise autonomy, control, and agency over their data and to freely give or withdraw consent to its use (OECD, 2022).
- **Cybersecurity (DTI_3):** Cybersecurity is the measures taken against cyber-attacks. Cybersecurity threats and cyber-attacks are the focus of government cybersecurity solutions. Government entities, including federal and local/state, can lower their risk of data breaches and other disruptive and destructive cyberattacks by establishing protections against the primary cyber-attack vectors (European Commission, 2021). Governments needs to prioritize their strategies to establish cybersecurity procedures effectively, create internal awareness, train their employees, strengthen their cybersecurity infrastructure and ultimately increase their cyber resilience (Erdoğan et al., 2020). Cyber security frameworks must guide management at various security levels before implementation (Atoum & Otoom, 2016).
- **Functional Interoperability (DTI_4):** Functional interoperability is characterized by the ability to implement two or more integrations and have

the services supplied by the integrations work together to satisfy end-to-end business processes. Ensuring functional interoperability across all levels of government and across public services is necessary for a successful DGT implementation (European Commission, 2021; Makki & Alqahtani, 2022).

- **Systems Integration (DTI_5):** Concerning software solutions, system integration is typically defined as the process of linking together various IT systems, services, and software to enable all of them to work functionally together. System integration brings together multiple systems to work as a single system. System integrators combine disparate systems using various techniques such as computer networking, enterprise application integration, business process management, or programming. DG service provision requires different public administrations to work together to meet end users' needs and provide public services in an integrated way (Al Sulaimani, Ahmed Hamed Abdullah and Ozuem, 2022; EIF, 2017; Mujali Al-rawahna et al., 2018; Petter et al., 2008).
- **Standardization of Technologies (DTI_6):** Standardization of technologies establishes, promotes, and mandates standards-based and comparable procedures and technologies. This factor represents specifications and guidelines, alongside the consensus on identifying patterns of when to apply different standards and the availability of digital technologies and connection with new technologies (United Nations, 2022b; Vaccari et al., 2021; Wilson & Mergel, 2022).
- **Network Connectivity (DTI_7):** Network connectivity refers to the comprehensive process of connecting various elements of a network to one another, which may be accomplished through routers, switches, and gateways, as well as how the process is accomplished. The public and private sectors must work together to facilitate the deployment of the connectivity network and encourage sustainable adoption of it (Economic Commission for Latin America and the Caribbean (ECLAC), 2021).
- **IT Capacity (DTI_8): Concerning** computer and information systems, capacity refers to the storage and transaction processing capability of computer systems, the network, and/or the data center. IT capacity management is a business process that ensures IT resources are sufficient to

meet future needs. IT capacity managers must understand current and future business needs. Increasing computing capacity ensures seamless interactions and transactions (European Commission, 2021; KPMG International, 2021).

- **Capacity and Skills Development (DTI_9):** Capacity and skills development refers to acquiring the ability or facility to do complex activities or job functions smoothly and adaptively through continuous and methodical efforts. Skills development is recognizing skill gaps and working to improve them. The successful completion of DGT requires qualified, skilled, and experienced professionals. However, it is still a challenge for the public sector to find relevant expertise and then retain it on a long-term basis (Hassan & Lee, 2019).
- **Open Sources Software (DTI_{10}):** Open source software is a type of computer software in which the source code is released under a license that grants the copyright owner the rights to use, study, modify, and distribute the software to anyone and for any purpose. Open source software can be developed in a collaborative manner (Al Sulaimani, Ahmed Hamed Abdullah and Ozuem, 2022; European Commission, 2022b; Mujali Al-rawahna et al., 2018; The World Bank, 2022). Open source code help reap socio-economic benefits and foster citizen engagement and innovation while securing the transparency, accountability, and public scrutiny of governments' decisions and policy outcomes (OECD, 2022). Expanding open-source software in the public sector aims to save on IT expenses, reduce manufacturer dependency, and strengthen cybersecurity.
- **AI and Technological Innovations (DTI_{11}):** Governments can create new revenue streams, attract new business opportunities and investments, and increase the competitiveness of their economies globally by using AI technology. For example, AI tools developed for earthquakes, floods, and extreme weather conditions are an area that is rapidly finding response in the public sector for public health and safety. Technological innovation is an extended concept of innovation. A technological innovation is a new or better product or procedure with considerably different technological qualities than previous versions. Implemented technological product innovations are newly released products (product innovations) or processes in use (process

innovations). If technological innovations meet citizens' needs, they are easily adopted and are merely diffused in society (Hassan & Lee, 2019).

- **Technological Capabilities (DTI_{12}):** Technological capability has been defined as an organization's ability to build and develop new processes and products, upgrade information and skills about the physical world uniquely, and then turn that knowledge into instructions and designs to develop desired performance efficiently (Y. Wang et al., 2006). In addition to building sophisticated technological capabilities, "being digital" necessitates a mindset shift and the cultural capabilities that go along with it (William D. Eggers, Jason Manstof, Pankaj Kamleshkumar Kishnani, 2021).
- **Existence of Traditional Channels (DTI_{13}):** Traditional channels may affect the citizens' DG utilization since they prefer to use traditional channels based on their habits. Therefore, government activities on the web and DG business models may be less utilized than those delivered via traditional channels (European Commission, 2021; Vaccari et al., 2021). As technology investment increases, the government should also support using created and produced technologies to encourage new channels.

4.1.3 Digital Service Improvement

- **End-To-End Service Design (DSI_1):** The concept of End-to-End Service Design entails designing the user experience across all touchpoints from start to finish. This includes all user interactions with a service, from the initial contact to the final outcome and everything in between. It is crucial for delivering a seamless and satisfactory experience for the user. Designing end-to-end services around citizens' needs rather than the government's organizational structure increases demand for DG services (PwC, 2022). Government agencies that skillfully manage the end-to-end journey report higher levels of citizen satisfaction (Dudley et al., 2015).
- **User-friendly Service Design (DSI_2):** User-friendly service design considers all aspects of a customer journey from beginning to end. For DG services to succeed, citizens and other users must perceive them as valuable and easy to use. Therefore, user-friendly-service design is an essential (Gil-Garcia &

Flores-Zúñiga, 2020b; Ionescu et al., 2022; KPMG International, 2021).

- **Government as a Platform Approach (DSI_3):** Government as a Platform approach involves reconstructing the Central Government's IT infrastructure and architecture to create a central, cross-departmental digital platform. This strategy encourages improved interoperability between IT systems and their management departments. Government as a Platform approach enables the development of government services that are shareable, reusable, and interoperable, with reduced cost and faster turnaround time (William D. Eggers, Jason Manstof, Pankaj Kamleshkumar Kishnani, 2021). Institutionalization of this approach provides holistic and easy access to public services with a seamless interplay (European Commission, 2021; Idzi & Gomes, 2022; OECD, 2020).
- **Available Funding and Initiatives (DSI_4):** The funding and initiatives aim to provide seed funding for new projects, including activities, programs, and test projects. This factor indicates the availability of internal and external funds provided by various organizations (Elsheikh et al., 2022; Vaccari et al., 2021).
- **Integrated Partner Ecosystem (DSI_5):** A partner ecosystem is a network of organizations that offer complementary services within a specific industry. Developing DG platforms integrating services across various actors enhances the quality of the partner ecosystem. The partners in the ecosystem can be listed as private sector entities, critical infrastructure sectors, communities, non-governmental organizations (NGOs), local governments, individuals, families, and households (European Commission, 2021, 2022b; Ionescu et al., 2022; Tangi et al., 2021; The World Bank, 2022; Weerakkody et al., 2011). For example, in the event of a disaster, both public institutions and software-focused NGOs carry out important work supporting effective aid distribution through data analysis.
- **Digital Leadership Strategy (DSI_6):** Digital leadership is a type of management that focuses on implementing digital transformation within a business. It enables businesses to digitize their workplaces and learning cultures. Support from top management is often considered a necessary condition for transformation. The manager's role is to implement a series of

actions to change the organizing logic, starting from ensuring the need for change and clarifying the vision (Haneem et al., 2019; Tangi et al., 2021).

- **Risk Mitigation Activities (DSI_7):** The practice of lowering risk exposure and minimizing the chance of an incident is known as risk mitigation. Risk management and mitigation plans should be prepared to identify risks, assess their potential impact, and plan responses with appropriate technical and organizational measures. Based on the latest technological developments, those measures must ensure that the level of security is commensurate with the degree of risk. Business continuity, backup, and recovery plans should be used to put the procedures needed for functions and operations after a disastrous event and bring all functions back to normal in the earliest possible field (IDB, 2020).
- **Cost of Digital Systems (DSI_8):** The installation, operation, and maintenance of digital systems are considered the main components of the digital systems' cost (Mujali Al-rawahna et al., 2018).
- **Cost of Consulting (DSI_9):** Consulting fees are the fees charged by freelancers or consultants who supply government organizations with specialist knowledge and services. The training provided by the professionals and consultants constitutes the cost of the consulting (Mujali Al-rawahna et al., 2018).
- **Favorable Political Context (DSI_{10}):** Political factors may be classified as either external or internal, but for this research, the focus is on external issues, which tend to lie outside the scope and power of the organization. These include the government's political will and political participation in the policy-making sense, where political instability is often observed. The favorable political context describes the political scenario influencing digital transformation directly or indirectly. Changes in the favorable political context, strategies, and political coordination affect the DGT (Vaccari et al., 2021; Wilson & Mergel, 2022). Moreover, Ashaye & Irani (2019) demonstrated that political context will influence DGT.
- **Resistance to Change (DSI_{11}):** The refusal to adjust to new conditions or ways of doing things is referred to as resistance to change. It can happen to people, relationships, or institutions. Resistance to change coming from

employees within the organization acts as a barrier to the DGT (Ashaye & Irani, 2019; Mujali Al-rawahna et al., 2018; Tangi et al., 2021; Weerakkody et al., 2011).

- **Organizational Culture Change (DSI_{12}):** An organization's culture establishes the right way to conduct within the organization. This culture is made up of standard views and values that are developed by leaders and then conveyed and reinforced through various techniques, impacting employee perceptions, behaviors, and understanding. Public sector organizations are hierarchical, which is a structure that focuses on internal stability. However stable this structure may be, it doesn't help to create the right environment for wide-reaching, innovative change. Alongside this, public sector organizations are up against much external pressure, so are less likely to take risks (GovNet, 2023; William D. Eggers, Jason Manstof, Pankaj Kamleshkumar Kishnani, 2021).
- **Legislation and Regulation Change (DSI_{13}):** Legislation and regulation are two distinct concepts with a clear division: while legislation establishes the principles of public policy, regulation puts these principles into action, bringing legislation into practice. The legal environment facilitates the DGT. Developing countries require an appropriate legal framework to provide the necessary legislation for the DGT and its adoption in the public sector. Moreover, the quality of the regulatory framework also matters for the advancement and sophistication of the DG services (Hassan & Lee, 2019).
- **Good Governance (DSI_{14}):** Governance is making and implementing decisions within an organization or society. It is the process of interaction that occurs through laws, social norms, power, or language structured in the communication of an organized society on a social system. In other words, governance refers to the process through which decisions are made and implemented, especially by public institutions at the national and local levels. Good governance describes a decision-making system based on these principles: transparency, responsibility, accountability, participation, and responsiveness to the needs of the people. Citizen participation, coordination, communication, and monitoring are the key elements of a thriving governance system (Action Aid, 2023; EIF, 2017; Makki & Alqahtani, 2022).

4.2 Hesitant Fuzzy Linguistic Fuzzy Cognitive Map (HFLCM) Approach

The proposed HFLCM approach improves the CM approach by applying HFSs operations. HFLCM utilizes the HFLTS so that experts can easily and freely express their hesitant and uncertain judgments on the relationships between the factors. HFLCM is more realistic and flexible than traditional fuzzy cognitive maps because of its ability to reflect experts' knowledge and experiences expressed by hesitant linguistic values. The steps of the proposed approach are as follows:

Step 1: The concepts are defined based on literature review, industry reports, and DMs' views.

Step 2: The interactions between concepts are determined, and their strengths are indicated by DMs. Each factor is evaluated by DMs by using "*Lower than* s_i", *"Greater than* s_i*", "At least* s_i*", "At most* s_i*", "Between* s_i *and* s_j*"* and the linguistic terms listed in Table 4.1.

Table 4.1: Linguistic scale for HFLCM (Beg & Rashid, 2013)

Linguistic term	Fuzzy Numbers
Perfect (P)	(0.83,1,1)
Very Good (VG)	(0.67,0.83,1)
Good (G)	(0.5,0.67,0.83)
Medium (M)	(0.33,0.5,0.67)
Bad (B)	(0.17,0.33,0.5)
Very Bad (VB)	(0,0.17,0.33)
None (N)	(0,0,0.17)

Step 3: The linguistic evaluations are transformed into HFLTS by using the E_{GH} given in Definition 3.6.

Step 4: The fuzzy envelope for HFLTS is built with the aid of the the Ordered Weight Averaging (OWA) operator (Liu & Rodríguez, 2014). This aggregation procedure results in a trapezoidal fuzzy number.

Definition 4.1: $A = \{a_1, a_2, \ldots, a_n\}$ is a set of elements that will be aggregated. Here, F, the OWA operator can be defined as (Liu & Rodríguez, 2014):

$$F(a_1, a_2, \ldots, a_n) = wb^T = \sum_{i=1}^{n} w_i b_i, \quad (4.1)$$

where $w = (w_1, w_2, \ldots, w_n)^T$ is a weighting vector, with $w_i \in [0, 1]$ and $\sum_{i=1}^{n} w_i = 1$ and b being the associated ordered value vector, and $b_i \in b$ is the i^{th} biggest value in A.

Definition 4.2 (Liu & Rodríguez, 2014)**:** For the expression *"At least s_i",* the factors of the trapezoidal fuzzy membership function, denoted by $A = (\alpha,\beta,\gamma,\delta)$, is computed as:

$$\alpha = \min \{a_L^i, a_M^i, a_M^{i+1}, \ldots, a_M^g, a_R^g\} = a_L^i \quad (4.2)$$

$$\delta = \max \{a_L^i, a_M^i, a_M^{i+1}, \ldots, a_M^g, a_R^g\} = a_R^g \quad (4.3)$$

$$\beta = OWA_{w^2}\left(a_M^i, a_M^{i+1} \ldots, a_M^g\right) \quad (4.4)$$

$$\gamma = a_M^g \quad (4.5)$$

Here, the OWA operation requires a weight vector that consists of the 2nd types of weights between [0,1]. The 2nd type of weights $W^2 = (w_1^2, w_2^2, \ldots, w_{g-i+1}^2)^T$ is defined as:

$$w_1^2 = \alpha_1^{g-i}, w_2^2 = (1-\alpha)\,\alpha^{g-i-1}, \ldots, w_{g-i+1}^2 = 1-\alpha \quad (4.6)$$

where $\alpha = g/i$, and g is the number of elements in the evaluation scale, and i is the rank of the lowest evaluation value within its defined interval.

Definition 4.3 (Liu & Rodríguez, 2014)**:** For the expression *"At most s_i"*, the factors of the trapezoidal fuzzy membership function, denoted by $A = (\alpha,\beta,\gamma,\delta)$, is computed as:

$$\alpha = \min \{a_L^0, a_M^0, a_M^1, \ldots, a_M^i, a_R^i\} = a_L^0 \quad (4.7)$$

$$\delta = \max \{a_L^0, a_M^0, a_M^1, \ldots, a_M^i, a_R^i\} = a_R^i \quad (4.8)$$

$$\beta = a_M^0 \tag{4.9}$$

$$\gamma = OWA_{w^1}\left(a_M^0, a_M^1 \ldots, a_M^i\right) \tag{4.10}$$

Here again, the OWA operation requires a weight vector that consists of the 1st types of weights between [0,1]. The 1st type of weights $W^1 = (w_1^1, w_2^1, \ldots, w_{i+1}^1)^T$ is defined as:

$$w_1^1 = \alpha,\ w_2^1 = (1-\alpha)\,\alpha, \ldots,\ w_{i+1}^1 = (1-\alpha)^i \tag{4.11}$$

where $\alpha = i/g$, and g is the number of elements in the evaluation scale, and i is the rank of the highest evaluation value within its defined interval.

Definition 4.4 (Liu & Rodríguez, 2014)**:** For the expression *"Between s_i and s_j"*, the factors of the trapezoidal fuzzy membership function, denoted by $A = (\alpha,\beta,\gamma,\delta)$, is computed as:

$$\alpha = \min\left\{a_L^i, a_M^i, a_M^{i+1}, \ldots, a_M^j, a_R^j\right\} = a_L^i \tag{4.12}$$

$$\delta = \max\left\{a_L^i, a_M^i, a_M^{i+1}, \ldots, a_M^j, a_R^j\right\} = a_R^i \tag{4.13}$$

$$\beta = \begin{cases} a_M^i & \text{if } i+1=j \\ OWA_{w^2}\left(a_M^i, \ldots, a_M^{\frac{i+j}{2}}\right) & \text{if } i+j \text{ is even} \\ OWA_{w^2}\left(a_M^i, \ldots, a_M^{\frac{i+j-1}{2}}\right) & \text{if } i+j \text{ is odd} \end{cases} \tag{4.14}$$

$$\gamma = \begin{cases} a_M^{i+1} & \text{if } i+1=j \\ OWA_{w^1}\left(a_M^j, a_M^{j-1}, \ldots, a_M^{\frac{i+j}{2}}\right) & \text{if } i+j \text{ is even} \\ OWA_{w^1}\left(a_M^j, a_M^{j-1}, \ldots, a_M^{\frac{i+j+1}{2}}\right) & \text{if } i+j \text{ is odd} \end{cases} \tag{4.15}$$

In this case, the OWA operation requires two types of weight vector. For this reason, the 1st and 2nd types of weights between [0,1] must be described.

If $i+j$ is odd, then the 1st type of weights $W^1 = (w_1^1, w_2^1, \ldots, w_{(j-i+1)/2}^1)^T$ is defined as:

$$w_1^1 = \alpha_2,\ w_2^1 = \alpha_2(1-\alpha_2),\ \ldots,\ w_{(j-i+1)/2}^1 = \alpha_2(1-\alpha_2)^{(j-i-1)/2} \tag{4.16}$$

The 2nd type of weights $W^2 = (w_1^2, w_2^2, \ldots, w_{(j-i+1)/2}^2)^T$ is defined as:

$$w_1^2 = \alpha_1^{(j-i-1)/2},\ w_2^2 = (1-\alpha_1)\,\alpha_1^{(j-i-3)/2},\ldots,\ w_{(j-i-1)/2}^2 = 1-\alpha_1 \tag{4.17}$$

If $i+j$ is even, then the 1st type of weights $W^1 = (w_1^1, w_2^1, \ldots, w_{(j-i+2)/2}^1)^T$ is defined as:

$$w_1^1 = \alpha_2,\ w_2^1 = \alpha_2(1-\alpha_2),\ \ldots,\ w_{(j-i+2)/2}^1 = \alpha_2(1-\alpha_2)^{j-i/2} \tag{4.18}$$

The 2nd type of weights $W^2 = (w_1^2, w_2^2, \ldots, w_{(j-i+2)/2}^2)^T$ is defined as:

$$w_1^2 = \alpha_1^{j-i/2},\ w_2^2 = (1-\alpha_1)\,\alpha_1^{(j-i-2)/2},\ldots,\ w_{(j-i+2)/2}^2 = 1-\alpha_1 \tag{4.19}$$

where $\alpha_1 = \frac{g-(j-i)}{g-1}$, $\alpha_2 = \frac{(j-i)-1}{g-1}$, g is the number of elements, j is the rank of the highest evaluation, and i is the rank of the lowest evaluation value within its defined interval.

Step 5: The assessments of DMs are aggregated with Hesitant Fuzzy Linguistic Weighting Averaging Operator (HFLWA). A collective $H_c = (h_{ij,c})_{nxn}$ can be derived from individual judgments by using:

$$h_{ij,c}^{\sigma(s)} = \sum_{t=1}^{m} \lambda_t\, \bar{h}_{ij,t}^{\sigma(s)}\ (i,j = 1,2,\ldots,n,\ s = 1,2,\ldots,l) \tag{4.20}$$

where λ_t is the weights of DMs.

Step 6: Trapezoidal fuzzy membership functions are transformed within the [−1, 1] interval by centroid of area defuzzification method (Shemshadi et al., 2011), and adjacency matrix of the concepts is accepted as a weight matrix (*W*) of the HFLCM.

$$\text{Defuzz(Xij)} = \int \frac{\mu(x).\,x\,dx}{\mu(x).\,dx} = \frac{\int_{x_{ij1}}^{x_{ij2}} \left(\frac{x-x_{ij1}}{x_{ij2}-x_{ij1}}\right).\,x\,dx + \int_{x_{ij2}}^{x_{ij3}} x\,dx + \int_{x_{ij3}}^{x_{ij4}} \left(\frac{x_{ij4}-x}{x_{ij4}-x_{ij3}}\right).\,x\,dx}{\int_{x_{ij1}}^{x_{ij2}} \left(\frac{x-x_{ij1}}{x_{ij2}-x_{ij1}}\right) dx + \int_{x_{ij2}}^{x_{ij3}} dx + \int_{x_{ij3}}^{x_{ij4}} \left(\frac{x_{ij4}-x}{x_{ij4}-x_{ij3}}\right) dx} =$$

$$\frac{-x_{ij1}x_{ij2}+x_{ij3}x_{ij4}+\frac{1}{3}(x_{ij4}-x_{ij3})^2-\frac{1}{3}(x_{ij2}-x_{ij1})^2}{-x_{ij1}-x_{ij2}+x_{ij3}+x_{ij4}} \qquad (4.21)$$

Step 7: Initial state vector of the concepts and iterate in the activation function for each time step.

4.3 Modeling of DGT Framework with HFLCM Approach

The proposed approach models the success and risk factors of the DGT framework in three consecutive steps. DMs evaluated the interactions between concepts under three sub-systems. The flowchart of the proposed approach is provided in Figure 4.4.

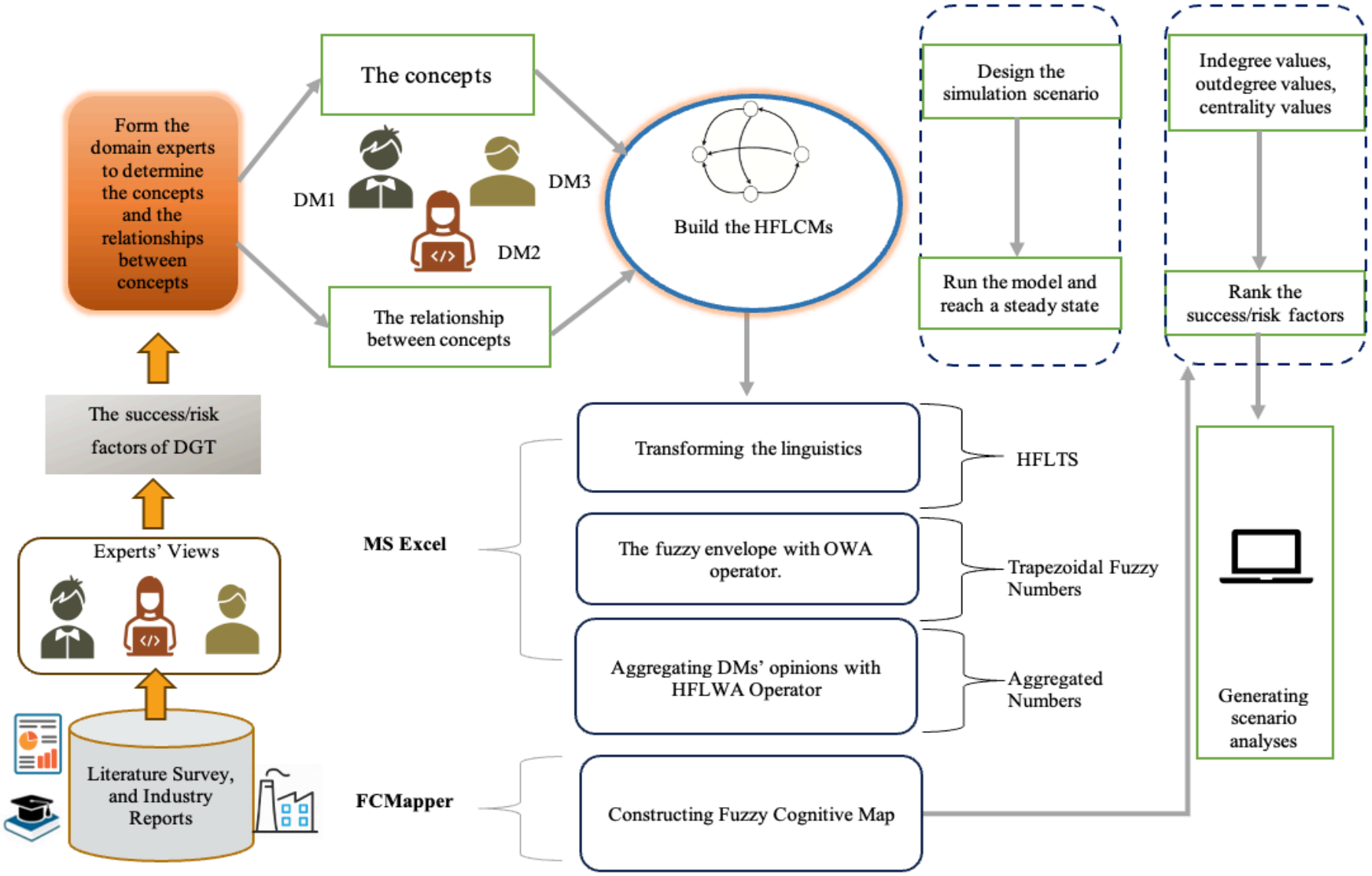

Figure 4.4: The flowchart of the proposed approach

In the first step, the HFLTS operations are conducted in MS Excel. Secondly, FCMapper modeling software is utilized for mathematical operations. Thirdly, Mental Modeler modeling software is used to visualize the HFLCM graphs, and FCMapper is used to conduct the scenarios.

The first expert is an academician at a public university who completed his undergraduate and graduate education in industrial engineering departments of universities, has realized many projects about digital transformation in the public and private sectors, and has worked in advisory boards of a public university. The second expert is a cybersecurity specialist, founder, and chairman of a cybersecurity R&D company, who completed his undergraduate and graduate education in engineering departments of universities, has an information security and risk management background, has realized many projects on cybersecurity in the public and private sectors, and has worked on the advisory boards of public institutions. Also the second expert is a digital citizen of Estonia. The third expert is a big data engineer in a company operating in Türkiye, has an industrial engineering and computer engineering background, has realized various data, machine learning, and artificial intelligence projects, and has deep technical knowledge of IT strategies.

Three DMs have defined fourteen concepts for the Digital Citizenship Improvement sub-system, thirteen for the Digital Technology Improvement sub-system, and fourteen for the Digital Service Improvement sub-system. The sub-systems have inter-causal interactions and intra-causal interactions. The sub-systems influence the whole system by interacting with Digital Citizenship Improvement, Digital Technology Improvement, and Digital Service Improvement. Arrows from one concept to another represent the relationship among concepts. The "+" sign displays the positive interactions between concepts, whereas the "-" sign displays the negative interactions between concepts. The graphical illustration of these interactions is illustrated in Figure 4.5.

The three experts' evaluations are provided in Appendix A, Table A.1, Table A.2, and Table A.3. DMs' judgments are gathered in linguistic terms and then transformed into HFLTSs. The fuzzy envelope with the OWA operator is applied to obtain trapezoidal fuzzy numbers. The judgments of the three DMs are aggregated by using the HFLWA operator to describe the influence of concepts. The importance degrees of DMs are

determined as 0.35, 0.35, and 0.30, respectively. Trapezoidal fuzzy membership functions are transformed within the [−1, 1] interval by the centroid of area defuzzification method, and the adjacency matrix of the concepts is accepted as a weight matrix (W) of the HFLCM. The adjacency matrix is provided in Table A.4.

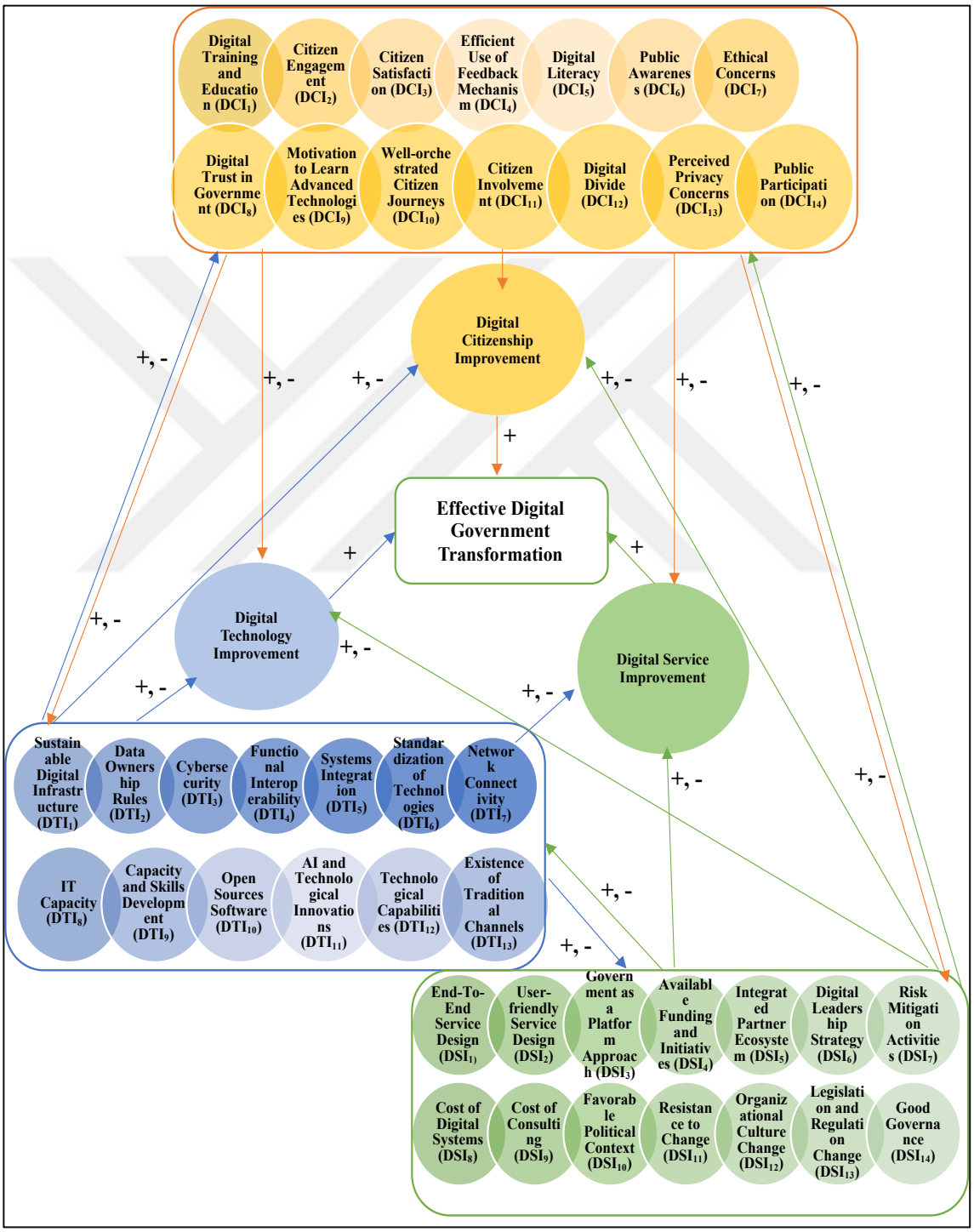

Figure 4.5: The graphical illustration of the DGT cognitive map

Figure 4.6, Figure 4.7, and Figure 4.8 present graphically the interactions among the concepts of sub-systems. The graphical representation of the interactions between all factors is provided in Figure 4.9. Blue lines represent a positive causal relationship, and red lines signify a negative relationship between concepts.

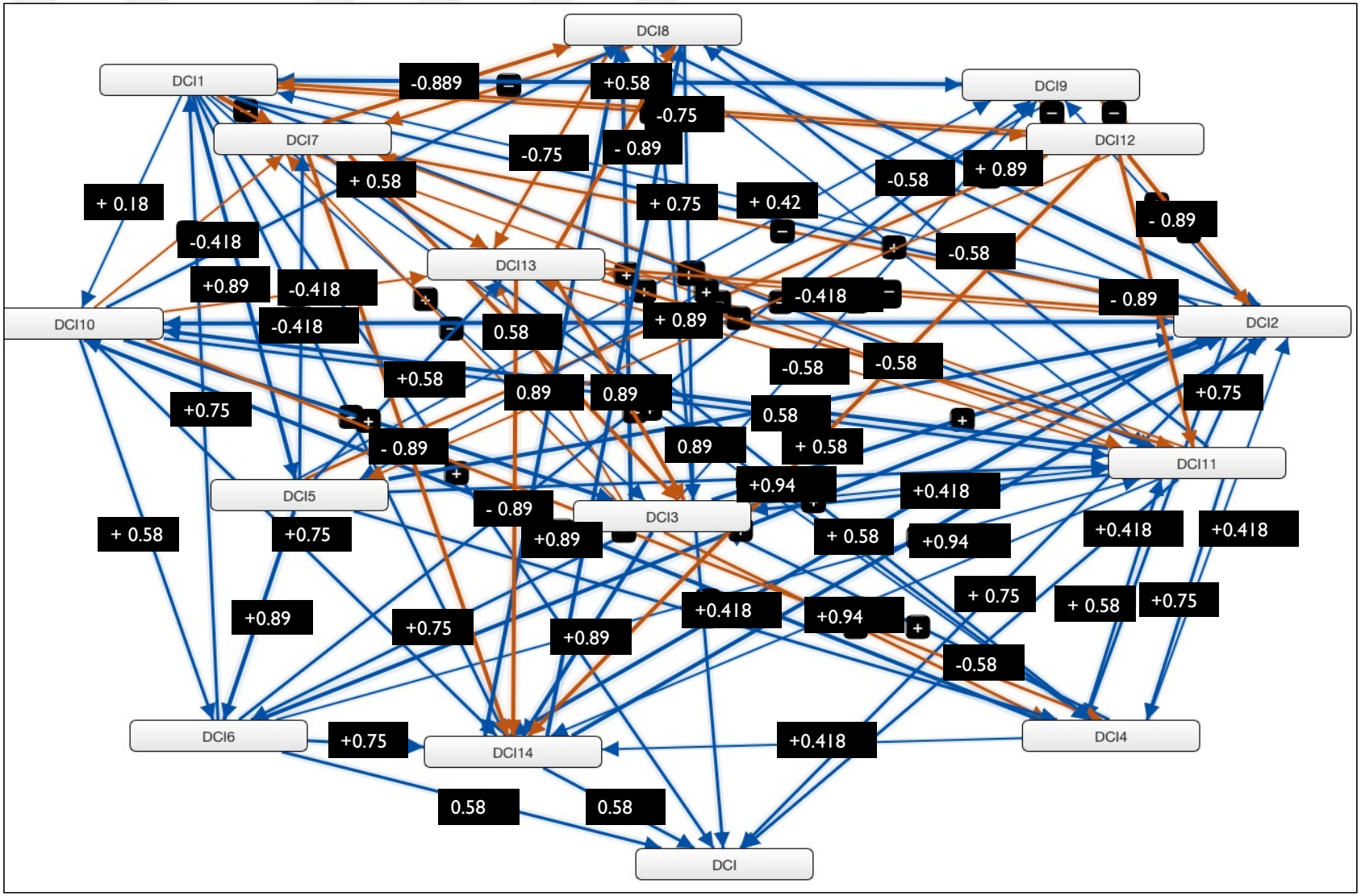

Figure 4.6: The cognitive map of digital citizenship improvement

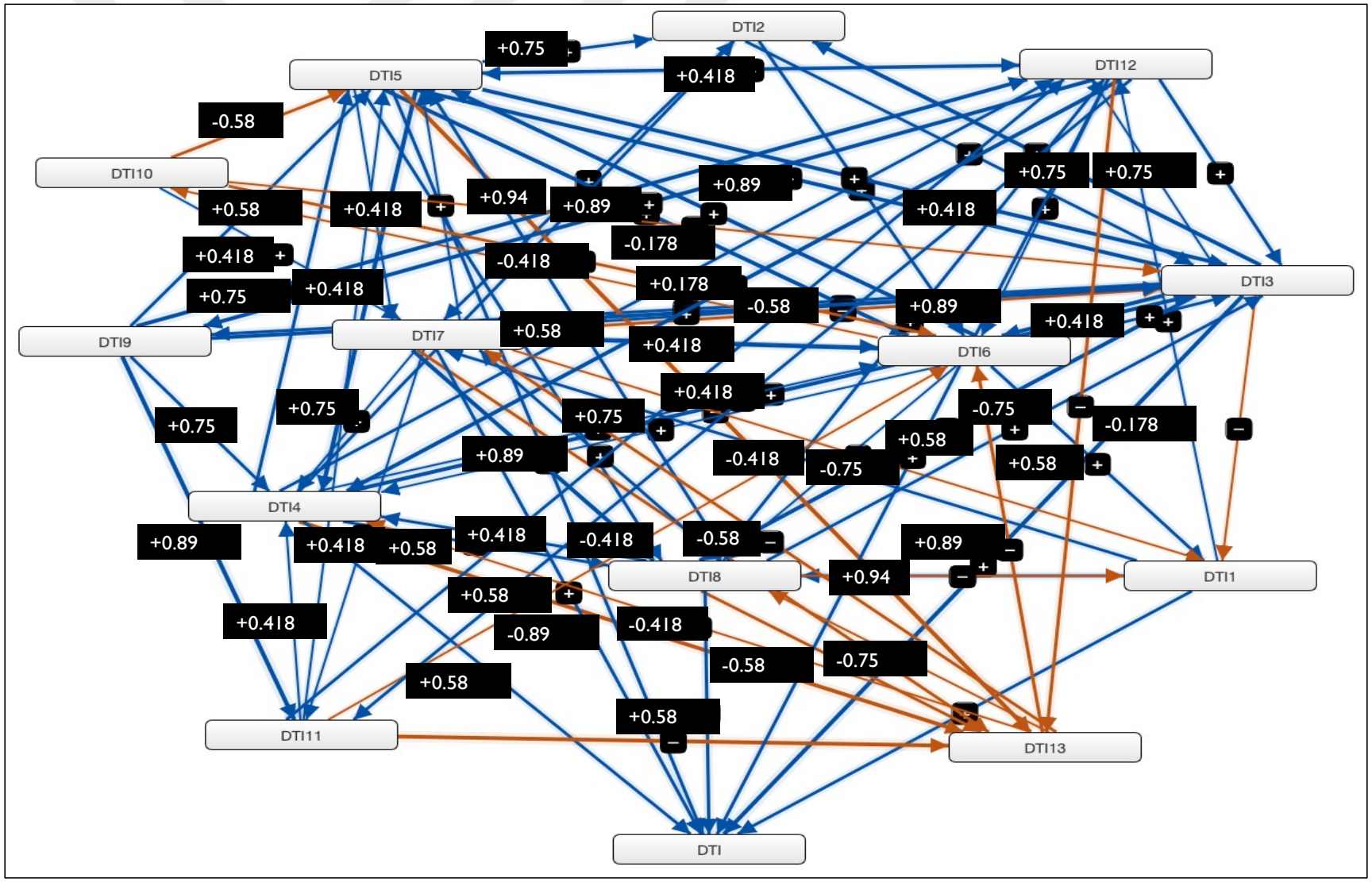

Figure 4.7: The cognitive map of digital technology improvement

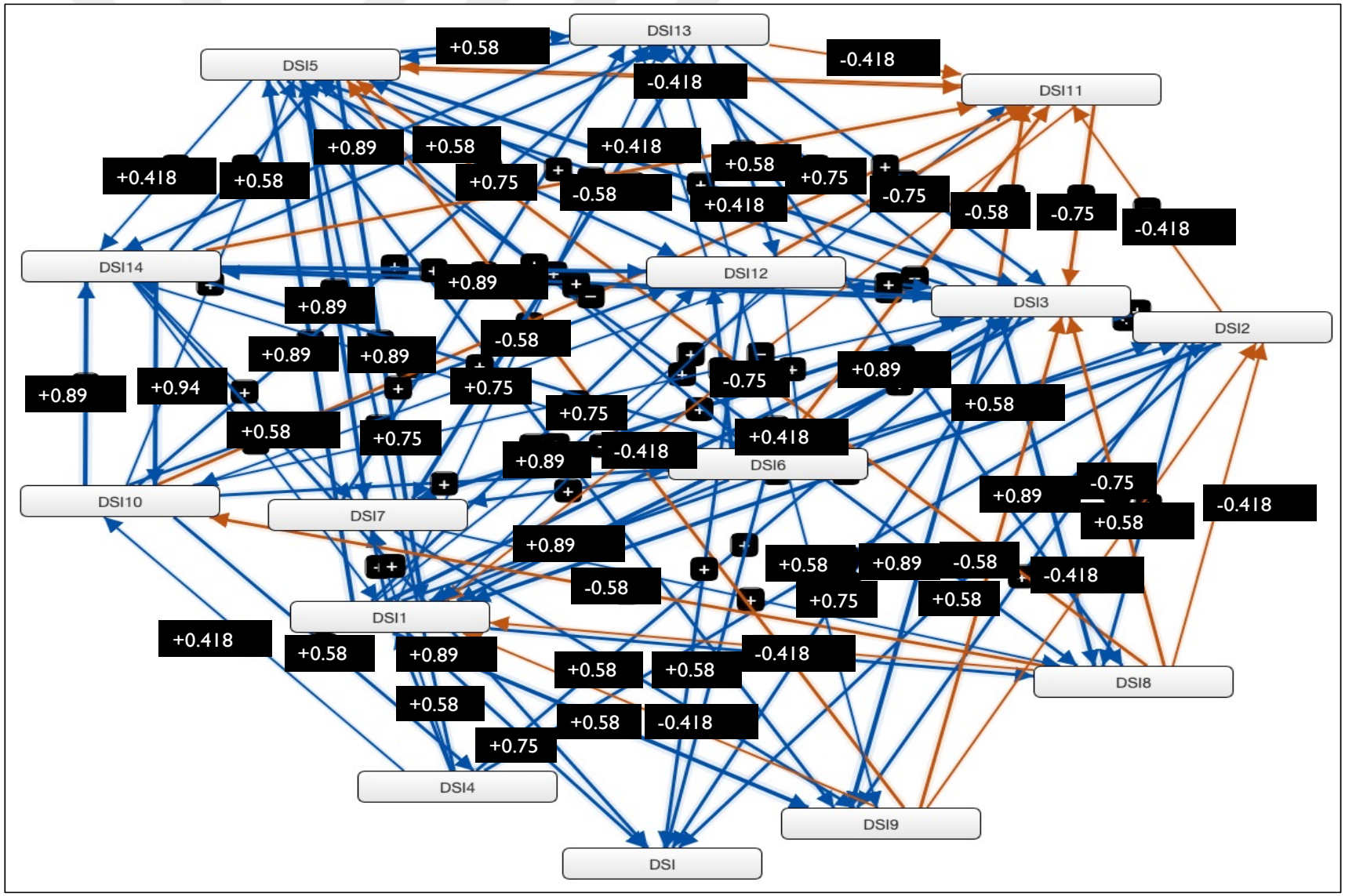

Figure 4.8: The cognitive map of digital service improvement

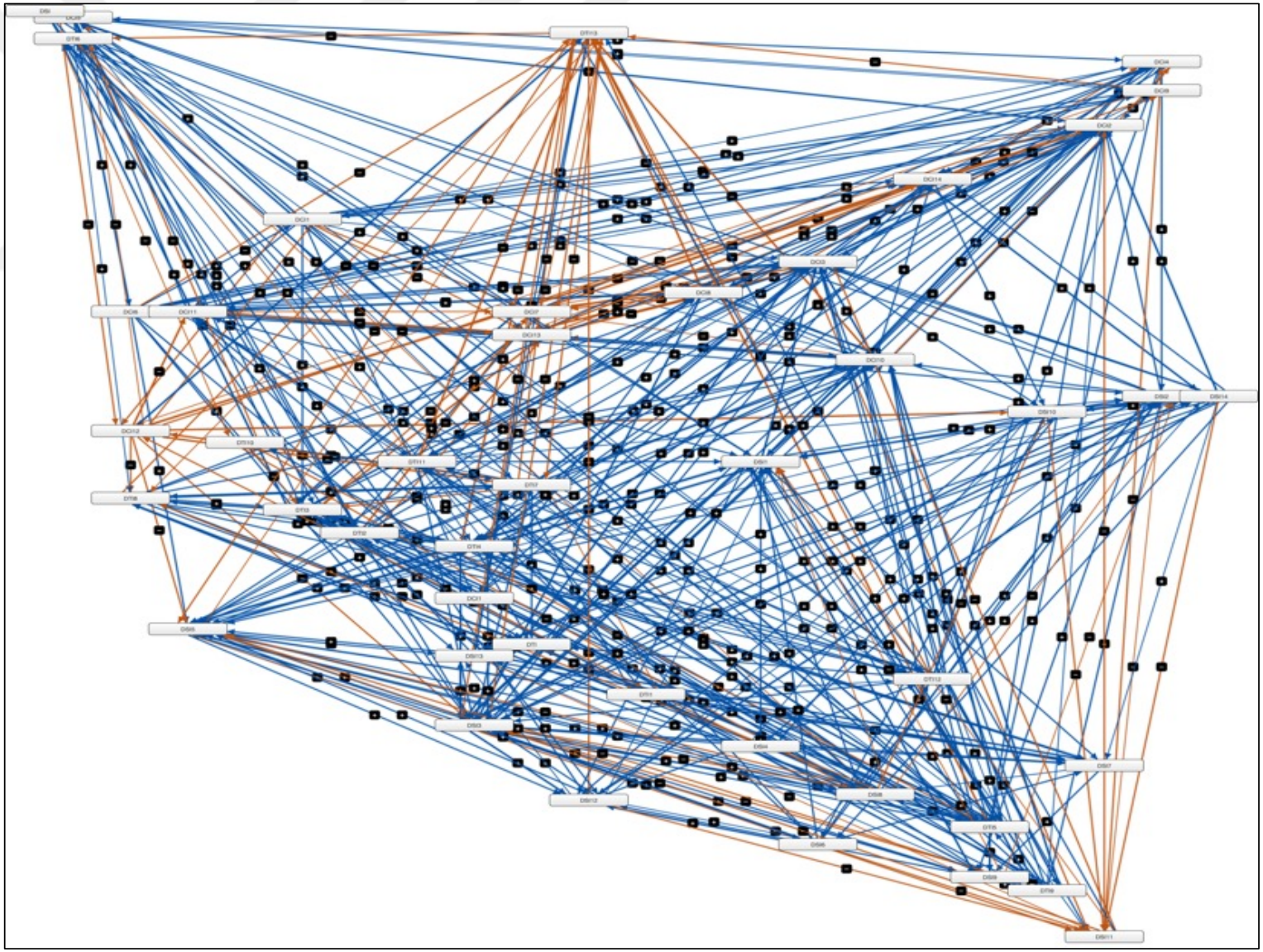

Figure 4.9: The cognitive map of the DGT

To find the solution, the overall matrix is utilized in the FCMapper software. The simulation process is completed after 25 iterations, at which point all factors stabilize and converge to a fixed point. Figure 4.10 provides the number of iterations needed to reach a steady state.

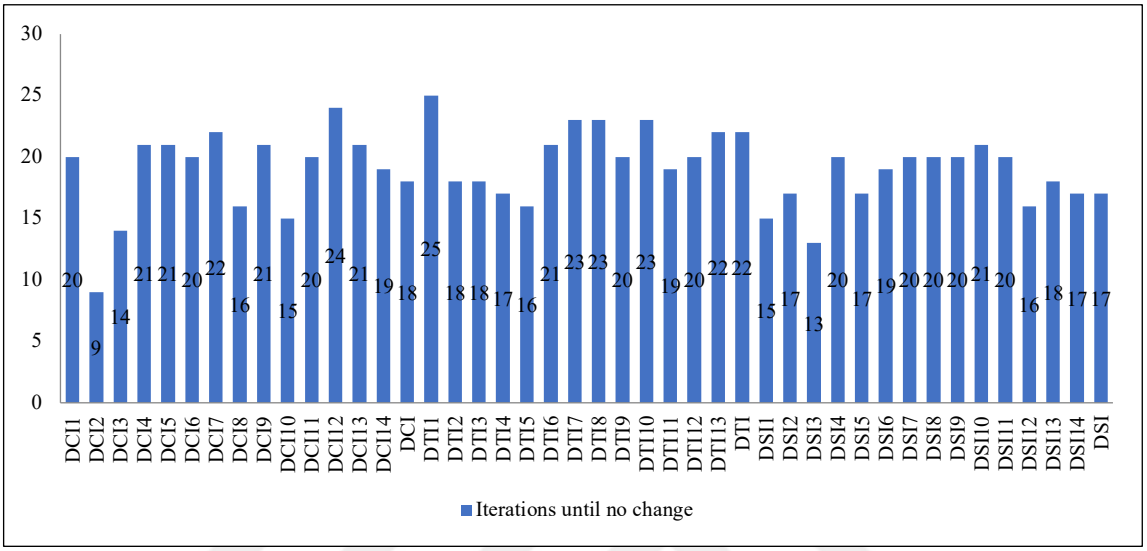

Figure 4.10: Number of iterations until no change

The sigmoid function is a threshold function, limiting the function values to the interval [0,1]. The indices of the HFLCM can be computed accordingly. The model comprises 44 concepts and 445 connections. The density index is calculated as 0.230. There is no transmitter concept; there are three receiver concepts and 41 ordinary concepts. The indegree value, outdegree value and the centrality value of a concept can be summarized as:

- An indegree value of a node determines the node's stability or influence in the final state. A node with a high indegree value is one that is heavily influenced by other nodes and is more dependent on them.
- A node with a high outdegree value is one that has a large number of outputs, influences other nodes, and is less dependent on others to keep its state. Concepts having a high outdegree value are more likely to change their states.
- The sum of outdegree and indegree values yields the total degree value known as centrality. Moreover, a node's centrality value can be used to determine its relative importance.

The result of the simulation including the concepts' indegree, outdegree, centrality values, their ranking, and their number of iterations are listed in Table 4.2.

Table 4.2: The result of the simulation

Concepts	Outdegree	Indegree	Centrality	Iterations until no change	Rank (Centrality)	Rank (Outdegree)	Rank (Indegree)	Type
DCI1	8.81	2.81	11.62	20	25	14	38	Ordinary
DCI2	5.54	18.58	24.12	9	2	28	2	Ordinary
DCI3	7.71	14.94	22.65	14	8	16	3	Ordinary
DCI4	6.14	6.16	12.30	21	24	26	21	Ordinary
DCI5	6.94	1.73	8.67	21	37	20	40	Ordinary
DCI6	6.86	2.22	9.08	20	35	21	39	Ordinary
DCI7	6.64	4.74	11.37	22	27	22	28	Ordinary
DCI8	7.97	6.94	14.91	16	14	15	17	Ordinary
DCI9	2.31	2.93	5.24	21	39	40	37	Ordinary
DCI10	12.11	11.90	24.01	15	3	4	5	Ordinary
DCI11	9.97	6.48	16.45	20	12	10	19	Ordinary
DCI12	9.50	3.11	12.61	24	23	12	36	Ordinary
DCI13	7.55	5.39	12.95	21	21	18	26	Ordinary
DCI14	4.80	9.81	14.61	19	15	30	11	Ordinary
DCI	0.00	3.83	3.83	18	43	42	34	Receiver
DTI1	4.52	1.60	6.12	25	38	33	42	Ordinary
DTI2	5.19	4.47	9.66	18	33	29	31	Ordinary
DTI3	12.87	10.84	23.71	18	4	3	8	Ordinary
DTI4	11.73	9.39	21.12	17	9	5	12	Ordinary
DTI5	12.92	9.89	22.80	16	7	1	10	Ordinary
DTI6	6.03	5.54	11.57	21	26	27	25	Ordinary
DTI7	11.36	5.55	16.92	23	11	6	24	Ordinary
DTI8	7.69	5.86	13.55	23	17	17	23	Ordinary
DTI9	9.64	3.55	13.19	20	19	11	35	Ordinary
DTI10	2.34	1.00	3.34	23	44	39	43	Ordinary
DTI11	6.39	4.72	11.11	19	28	24	29	Ordinary
DTI12	10.92	7.36	18.28	20	10	8	15	Ordinary
DTI13	4.50	11.66	16.16	22	13	34	7	Ordinary
DTI	0.00	4.60	4.60	22	40	42	30	Receiver
DSI1	11.28	11.79	23.07	15	5	7	6	Ordinary
DSI2	6.36	7.07	13.43	17	18	25	16	Ordinary
DSI3	12.91	19.64	32.55	13	1	2	1	Ordinary
DSI4	3.91	0.58	4.50	20	41	37	44	Ordinary
DSI5	10.14	12.86	23.00	17	6	9	4	Ordinary
DSI6	7.02	1.68	8.70	19	36	19	41	Ordinary
DSI7	1.58	7.56	9.14	20	34	41	14	Ordinary
DSI8	4.08	9.91	14.00	20	16	36	9	Ordinary
DSI9	2.58	7.97	10.55	20	30	38	13	Ordinary
DSI10	4.80	5.09	9.90	21	32	31	27	Ordinary
DSI11	4.42	5.91	10.33	20	31	35	22	Ordinary
DSI12	4.54	6.50	11.04	16	29	32	18	Ordinary
DSI13	6.61	6.16	12.77	18	22	23	20	Ordinary
DSI14	9.05	3.95	13.00	17	20	13	33	Ordinary
DSI	0.00	4.00	4.00	17	42	42	32	Receiver

The centrality values, indegree values, and outdegree values of the concepts are provided in Figure 4.11, Figure 4.12, and Figure 4.13, respectively.

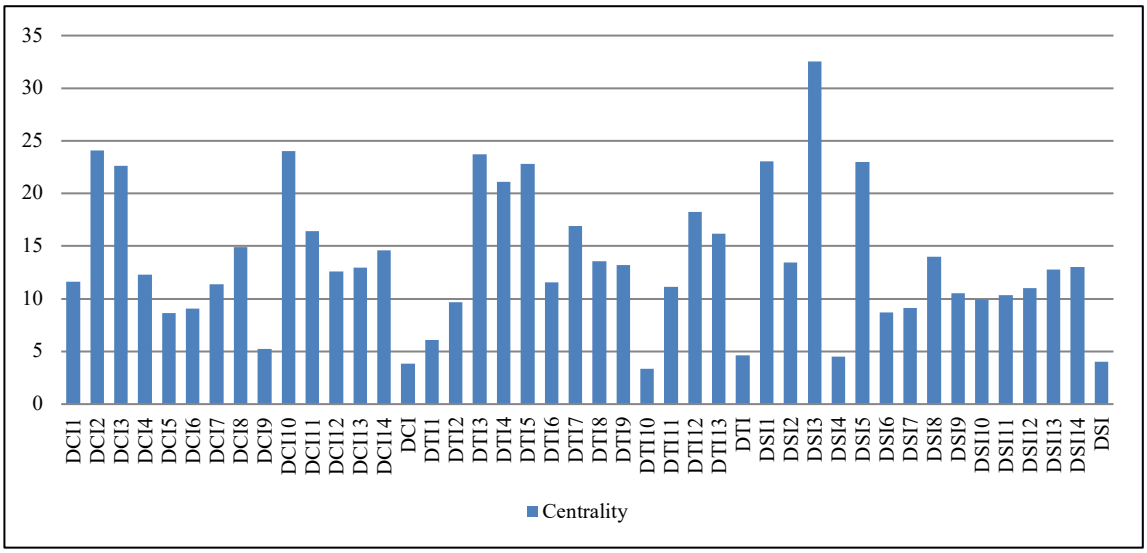

Figure 4.11: The centrality values of the concepts

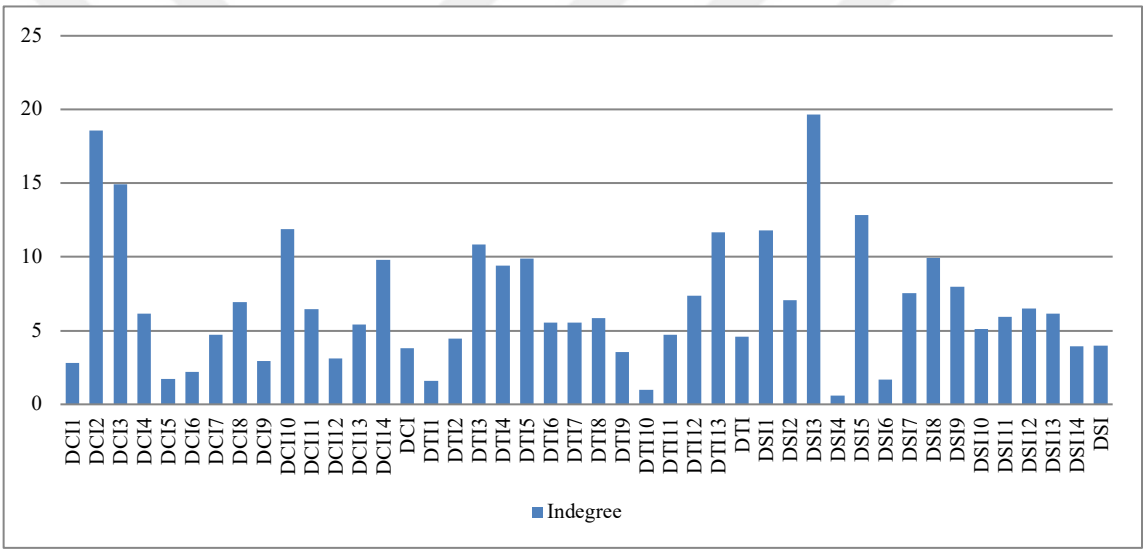

Figure 4.12: The indegree values of the concepts

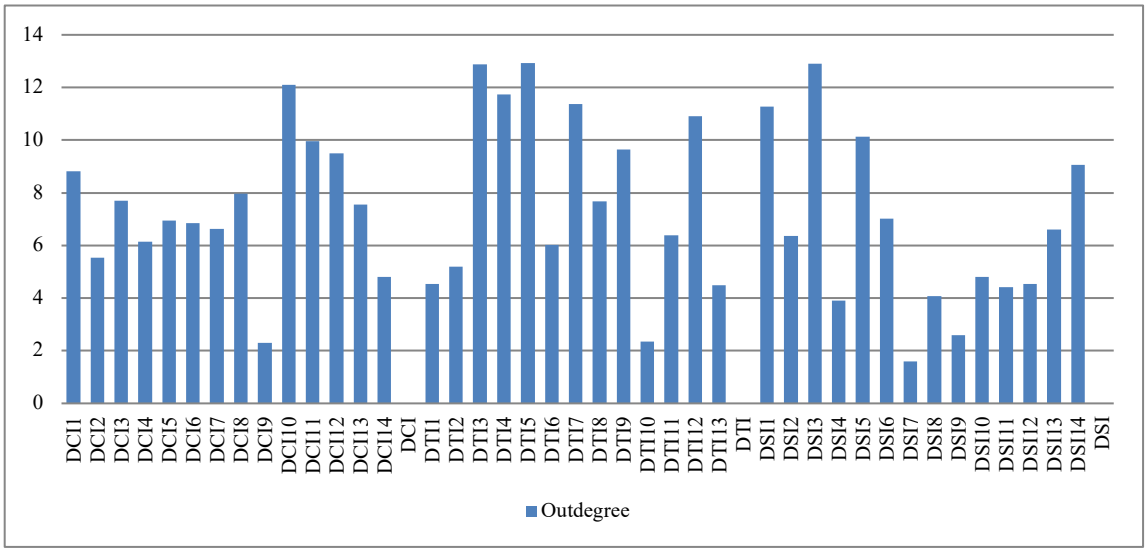

Figure 4.13: The outdegree values of the concepts

The concept with a higher centrality score denotes a critical concept in the DGT model. These nodes significantly impact other nodes and the overall system and can drive changes in the state of other nodes.

- For Digital Citizenship Improvement, Citizen Engagement (DCI2), whose centrality value is 24.12; Well-Orchestrated Citizen Journeys (DCI10), whose centrality value is 24.01; and Citizen Satisfaction (DCI3), whose centrality value is 22.65, are the most critical factors.
- For Digital Technology Improvement, Cybersecurity (DTI3), whose centrality value is 23.71; Systems Integration (DTI5), whose centrality value is 22.80; and Functional Interoperability (DTI4), whose centrality value is 21.12, are the most critical factors.
- For Digital Service Improvement, Government as a Platform Approach (DSI3), whose centrality value is 32.55; End-To-End Service Design (DSI1), whose centrality value is 23.07; and Integrated Partner Ecosystem (DSI5), whose centrality value is 23.00, are the most critical factors.

4.4 Scenario Analysis

Scenario analysis is performed to analyze the behavior of the cognitive map under the dynamic environment. The impacts of interactions between concepts are examined by utilizing what-if scenarios. Different scenarios are conducted under various what-if scenarios to observe the system's attitude. Six scenarios are built to investigate the DGT system's behavior according to the changes in the selected concepts. The sigmoid function in the FCMapper software is used to generate these scenarios. The results are provided in Table A.11. These scenarios are summarized in the following section.

- **Scenario 1: The Lowest Technology Investment Approach**

The cost of technology investment in governments and digital public services is a multifaceted consideration that encompasses various elements, from infrastructure development to ongoing maintenance and security measures. Governments need to carefully plan and budget for these factors to ensure the successful implementation and sustainability of digital initiatives. Therefore, first scenario is generated based on the lowest value of the concepts in digital technology improvement. The concepts' values of success factors (i.e., DTI1, DTI2, DTI3, DTI4, DTI5, DTI6, DTI7, DTI8, DTI9, DTI10,

DTI11, DTI12) are modified to -1. In contrast, the concept value of risk factor (i.e., DTI13) is modified to 1 to simulate how the DGT system responds to changes in these factors. The result of this scenario is depicted in Figure 4.14.

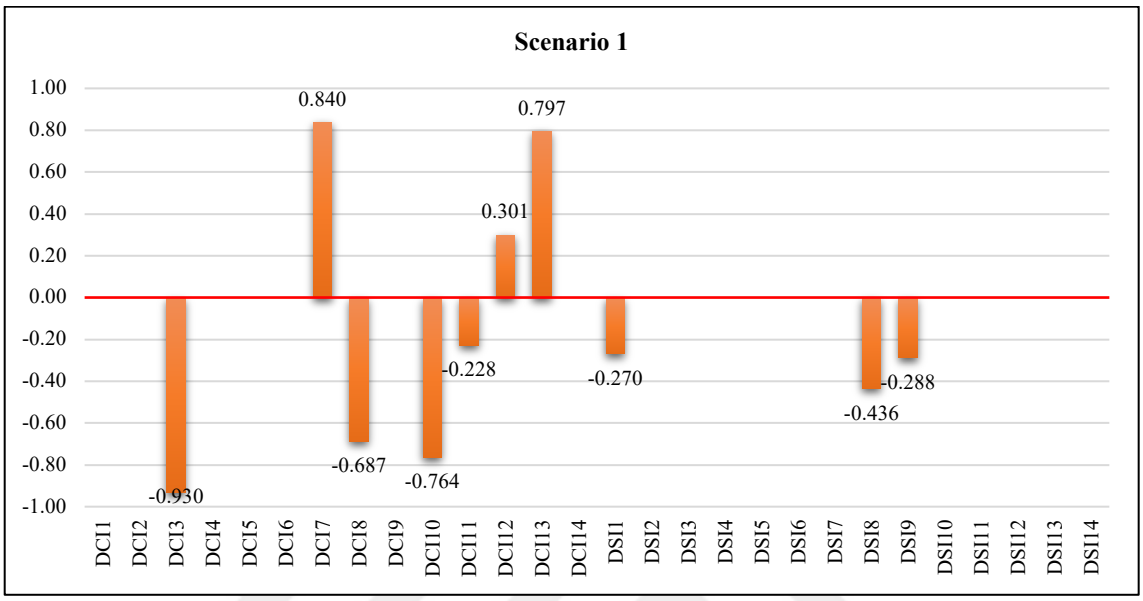

Figure 4.14: The result of the first scenario

The results show that the absence of technology investment decreases by 93% the "citizen satisfaction." "Well-orchestrated citizen journeys" and "citizen involvement" are negatively affected in this scenario, with a decrease of approximately 76% and 22%. The infrastructure is fundamental, implying citizen engagement, inclusiveness, leadership, citizen involvement, community vision, diversity, and networking (Oe et al., 2016). "Ethical concerns" and "perceived privacy concerns" increased by 84% and approximately 80%, whereas "digital trust in government" decreased by approximately 69%. If the public trust is supported by the digital technologies supplied by public institutions, the DG policy can spread (Y. Zhang et al., 2022). The "Digital divide" is increased by 30% in this scenario since the digital skill development of citizens relies on technological investments. The accessibility level of public service can be improved by increasing the penetration level of broadband to develop citizens' digital skills and decrease the digital gap between citizens (Choi et al., 2018).

The "end-to-end service design" is negatively affected in from the lowest technology investment by a decrease of 27%. Increasing technological operability and ensuring

service quality can be measured and supervised is also beneficial to DG service design. With a high level of functional interoperability, public institutions provide services more professionally so that DG services can be diffused (Zhang et al., 2022). The rapidity and effectiveness of public service delivery can be improved by enhancing end-to-end service design, and the number of digital services by increasing the penetration rate of broadband and network connectivity (Choi et al., 2018). In this scenario, the "cost of digital systems" and "cost of consulting" are decreased of approximately 44% and 29%. Nevertheless, the procurement of digital technology products offers digital services by public institutions and organizations in a cost-effective manner (OECD, 2023). Therefore, low technology investment may be seen decreasing the costs in the short-term, but in the long-term this situation changes.

- **Scenario 2: The Worst Citizen-Centric Approach**

Implementing a citizen-centric approach in DG efforts involves putting citizens at the center of service design, delivery, and interaction. The second scenario is generated based on the lowest value of the concepts in digital citizenship improvement. The concepts' values of success factors (i.e., DCI1, DCI2, DCI3, DCI4, DCI5, DCI6, DCI8, DCI9, DCI10, DCI11, DCI14) are modified to -1. In contrast, the concepts' values of risk factors (i.e., DCI7, DCI12, DCI13) are modified to 1 to simulate how the DGT system responds to changes in these factors. The result of this scenario is depicted in Figure 4.15.

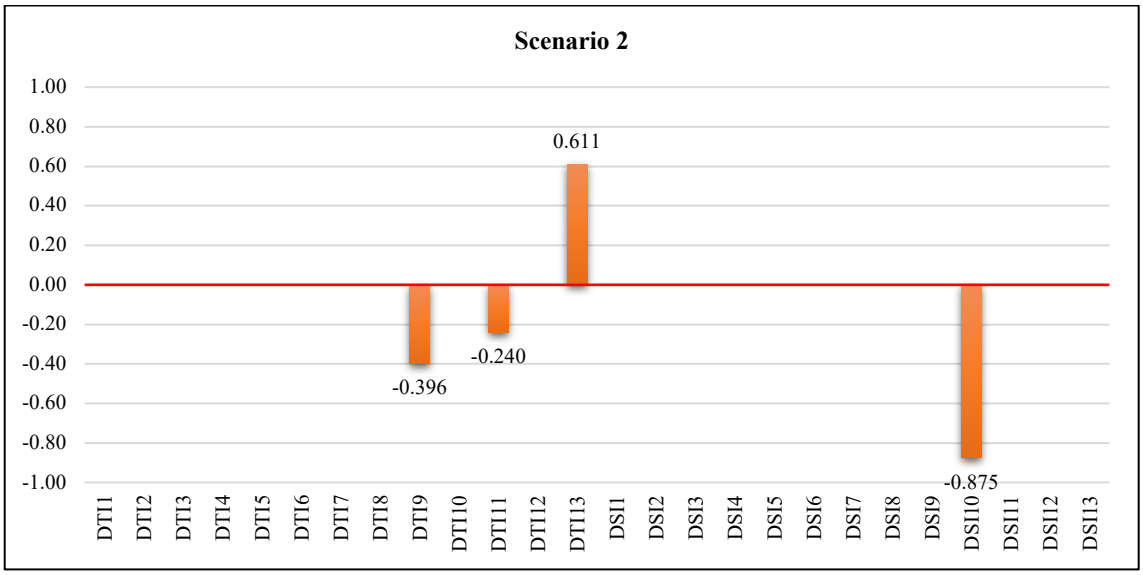

Figure 4.15: The result of the second scenario

“Capacity and skills development” is decreased by approximately 40%. The citizen-centric approach requires recruiting skilled IT staff to build the competencies in-house; even if implementation houses are brought in for larger implementation projects, the in-house expertise in the public institutions is indispensable (Bozkurt et al., 2023). Therefore, public employees' capacity and skill development are negatively affected in this scenario. By focusing less on citizens’ requirements, the “AI and technological innovations” decreased by 24%, whereas the “existence of traditional channels” increased by 61%. If technological innovations meet citizens’ needs, they are quickly adopted and are merely diffused in society. The existence of traditional channels is a recognition that the digital divide still exists, and not all citizens have equal access to or comfort with online services (Hassan & Lee, 2019). Favoring frequent interactions between citizens and governments might crack the cultural barriers between such pivotal technological innovation players in many countries (Greco et al., 2017). Employing a less citizen-centric approach led to an approximate 88% decrease in “favorable political context.” Trust and satisfaction from citizens to the DG are critical for managerial flexibility and political accountability in the modern administrative state (Oe et al., 2016).

- **Scenario 3: The Worst Service Approach**

Governments need to carefully plan and budget for DSI factors to ensure the successful implementation and sustainability of digital services. Therefore, the third scenario is generated based on the lowest value of the concepts in digital service improvement. The concepts’ values of success factors (i.e., DSI1, DSI2, DSI3, DSI4, DSI5, DSI6, DSI7, DSI10, DSI12, DSI14) are modified to -1. In contrast, the concepts’ values of risk factors (i.e., DSI8, DSI9, DSI11) are modified to 1 to simulate how the DGT system responds to changes in these factors. The result of this scenario is depicted in Figure 4.16.

The worst service scenario does not create a significant change in the DGT system. The system respond this scenario with one increase in the “digital divide”. Governments can favor investments in digital services and lifelong learning initiatives for citizens (Greco et al., 2017). Government spending on digital services affects citizens’ digital skill improvement, thus decreasing the digital divide (Choi et al., 2018).

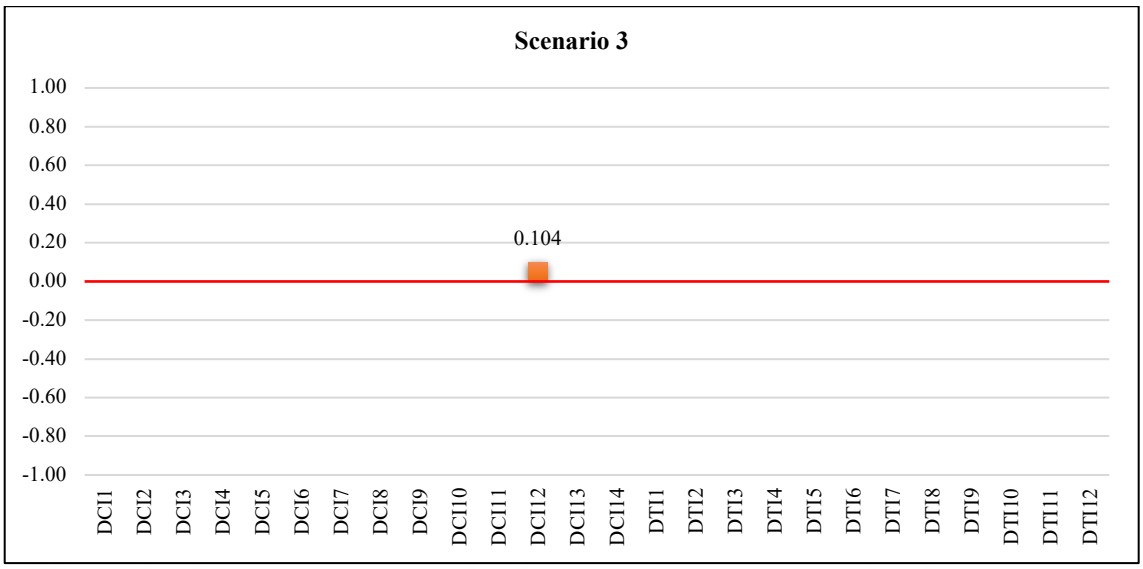

Figure 4.16: The result of the third scenario

- **Scenario 4: Citizen-Centric but Low Technology Approach**

A citizen-centric but low-technology approach refers to a strategy in which government services prioritize the needs and preferences of citizens while relying on minimal or low-level technology. The goal is to design and deliver services in a manner that is accessible, inclusive, and user-friendly without heavily relying on sophisticated digital tools. Thus, the fourth scenario is generated based on the highest value of the concepts in digital citizenship improvement with the lowest value of the concepts in digital technology improvement. For digital citizenship improvement, the concepts' values of success factors (i.e., DCI1, DCI2, DCI3, DCI4, DCI5, DCI6, DCI8, DCI9, DCI10, DCI11, DCI14) are modified to 1. In contrast, the concepts' values of risk factors (i.e., DCI7, DCI12, DCI13) are modified to -1. For digital technology improvement, the concepts' values of success factors (i.e., DTI1, DTI2, DTI3, DTI4, DTI5, DTI6, DTI7, DTI8, DTI9, DTI10, DTI11, DTI12) are modified to -1. In contrast, the concept value of risk factor (i.e., DTI13) is modified to 1 to simulate how the DGT system responds to changes in these factors. The result of this scenario is depicted in Figure 4.17.

"End-to-end service design" is negatively affected, with an approximate 98% decrease due to the gaps in technical requirements. At the layer of digital service characteristics, improving the operability of services is essential to ensure an end-to-end citizen journey. End-to-end digital service design involves the comprehensive planning, development,

and implementation of digital services that seamlessly address the needs and expectations of citizens (Y. Zhang et al., 2022). “User-friendly service design” is negatively affected by 21% despite improvements in digital citizenship. Creating user-driven value in proactive public service design is essential. Regularly gathering citizen feedback and making technological improvements based on user insights is essential for maintaining user-friendly service design (OECD, 2023). The “cost of consulting” is decreased by 41% in this scenario. Technological innovation novelty plays a pivotal role in enhancing purposive collaborations. In this perspective, advising consultants about technological infrastructure is critical (Greco et al., 2017). “Favorable political context” is decreased by 26%. The political background and institutional framework mediate the technology implemented and citizen interaction. These contextual factors are critical in producing the expected benefits of DGT (Eom & Lee, 2022).

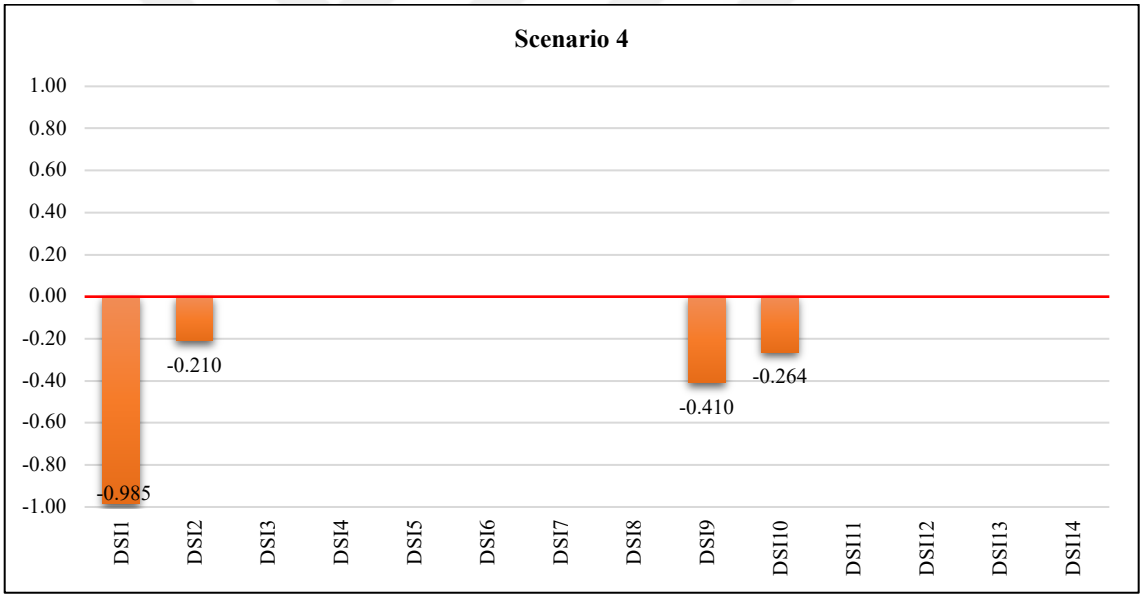

Figure 4.17: The result of the fourth scenario

- **Scenario 5: Best Service but Low Technology Investment Approach**

DG approach generally refers to using technology to enhance the efficiency, transparency, and accessibility of public services. While many DG initiatives focus on cutting-edge technologies, there are instances where a low-technology approach can be practical, especially in regions or situations where advanced infrastructure is not readily available or affordable. For this reason, the fifth scenario is generated based on the highest

value of the concepts in digital service improvement with the lowest value of the concepts in digital technology improvement. For digital service improvement, the concepts' values of success factors (i.e., DSI1, DSI2, DSI3, DSI4, DSI5, DSI6, DSI7, DSI10, DSI12, DSI14) are modified to 1. In contrast, the concepts' values of risk factors (i.e., DSI8, DSI9, DSI11) are modified to -1. For digital technology improvement, the concepts' values of success factors (i.e., DTI1, DTI2, DTI3, DTI4, DTI5, DTI6, DTI7, DTI8, DTI9, DTI10, DTI11, DTI12) are modified to -1. In contrast, the concept value of risk factor (i.e., DTI13) is modified to 1 to simulate how the DGT system responds to changes in these factors. The result of this scenario is depicted in Figure 4.18.

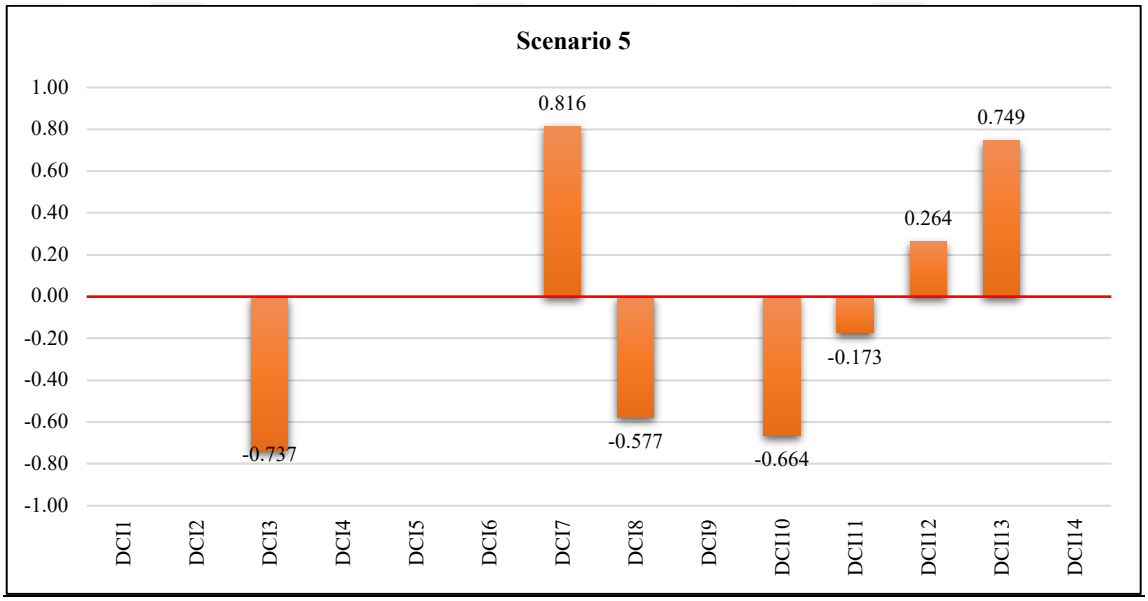

Figure 4.18: The result of the fifth scenario

"Citizen satisfaction" is negatively affected in this scenario, with an approximate 74% decline. Citizens' satisfaction with DG is strongly associated with their perceived value and cognition of service quality (Y. Li & Shang, 2020). "Ethical concerns" increased by 81% in this scenario. Ethics predicts citizens' trust in governance (Janssen et al., 2018). "Digital trust in government" decreased by approximately 57%, whereas "perceived privacy concerns" increased by approximately 26%. Privacy concerns are critical when individuals' personal information is used to explore and avail of certain transactional DG services, and they are prerequisites to predisposition to the trustworthiness of DG (Janssen et al., 2018). "Well-orchestrated citizen journeys" were affected with an approximate %66 declines. Government services are expected to be delivered digitally

and uninterrupted; public institutions are encouraged to provide multiple channel options for digital services to provide well-orchestrated citizen journeys (Lamid et al., 2021). "Citizen involvement" slightly decreases with 17%. When citizens experience a feeling of competence in successfully using a particular service, they feel empowered, creating value for them, and vice versa (El-Haddadeh et al., 2019). The "Digital divide" shows a significant inclination, approximately 75%. Government spending on digital services affects citizens' digital skill improvement, thus decreasing the digital divide. Nevertheless, addressing the digital divide in DG requires a comprehensive approach involving investments in infrastructure (Choi et al., 2018).

- **Scenario 6: The Worst "Citizen Engagement, Well-orchestrated Citizen Journeys, Citizen Satisfaction" Approach**

The sixth scenario is generated based on the lowest value of the most critical concepts in digital citizenship improvement to examine the systems' response to the worst-case scenario for citizen engagement, well-orchestrated citizen journeys, and citizen satisfaction. The concepts' values of these factors (i.e., DCI2, DCI3, DCI10) are modified to -1 to simulate how the DGT system responds to changes in these factors. The result of this scenario is depicted in Figure 4.19.

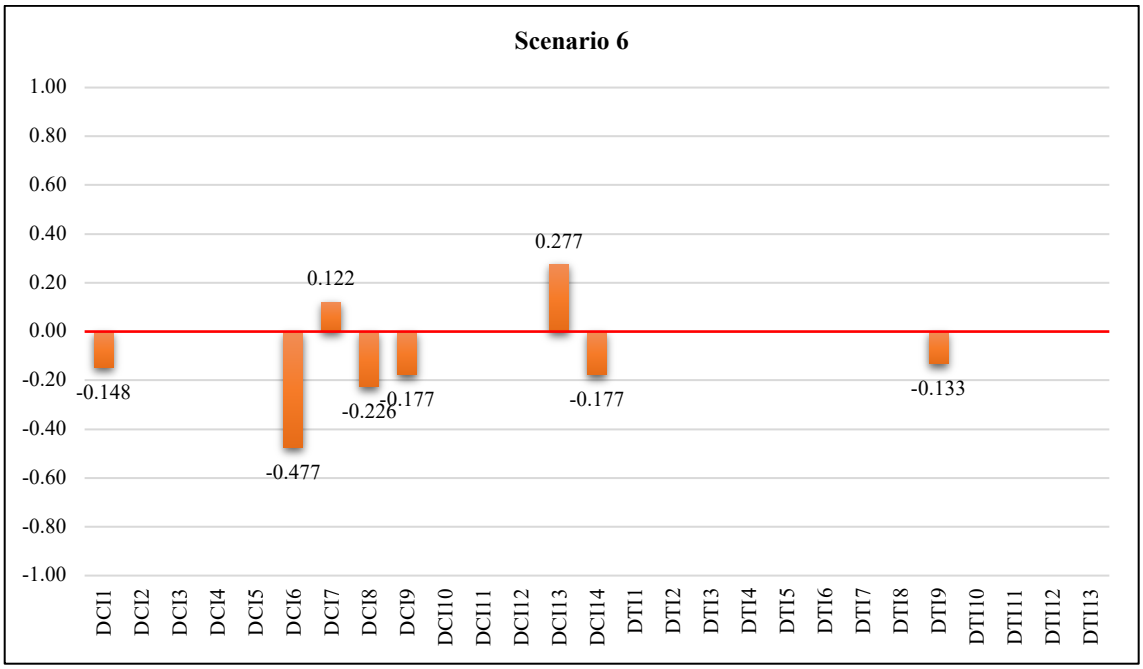

Figure 4.19: The result of the sixth scenario

“Digital training and education” decreases approximately 15%. DG requires a comprehensive approach involving investments in education to ensure that everyone, regardless of socioeconomic status or geographic location (Choi et al., 2018). All citizens in adopting digital technologies should be able to provide and receive services equally. Accessibility includes cost-effective, user-friendly, and language-friendly tools that everybody can afford and understand the procedure without training (David et al., 2023). “Public awareness” shows a decrease of approximately 48%. The decreased citizen engagement and satisfaction create cultural barriers; therefore, public awareness campaigns for internal and external stakeholders should be increased (Bozkurt et al., 2023). “Ethical concerns” increased by 12%, “digital trust in government” decreased by 23%, and “perceived privacy concerns” increased by 27%. It is challenging to gain citizens’ trust, and adopting technology for government services will be challenging if it cannot safeguard privacy protection and diminish the collection and storage of personal information (David et al., 2023). “Motivation to learn advanced technologies” decreases by 18% in this scenario. In the related literature, it is indicated that “The easier an organization perceives a new technology to learn and use, the less complex the former perceive the latter to learn and use, and vice versa.” (David et al., 2023). “Public participation” decreases by 18%. Public participation in the digital ecosystem boosts novelty, training, and entrepreneurship and improves the digital economy (Lamid et al., 2021). Thus, governments should create social media platforms and well-orchestrated citizen journeys to encourage active public participation (David et al., 2023).

“Capacity and skills development” is negatively affected in this scenario, with an approximate 13% decline. Citizen engagement, citizen satisfaction, and well-orchestrated user journeys require recruiting skilled IT staff to build the competencies in-house; even if implementation houses are brought in for larger implementation projects, the in-house expertise in the public institutions is indispensable (Bozkurt et al., 2023).

- **Scenario 7: The Worst “Cybersecurity, Systems Integration, Functional Interoperability” Approach**

The seventh scenario is generated based on the lowest value of the most critical concepts in digital technology improvement to examine the systems’ response to the worst-case scenario for cybersecurity, systems integration, and functional interoperability. The

concepts' values of these factors (i.e., DTI3, DTI4, DTI5) are modified to -1 to simulate how the DGT system responds to changes in these factors. The result of this scenario is depicted in Figure 4.20.

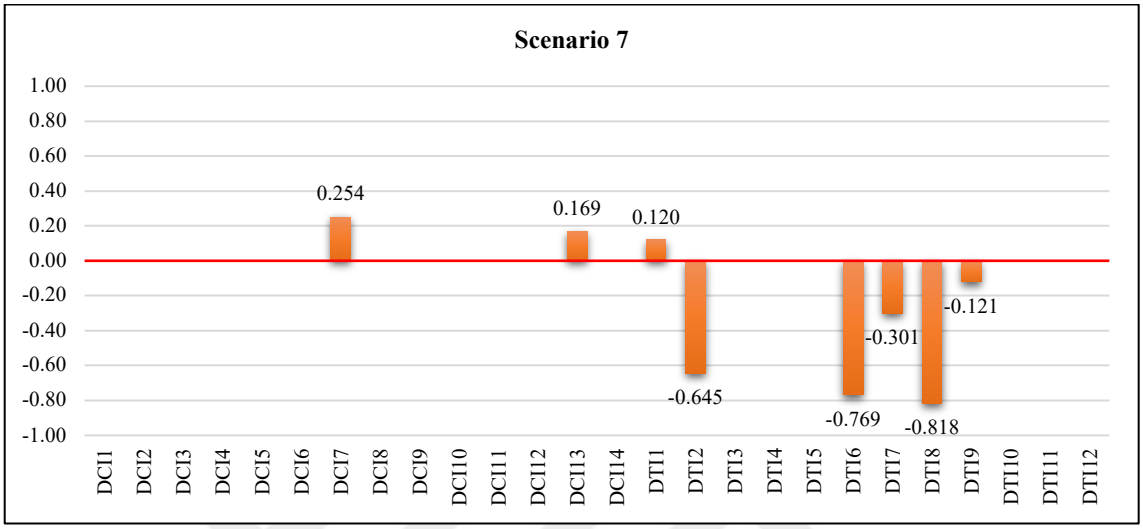

Figure 4.20: The result of the seventh scenario

"Ethical concerns" are increased by approximately 25%, and "perceived privacy concerns" are increased by approximately 17%. Advanced digital technologies shape the future of public organizations by potentially developing the quality of public services, fostering citizen trust, enhancing efficiencies, tackling complexity, managing repetitive tasks, and automating routine decisions. Nonetheless, risks and ethical and privacy concerns exist if these technologies are built on misinformation or incomplete or biased information (David et al., 2023).

In this scenario, "sustainable digital infrastructure" shows an increase of 17% since potential risks may have been raised due to the lack of cybersecurity measures, functional interoperability, and system integration. To be prepared for all possible potential dangers, public institutions should implement a secure and sustainable digital technology infrastructure and plan for business continuity (Lamid et al., 2021). "Data ownership rules" decreased by approximately 65%. Data ownership rules in DG refer to the policies and regulations determining who owns and controls the data. Thus, data ownership and governance are instrumental in the standardization and integration processes through their central role (Bozkurt et al., 2023). "Standardization of technologies" decreases by

approximately 77%. The literature indicates that there has been a lack of standardization of technological devices with many competing standards. Thus, functional interoperability is problematic (El-Haddadeh et al., 2019). “Network connectivity” shows a 30% decrease, while “IT capacity” shows an approximate 82% decrease. When introducing digital technologies, governments need a proper strategy to maintain their IT capacity and network connectivity. The managerial capabilities, comparative advantage, current organizational operations, and other factors influence the decision of the government authorities to accept or refuse the novel digital technology (David et al., 2023). “Capacity and skills development” decreases by 12% in this scenario. It is about embracing new practices, procedures, and strategies that can improve the capacity of public employees. This involves building public employees’ necessary expertise, competencies, and capabilities to effectively leverage digital technologies (David et al., 2023).

- **Scenario 8: The Worst “Government as a Platform, End-To-End Service Design, Integrated Partner Ecosystem” Approach**

The eighth scenario is generated based on the lowest value of the most critical concepts in digital service improvement to examine the systems’ response to the worst-case scenario for government as a platform approach, end-to-end service design, and integrated partner ecosystem. The concepts’ values of these factors (i.e., DSI1, DSI3, DSI5) are modified to -1 to simulate how the DGT system responds to changes in these factors. The result of this scenario is depicted in Figure 4.21.

“Organizational culture change” decreased by 15%. Making the DGT shift isn’t easy. It requires new leadership competencies and reconfiguring workforce design, capacity, skills, working methods, culture, and employee experience (Ernst and Young, 2022). Government leaders could build on an existing culture with their partners to positively contribute to DG's success and use (David et al., 2023). “Legislation and regulation change” is negatively affected in this scenario, with an approximate 17% decline. A policy priority should be planning for the long-term innovation needed (e.g., government as a platform approach, end-to-end service design) and supporting this by setting the background with laws and regulations to incentivize the DG paradigm (Greco et al., 2017).

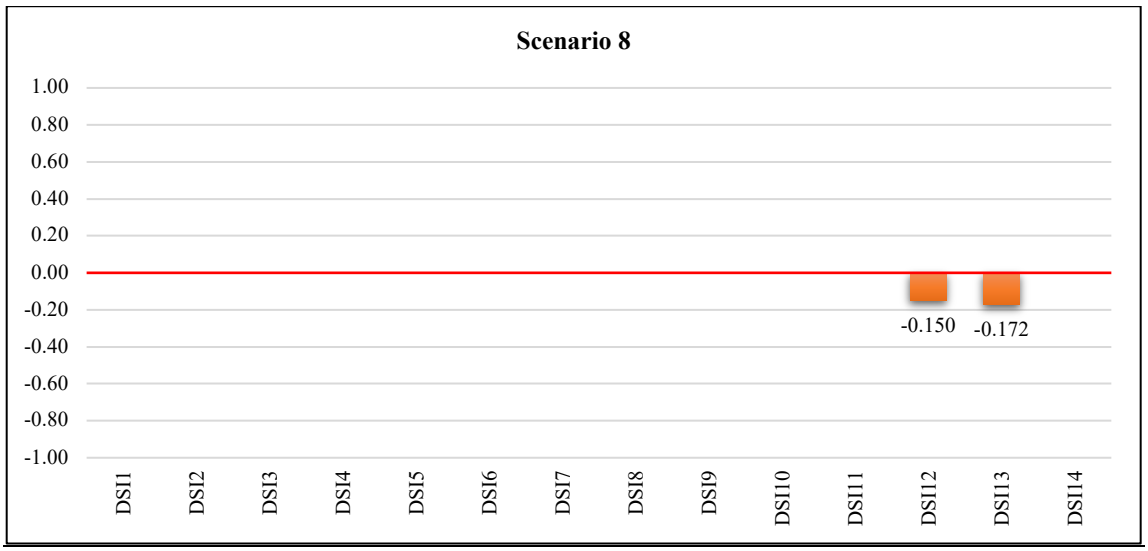

Figure 4.21: The result of the eighth scenario

- **Scenario 9: The Worst "Citizen Engagement" Approach**

The ninth scenario is generated based on the lowest value of the most critical concept in digital citizenship improvement to examine the systems' response to the worst-case scenario for citizen engagement. The concept value of the DCI3 factor is modified to -1 to simulate how the DGT system responds to a negative change in this factor. The result of this scenario is depicted in Figure 4.22.

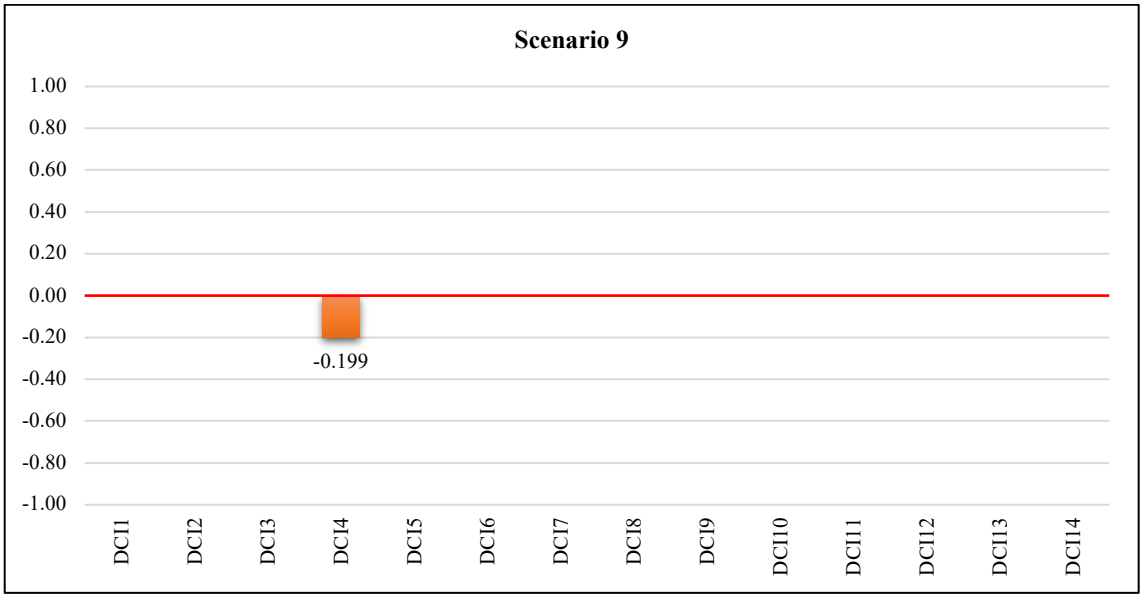

Figure 4.22: The result of the ninth scenario

"Efficient use of feedback mechanism" is decreased by approximately 20% in this scenario. The key to developing an accessible and transparent DG starts with focusing on the citizens' requirements and enhancing citizen engagement. Getting feedback and adopting the user-centric design principle is critical to successful DG delivery (Lamid et al., 2021).

- **Scenario 10: The Worst "Cybersecurity" Approach**

The tenth scenario is generated based on the lowest value of the most critical concept in digital technology improvement to examine the systems' response to the worst-case scenario for cybersecurity. The concept value of the DTI3 factor is modified to -1 to simulate how the DGT system responds to a negative change in this factor. The result of this scenario is depicted in Figure 4.23.

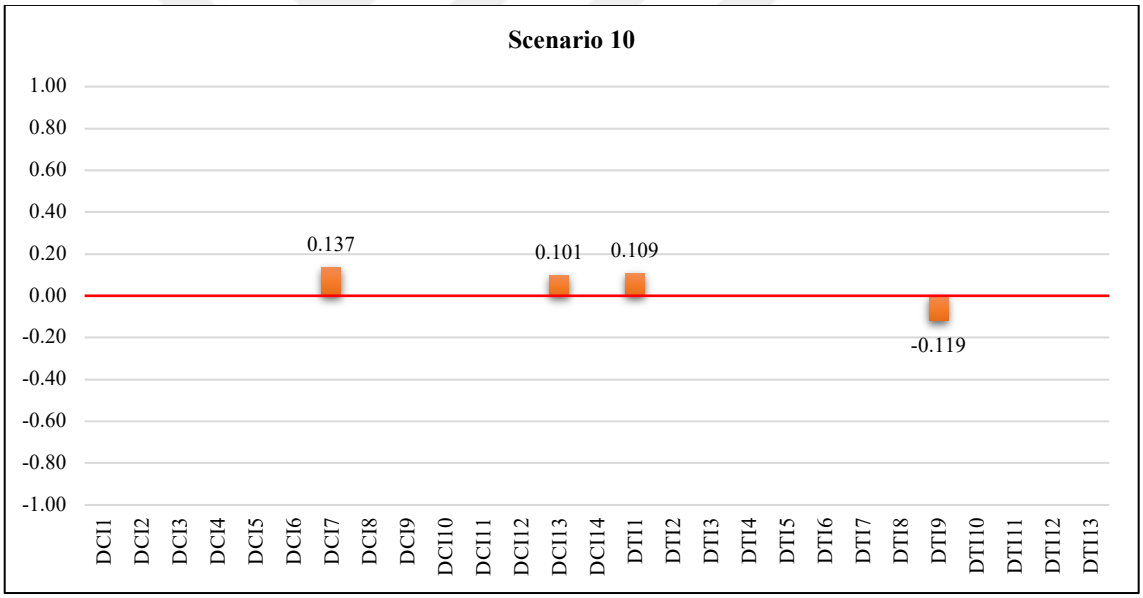

Figure 4.23: The result of the tenth scenario

"Ethical concerns" increased by approximately 14%, whereas "perceived privacy concerns" increased by 10%. Privacy and ethical concerns are related to information safety, thus cybersecurity. Transactional services require citizens to disclose personal information before a transaction can be completed; thus, perceived privacy and security of information are critical to instilling citizens' confidence (Janssen et al., 2018).

In this scenario, “sustainable digital infrastructure” shows an increase of approximately 11% since potential risks may have been raised due to the lack of cybersecurity measures. Public institutions are expected to stand by national and international best practices and standards on cybersecurity. Among others, public institutions will be assessed on the measures to secure digital technology infrastructure and comply with the country’s data protection regulation and other privacy-related legal frameworks (Lamid et al., 2021). “Capacity and skills development” is decreased by approximately 12%. The strategies and measures to ensure the cybersecurity and recovery of any risks from undefined cyber threats, disasters, and pandemics should be prepared and treated as an utmost priority (Lamid et al., 2021). Therefore, it is crucial to recruit skilled IT staff to build the competencies and skills in-house (Bozkurt et al., 2023)

- **Scenario 11: The Worst “Government as a Platform” Approach**

The eleventh scenario is generated based on the lowest value of the most critical concept in digital service improvement to examine the systems’ response to the worst-case scenario for government as a platform approach. The concept value of the DSI3 factor is modified to -1 to simulate how the DGT system responds to a negative change in this factor. However, this scenario does not create a significant change in the DGT system.

- **Scenario 12: The Worst “Citizen Engagement, Cybersecurity, Government as a Platform” Approach**

The twelfth scenario is generated based on each sub-system's lowest value of the most critical concepts. The concepts’ values of these factors (i.e., DCI2, DTI3, DSI3) are modified to -1 to simulate how the DGT system responds to changes in these factors. The result of this scenario is depicted in Figure 4.24.

“Efficient use of feedback mechanism” is decreased by approximately 15% in this scenario. For developing an accessible and transparent DG, it is essential to enhance citizen engagement (Lamid et al., 2021). Regularly gathering citizen feedback and making technological improvements based on citizens’ insights is essential for maintaining a successful DGT (OECD, 2023).

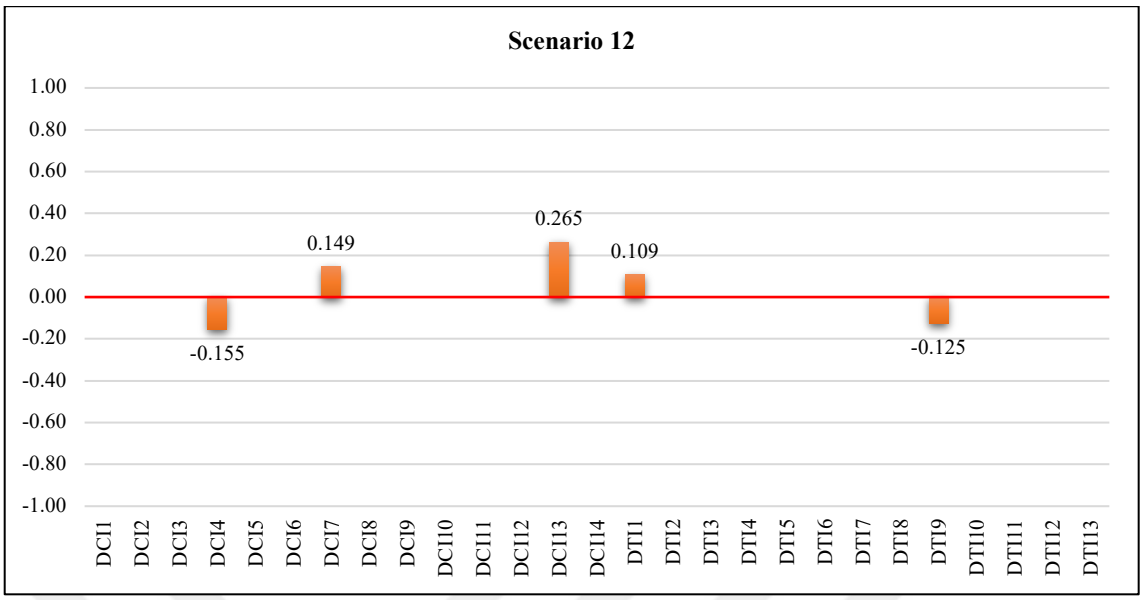

Figure 4.24: The result of the twelfth scenario

"Ethical concerns" are increased by approximately 15%, whereas "perceived privacy concerns" are increased by approximately 26%. It is important to note that DG service providers addressing citizens' information privacy and ethical concerns could positively influence their perceived value for technological implementations in the public sector (El-Haddadeh et al., 2019).

"Sustainable digital infrastructure" shows an increase of approximately 11% since potential risks may have been raised due to the lack of cybersecurity measures. Public institutions are expected to stand by national and international best practices and standards on cybersecurity (Lamid et al., 2021). "Capacity and skills development" is decreased by approximately 12%. Public employees need greater digital literacy to understand technology's potential, adapt to new tools and working methods, and use the data insights generated. Thus, digital specialists (e.g., data scientists, cybersecurity experts, and programmers) should keep up-to-date with technological innovation so the organization can maximize its potential in the long term (Ernst and Young, 2022).

4.5 Concluding Remarks on HFLCM Implementation of the DGT Framework

The success of an effective DGT is analyzed in this chapter by using an HFLCM approach. The causal relationships between success and risk factors are considered in this

approach with the utilization of the cognitive map approach. HFLCM technique allowed a more straightforward representation of expert(s) judgments for the concept values and causal influences between the concepts since it can model the hesitancy in one expert's judgments (intrapersonal hesitancy) and the judgments among experts (interpersonal hesitancy). Moreover, HFLTS provides flexibility with linguistic expressions.

Three experts determined the concepts and the relationships between concepts. At the end of this chapter, the most central success/risk factors are determined. The dynamic structure of the DGT framework is analyzed using scenario analyses. The responses of the DGT system for the potential changes in the success/risk factors are analyzed. The most central factor for digital citizenship improvement is determined as citizen engagement; the most central factor for digital technology improvement is determined as cybersecurity, and the most central factor for digital service improvement is determined as government as a platform approach.

5. CYBERSECURITY MATURITY ASSESSMENT

5.1 Cybersecurity

Recently, cyber-attacks and security breaches of information systems have been rapidly increasing. In particular, elements such as communication, banking services, public activities, defense systems, military systems, and network systems have become the main target (Kurtul et al., 2020). Therefore, cybersecurity threats have become a bigger problem for any critical digital infrastructure, and various online cyberattacks are also becoming a significant problem for society. The common cyberattacks can be summarized as (McKinsey, 2023):

- Malware: It is a malicious software including ransomware, spyware, and viruses.
- Phishing: It is sending fraudulent messages by an actor that appears come from a legitimate source for stealing information.
- Man-in-the middle attacks: It is eavesdropping personal information between two transactions, it is common on public Wi-Fi networks.
- Denial-of-service attacks: It is flooding systems with traffic to shut down the systems.
- Password attacks: It is stealing passwords by trickery or guesswork.

Cybersecurity can be defined as "…protecting computers, mobile devices, servers, electronic systems and networks from malicious digital attacks." (Erdoğan et al., 2020). Cybersecurity is a generic name and it refers to five security domains: availability, integrity, authentication, confidentiality, and non-repudiation (Gimenez-Aguilar et al., 2021). Cybersecurity is not just an IT concern; it is an enterprise-wide issue that calls for an interdisciplinary approach and a thorough governance commitment to ensure that all facets of the business are in line with effective cybersecurity practices (Morris et al., 2020; Rajan et al., 2021). Cybersecurity technology underpins but does not drive an effective cybersecurity policy. However, the use of technology is seen as the resolution rather than just a part of a broader strategy (Juno Risk Solutions, 2015).

Cybersecurity impacts every facet of the organization and has a direct impact on business performance (Accenture, 2020). As a result of the increased threats and actual attacks, the cyber resilience of critical infrastructures has become an important requirement of national security (Karabacak et al., 2016).

5.1.1 The Concept of Cybersecurity

For countries that can afford it, digital technologies will provide partial solutions to a range of emerging crises, from addressing new health threats and a crunch in healthcare capacity to scaling food security and climate mitigation for those that cannot, inequality and divergence will grow. Alongside a rise in cybercrime, attempts to disrupt critical technology-enabled resources and services will become more common, with attacks anticipated against agriculture and water, financial systems, public security, transport, energy, and domestic, space-based and undersea communication infrastructure (WEF, 2023). Therefore, it is inevitable for governments to consider cybersecurity as a part of their national security.

Beyond the world, the majority public is also facing its own set of risks. Today, many citizens understand that cybersecurity breaches can impact their personal data. The notion of cyber warfare as a genuine threat to their community is even becoming more conceivable. Due to its strategic significance for individuals, society as a whole, businesses, and the nation as a whole, cybersecurity as a whole has been gaining relevance (Daim et al., 2020; Serna Patiño & Giraldo Ramírez, 2019). A potential seizure of public sector information not only poses a threat to national security but also has the potential to undermine citizens' trust in the government. According to a cybersecurity survey conducted on public sector, 68% of the respondents explicitly say that keeping up with cybersecurity requirements (i.e., deploying/tuning controls, monitoring network behavior, following threat intelligence, etc.) is more difficult today than it was two years ago (Splunk, 2023). Therefore, public cybersecurity investments have largely been made. However, public institutions should measure the success of their cybersecurity investment.

5.1.2 Literature Review on Cybersecurity

Studies on cybersecurity using MCDM techniques have been conducted by searching the Web of Science, Scopus, and Google Scholar databases to analyze and discuss the convenience of the proposed approach and cybersecurity research in the existing literature. The selected 15 papers are listed in Table 5.1.

Table 5.1: Studies about cybersecurity integrated with MCDM approach

Study	Research Area	MCDM Method(s)	Fuzzy Extension	Application
(Abdel-Basset et al., 2021)	Cyber risk	AHP, MABAC, PROMETHEE II	Single-valued neutrosophic sets	Illustrative Example
(Abushark et al., 2022)	Cybersecurity analysis	AHP, TOPSIS	Type 1 fuzzy sets	Illustrative Example
(Alharbi et al., 2021)	Cybersecurity analysis	AHP, TOPSIS	Hesitant fuzzy sets	Illustrative Example
(Bojanić et al., 2020)	Cybersecurity management systems	AHP	Type 1 fuzzy sets	Illustrative Example
(Moreira et al., 2021)	Cybersecurity controls	MCDA-C, MACBETH	N/A	Case Study
(Alenezi et al., 2020)	Cybersecurity design	AHP, TOPSIS	Type 1 fuzzy sets	Case Study
(Noor et al., 2020)	Cyber threat intelligence	AHP	N/A	Case Study
(Polireddi & Sekhar, 2023)	Cybersecurity risks	TOPSIS	Type 1 fuzzy sets	Illustrative Example
(Priyadarshini et al., 2021)	Cyber insecurities	AHP	N/A	Illustrative Example
(Torbacki, 2021)	Cybersecurity in Industry 4.0	DEMATEL, ANP (DANP), PROMETHEE II	N/A	Case Study
(Ungkap & Daengsi, 2022)	Cybersecurity awareness	AHP	N/A	Case Study
(Bhol et al., 2020)	Cybersecurity metrics	AHP, ELECTRE III	N/A	Illustrative Example
(Gupta Gourisetti et al., 2019)	Blockchain cybersecurity	MCDA	N/A	Illustrative Example
(Zaidan et al., 2023)	Cyber-physical metaverse systems	PROMETHEE II	Interval-valued spherical fuzzy rough sets	Illustrative Example
(Camgöz Akdağ & Menekşe, 2023)	Cybersecurity framework	CRITIC	Interval-valued Pythagorean fuzzy sets	Illustrative Example

Kalhoro et al. (2021) conducted a systematic literature review between 2010-2020 to examining the critical factors of cyber hygiene behavioral intention. Studies on

cybersecurity standards between 2000-2022 were reviewed by Taherdoost (2022). Almansoori et al. (2023) conducted a systematic review of cybersecurity behavior from an information science perspective between 2012-2021. Apart from these studies, our study briefly focuses on the current cybersecurity research using the MCDM approach.

The research areas examined in Table 5.1 generally focus on cybersecurity risk management (Abdel-Basset et al., 2021; Noor et al., 2020; Polireddi & Sekhar, 2023; Priyadarshini et al., 2021), cybersecurity frameworks (Abushark et al., 2022; Alenezi et al., 2020; Alharbi et al., 2021; Bhol et al., 2020; Camgöz Akdağ & Menekşe, 2023), and digital technologies with cybersecurity (Gupta Gourisetti et al., 2019; Torbacki, 2021; Zaidan et al., 2023).

Several MCDM methods were applied (AHP, MABAC, PROMETHEE, TOPSIS, DEMATEL, ELECTRE, CRITIC, ANP, and MACBETH). However, fuzzy extension was not preferred in almost half of the studies listed in Table 5.1. Type 1 fuzzy sets were primarily applied in the examined studies (Abushark et al., 2022; Alenezi et al., 2020; Bojanić et al., 2020; Polireddi & Sekhar, 2023), advanced fuzzy extensions were applied in some of these studies. Single-valued neutrosophic fuzzy sets (Abdel-Basset et al., 2021), hesitant fuzzy sets (Alharbi et al., 2021), interval-valued spherical fuzzy rough sets (Zaidan et al., 2023), and interval-valued Pythagorean fuzzy sets (Camgöz Akdağ & Menekşe, 2023) were applied.

5.2 Cybersecurity Maturity Model

Cybersecurity impacts every facet of the organization and has a direct impact on business performance (Accenture, 2020; Rajan et al., 2021). The cyber resilience of critical infrastructures has evolved into a crucial requirement of national security as a result of the rise in threats and actual attacks (Alladi et al., 2020; Baldini, 2022; Jmila & Khedher, 2022; Karabacak et al., 2016; Krawczyk-Sokołowska & Caputa, 2023; Macas et al., 2022; Sepúlveda Estay et al., 2020; Sheikh et al., 2022; Shokry et al., 2022; Varela-Vaca et al., 2021). Organizations can currently choose from a wide variety of frameworks on the market to increase the efficiency of their cybersecurity. Action is supported by these frameworks on both the individual and organizational levels. Offering a pertinent security

awareness program is the first step in creating a secure environment. To increase the level of cybersecurity, the institution can adopt management and audit changes. As a result, maturity models are a crucial set of tools that institutions can use to assess their level of cybersecurity readiness (Aliyu et al., 2020).

An organization with a successful approach to cybersecurity is expected to have a wide range of capabilities, which are described in a cybersecurity maturity model. Each capability includes a description of the types of processes and activities that are anticipated at various levels of maturity. In order to evaluate an organization's overall cybersecurity maturity, it compares its own practices to those outlined in the levels of each capability. It supports the assessment's findings with some data. Maturity models offer an extremely condensed and practical view of reality. They are different from a thorough audit, gap analysis, or review, which are still essential in cybersecurity (EuroControl, 2017).

5.2.1 Concept of Cybersecurity Maturity Model

A cybersecurity maturity model enables an organization to evaluate its personnel, operational procedures, and technological capabilities in light of a predetermined set of external benchmarks. An organization's ability to respond to "how do we know?" questions is also aided by a maturity model (Roberts, 2016).

- How do we know our current state of affairs?
- How do we know our destination?
- How do we know our areas of strength?
- How do we know if we are progressing?
- How do we know if our current procedures are effective?
- How do we know how we stack up against our competitors?
- How do we compare to our peers?

The foundation of cybersecurity maturity models is based on the capability maturity model. Figure 5.1 illustrates the evolution of the cybersecurity maturity models.
Cybersecurity maturity models (REBIT, 2017):

- try to gather the best cybersecurity exercises,

- are established by the teamwork of experts from various backgrounds,
- take into account how different the organizations using the model are in terms of their size, experience, knowledge, and other attributes,
- approach cybersecurity with a focus on life cycles and continuous improvement.

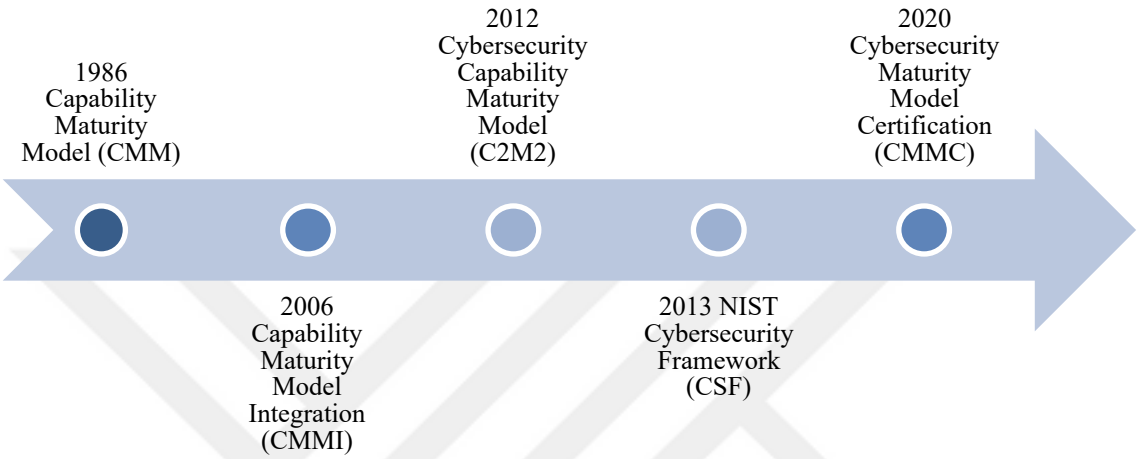

Figure 5.1: The evolution of cybersecurity maturity models

In addition, cybersecurity maturity models help the institutions to (REBIT, 2017):

- tackle their security gaps,
- propose an actionable security roadmap through well-defined guidance,
- assess themselves and allow benchmarking,
- help organizations in making strategic investment decisions in cybersecurity core domains according to their needs for business and level of risk tolerance,
- deliver services to customers without disconnection,
- safeguard sensitive client and exclusive information,
- fulfill with laws and regulations that govern their processes.

The model also helps develop additional specifications, best practices, and tools in a structured manner (REBIT, 2017). A comparison of the existing models and the proposed model in this study is detailed in Table 5.2.

Table 5.2: Comparison with the existing models

Model/ Edition	Scope	Dimensions/ Levels	Development Methodology	Benefits	Drawbacks
CMMI v2.0/2018	Industrial	3/5	Expert opinions, surveys	-Applicable in any industry -Offering comprehensive guides	-No holistic/hierarchical model
NIST v1.1. /2018	Industrial	5/4	Public-private partnership, best practices	-Applicable in any industry -Based on globally recognized standards	-Long data collection
C2M2 v2.0/2019	Industrial	10/4	Public-private partnership, best practices	-Applicable in any industry -Applicable in any size of organization -Descriptive model	-Long data collection processes -Lack of guidance
CMMC v1.0/2020	Industrial	17/5	Expert opinions, best practices	-Coupled with a certification program -Aligning processes and practices	-No holistic/hierarchical model
CMM/ 2021	Industrial	5/5	Expert opinions	-Holistic model -Multi-faceted, multi-stepped and multi-stakeholder process	-Long data collection processes -Only country-level assessments
The Proposed Model/ 2023	Academic/ Industrial	15(factors) below 5(dimensions)/ 5	Systematic Literature Review, Kitchenham's three-phased guidelines, Expert opinions	-Hierarchical model -Applicable in any industry -Applicable in any size of organization -Based on bibliometric analysis -Based on academic papers, industry reports, and experts' views	-

The scope of CMMI, NIST, C2M2, CMMC, and CMM are industrial, while our proposed model's scope is industrial and academic. Some of the models have a holistic structure (e.g., CMM), while some of them have no holistic/hierarchical model (e.g., CMMI, CMMC). Long data collection processes are needed in NIST and CMM (CMM, 2021; CMMI, 2017; NIST Cybersecurity Framework Team, 2018; US DoD, 2020; US DoE, 2019). Therefore, the proposed model has several benefits together as proposing a hierarchical model without a long data collection process, applicability in any industry

and any size of the industry, and development based on literature review, bibliometric analysis, and expert opinions.

5.2.2 Literature Review on Cybersecurity Maturity Model

This study is aimed to answer the following research questions:

- RQ1: What are the most common keywords, research areas, sources, and countries based on cybersecurity maturity models literature?
- RQ2: What are the main characteristics (i.e., dimensions, levels, foundations, names, application fields) of the research on cybersecurity maturity models? What are the most frequently used cybersecurity maturity dimensions/factors in the related literature?
- RQ3: How can a list of cybersecurity maturity factors be identified for developing a framework?

The flowchart of the proposed evaluation framework is illustrated in Figure 5.2.

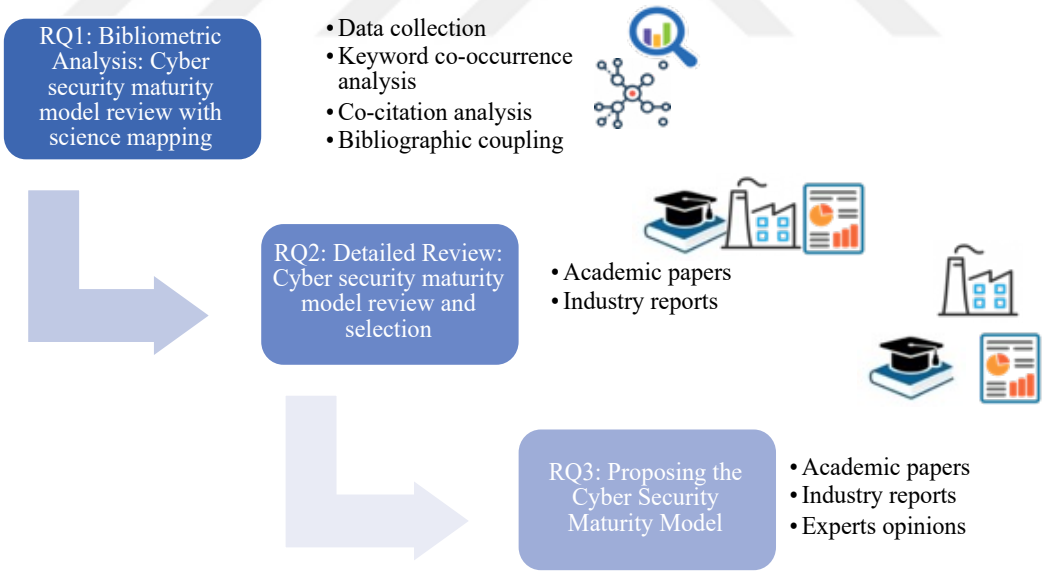

Figure 5.2: The flowchart of the CMM literature review

First, we conducted a bibliometric analysis. Then, we reviewed the papers and reports in detail. Finally, we have proposed the cybersecurity maturity model. The proposed

cybersecurity maturity model is developed based on bibliometric analysis, a literature review of academic papers, industry reports, and advising experts' views.

We conducted our review in accordance with Kitchenham's three-phased guidelines (Kitchenham, 2004), which include creating a review procedure, carrying out the review, and reporting the review. In the subsections that follow, we outline the primary steps of this systematic literature review, describing the procedure seen in Figure 5.3.

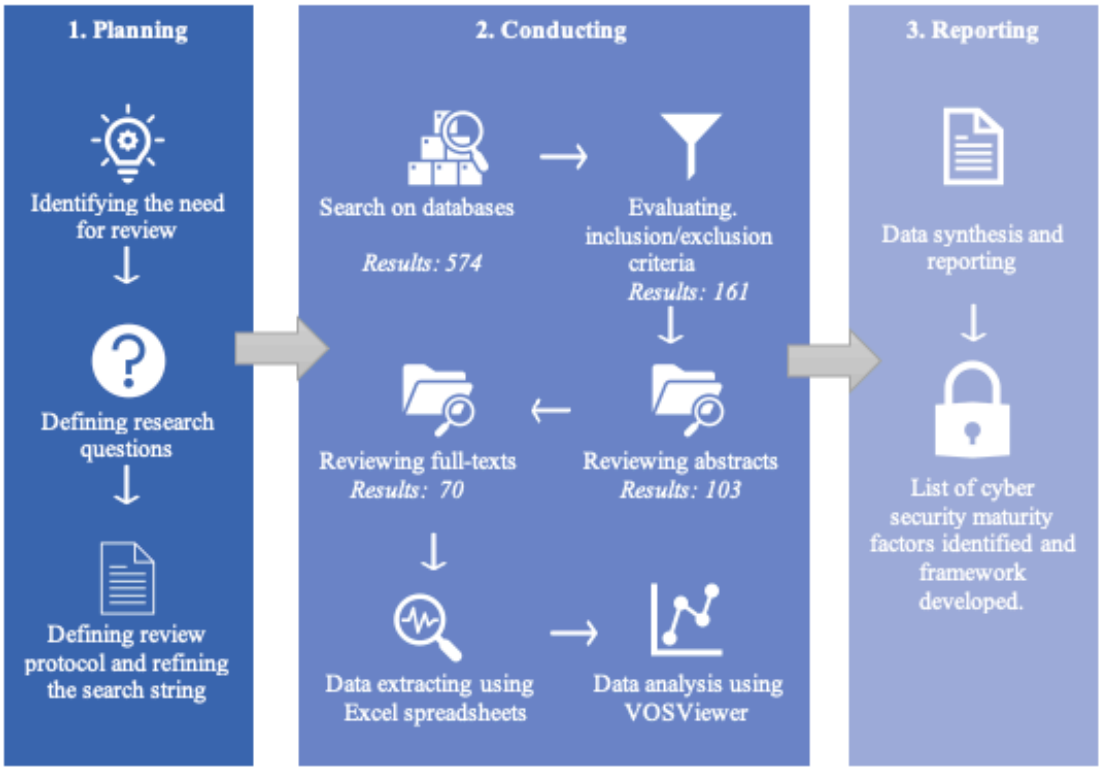

Figure 5.3: Systematic literature review stages

In this paper, data is collected on Scopus from Elsevier and the Web of Science (WoS) from Clarivate Analytics. In the WoS core collection, the search strings are used for the "topic" field. In Scopus, the search strings are used for the "article title, abstract, keywords" field. The databases are searched with the following keywords:

> "cyber security" AND "maturity"; "cyber security" AND "readiness"; "cyber maturity"; "cyber security maturity"; "cyber security readiness."

The number of papers on databases is shown in Table 5.3. It's important to note that no geographic constraints, university or research center restrictions, and publication year restrictions were not used for this initial search. The inclusion/exclusion criteria from Table 5.3 applied. The year (documents published after 2000), language (English), and document type are then restricted (articles).

Table 5.3: The number of papers on databases

Search Keywords	1. Initial Search		2. Year (2000-2022)		3. Language (English)		4. Document type (Article)	
	WoS	Scopus	WoS	Scopus	WoS	Scopus	WoS	Scopus
1. “cyber security” AND “maturity”	80	204	80	204	77	198	27	45
2. “cyber security” AND “readiness”	68	155	68	155	67	154	31	36
3.“cyber maturity”	7	8	7	8	7	7	3	2
4.“cyber security maturity”	13	28	13	28	13	28	5	5
5.“cyber security readiness”	5	6	5	6	5	6	4	3
Total	173	401	173	401	169	393	70	91

It's crucial to choose the right approach for extracting metadata for further analysis. Excel spreadsheets were used to store the data and organize the data. Python programming language is used in order to eliminate duplicates in the data. When the duplicates in the Scopus database were eliminated, 75 of the 91 publications remained, and when the duplicates in the WoS database were eliminated, 61 of the 70 publications remained. There were a total of 103 papers left after previous studies in both databases were removed. Then, the data is analyzed using VOSViewer software. The bibliometric analysis section comprises the analysis findings.

- **RQ1: Bibliometric Analysis**

A keyword co-occurrence analysis is performed using VOSviewer to build a visualization based on clustering. Figure 5.4 shows several clusters of the most common keywords found in the papers, and Table 5.4 lists the keywords found in each cluster. The most prominent themes in the literature are more noticeable thanks to different colors. Full counting is used as the counting method. All keywords are selected as the analysis unit, and the threshold value is determined as 2. Out of the 341 keywords, 43 keywords have met the threshold. In this analysis, 43 items, 6 clusters, and 203 links are found, with a total length strength of 243.

Table 5.4: Keywords for co-occurrence analysis

Clusters (colors)	# of items	Items and their occurrences
Cluster 1 (red)	9	1. Capability maturity model (2) 2. Culture (3) **3. Cyber security (14)*** 4. Cyber security readiness (2) 5. Developing countries (3) 6. Firm performance (2) 7. Impact (2) 8. Information security (8) 9. Maturity model (6)
Cluster 2 (green)	9	1. Digitalization (3) 2. Fourth industrial revolution (2) 3. Indonesia (2) 4. Industry 4.0 (3) 5. Internet of things (IoT) (2) 6. Maturity (3) **7. Model (4)*** 8. Policies (2) 9. Sustainability (2)
Cluster 3 (blue)	7	1. 0 (2) 2. Cyber (5) 3. Cyber threats (2) 4. **Cybersecurity (13)*** 5. Knowledge (2) 6. Management (4) 7. Readiness (3)
Cluster 4 (yellow)	7	**1. Challenges (5)*** 2. Cyber-security (2) 3. Framework (4) 4. Future (2) 5. IoT (3) 6. Security (4) 7. Vulnerabilities (2)
Cluster 5 (purple)	6	1. Assessment (2) **2. Awareness (3)*** 3. Behavior (2) **4. Information technology (3)*** 5. Organizations (2) 6. Systems (2)
Cluster 6 (light blue)	5	1. Cyber attacks (2) 2. Design (2) 3. Cyber-attack (2) **4. Governance (3)*** 5. Perceptions (2) 6. **Safety (3)***

* The keywords with the highest occurrences within clusters are highlighted in bold characters.

Beyond the first nine terms, "cyber security" appears most frequently in the first cluster. The terms "maturity model," "capability maturity model," and "cyber security readiness" all refer to assessment frameworks. The first cluster highlights the subject's significance for “developing countries.” When building maturity models, it is essential to take into account the "impact" of “information security” on "firm performance" and firm "culture."

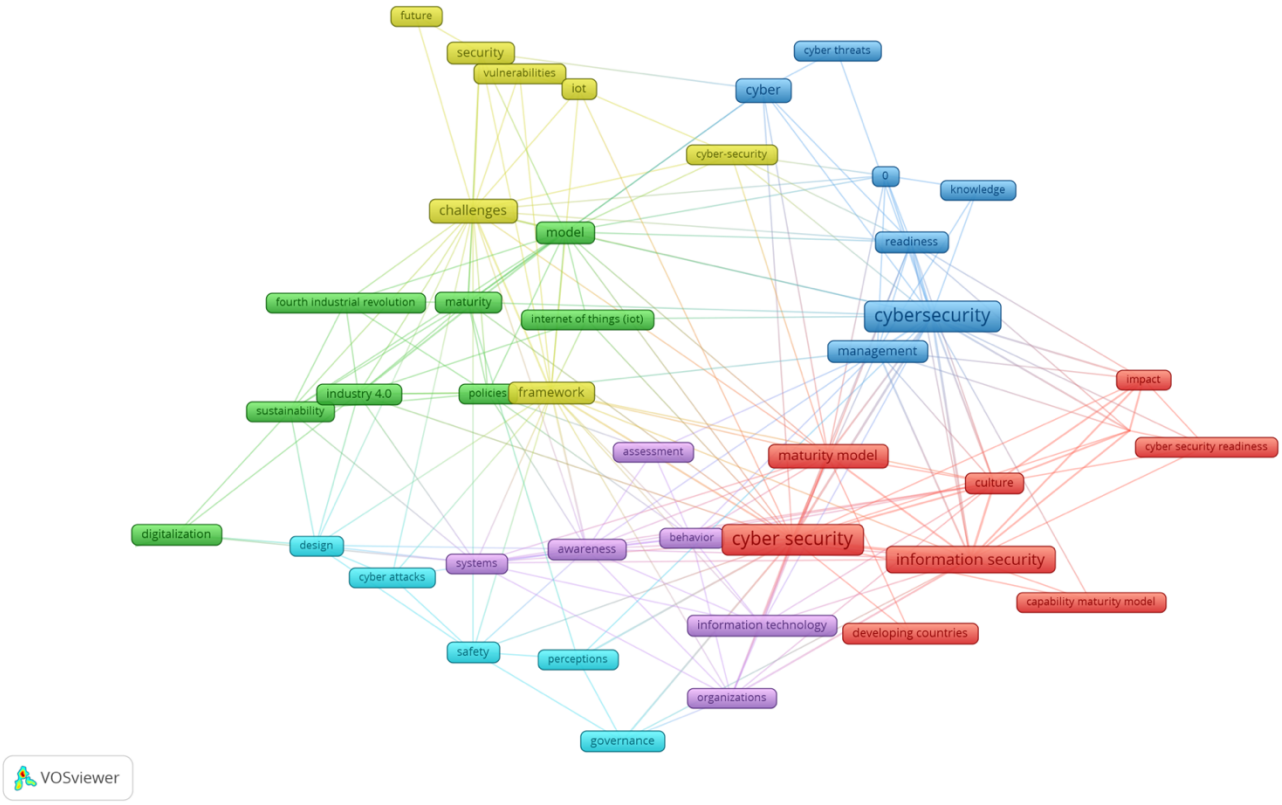

Figure 5.4: Network visualization of keyword co-occurrence analysis

Beyond the first nine terms, "model" dominates the second cluster of keywords. The term "Industry 4.0," also known as the "fourth industrial revolution," is used to refer to technologies that go beyond this "digitalization," such as the "Internet of Things (IoT) ." The cybersecurity "policies" behind the technologies are discussed. Additionally, the "sustainability" perspective is used when evaluating cybersecurity maturity frameworks.

Beyond the first seven terms, "cybersecurity" appears the most frequently in the third cluster. While "threats" and "cyber threats" refer to risk scenarios, "cyber" and "readiness" refer to assessment methods. In this case, it's crucial to "manage" the "knowledge" about existing cybersecurity systems.

"Challenges" is the word that appears the most frequently in the fourth cluster after the first seven. It is followed by "framework" and "security," as security frameworks are highly valued in "cyber-security" research. “Future” scenarios and possible “vulnerabilities” and “IoT” technology are listed in this cluster. Information technology

and awareness both occur equally frequently in the sixth cluster. "Assessment" refers to the assessment frameworks used to evaluate "organizations'" cybersecurity maturity level. This cluster lists the "system" and "behavior" against cyber-attacks.

"Governance" and "safety" underline the significance of cybersecurity governance in terms of secure system "design" in the seventh cluster. Furthermore, the "perception" of the risk of "cyber-attacks" is critical in ensuring organizational safety.

The distance between the journals in the visualization for the co-citation analysis represents their relationship in terms of co-citation relationships. In the first analysis, the counting method is selected as full counting, the unit of analysis is selected as cited sources, and the minimum number of citations of a source is selected as 5. Out of the 2080 sources, 50 sources have met the threshold. Figure 5.5 displays the document co-citation analysis regarding sources.

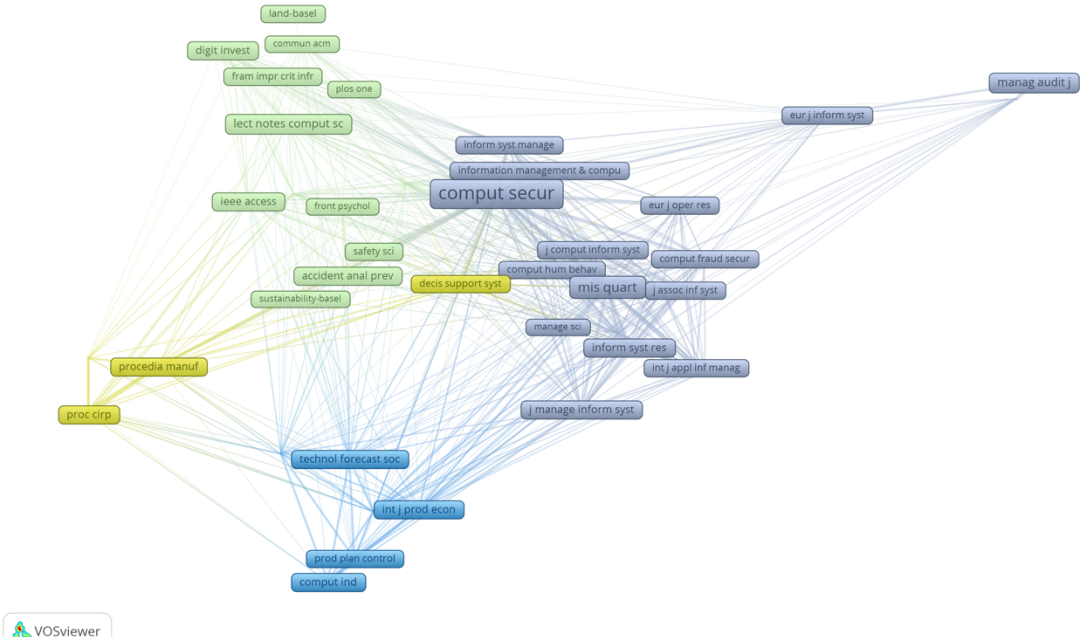

Figure 5.5: Network visualization of co-citation analysis regarding sources

According to Figure 5.5, Computers and Security is the most cited journal (58 citations, 1038 total link strength), followed by MIS Quarterly (24 citations, 736 total link strength).

For the bibliographic coupling analysis, the counting method is selected as full counting, the unit of analysis is selected as countries, and the maximum country number for each

document is selected as 25 to ignore those publications co-authored by many countries. The minimum number of documents of a country is determined as 2. Out of the 43 countries, 15 countries have met the threshold. This analysis found 15 items, 2 clusters, and 47 links, with a total length strength of 684. Figure 5.6 displays the bibliographic coupling regarding countries.

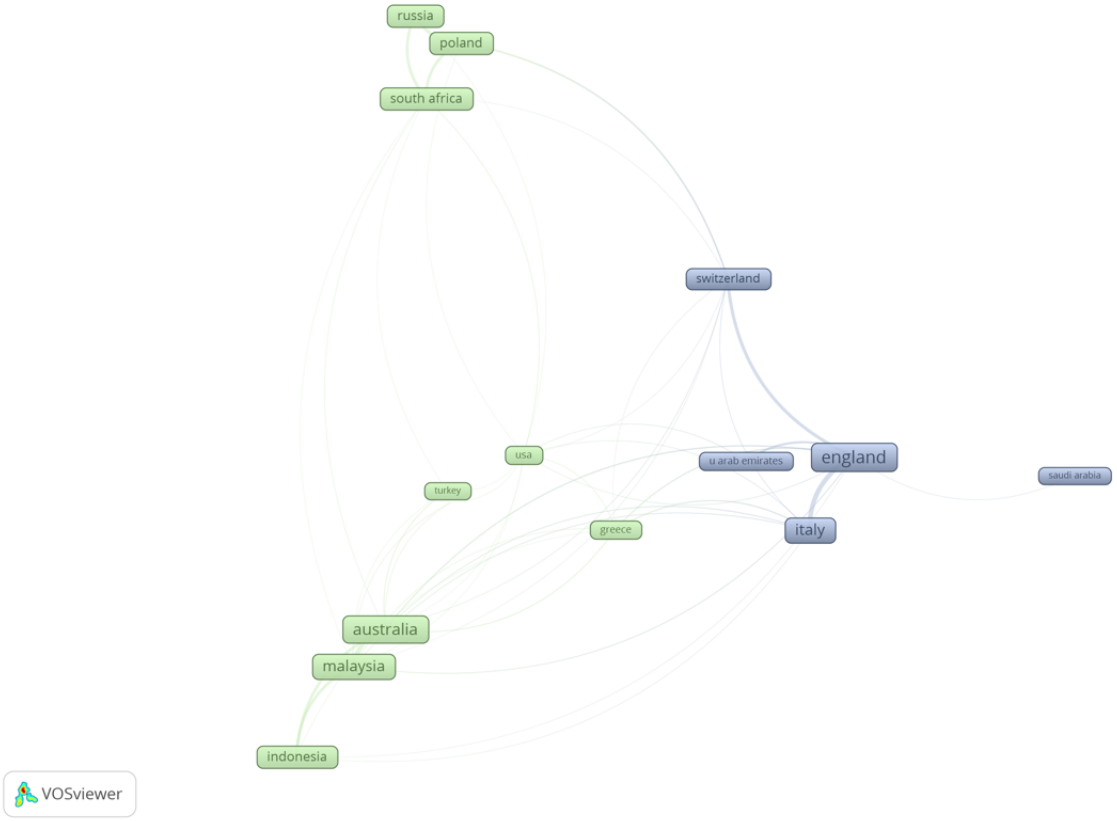

Figure 5.6: Network visualization of bibliographic coupling regarding countries

Figure 5.6 indicates England has the highest total link strength with 254 links. Australia and Malaysia are ranked second and third-ranked countries, with 194 and 180 links, respectively. Moreover, this bibliographic coupling analysis showed that the themes of the documents published in England, Italy, the United Arab Emirates, Switzerland, and Saudi Arabia show great similarities. Besides, the studies from Australia, India, Indonesia, Malaysia, Poland, Russia, Türkiye, the U.S., Greece, and South Africa are thematically related according to this analysis.

- **RQ2: Detailed review**

38 papers are selected based on the existence of a cybersecurity maturity model. The model name, number of maturity dimensions/number of maturity levels, type of model (generic/specific), field of application, assessment method (self-assessment/3rd party assisted), application method, evaluation criteria basis (ISO/ government agencies, etc.), dimensions, levels, the numeric calculation (Y/N) and cooperation in those papers are detailed in Table B.1. The fields in the academic papers are visualized in Tableau version 2021.3. software. Figure 5.7 illustrates application fields used in academic papers.

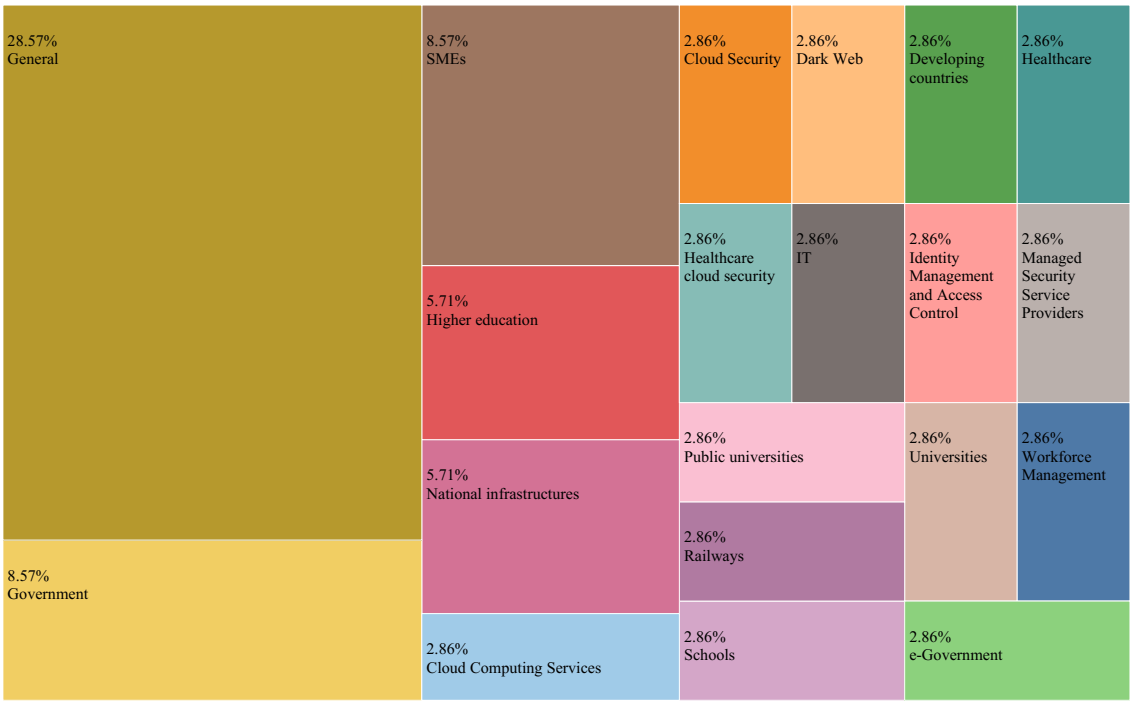

Figure 5.7: Distribution of academic papers by application fields

The fields of application include; general, government, SMEs, national infrastructures, higher education, cloud security, cloud computing services, the dark web, universities, workforce management, schools, railways, e-government, developing countries, and healthcare.

Application methods comprise; case studies, surveys, interviews, questionnaires, workshops, AHP, spreadsheets, path analysis, dashboards, multi-model analysis, gap

analysis, Delphi survey, soft systems methodology, technology-organization-environment framework, Cronbach's alpha, and design science research. Questionnaires, surveys, and reviews are the most frequently used methods in those papers.

There are 20 generic and 18 specific models. In papers with generic models, 70% of the studies have numeric application, while in papers with specific models, 61% of the studies have numeric application. The distribution of the assessment methods (i.e., self-assessment/3rd party assisted) according to generic and specific models are examined in In 3rd party assisted methods, 80% of the models are specific. In self-assessed methods, 42,86% of the models are specific. Therefore, specific models necessitate a 3rd party assessment in most papers.

Figure 5.8 shows the evaluation criteria basis used in academic papers. Capability maturity models (CMM, CSCMM, CMMI, C2M2) and CIS, NIST are the main criteria basis in most papers.

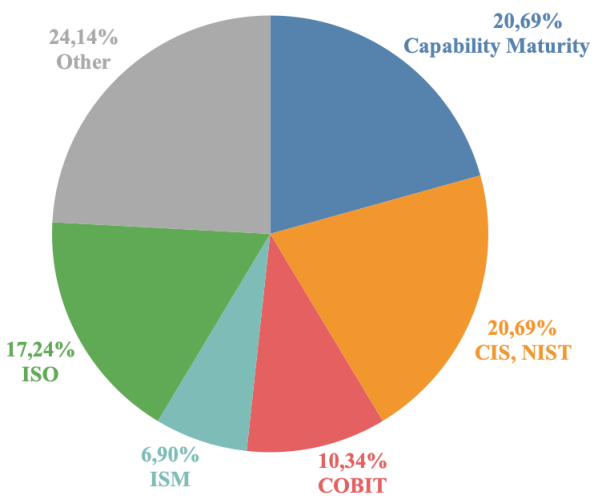

Figure 5.8: Distribution of academic papers by evaluation criteria basis

The list of the dimensions, their percentage, and the number of papers including these dimensions are provided in Table 5.5. The most frequently used dimensions in academic papers are protection, organization, workforce management, infrastructure, and identification.

Table 5.5: Classification of dimensions in academic papers

Name of dimensions	%	# of papers
Other	14,47%	22
Protect, Protect & Detect, Protection	9,87%	15
Organization, Organizational	9,21%	14
Workforce Management	6,58%	10
Infrastructure, Technical, Technical Measures	4,61%	7
Identification, Identify, Identify	4,61%	7
Awareness, Awareness And Training, Education	3,95%	7
Technological, Technologies, Technology	3,29%	5
Education, Training/Skills Development, Training	3,29%	5
Cooperation, Information Sharing	3,29%	5
Continuous Improvement, Process, Processes/Techniques	3,29%	5
Planning And Analysis	2,63%	4
Leadership And Planning, Management Activities	2,63%	4
Continuous Vulnerability Management, Mitigation Of External Threats, Threat	2,63%	4
Contingency, Identity And Access Management	2,63%	4
Compliance, Policies, Policies And Standards	2,63%	4
Capability, Capacity Building, Capacity Building And Awareness	2,63%	4
Recover, Respond, Respond & Recover	1,97%	3
Physical Security, Data Governance And Protection, Security Governance	1,97%	3
Legal, Legal And Regulatory Measures, Legal/Policies	1,97%	3
Information Security Technical Hygiene, Secure Configuration For Hardware And Software, Information Security Culture	1,97%	3
Event And Incident Response, Continuity Of Operations, Incident Response Management, Incident Management	1,97%	3
Enterprise Risk Management, Risk Management, Risk Management Process	1,97%	3
Supply Chain And External Dependencies Management & Supply Chain Management	1,32%	2
Inventory And Control Of Hardware Assets	1,32%	2
Environment & Environmental	1,32%	2
Detect & Diagnostics	1,32%	2
Asset, Change, Configuration Management & Asset Management	1,32%	2

Figure 5.9 illustrates the word cloud about the dimensions. Management, organizational, technical, recover, cybersecurity, identify, protect, information, awareness, and responses are the most frequent words in dimensions.

Figure 5.9: The word cloud of dimensions in academic papers

19 industry reports are selected based on the existence of an original cybersecurity maturity model. The model name, number of maturity dimensions/number of maturity levels, type of model (generic/specific), field of application, assessment method (self-assessment/3rd party assisted), evaluation criteria basis (ISO/ government agencies, etc.), dimensions and levels in those report are detailed in Table B.2.

The fields of application include; general defense industrial base contractors, governments, remote working, and air navigation service providers. Application methods are; scoring forms, questionnaires, interviews, and workshops. The questionnaire is the most frequently used method in those reports. There are 14 generic and five specific models. In 3rd party assisted methods, 33,33% of the models are specific. In self-assessed methods, 16,67% of the models are specific.

Figure 5.10 gives the distribution of the evaluation criteria basis used in industry reports. NIST is considered as main criteria basis in majority of the papers (%53,85).

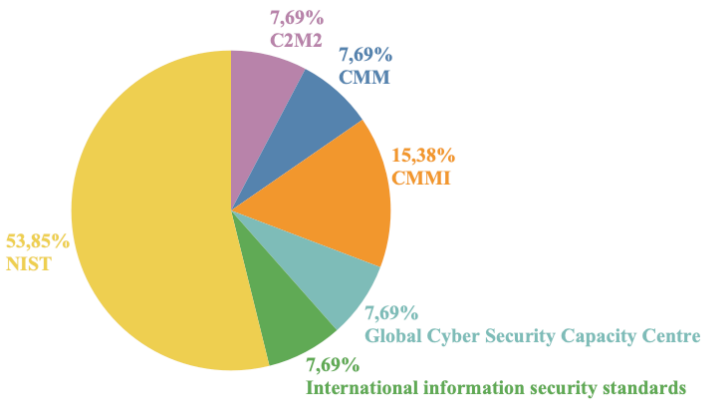

Figure 5.10: Distribution of industry reports by evaluation criteria basis

The list of the dimensions, their percentage, and the number of industry reports, including these dimensions, are provided in Table 5.6. Protection and resiliency, system and infrastructure, recovery and response, strategy and management, identity and access management, operation and technology are industry reports' most frequently used dimensions.

Figure 5.11 illustrates the word cloud about these dimensions. Management, cybersecurity, security, and protection are the most frequent words in dimension.

Table 5.6: Classification of dimensions in industry reports

Name of dimensions	%	# of reports
Protection and Resiliency	9,26%	10
System and Infrastructure	8,33%	9
Recovery, and Respond	8,33%	9
Strategy and Management	7,41%	8
Identity and Access Management	7,41%	8
Operation and Technology	7,41%	8
Other	4,63%	5
Workforce Management	4,63%	5
Leadership	4,63%	5
Training	3,70%	4
Risk Management	3,70%	4
Business and Organization	3,70%	4
Application Security	3,70%	4
Legal and Compliance	3,70%	4
Situational Awareness	2,78%	3
Processes	2,78%	3
Cybersecurity Culture	2,78%	3
Detect	2,78%	3
Data and Governance	2,78%	3
Threat and Vulnerability Management	1,85%	2
Asset Management	1,85%	2
Assessment and Audit	1,85%	2

Figure 5.11: The word cloud of dimensions in industry reports

- **RQ3 : Proposing the Cybersecurity Maturity Model**

The conceptual framework of the proposed model is provided in Figure 5.12. At the end of RQ2, 6 clusters are derived from keyword co-occurrence analysis. At the end of RQ2, 30 factors are determined based on analyzing academic papers and industry reports. Then, by advising the experts, the factors of the proposed model are determined. The proposed CMM is detailed in the next section.

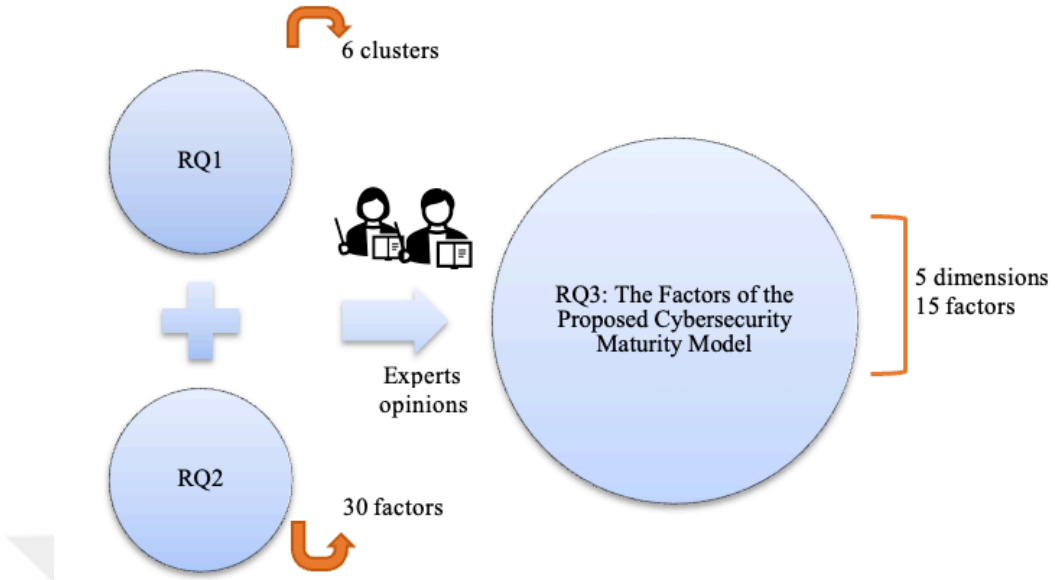

Figure 5.12: The conceptual framework of the proposed model

5.2.3 Critics of the Existing Cybersecurity Maturity Models

In the literature, two review papers have proposed cybersecurity maturity models. Giuca et al. (2021) and Marican et al. (2023) have proposed a model. Marican et al. (2023) conducted a systematic literature review, analyzed the literature using bibliometric maps, and reviewed academic papers and industry reports. Their proposed cybersecurity maturity assessment framework comprises five domains, and the model focuses on SMEs. Giuca et al. (2021) proposed a model applicable to any industry and any size of organization by reviewing the industry reports. Their proposed model comprises eleven evaluation criteria for evaluating cybersecurity risk management frameworks. Garba et al. (2020) conducted a systematic literature review of academic papers. Rabii et al. (2020), Muronga et al. (2019), and Rea-Guaman et al. (2017) reviewed academic papers and industry reports. This study differentiates itself from these studies by the following contributions:

- Proposing a model applicable in any industry and in any size of an organization,
- Proposing a hierarchical model,
- Developing a model based on a systematic literature review of academic

papers and industry reports, bibliometric analysis, and advising expert opinions,

- Including studies from 2000 to 2023.

Therefore, this study is one of the first attempts to propose a cybersecurity maturity model using bibliometric analysis, systematic literature review, and advising experts.

5.3 The Proposed Cybersecurity Maturity Model

The proposed cybersecurity maturity model comprises five dimensions, fifteen factors, and five levels. The first dimension is cybersecurity strategy, risk, and policy; the second one is cybersecurity culture, education, and workforce; the third one is cybersecurity infrastructure; the fourth one is cybersecurity identity, information, and organization; and the fifth one is cybersecurity standards, legislation, regulation, and protection. The proposed cybersecurity maturity model is detailed in Table 5.7 and illustrated in Figure 5.13.

5.3.1 The Factors of the Proposed Cybersecurity Maturity Model

After the determination of 5 dimension, and 15 factors, the sub-factors are determined based on literature review, industry reports, and advising the experts. A total of 60 sub-factors are identified in our proposed CMM to assess cybersecurity maturity of the institutions. The explanations of these factors are detailed in the following section.

Table 5.7: Construction of the proposed CMM

RQ1: Clusters	RQ2: Dimensions in Academic & Industry Papers	RQ3:Dimensions	RQ3: Factors	References
Cluster 6 • Cyber attacks (2) • Design (2) • Cyber-attack (2) • Governance (3) • Perceptions (2) • Safety (3)	• Continuous Improvement • Process, Processes/Techniques • Planning and Analysis • Leadership and Planning, Management Activities • Compliance, Policies, Policies And Standards • Physical Security, Data Governance and Protection, Security Governance • Event And Incident Response, Continuity Of Operations, Incident Response Management • Enterprise Risk Management, Risk Management, Risk Management Process • Assessment and Audit • Threat and Vulnerability Management	1. Cybersecurity Strategy, Risk and Policy	1.1. Cybersecurity Strategy, Planning and Transformation 1.2. Cybersecurity Threat, Risk, Vulnerability Management and Resiliency 1.3. Cyber Policy Compliance and Governance	(Aliyu et al., 2020; Al-Karaki et al., 2020; Allan et al., 2009; Almomani et al., 2021; Bahuguna et al., 2019; CMM, 2021; Edwards, 2018; EuroControl, 2017; Kour & Karim, 2020; KPMG, 2017; Malatji et al., 2020; REBIT, 2017; US DoE, 2019; Vicente Aceituno Canal, 2007; Wirnsperger, Peter; Yildiz, 2017; Yigit Ozkan et al., 2021)
Cluster 5 • Assessment (2) • Awareness (3) • Behavior (2) • Information technology (3) • Organizations (2) • Systems (2)	• Workforce Management • Awareness, Awareness And Training, Education • Capability, Capacity Building, Capacity Building And Awareness • Cybersecurity Culture • Training	2. Cybersecurity Culture, Education and Workforce	2.1. Cybersecurity Awareness, Culture and Capacity Building 2.2. Cybersecurity Training, Education and Skills 2.3. Cybersecurity Workforce Management	(Al-Karaki et al., 2020; Bahuguna et al., 2019; CMMI, 2017; Edwards, 2018; Kour & Karim, 2020; Putra et al., 2020; Results, 2022; Srinivas et al., 2019; Wirnsperger, Peter; Yildiz, 2017)
Cluster 4 • Challenges (5) • Cyber-security (2) • Framework (4) • Future (2) • IoT (3) • Security (4) • Vulnerabilities (2)	• System and Infrastructure, Technical, Technical Measures • Technological, Technologies, Operation and Technology • Information Security Technical Hygiene, Secure Configuration, Application Security	3. Cybersecurity Infrastructure	3.1. Cybersecurity Methodology 3.2. Cybersecurity Systems and Software Security 3.3. Cybersecurity Intelligence	(Bahuguna et al., 2019; Boccardo et al., 2021; Cäsar et al., 2022; Deloitte, 2014; Jaquire & Von Solms, 2017; Spruit & Roeling, 2014; Wirnsperger, Peter; Yildiz, 2017)

Table 5.7: Construction of the proposed CMM (*continue*)

RQ1: Clusters	RQ2: Dimensions in Academic & Industry Papers	RQ3:Dimensions	RQ3: Factors	References
Cluster 3 • Cyber (5) • Cyber threats (2) • Cybersecurity (13) • Knowledge (2) • Management (4) • Readiness (3)	• Business and Organization, Organizational • Identification • Education, Training/Skills Development, Training • Cooperation, Information Sharing • Continuous Vulnerability Management, Mitigation Of External Threats, Threat • Contingency, Identity and Access Management • Recover, Respond, Respond & Recover • Inventory and Control of Hardware Assets • Detect & Diagnostics • Asset, Change, Configuration Management & Asset Management	4. Cybersecurity Identity, Information and Organization	4.1. Cybersecurity Identity, Access and Authorization Management 4.2. Cybersecurity Information Management and Cooperation 4.3. Cybersecurity Organization and Incident Management	(Al-Karaki et al., 2020; Allan et al., 2009; Andreasson et al., 2021; Bahuguna et al., 2019; Barnes & Daim, 2022; Bitzer et al., 2023; CISA, 2021; Multi-State Information Sharing & Analysis Center, 2016; NIST Cybersecurity Framework Team, 2018; Porrúa & Contreras B, 2020; Tokerud, 2022; US DoD, 2020; Zivanovic, Jasmina, 2018)
Cluster 2 • Digitalization (3) • Fourth industrial revolution (2) • Indonesia (2) • Industry 4.0 (3) • Internet of things (IoT) (2) • Maturity (3) • Model (4) • Policies (2) • Sustainability (2)	• Protect, Protect & Detect, Protection and Resiliency • Legal, Legal and Regulatory Measures, Legal/Policies	5. Cybersecurity Standards, Legislation, Regulation and Protection	5.1. Cybersecurity Standards 5.2. Cybersecurity Legal and Regulatory Measures 5.3. Cybersecurity Information Privacy and Protection	(Al-Karaki et al., 2020; Bahuguna et al., 2019; Mattioli & Moulinos, Konstantinos, 2015; Wirnsperger, Peter; Yildiz, 2017)

Figure 5.13: The proposed CMM

- **1. Cybersecurity Strategy, Risk and Policy**

Protecting assets, including people; addressing vulnerabilities in critical infrastructures, and preventing potential cyber-attacks; and completing the transformation needed to have a reliable system where recovery time is shortened and downtime is minimized when a cyberattack occurs (Almomani et al., 2021; Edwards, 2018; EuroControl, 2017; Malatji et al., 2020; Wirnsperger, Peter; Yildiz, 2017; Yigit Ozkan et al., 2021).

- **1.1. Cybersecurity Strategy, Planning, and Transformation:** Organizations must effectively integrate their business requirements with their cybersecurity strategy. The sub-factors below this factor can be explained as (Aliyu et al., 2020; Al-Karaki et al., 2020; Allan et al., 2009; Almomani et al., 2021; Bahuguna et al., 2019; CMM, 2021; Edwards, 2018; EuroControl, 2017; Kour & Karim, 2020; KPMG, 2017; Malatji et al., 2020; REBIT, 2017; US DoE, 2019; Vicente Aceituno Canal, 2007; Wirnsperger, Peter; Yildiz, 2017; Yigit Ozkan et al., 2021):
- **1.1.1. Cybersecurity Strategy:** Cybersecurity strategy should be aligned with business strategy, people, and the organization. A cybersecurity strategy should be comprehensive, proactive, and risk-based, including policies, procedures, guidelines, and technical controls to safeguard information assets. It should also align with the organization's overall mission, goals, and objectives and comply with applicable laws, regulations, and standards. The cybersecurity strategy should be regularly reviewed, updated, and tested to ensure its effectiveness against evolving threats and vulnerabilities.
- **1.1.2. Cybersecurity Program Integration with Business Needs:** It aligns an organization's cybersecurity program with its overall business objectives and needs. This ensures that cybersecurity measures are not implemented in a silo but are integrated into the organization's overall strategy and operations. It is essential to build a robust and effective cybersecurity program aligned with the organization's overall business objectives and needs.
- **1.1.3. Planning and Allocation of Budget for Cybersecurity:** The planning and allocating budget for cybersecurity involves identifying potential risks, assessing the impact of those risks, and allocating resources to mitigate those

risks. This process should be ongoing, with regular reviews and updates to ensure the organization remains protected against emerging threats.

- **1.1.4. Cybersecurity Transformation:** It refers to rethinking and redesigning an organization's cybersecurity program to address emerging threats and improve overall security posture. It involves identifying gaps and weaknesses in existing security measures, evaluating new technologies and solutions, and implementing a comprehensive strategy to mitigate risks. Cybersecurity transformation requires a holistic approach integrating people, processes, and technology to ensure that all aspects of the organization's security program are aligned and working together effectively.
- **1.2. Cybersecurity Threat, Risk, Vulnerability Management and Resiliency:** Existing vulnerabilities in the corporate infrastructure can be detected before the attackers, and security breaches that may cause losses may occur (Sheikh et al., 2022). It is necessary to manage security vulnerabilities well. The sub-factors below this factor can be explained as (Carias et al., 2021; de Neira et al., 2023; Edwards, 2018; Morris et al., 2020):
- **1.2.1. Cybersecurity Threat Management:** It identifies, analyzes, and mitigates potential cyber threats to an organization's information systems and networks. It involves monitoring and analyzing network traffic, system logs, and security alerts to identify potential security breaches, vulnerabilities, and weaknesses in existing security measures. Once a threat has been identified, cybersecurity threat management teams work quickly to contain and mitigate the threat, minimizing the impact on the organization's systems and data.
- **1.2.2. Cybersecurity Risk Management:** It refers to identifying, assessing, and managing risks that could compromise the confidentiality, integrity, or availability of an organization's information assets by examining companies' internal and external data sources with a holistic approach and analytical tools by utilizing data analytics. This process helps organizations to stay proactive in their approach to cybersecurity, which could help prevent costly data breaches and protect the company's reputation.
- **1.2.3. Cybersecurity Vulnerability Management:** It refers to identifying, assessing, prioritizing, and mitigating security vulnerabilities in a system or network. It involves using tools and techniques to scan and analyze systems

for potential weaknesses or flaws that attackers could exploit. Once vulnerabilities are identified, they are prioritized based on their potential impact and likelihood of exploitation and then remediated through patches, configuration changes, or other controls. It is critical to maintain the security and integrity of systems and data and minimize the risk of cyber-attacks.

- **1.2.4. Cybersecurity Resiliency:** Cybersecurity resilience defines an organization's ability to adapt to and counter threats from inside or outside, caused consciously or unconsciously. It involves implementing measures to prevent, detect, and respond to cyber threats and having a plan to recover from any damage caused by such attacks quickly.
- **1.3. Cyber Policy Compliance and Governance:** Any business or function can implement a cybersecurity policy. Still, a higher-level implementation and enterprise viewpoint may help the organization by integrating operations and utilizing resource investments throughout the enterprise (US DoE, 2019). The sub-factors below this factor can be explained as (Aliyu et al., 2020; Bahuguna et al., 2019; Wirnsperger, Peter; Yildiz, 2017):
- **1.3.1. Cybersecurity Program Policy:** Refers to well-established security policies, frameworks, procedures, guidelines, and organizational best practices. This policy should outline the organization's measures to protect sensitive data, prevent cyber-attacks, and respond to security incidents. The policy should also establish roles and responsibilities for employees, contractors, and third-party vendors to ensure everyone knows their obligations and understands the importance of maintaining a secure computing environment.
- **1.3.2. Cybersecurity Governance:** A robust cybersecurity governance framework establishes clear roles, responsibilities, and accountability for managing cybersecurity risks. It fully integrates cybersecurity into an organization's strategy and operations and includes ongoing monitoring and reporting to detect and respond to threats promptly and effectively. This framework enables organizations to confidently reduce their exposure to cyber risks and protect their critical assets from potential attacks.
- **1.3.3. Regular Cybersecurity Policy Internal/External Audits:** The audits assess the organization's compliance with established policies, procedures,

and regulatory requirements by measuring its effectiveness and reporting security incidents. Internal audits are conducted by the organization's own staff, while independent auditors perform external audits. The audits help identify potential vulnerabilities and weaknesses in the organization's cybersecurity program and provide recommendations for improving security.

- **1.3.4. Compliance with Information Security Standards:** Organizations must ensure that their sensitive data and critical assets are well protected against cyber threats. Common information security standards include ISO/IEC 27001, NIST Cybersecurity Framework, and PCI DSS.

- **2. Cybersecurity Culture, Education and Workforce**

The organization's personnel need to be more robust regarding cybersecurity, even with great people and technology in place.

- **2.1. Cybersecurity Awareness, Culture and Capacity Building:** The sub-factors below this factor can be explained as (Al-Karaki et al., 2020; Bahuguna et al., 2019; CMMI, 2017; Edwards, 2018; Kour & Karim, 2020; Putra et al., 2020; Results, 2022; Srinivas et al., 2019; Wirnsperger, Peter; Yildiz, 2017):
- **2.1.1. Cybersecurity Training and Education:** Cybersecurity education and training should be integrated into the organization's overall security strategy and provided to all employees, not just IT staff. There are several types of cybersecurity training and education programs available. Some organizations opt for in-house training programs, while others outsource to third-party providers. Additionally, employees can complete online training programs at their own pace. The content of cybersecurity training and education programs should be tailored to the organization's specific needs and should be updated regularly to reflect new threats and best practices.
- **2.1.2. Innovation, Research, And Development Programs:** The main focus of the innovation, research**,** and development programs is on advancing the field of cybersecurity through the creation of new technologies, tools, and techniques for protecting against cyber threats. These programs typically involve industry, academia, and government agencies collaborating to

develop cutting-edge solutions to complex cybersecurity challenges. These programs provide introductory and highly specialized technical training in cybersecurity, on-site or through a purpose-built platform.

- **2.1.3. Cybersecurity Coaching and Training:** Cybersecurity coaching and training programs aim to produce a skilled and knowledgeable workforce that can help organizations protect their networks, systems, and data from cyber threats. Coaching and training programs can be delivered in various formats, including in-person classes, online courses, and self-paced study.
- **2.1.4. Continuous Improvements in Cybersecurity Skills:** The competence of the security team is influenced by continuous improvement in skills, recruitment of qualified practitioners in the security field, screening of the security workforce, and development of security leadership skills. Continuous improvement in cybersecurity skills involves regularly updating knowledge and skills and staying up-to-date with the latest cybersecurity trends and best practices.
- **2.2. Cybersecurity Training, Education, and Skills:** The sub-factors below this factor can be explained as (Krawczyk-Sokołowska & Caputa, 2023; L. Li et al., 2019; Wirnsperger, Peter; Yildiz, 2017):
- **2.2.1. Situational Awareness Mechanisms:** Situational awareness mechanisms refer to the processes, technologies, and techniques used to gather, analyze, and disseminate information about a particular environment or situation. These mechanisms are designed to provide individuals, organizations, and communities with a comprehensive understanding of their surroundings and the potential threats or opportunities they may encounter. The organization communicates with stakeholders regarding situational awareness during a cyber threat.
- **2.2.2. Cyber-focused Mindset And Cyber-conscious Culture:** The organization should have a cyber-focused mindset and a cyber-conscious culture. This means being aware of the potential risks and threats of using technology and taking steps to protect itself and the organization from cyber-attacks. It involves being vigilant about its online activity, using strong passwords and multi-factor authentication, keeping its software and security systems up to date, and regularly backing up its data.

- **2.2.3 Committed Cybersecurity Team:** A committed cybersecurity team is a group of professionals protecting an organization's digital assets from cyber threats. This team is responsible for developing and implementing cybersecurity policies and procedures, conducting regular security assessments, identifying and mitigating security risks, and responding to and recovering from cyber-attacks.
- **2.2.4. Cybersecurity Capacity Building:** It refers to enhancing the ability of individuals, organizations, and countries to protect themselves against cyber threats. It involves developing the necessary skills, knowledge, and technical capabilities to detect, prevent, and respond to cyber-attacks.
- **2.3. Cybersecurity Workforce Management:** The sub-factors below this factor can be explained as (Al-Karaki et al., 2020; Gartner, 2019):
- **2.3.1. Identification of Appropriate Experts and Policymakers in Government, Private Sector, and Academia:** By engaging with appropriate experts and policymakers, organizations can gain valuable insights into emerging cyber threats and trends and best practices for managing cybersecurity risks. It helps bring together individuals with diverse expertise and experiences, leading to better decision-making and problem-solving. Additionally, having the right experts and policymakers in place ensures that policies are well-informed, effective, and implemented efficiently.
- **2.3.2. Well-defined Cybersecurity Roles:** These refer to clearly defined responsibilities and job descriptions for individuals within an organization who are responsible for managing and implementing cybersecurity policies, procedures, and technologies. Having well-defined roles also helps identify potential gaps or overlaps in responsibilities and tailor security measures to address specific threats.
- **2.3.3. Certification and Promotion of Workforce:** Certification and promotion of the workforce refers to recognizing and validating employees' skills, knowledge, and experience through certification programs and promoting them to higher positions within the organization. The goal is to ensure that employees have the necessary qualifications to perform their duties effectively and efficiently while providing them with opportunities for career advancement and personal growth.

- **2.3.4. Skilled Cybersecurity Team:** The development of security leadership abilities, recruiting qualified security professionals, workforce screening, and continual skill enhancement all impact how competent a security team is. Members of a skilled cybersecurity team should have experience in identifying and analyzing security risks and vulnerabilities, developing and implementing security policies and procedures, monitoring and responding to security incidents, and conducting security audits and assessments.

- **3. Cybersecurity Infrastructure**

Businesses rely on an IT infrastructure that is reliable and secure as the building block for new digital innovations and products. Large amounts of data, a sizable fraction of which will be sensitive, must be continuously acquired, stored, and used by devices connected to corporate infrastructures. Technologies and products selected following the design should be matured to support the institution's business objectives.

- **3.1. Cybersecurity Methodology:** The sub-factors below this factor can be explained as (Bahuguna et al., 2019; Boccardo et al., 2021; Cäsar et al., 2022; Deloitte, 2014; Jaquire & Von Solms, 2017; Spruit & Roeling, 2014; Wirnsperger, Peter; Yildiz, 2017):
- **3.1.1. Cryptography:** Cryptography is the practice of securing communication from unauthorized access or interference. It involves techniques such as encryption, decryption, and code-breaking to protect information from being read or modified by unauthorized parties.
- **3.1.2. Infrastructure Protection and Firewall Management:** The IT infrastructure and operation should follow the organization's priorities. Firewall management refers to the process of configuring, monitoring, and maintaining a firewall in order to ensure that it is providing effective protection against unauthorized access to a network or device.
- **3.1.3. Physical Asset Management:** Physical asset management is an important aspect of cybersecurity. It involves identifying, tracking, and managing physical assets such as servers, routers, switches, and other network devices. These assets are critical components of an organization's IT

infrastructure and must be protected from physical threats such as theft, damage, or unauthorized access. The technologies and products selected following this design should be matured and managed in the most appropriate way to support the business objectives of the organization.

- **3.1.4. Enterprise Cybersecurity Architecture:** The goal of an enterprise cybersecurity architecture is to provide a holistic approach to cybersecurity by ensuring that all areas of the organization are protected against potential cyber threats. This approach helps to minimize the risk of data breaches, cyber-attacks, and other cybersecurity incidents.
- **3.2. Cybersecurity Systems and Software Security:** The sub-factors below this factor can be explained as follows (Cäsar et al., 2022; Wirnsperger, Peter; Yildiz, 2017):
- **3.2.1. Secure Software Development Life Cycle (Secure-SDLC):** Today, the importance of software security is increasing with the widespread use of the internet and mobile devices. It is necessary to integrate source code analysis into the Software Development Life Cycle (SDCL) to meet software in your organization, to create a continuous control environment, to ensure that the software has appropriate security features and that the assurance provided by the software development process is at the expected level.
- **3.2.2. Systems and Applications Security:** Applications are essential to every information technology environment. Ensuring their protection requires secure design, implementation, and configuration.
- **3.2.3. Network Security:** Implementing internal and external network security controls is the first step in protecting organizations' digital assets. Once these controls are in place, their adequacy and effectiveness should be regularly tested.
- **3.2.4. Cloud and Mobile Security:** The deployment of cloud technology is no different from the deployment of other IT functions. A good governance model and architecture should be designed and implemented. However, the governance model should be feasible and designed in a way that does not undermine the benefits of cloud technology.
- **3.3. Cybersecurity Intelligence:** The sub-factors below this factor can be explained as (Deloitte, 2014; Wirnsperger, Peter; Yildiz, 2017) (Gaehtgens et

al., 2022):

- **3.3.1. Advanced Cyber-Threat Readiness and Preparation:** Threat techniques evolve daily in volume, intensity, and sophistication as hackers seek new vulnerabilities in software to compromise key systems across organizations.
- **3.3.2. Systems Testing/ DDoS Testing:** DDoS/DoS (Denial of Service) testing is a type of security testing that simulates a DDoS attack on a network or website to identify vulnerabilities and test the effectiveness of DDoS mitigation strategies. DDoS attacks are a type of cyber-attack that involves overwhelming a network or website with traffic from multiple sources, making it unavailable to legitimate users. DDoS testing involves simulating a DDoS attack using various tools and techniques to test the resilience of a network or website under such an attack.
- **3.3.3. Cyber Threat Intelligence:** Cyber threat intelligence is evidence-based information (e.g., context, mechanisms, indicators, inferences, and recommendations for action) about current or emerging threats or hazards to assets.
- **3.3.4. Red-Teaming:** With advanced cyber threat simulation (i.e., red teaming), it is possible to simulate a comprehensive cyber-attack that tests the organization's prevention, detection, and response mechanisms. It involves the three critical elements of security: physical, cyber, and human.

- **4. Cybersecurity Identity, Information and Organization**

Since cybersecurity is a worldwide issue, collaboration and partnership with regional, national, and international organizations are essential. Additionally, networks for information sharing and cooperative frameworks will encourage cooperation (Al-Karaki et al., 2020).

- **4.1. Cybersecurity Identity, Access and Authorization Management:** Identity and access management offers tools, procedures, and techniques to improve online transaction security while reducing user friction. The sub-factors below this factor can be explained as (Al-Karaki et al., 2020; Allan et

al., 2009; Andreasson et al., 2021; Bahuguna et al., 2019; Barnes & Daim, 2022; Bitzer et al., 2023; CISA, 2021; Multi-State Information Sharing & Analysis Center, 2016; NIST Cybersecurity Framework Team, 2018; Porrúa & Contreras B, 2020; Tokerud, 2022; US DoD, 2020; Zivanovic, Jasmina, 2018):

- **4.1.1. Identity Management and Access Control:** Organizations whose identity and access management processes are not well managed are a blessing for attackers in the digital world. Identity Management and Access Control form the foundation of a comprehensive cybersecurity strategy, helping organizations to protect their sensitive data and resources from unauthorized access and data breaches.
- **4.1.2. Two-Factor/Multi-Factor Authentication:** It is a security measure that requires users to provide two or more forms of identification to access a system or application by adding an extra layer of security to prevent unauthorized access to sensitive information or accounts.
- **4.1.3. Access Control and Authorization:** Access control can be defined as determining who has access to what resources within a system. Authorization, on the other hand, refers to determining what actions a user can perform once they have been granted access to a particular system or resource. It is necessary to design the processes that should be in place and then automate the operations with the help of applications ensuring that only authorized users can access sensitive data or perform specific actions within a system.
- **4.1.4. Automated Reporting Mechanisms:** These refer to systems and tools that automate generating and distributing reports. These mechanisms are designed to streamline the reporting process, save time and resources, and improve the accuracy and consistency of reports.
- **4.2. Cybersecurity Information Management and Cooperation:** Information and data are managed consistently with the organization's risk strategy to protect information confidentiality, integrity, and availability. The sub-factors below this factor can be explained as (NIST Cybersecurity Framework Team, 2018):
- **4.2.1. Integrity of Cybersecurity Information over the Organization:** Information and records (data) are managed consistently with the

organization's risk strategy to protect information confidentiality, integrity, and availability. In addition, collaborative frameworks and information-sharing networks will support collaboration.

- **4.2.2. Confidence/Privacy Based Data Management:** It is a data management approach that prioritizes the protection of privacy and confidentiality of sensitive data. This approach involves implementing strict access controls, encryption, and other security measures to ensure that only authorized personnel can access the data.
- **4.2.3. Cooperation with Stakeholders and Agencies for Cybersecurity:** It refers to the collaborative efforts between different entities, such as businesses, governments, and individuals, to ensure the security and protection of digital assets and systems. By working together, stakeholders and agencies can share information, resources, and expertise to identify threats, prevent attacks, and respond to cybersecurity incidents effectively. This approach helps to establish a more resilient and secure environment for all parties involved.
- **4.2.4. International Cooperation and/or Engagement:** The collaborative efforts and interactions between countries or international organizations to achieve common goals or solve global issues can be defined as international cooperation and/or engagement. It can take various forms, such as diplomatic negotiations, joint research, aid programs, cultural exchanges, and trade agreements. The aim is to promote mutual understanding, peaceful relations, and shared prosperity among nations.
- **4.3. Cybersecurity Organization and Incident Management Cybersecurity:** Organization management enables consistent process execution and is a foundation for the organization's cumulative, long-term benefits (NIST Cybersecurity Framework Team, 2018). The sub-factors below the this factor can be explained as (Al-Karaki et al., 2020; US DoD, 2020):
- **4.3.1. Establishing Standard Workflows of Cybersecurity Processes:** Written procedures/workflows should be established to ensure a more standardized and controlled operation of processes. Without standardization, cybersecurity teams may struggle to manage security incidents effectively,

leading to increased risk of cyber-attacks and data breaches. Standard workflows ensure that all security incidents are handled consistently and methodically, which helps to reduce errors and improve response times

- **4.3.2. Comparison with Best Practices:** The controls in the processes should be benchmarked against best cybersecurity practices. By comparing with best practices, organizations can ensure that they follow the latest security guidelines and protect their sensitive information against cyber threats. It is crucial to maintain a robust cybersecurity posture and safeguard against potential cyber-attacks.
- **4.3.3. Business Continuity Management Plan (Disaster Recovery Plan and Implementation):** A business continuity plan summarizing relevant individuals and teams' resources, procedures, activities, and responsibilities should be prepared. It helps organizations recover from significant disruptions, such as natural disasters, cyber-attacks, or other unforeseen incidents. The goal is to minimize the impact of any disruption and ensure that the organization can continue to operate with as little disruption as possible.
- **4.3.4. Cybersecurity Incident Management (Real-Time Logging and Inspection):** The primary objective of security incident management is to develop a well-understood and predictable response to malicious events and computer intrusions. It includes technical actions, management responses to incidents, and public relations efforts. Real-time logging and inspection refers to the practice of monitoring and analyzing system logs in real-time to identify and troubleshoot issues as they occur. This allows system administrators and developers to keep a close eye on their systems and applications, quickly identify and resolve any problems, and improve overall system performance and reliability. By using real-time logging and inspection tools, administrators and developers can gain valuable insights into how their systems perform and make informed decisions about optimizing and improving them.
- **5. Cybersecurity Standards, Legislation, Regulation and Protection**

All organizations can set up a unified legal system with the help of a legislative framework. Cybersecurity standards measure the ability to implement a framework that captures international cybersecurity standards.

- **5.1. Cybersecurity Standards:** The sub-factors below this factor can be explained as (Al-Karaki et al., 2020; Bahuguna et al., 2019; Mattioli & Moulinos, Konstantinos, 2015; Wirnsperger, Peter; Yildiz, 2017):
- **5.1.1. Cooperation and Coordination with National/International Teams (e.g., CERT/CIRT/CSIRT):** Cooperation and Coordination with National/International Teams refers to the process of working together with other teams and organizations in order to develop a better understanding of information security threats, and to share information on how to mitigate them. This may involve collaborating with national or international teams such as Computer Emergency Response Teams (CERTs), Computer Incident Response Teams (CIRTs), or Computer Security Incident Response Teams (CSIRTs) to exchange information on cyber-attacks, vulnerabilities, and other security incidents. By working together and sharing information, organizations can improve their response times, better manage cyber risks, and ultimately enhance their overall cybersecurity posture.
- **5.1.2. Adherence to Standards (ISO/IEC 27001:2013/SOC2):** It refers to the compliance of an organization's information security policies and procedures with the guidelines established by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC). SOC2 is a type of audit report that evaluates an organization's information systems and procedures based on the Trust Services Criteria (TSC) established by the American Institute of Certified Public Accountants (AICPA). Compliance with standards is important for organizations to ensure that their information security practices meet the industry's best practices and are aligned with the legal and regulatory requirements.
- **5.1.3. Periodic Cybersecurity Tests (e.g., Pentest and Social Engineering Tests):** Pentest, short for penetration testing, is a method of evaluating the security of a computer system or network by simulating an attack from a malicious source. Pentesting can be done using various techniques, including manual testing by security experts and automated tools. Social engineering tests, on the other hand, are a type of security test that involves attempting to manipulate people into divulging confidential information or performing actions that could compromise the security of a system or network. This can

include techniques such as phishing emails, phone calls, or in-person interactions. Social engineering tests aim to identify weaknesses in an organization's security awareness training and policies and to help improve employee awareness of security risks.

- **5.1.4. Certification:** Certification measures whether an internationally recognized cybersecurity certification and accreditation program is in place for professionals in the organization. The goal of certification is to provide assurance to stakeholders that the organization has implemented effective cybersecurity measures to protect against cyber threats.
- **5.2. Cybersecurity Legal and Regulatory Measures:** Laws are introduced by cybercrime legislation to address unlawful access to computers, systems, and data. The sub-factors below the "factor can be explained as (Al-Karaki et al., 2020; Smith et al., 2021):
- **5.2.1. Legal Compliance Roadmap:** A legal compliance roadmap is a plan that outlines the steps an organization needs to take to ensure that it is operating in compliance with all relevant laws and regulations. The goal of a legal compliance roadmap is to minimize legal and regulatory risk, protect the organization from liability, and ensure that the organization is operating in an ethical and responsible manner.
- **5.2.2. Cybercriminal Legislation:** Cybercrime legislation enacts laws to deal with unauthorized access to computers, systems, and data. These laws can be partial or comprehensive, where partial legislation refers to the existing simple criminal law or code, while comprehensive legislation has specific laws to deal with particular aspects of computer crime.
- **5.2.3. Compliance with Government Regulations:** Regulations deal with data protection, breach notification, certification, and standardization requirements. The purpose of these regulations is to ensure that businesses operate fairly and safely, and that they do not engage in activities that are harmful to the public or the environment. Compliance with government regulations is important not only to avoid legal penalties and fines but also to maintain a good reputation and build trust with customers and stakeholders.
- **5.2.4. Formal/Informal Cooperation to Cybercrime:** Formal mechanisms for international cooperation include bilateral, regional, and multilateral

cybercrime agreements. Formal cooperation to cybercrime refers to the legal and official agreements between two or more countries or organizations to combat cybercrime. On the other hand, informal cooperation to cybercrime refers to the non-legal and unofficial collaborations between different entities to address cybercrime. This could involve sharing of information or intelligence, or even joint operations to investigate and prevent cybercrime.

- **5.3. Cybersecurity Information Privacy and Protection:** Organizations must be able to use, analyze, and share their data while complying with invasive regulatory control requirements and employee and consumer privacy expectations. The sub-factors below this factor can be explained as (Schlatt et al., 2023; Wirnsperger, Peter; Yildiz, 2017):
- **5.3.1. Data Classification and Data Ownership:** Organizations must be able to use, analyze, and share their data while ensuring compliance with invasive regulatory control and customer/employee privacy expectations. Data classification refers to the process of categorizing data based on its level of sensitivity and the degree of protection required. This helps organizations ensure that sensitive data is handled appropriately and protected from unauthorized access. Establishing clear data ownership is important to ensure data privacy, security, and compliance with relevant regulations.
- **5.3.2. Data Protection Laws:** Increased reliance on effective data use and increased regulatory and control requirements such as the General Data Protection Regulation (GDPR) place significant operational pressure on organizations. This requires a holistic and integrated approach to data privacy in a highly fragmented environment. Furthermore, organizations are expected to keep personal and corporate data private, yet data breaches still occur. Common challenges are identifying the organization's business-critical information and ensuring that it is adequately protected in a world where rapid information exchange is integral to business success.
- **5.3.3. Data Leakage Protection (DLP):** DLP refers to the set of measures and technologies put in place to prevent unauthorized access, transmission, or exposure of sensitive and confidential information. It involves implementing policies and procedures to control the flow of data both within and outside an organization to minimize the risk of data breaches, theft, or loss. Some

common examples of Data Leakage Protection measures include encryption, access controls, data backup and recovery, and monitoring systems to detect and respond to potential threats in real-time.

- **5.3.4. System Tightening and Configuration Management:** System tightening refers to the process of securing a computer system by reducing its attack surface and minimizing vulnerabilities. Configuration management, on the other hand, is the process of managing the configuration of a system or software application throughout its lifecycle. This involves identifying and tracking changes to the system or application, ensuring that all components are properly configured and integrated, and maintaining documentation of the system's configuration.

5.3.2 The Levels of the Proposed Cybersecurity Maturity Model

The maturity levels indicate the actual situation of the organization in terms of cybersecurity. Figure 5.14 illustrates the maturity levels and their explanations in the following section.

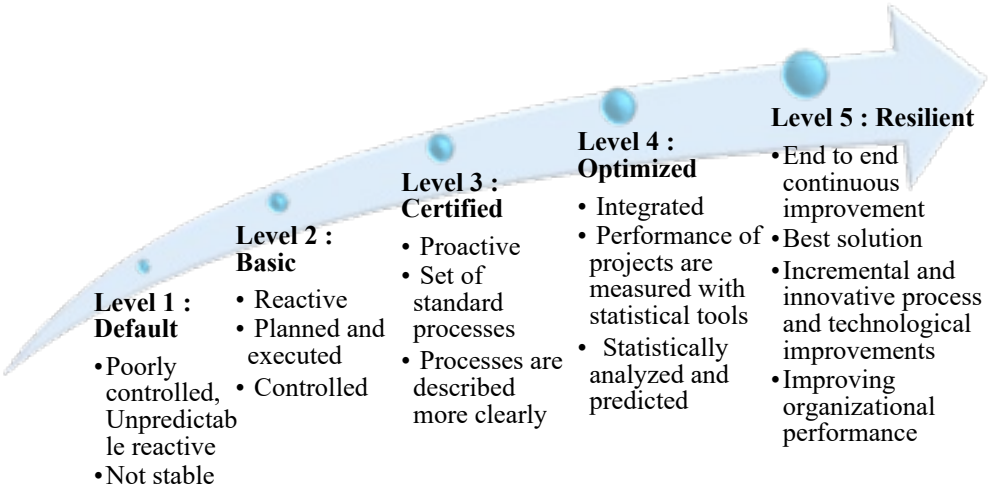

Figure 5.14: The levels in the proposed CMM

- **Level 1: Default**

At maturity level 1, processes are usually ad hoc and chaotic. The organization usually does not provide a stable environment to support processes. Success in these organizations depends on the competence and heroics of the people in the organization and not on the use of proven processes. Despite this chaos, maturity level 1 organizations often produce products and services that work but frequently exceed the budget and schedule documented in their plans. Maturity level 1 organizations tend to overcommit, abandon their processes in a crisis, and be unable to repeat their successes.

- **Level 2: Basic**

At maturity level 2, the projects have ensured that processes are planned and executed by the policy; they employ skilled people with adequate resources to produce controlled outputs; involve relevant stakeholders; are monitored, controlled, and reviewed; and are evaluated for adherence to their process descriptions. The process discipline reflected by maturity level 2 helps to ensure that existing practices are retained during times of stress. When these practices are in place, projects are performed and managed according to their documented plans. Also, at maturity level 2, the status of the work products is visible to management at defined points (e.g., at significant milestones, after major tasks). Commitments are established among relevant stakeholders and are revised as needed. Work products are appropriately controlled. The work products and services satisfy their specified process descriptions, standards, and procedures.

- **Level 3: Certified**

At maturity level 3, processes are well characterized and understood and are described in standards, procedures, tools, and methods. The organization’s standard processes, the basis for maturity level 3, is established and improved over time. These standard processes are used to establish consistency across the organization. Projects establish their defined processes by tailoring the organization’s standard processes according to the guidelines. At maturity level 3, the organization further improves its processes related to the maturity level 2 process areas. Generic practices associated with generic goal 3 that were not addressed at maturity level 2 are applied to achieve maturity level 3.

- **Level 4: Optimized**

At maturity level 4, the organization and projects establish quantitative objectives for quality and process performance and use them as criteria in managing projects. Quantitative objectives are based on the needs of the customer, end users, organization, and process implementers. Quality and process performance is understood in statistical terms and is managed throughout the life of projects. For selected subprocesses, specific measures of process performance are collected and statistically analyzed. When selecting subprocesses for analyses, it is critical to understand the relationships between different subprocesses and their impact on achieving the objectives for quality and process performance. Such an approach helps to ensure that subprocess monitoring using statistical and other quantitative techniques is applied to where it has the most overall value to the business. Process performance baselines and models can be used to help set quality and process performance objectives that help achieve business objectives.

- **Level 5: Resilient**

At maturity level 5, an organization continually improves its processes based on a quantitative understanding of its business objectives and performance needs. The organization uses a quantitative approach to understand the inherent variation and the causes of process outcomes.

Maturity level 5 focuses on continually improving process performance through incremental and innovative process and technological improvements. The organization's quality and process performance objectives are established, continually revised to reflect changing business objectives and organizational performance, and used as criteria in managing process improvement. The effects of deployed process improvements are measured using statistical and other quantitative techniques and compared to quality and process performance objectives. The project's defined processes, the organization's standard processes, and supporting technology are targets of measurable improvement activities. At maturity level 5, the organization is concerned with overall organizational performance using data collected from multiple projects. Analysis of the data identifies shortfalls or gaps in performance. These gaps are used to drive organizational process improvement that generates measurable performance improvement.

5.4 Incomplete Hesitant Fuzzy Linguistic AHP Method and Bonferroni Means Operator

The incomplete HFPR-AHP technique with HFL Bonferroni means is used for calculating the weight of the cybersecurity maturity factors' weights. The following sections provides the computational steps of the proposed methodology.

The consecutive steps of the incomplete HFPR-AHP method with the HFLBM aggregation operator are explained next:

The criteria are formulated as $X = \{x_1, x_2, ..., x_n\}$ with n indicating the number of criteria. The decision-making team is built as $D = \{d_1, d_2, ..., d_k\}$ with k DMs.

Step 1. First, DMs provide incomplete HFPRs by expressing their opinions by using expressions such as "*Lower than* s_i", *"Greater than* s_i*", "At least* s_i*",* "*At most* s_i*", "Between* s_i *and* s_j*"* and the linguistic terms listed in Figure 5.15. These expressions are then expressed as a HFE $h_{ij} = \left\{h_{ij}^{\sigma(s)} | s = 1,2, \dots, l_{h_{ij}}\right\}$.

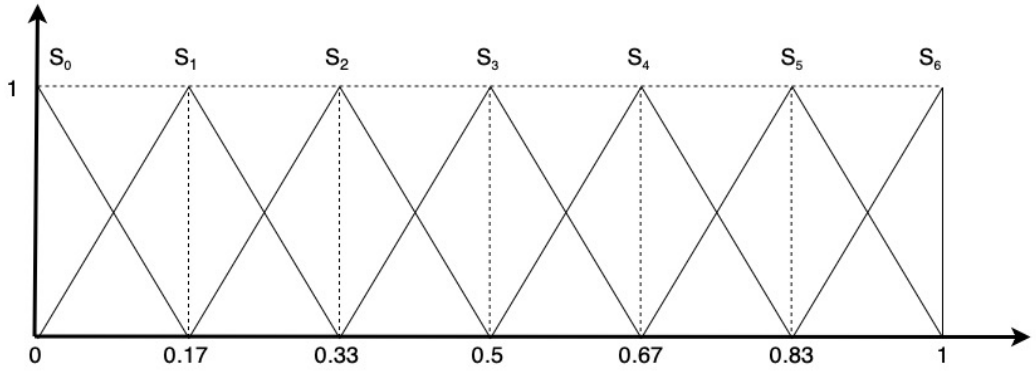

Figure 5.15: Linguistic scale (Beg & Rashid, 2013)

Step 2. The normalized incomplete HFPRs $\overline{H} = (\overline{h}_{ij})_{nxn}$ is obtained by *Definition 3.11.*

Step 3. The individual complete HFPRs are estimated by the following procedure. First, each missing element $h_{j_{k-1}j_k}$ in $H = (h_{ij})_{nxn}$ is transformed into a normalized HFE $\overline{h}_{j_{k-1}j_k}$. Then, a sequence of HFEs that include one and only unknown HFE is located in

the middle of the sequence. Then, the missing element is estimated as $\dot{\bar{h}}_{j_{k-1}j_k} = \{\dot{\bar{h}}^{\sigma(s)}_{j_{k-1}j_k} | s = 1,2, \dots, l\}$ where (Z. Zhang et al., 2015):

$$\dot{\bar{h}}^{\sigma(s)}_{j_{k-1}j_k} = \frac{1}{L}\sum_{i<j_1<j_2<\cdots<j_t}\left(\frac{t+1}{2} - \left(\bar{h}^{\sigma(s)}_{ij_1} + \bar{h}^{\sigma(s)}_{j_1j_2} + \cdots + \bar{h}^{\sigma(s)}_{j_{k-2}j_{k-1}} + \bar{h}^{\sigma(s)}_{j_kj_{k+1}} + \cdots + \bar{h}^{\sigma(s)}_{j_{t-1}j_t} + \bar{h}^{\sigma(l-s+1)}_{j_ti}\right)\right) \quad (5.1)$$

For all $\bar{h}_{ij_1}, \bar{h}_{j_1j_2}, \dots, \bar{h}_{j_{k-2}j_{k-1}}, \bar{h}_{j_kj_{k+1}}, \dots, \bar{h}_{j_{t-1}j_t}, \bar{h}_{j_ti} \in \Omega$.

If $j_{k-1} > j_k$; $\bar{h}_{j_{k-1}j_k}$is the last value in the sequence, and $\bar{h}_{j_{k-1}j_k}$ is equal to $\bar{h}_{j_ti}$. In this situation, it can be estimated as $\dot{\bar{h}}_{j_{k-1}j_k} = \{\dot{\bar{h}}^{\sigma(s)}_{j_{k-1}j_k} | s = 1,2, \dots, l\}$ by employing (3.12), where:

$$\dot{\bar{h}}^{\sigma(s)}_{j_{k-1}j_k} = \frac{1}{L}\sum_{i<j_1<j_2<\cdots<j_t}\left(\frac{t+1}{2} - \left(\bar{h}^{\sigma(l-s+1)}_{ij_1} + \bar{h}^{\sigma l-s+1}_{j_1j_2} + \cdots + \bar{h}^{\sigma l-s+1}_{j_{t-1}j_t}\right)\right) \quad (5.2)$$

For all $\bar{h}_{ij_1}, \bar{h}_{j_1j_2}, \dots, \bar{h}_{j_{t-1}j_t} \in \Omega$.

Ω is the set of all the known HFEs in $\bar{H} = (\bar{h}_{ij})_{nxn}$; L is the number of eligible sequence $\bar{h}_{ij_1}, \bar{h}_{j_1j_2}, \dots, \bar{h}_{j_ti} (i < j_1 < j_2 < \cdots < j_t)$; $\bar{h}_{j_kj_{k-1}}$can be estimated as $\dot{\bar{h}}_{j_{k-1}j_k} = \{\dot{\bar{h}}^{\sigma(s)}_{j_{k-1}j_k} | s = 1,2, \dots, l\}$ by employing (7), where (Z. Zhang et al., 2015):

$$\dot{\bar{h}}^{\sigma(s)}_{j_kj_{k-1}} = 1 - \dot{\bar{h}}^{\sigma(s)}_{j_{k-1}j_k} \quad (5.3)$$

Step 4. A collective HFPR $H_c = (h_{S,c})_{nxn}$ can be derived from individual HFPRs. The collective HFPR is obtained by using the HFLBM operator.

Let $S = \{s_t \,|t = -\tau, \dots, -1,0,1, \dots, \tau\}$ be a finite and totally ordered discrete linguistic term set, $h_s = \{s_t \,|t \in [-\tau, \tau]\}$ be a Hesitant Fuzzy Linguistic Element (HFLE), and $H = \{\gamma \,|\gamma \in [0,1]\}$ be a HFS. Then, the linguistic variable s_t that expresses the equivalent information to the membership degree γ is obtained with the following function g as (Gou et al., 2017):

$$g: [-\tau, \tau] \rightarrow [0,1],$$

$$g(s_t) = \frac{t}{2\tau} + \frac{1}{2} = \gamma \tag{5.4}$$

The membership degree γ that expresses the equivalent information to the linguistic variable s_t is obtained with the following function g^{-1} as (Gou et al., 2017):

$$g^{-1}: [0,1] \rightarrow [-\tau, \tau],$$

$$g^{-1}(h_\gamma) = \{g^{-1}(h_\gamma) = s_{(2\gamma-1)\tau} | \gamma \in [0,1]\} = h_S \tag{5.5}$$

Let $p, q > 0$ and h_{Si} $(i = 1,2, \dots, n)$ be a collection of HFLEs.

If

$$HFLB^{p,q}(h_{S1}h_{S1}, \dots, h_{Sn}) =$$

$$g^{-1}\left(\left(\frac{1}{n(n-1)}\left(\oplus_{i,j=1,i\neq j}^{n}\left(\left(g(h_{Si})\right)^p \otimes \left(g(h_{Sj})\right)^q\right)\right)\right)^{\frac{1}{p+q}}\right) \tag{5.6}$$

then, the $HFLB^{p,q}$ can be called a HFLBM operator (Gou et al., 2017).

Then, the score function is used to finalize the aggregation process as (Gou et al., 2017):

$$s(h_s) = \frac{1}{l}\sum_{i=1}^{l} g(s_t) \tag{5.7}$$

can be called the score function of h_s, where l is the number of the elements of h_s.

Step 5. The consistency ratios of the collective matrices are verified. The following equations are used to calculate the consistency ratio *(CR)* (Saaty, 1990)*:*

$$CI = \frac{\lambda_{max}-n}{n-1} \tag{5.8}$$

$$CR = \frac{CI}{RI} \tag{5.9}$$

CI signifies the consistency index, and the matrix's largest eigenvector is symbolized by λ_{max}, while *n* symbolizes the number of criteria, and *RI* signifies the random index, which varies as the matrix's dimension changes. The *CR* value must be less than 0.1 to accept the results. If the evaluations are inconsistent, experts are asked to reevaluate the criteria/alternatives until the consistency is achieved. If they are consistent, next step begins directly.

Step 6. The normalized pairwise comparison matrix (A) is calculated as follows:

$$\bar{a}_{jk} = \frac{a_{jk}}{\sum_{i=1}^{m} ajk} \tag{5.10}$$

Step 7. The weights of the main criteria and local weights of sub-criteria are calculated as follows:

$$w_j = \frac{\sum_{i=1}^{m} \bar{a}_{jk}}{m} \tag{5.11}$$

Where w_j is a m-dimensional column vector.

Step 8. Each sub-criteria global weight are computed:

$$w_j^G = w_j^{main} * w_j^L \tag{5.12}$$

where w_j^G is the global weight of sub-criteria, w_j^{main} is the weight of main-criteria, w_j^L is the local weight of sub-criteria.

Step 9. Cybersecurity Maturity Score Calculation- Experts respond to the questions in the questionnaire (please refer to Table B.3, Appendix B) about the factors of the proposed CMM framework. After getting the responses, the cybersecurity maturity score of the institution is calculated with the following equation (Schumacher et al., 2016):

$$M_D = \frac{\sum_{i=1}^{n} M_{DIi} * g_{DIi}}{\sum_{i=1}^{n} g_{DIi}} \tag{5.13}$$

where M denotes the maturity, D denotes the dimension, n denotes the number of the maturity factors, I denotes the factor, and g denotes the weighting factor.

5.5 Cybersecurity Maturity Assessment of Public Institutions

This case study is motivated by the real-world necessity of public institutions in Türkiye. The cybersecurity maturity levels of four public institutions that have invested in cybersecurity were evaluated by collecting data from three DMs. The GDM approach is preferred because it removes partiality in decision-making by aggregating different DMs' evaluations of criteria and alternatives. However, DMs may be unfamiliar with a particular object or unwilling to express their opinions sometimes, where their evaluations could be constructed as incomplete HFPRs. The decision-making committee comprised

three DMs with experience in different sectors and backgrounds. The first DM is a cybersecurity specialist, founder, and chairman of a cybersecurity R&D company who completed his undergraduate and graduate education in engineering departments of universities, has an information security and risk management background, has realized many projects on cybersecurity in the public and private sectors, and has worked on the advisory boards of public institutions. The second DM is an engineer in an R&D company who has an engineering and information management background and has worked as a security consultant. The third DM is a manager in an R&D company with an information security and cybersecurity infrastructure background, who has realized several projects on cybersecurity and cyber threats and has technical knowledge of computer programs. The names of these four public institutions cannot be shared because of privacy and security concerns. These public institutions operate in the information technology (IT), finance, energy, and health sectors.

Step 1: DMs evaluated the criteria using the linguistic scale in Figure 5.15. DMs cannot express their opinions at some points where incomplete HFPRs handle this situation. An example evaluation for the sub-factors in "1.1. Cybersecurity Strategy, Planning and Transformation" is provided in Table 5.8.

Table 5.8: The evaluations for Cybersecurity Strategy, Planning and Transformation

DM1	1.1.1.	1.1.2.	1.1.3.	1.1.4.
1.1.1. Cyber Strategy and Capability Assessment		Between M and VH	At least H	Between H and P
1.1.2. Security Program Integration with Business Needs			At least VH	Greater than H
1.1.3.Allocation of Budget for Cybersecurity				Between VL and L
1.1.4. Cybersecurity Governance				
DM2				
1.1.1. Cyber Strategy and Capability Assessment		Between M and VH	At least VH	At least VH
1.1.2. Security Program Integration with Business Needs			x	x
1.1.3.Allocation of Budget for Cybersecurity				x
1.1.4. Cybersecurity Governance				
DM3				
1.1.1. Cyber Strategy and Capability Assessment		Between L and M	At least H	Greater than H
1.1.2. Security Program Integration with Business Needs			Between L and M	x
1.1.3.Allocation of Budget for Cybersecurity				Between VL and L
1.1.4. Cybersecurity Governance				

Step 2. Normalized incomplete HFPRs, $\bar{H} = (\bar{h}_{ij})_{nxn}$ is obtained. The optimized parameter ç was set to 1.

Step 3. Individual complete HFPRs were assessed. For example, in Table 3, in DM3's evaluation $\bar{h}_{24}$ is incomplete. 2 sequences are determined as $\{\bar{h}_{12,}\, \bar{h}_{24}, \bar{h}_{41}\}$, and $\{\bar{h}_{31}, \bar{h}_{12}, \bar{h}_{24}, \bar{h}_{41}\}$ where $\bar{h}_{12} = \{0.33,0.5,0.5\}$, $\bar{h}_{31} = \{0,0.17,0.33\}$, and $\bar{h}_{41} = \{0,0.17,0.33\}$. $\bar{h}_{24}$ is estimated as $\{1.09, 0.995,1.585\}$, by using Equations (5.1)-(5.3). In this way, the complete matrices are obtained.

Step 4. HFL Bonferroni mean operator is applied to aggregate DMs' opinions. Equations (5.4)-(5.7) are employed, and the collective matrix is obtained. Table 5.9 presents the collective matrix for "1.1. Cybersecurity Strategy, Planning and Transformation".

Table 5.9: The collective matrix for Cybersecurity Strategy, Planning and Transformation

	1.1.1.	1.1.2.	1.1.3.	1.1.4.
1.1.1. Cyber Strategy and Capability Assessment	1.00	0.587	0.820	0.820
1.1.2. Security Program Integration with Business Needs	1.70	1.00	0.706	0.621
1.1.3.Allocation of Budget for Cybersecurity	1.22	1.42	1.00	0.338
1.1.4. Cybersecurity Governance	1.22	1.61	2.96	1.00

Step 5. The consistency ratios of the collective matrices were determined by implementing (17)-(18). $CR_{1.1.}$=0.076, $CR_{1.2.}$=0.037, $CR_{1.3.}$=0.045, $CR_{2.1.}$=0.022, $CR_{2.2.}$=0.021, $CR_{2.3.}$=0.021, $CR_{3.1.}$=0.053, $CR_{3.2.}$=0.034, $CR_{3.3.}$=0.080, $CR_{4.1.}$=0.049, $CR_{4.2.}$=0.015, $CR_{4.3.}$=0.017, $CR_{5.1.}$=0.057, $CR_{5.2.}$=0.026, $CR_{5.3.}$=0.057. All of the matrices were consistent.

Steps 6-8. The weights of the CMM factors are calculated by employing Equations (5.8)-(5.12). The weights of the factors are provided in Table 5.10.

Step 9. By using the responses in the questionnaire (see Appendix) and the factors' weights, the cybersecurity maturity score of the institution is calculated by Equation (5.13). For example, for the health sector, the maturity score of the institution for the first factor is calculated as:

$$M_{D1.1} = \frac{(0.0575 * 4.25 + 0.0675 * 4.25 + 0.0636 * 3 + 0.01114 * 3.25)}{(0.0575 + 0.0675 + 0.0636 + 0.1114)} = 3.614$$

In the same way, other factors are calculated. $M_{D1.2} = 3.413$, $M_{D1.3} = 4.073$, $M_{D2.1} = 3.000$, $M_{D2.2} = 2.977$, $M_{D2.3} = 3.391$, $M_{D3.1} = 3.672$, $M_{D3.2} = 2.983$, $M_{D3.3} = 2.875$, $M_{D4.1} = 3.129$, $M_{D4.2} = 3.177$, $M_{D4.3} = 3.141$, $M_{D5.1} = 4.289$, $M_{D5.2} = 4.500$, and $M_{D5.3} = 3.4711$.

The maturity scores of public institutions are provided in Table 5.11, and their maturity levels are illustrated in Figure 5.16 and Figure 5.17.

Table 5.10: The weights of CMM factors

Dimensions	Weights	Factors	Weights	Sub-Factors	Local Weights	Global Weights
1. Cybersecurity Strategy, Risk and Policy	0.3	1.1. Cybersecurity Strategy, Planning and Transformation	0.3	1.1.1. Cybersecurity Strategy	0.192	0.057
				1.1.2. Cybersecurity Program Integration with Business Needs	0.225	0.068
				1.1.3. Planning and Allocation of Budget for Cybersecurity	0.212	0.064
				1.1.4. Cybersecurity Transformation	0.371	0.111
		1.2. Cybersecurity Threat, Risk, Vulnerability Management and Resiliency	0.4	1.2.1. Cybersecurity Threat Management	0.189	0.076
				1.2.2. Cybersecurity Risk Management	0.202	0.081
				1.2.3. Cybersecurity Vulnerability Management	0.247	0.099
				1.2.4. Cybersecurity Resiliency	0.361	0.145
		1.3. Cyber Policy Compliance and Governance	0.3	1.3.1. Cybersecurity Program Policy	0.168	0.050
				1.3.2. Cybersecurity Governance	0.206	0.062
				1.3.3. Regular Cybersecurity Policy Internal/External Audits	0.264	0.079
				1.3.4. Compliance with Information Security Standards	0.362	0.109
2. Cybersecurity Culture, Education and Workforce	0.3	2.1. Cybersecurity Training, Education and Skills	0.4	2.1.1. Cybersecurity Training and Education	0.186	0.075
				2.1.2. Innovation, Research And Development Programs	0.234	0.094
				2.1.3. Cybersecurity Coaching and Training	0.291	0.116
				2.1.4. Continuous Improvements in Cybersecurity Skills	0.288	0.115
		2.2. Cybersecurity Awareness, Culture and Capacity Building	0.3	2.2.1. Situational Awareness Mechanisms	0.201	0.060
				2.2.2. Cyber-focused Mindset And Cyber-conscious Culture	0.222	0.067
				2.2.3. Committed Cybersecurity Team	0.288	0.086
				2.2.4. Cybersecurity Capacity Building	0.290	0.087

Table 5.10: The weights of CMM factors (*continue*)

Dimensions	Weights	Factors	Weights	Sub-Factors	Local Weights	Global Weights
		2.3. Cybersecurity Workforce Management	0.3	2.3.1. Identification of Appropriate Experts and Policymakers in Government, Private Sector and Academia	0.172	0.052
				2.3.2. Well-defined Cybersecurity Roles	0.234	0.070
				2.3.3. Certification and Promotion of Workforce	0.262	0.079
				2.3.4. Skilled Cybersecurity Team	0.332	0.100
3. Cybersecurity Infrastructure	0.2	3.1. Cybersecurity Methodology	0.3	3.1.1. Cryptography	0.206	0.068
				3.1.2. Infrastructure Protection and Firewall Management	0.176	0.058
				3.1.3. Physical Asset Management	0.253	0.083
				3.1.4. Enterprise Cybersecurity Architecture	0.365	0.120
		3.2. Cybersecurity Systems and Software Security	0.3	3.2.1. Secure Software Development Life Cycle (Secure-SDLC)	0.191	0.065
				3.2.2. Systems and Applications Security	0.260	0.088
				3.2.3. Network Security	0.233	0.079
				3.2.4. Cloud and Mobile Security	0.316	0.108
		3.3. Cybersecurity Intelligence	0.3	3.3.1. Advanced Cyber-Threat Readiness and Preparation	0.106	0.035
				3.3.2. Systems Testing/ DDoS Testing	0.203	0.067
				3.3.3. Cyber Threat Intelligence	0.396	0.131
				3.3.4. Red-Teaming	0.295	0.097
4. Cybersecurity Identity, Information and Organization	0.2	4.1. Cybersecurity Identity, Access and Authorization Management	0.3	4.1.1. Identity Management and Access Control	0.162	0.053
				4.1.2. Two-Factor/Multi-Factor Authentication	0.285	0.094
				4.1.3. Access Control and Authorization	0.244	0.081
				4.1.4. Automated Reporting Mechanisms	0.309	0.102
		4.2. Cybersecurity Information Management and Cooperation	0.3	4.2.1. Integrity of Cybersecurity Information over the Organization	0.174	0.058

Table 5.10: The weights of CMM factors (*continue*)

Dimensions	Weights	Factors	Weights	Sub-Factors	Local Weights	Global Weights
				4.2.2. Confidence/Privacy Based Data Management	0.236	0.078
				4.2.3. Cooperation with Stakeholders and Agencies for Cybersecurity	0.256	0.085
				4.2.4. International Cooperation and/or Engagement	0.334	0.110
		4.3. Cybersecurity Organization and Incident Management	0.3	4.3.1. Establishing Standard Workflows of Cybersecurity Processes	0.111	0.038
				4.3.2. Comparison with Best Practices	0.121	0.041
				4.3.3. Business Continuity Management Plan (Disaster Recovery Plan and Implementation)	0.358	0.122
				4.3.4. Cybersecurity Incident Management (Real-Time Logging and Inspection)	0.410	0.140
5. Cybersecurity Standards, Legislation, Regulation and Protection	0.2	5.1. Cybersecurity Standards	0.3	5.1.1. Cooperation and Coordination with National/International Teams (e.g. CERT/CIRT/CSIRT)	0.137	0.045
				5.1.2. Adherence to Standards (ISO/IEC 27001:2013/SOC2)	0.167	0.055
				5.1.3. Periodic Cybersecurity Tests (e.g. Pentest and Social Engineering Tests)	0.386	0.127
				5.1.4. Certification	0.311	0.103
		5.2. Cybersecurity Legal and Regulatory Measures	0.3	5.2.1. Legal Compliance Roadmap	0.172	0.057
				5.2.2. Cybercriminal Legislation	0.229	0.075
				5.2.3. Compliance with Government Regulations	0.262	0.087
				5.2.4. Formal/Informal Cooperation to Cybercrime	0.337	0.111
		5.3. Cybersecurity Information Privacy and Protection	0.3	5.3.1. Data Classification and Data Ownership	0.137	0.047
				5.3.2. Data Protection Laws	0.167	0.057
				5.3.3. Data Leakage Protection (DLP)	0.386	0.131
				5.3.4. System Tightening and Configuration Management	0.311	0.106

Table 5.11: The cybersecurity maturity scores of public institutions

	Information Technology	Finance	Energy	Health
1.1. Cybersecurity Strategy, Planning and Transformation	3.973	4.233	3.529	3.614
1.2. Cybersecurity Threat, Risk, Vulnerability Management and Resiliency	4.214	4.533	3.538	3.413
1.3. Cyber Policy Compliance and Governance	4.150	4.590	3.813	4.073
2.1. Cybersecurity Training, Education and Skills	4.331	3.696	2.771	3.000
2.2. Cybersecurity Awareness, Culture and Capacity Building	4.238	4.349	2.746	2.977
2.3. Cybersecurity Workforce Management	4.334	4.257	2.897	3.391
3.1. Cybersecurity Methodology	4.397	4.551	3.469	3.672
3.2. Cybersecurity Systems and Software Security	4.437	4.588	2.912	2.983
3.3. Cybersecurity Intelligence	4.426	4.577	3.154	2.875
4.1. Cybersecurity Identity, Access and Authorization Management	4.191	4.723	3.475	3.129
4.2. Cybersecurity Information Management and Cooperation	4.686	4.745	3.705	3.177
4.3. Cybersecurity Organization and Incident Management	4.692	4.914	3.529	3.141
5.1. Cybersecurity Standards	4.716	4.862	4.579	4.289
5.2. Cybersecurity Legal and Regulatory Measures	4.500	4.500	4.500	4.500
5.3. Cybersecurity Information Privacy and Protection	4.752	4.839	4.307	3.471

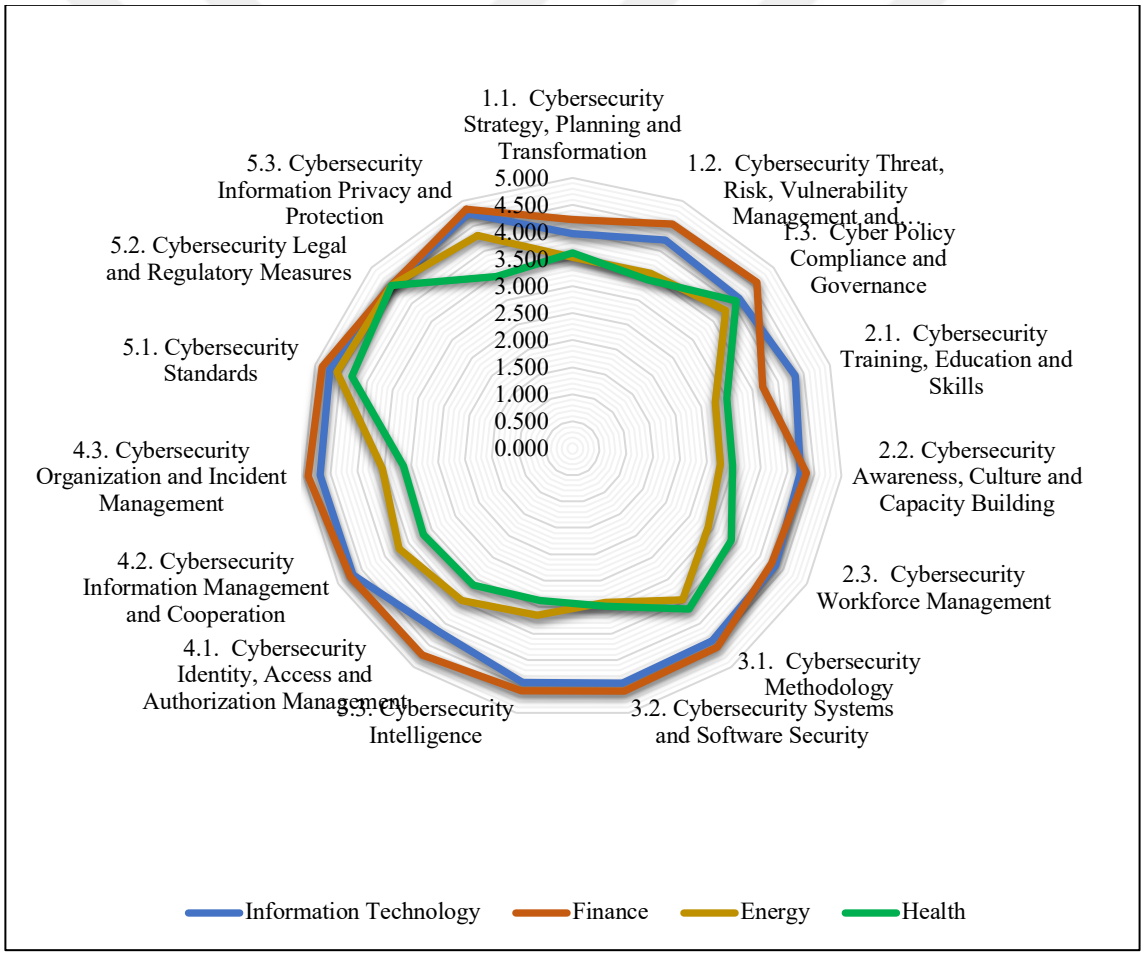

Figure 5.16: The cybersecurity maturity levels of institutions

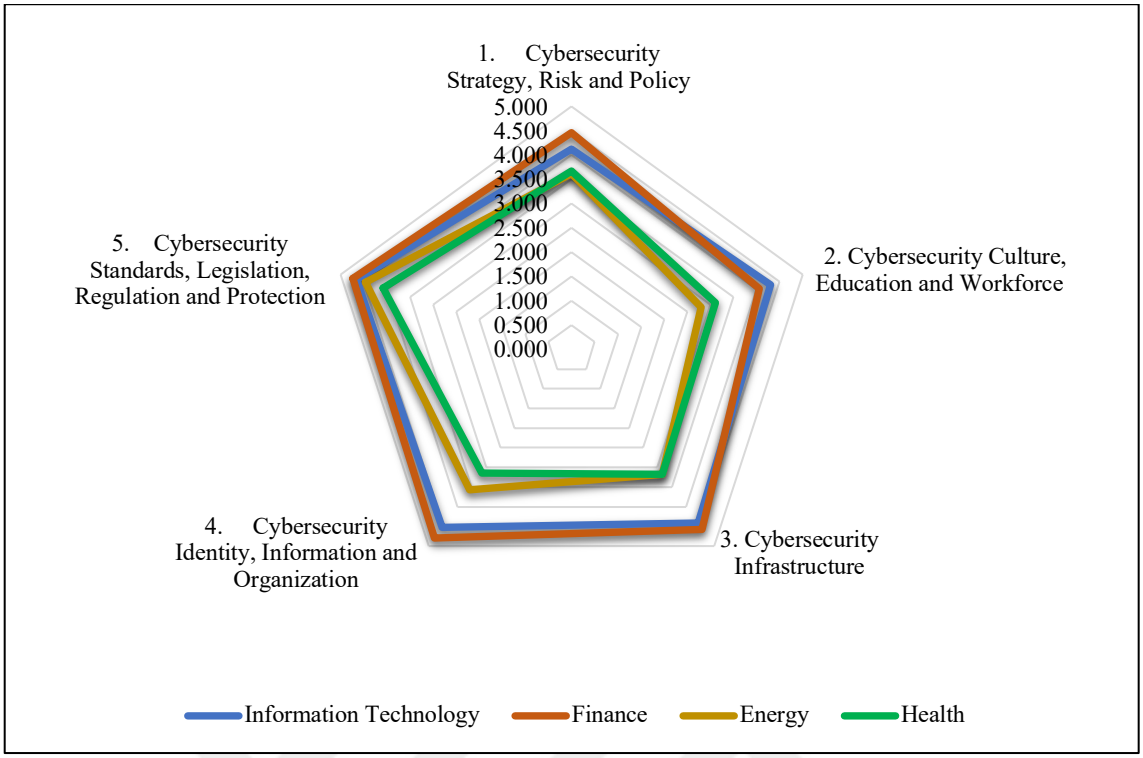

Figure 5.17: The overall cybersecurity maturity levels of institutions

According to the overall results, the finance and information technology sectors have higher cybersecurity maturity levels than the energy and health sectors.

- For "cybersecurity strategy, risk and policy", the institution in the finance sector is between level 4 and level 5; the institution in the information technology sector is between level 4; and the institutions in the energy and health sectors are between level 3 and level 4.
- For "cybersecurity culture, education and workforce", the institution in the information technology sector is between level 4 and level 5; the institution in the finance sector is in level 4; the institution in the health sector is in level 3; the institution in the energy sector is between level 2 and level 2.
- For "cybersecurity infrastructure", the institution in the finance sector is between level 4 and level 5; the institution in the information technology sector is in level 4; the institution in the energy sector is in level 3; the institution in the health sector is in level 3.
- For "cybersecurity identity, information and organization," the institution in the finance sector is between level 4 and level 5; the institution in the

information technology sector is between level 4 and level 5; the institution in the energy sector is between level 3 and level 4; the institution in the health sector is in level 3.

- For "cybersecurity standards, legislation, regulation and protection," the institution in the finance sector is between level 4 and level 5; the institution in the information technology sector is between level 4 and level 5; the institution in the energy sector is between level 4 and level 5; the institution in the health sector is in level 4.

5.6 Cybersecurity Action Plans

The cybersecurity journey and cybersecurity roadmap are illustrated in Figure 5.18 and Figure 5.19. Cybersecurity action plans are determined based on industry reports (Gartner, 2019, 2021, 2023a, 2023b; Office of the Under Secretary of Defense For Acquisition, 2003; Splunk, 2023). These action plans can be listed as:

- **Cybersecurity Strategy, Planning and Transformation, Cyber Policy Compliance and Governance**

- Identify target goal; develop strategic plan for next 3-5 years.
- Build governance structures that foster effective autonomous risk decision-making.
- Come up with ongoing, enforceable policies for all personnel.
- Identify and obtain the resources needed (e.g., funds, expertise).
- Perform regular status checks against defined goals and milestones.
- Understand key business priorities; define program mission and vision; and identify business, technology and threat drivers.
- Define security controls in line with organizational strategies and map them to a standardized security framework.
- Revisit maturity assessment to further optimization.
- Implement a continuous threat and exposure management program.
- Increase visibility throughout the entire technology environment to increase

resiliency.

- Combine cyber resilience efforts with traditional business continuity/disaster recovery preparation.

- **Cybersecurity Culture, Education, And Workforce**

- Reset security team expectations about the importance of the human element and user experience.
- Get ahead of the change to promote and support cybersecurity to your board.
- Engage employees and embed the organizational change into the company culture to ensure these cybersecurity improvements last.
- Promote continuous learning to maintain an up-to-date awareness of the cybersecurity environment.
- Instill a culture of secure employee behavior and initiate tailor training and awareness campaigns.
- Introduce empathy-driven outcome-focused practices to enhance human and user interactions.
- Assign clear owners and inform leaders and staff of changes to come.
- Integrate capabilities, tools and technologies.
- Track workforce performance and address skills gaps creatively.

- **Cybersecurity Infrastructure**

- Move cybersecurity tools and systems into production.
- Look into a methodology for organizational change management and apply this based on what works for the organization.
- Employ advanced analytics for anomaly detection.
- Employ SOAR (Security Orchestration Automation and Responce) solutions.
- Improve endpoint detection and response.
- Implement privileged account monitoring.
- Conduct incident response activities like threat hunting and/or forensic investigations.

- Use data and analytics to optimize threat detection and response.
- Develop a program structure to monitor and combat advanced threats.
- Develop advanced reporting and response and craft a communications plan for cyber breaches.
- Make red teaming the subject of continuing intellectual activity.
- Ensure that your organization is aware of and committed to using data encryption techniques.

- **Cybersecurity Identity, Access and Authorization Management**

- Develop a strategy for privacy that, first and foremost, aligns compliance targets with business targets.
- Weaponize" privacy as a prospect conversation tool and a competitive advantage.
- Identify sponsorship, stakeholders, and givens; gain initial support from leadership.
- Develop a communications strategy to handle potential cyber incidents; include internal and external communication plans.
- Create a plan to communicate value to the organization and the board.
- Move new tools and systems into production environment and continue to operate and maintain them.
- Operationalize and maintain the new processes as part of business-as-usual practices; this turns the "new" practices into "standard" practices.
- Accelerate response and remediation of incidents.
- Speed the recovery of customer and user services.
- Evaluate and implement emerging best practices.

- **Cybersecurity Standards, Legislation, Regulation And Protection**

- Conduct vulnerability assessment and penetration testing.
- Develop security architecture, policy framework and solution layer.
- Put previously identified policies and procedures into regular use.

- Ensure you're meeting new regulatory mandates.
- Prevent future risks by updating decision makers on new security norms.
- Decide how to build — with a mix of proprietary integrations and open standards, a consolidated platform, layered composable products or a combined approach.
- Held in conjunction with local government stakeholders.
- Coordinate with national/international teams (e.g. CERT/CIRT/CSIRT).
- Proactively secure business use of AI.
- Identify potential security risks across shared data and infrastructure.

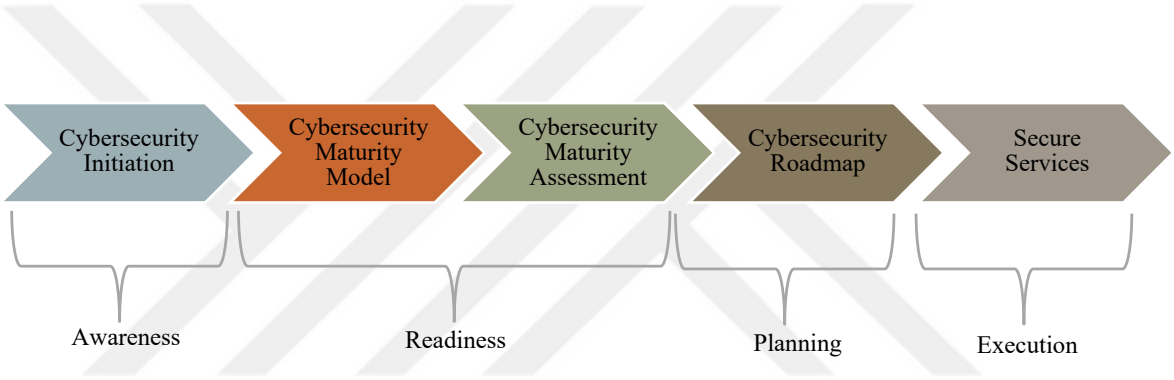

Figure 5.18: Cybersecurity journey

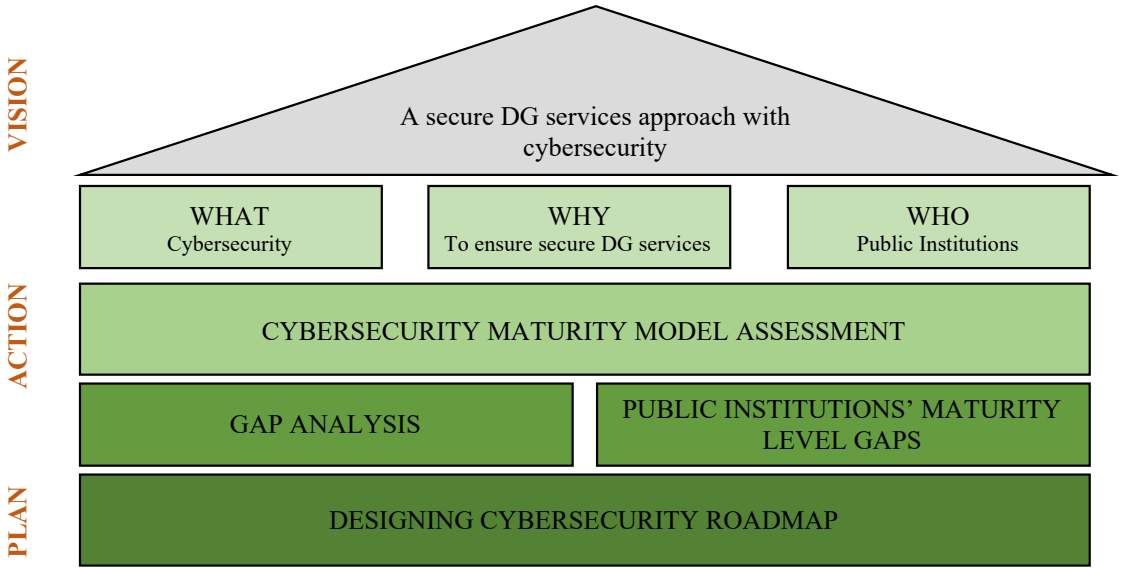

Figure 5.19: Cybersecurity framework

5.7 Gap Analysis

A gap analysis is a method of assessing the performance of a business unit to determine whether business requirements or objectives are being met and, if not, what steps should be taken to meet them. A gap analysis may also be called a needs analysis, needs assessment, or need-gap analysis. The "gap" in the gap analysis process refers to the space between "where we are" as a part of the business (i.e., the present state) and "where we want to be" (i.e., the target state or desired state) (Katie Terrell Hanna, 2023).

In this study, a gap analysis is realized to examine the differences between expected cybersecurity maturity levels and existing ones. This analysis is used to guide organizations in bridging the gap between their existing cybersecurity capabilities in our proposed CMM and their goals. At the end of this analysis, action plans are proposed as a guideline.

The gap analysis results for the public institutions are provided in Table 5.12 and visualized in Figures 5.20, 5.21, 5.22, and 5.23. Table 5.12 compares the existing levels after the cybersecurity maturity level assessment and the gaps with the expected situation.

Table 5.12: The results of maturity level gaps in public institutions

	IT Maturity			**Finance Maturity**			**Energy Maturity**			**Health Maturity**		
	Existing	**Expected**	**Gap**	**Existing**	**Expected**	**Gap**	**Existing**	**Expected**	**Gap**	**Existing**	**Expected**	**Gap**
1.1. Cybersecurity Strategy, Planning and Transformation	3.97	5	1.03	4.23	5	0.77	3.53	5	1.47	3.61	5	1.39
1.2. Cybersecurity Threat, Risk, Vulnerability Management and Resiliency	4.21	5	0.79	4.53	5	0.47	3.54	5	1.46	3.41	5	1.59
1.3. Cyber Policy Compliance and Governance	4.15	5	0.85	4.59	5	0.41	3.81	5	1.19	4.07	5	0.93
Average	4.12	5	0.88	4.46	5	0.54	3.62	5.00	1.38	3.67	5.00	1.33
2.1. Cybersecurity Training, Education and Skills	4.33	5	0.67	3.70	5	1.30	2.77	5	2.23	3.00	5	2.00

Table 5.14: The results of maturity level gaps in public institutions (*continue*)

	IT Maturity			Finance Maturity			Energy Maturity			Health Maturity		
	Existing	**Expected**	**Gap**	**Existing**	**Expected**	**Gap**	**Existing**	**Expected**	**Gap**	**Existing**	**Expected**	**Gap**
2.2. Cybersecurity Awareness, Culture and Capacity Building	4.24	5	0.76	4.35	5	0.65	2.75	5	2.25	2.98	5	2.02
2.3. Cybersecurity Workforce Management	4.33	5	0.67	4.26	5	0.74	2.90	5	2.10	3.39	5	1.61
Average	4.30	5	0.70	4.06	5	0.94	2.80	5.00	2.20	3.11	5.00	1.89
3.1. Cybersecurity Methodology	4.40	5	0.60	4.55	5	0.45	3.47	5	1.53	3.67	5	1.33
3.2. Cybersecurity Systems and Software Security	4.44	5	0.56	4.59	5	0.41	2.91	5	2.09	2.98	5	2.02
3.3. Cybersecurity Intelligence	4.43	5	0.57	4.58	5	0.42	3.15	5	1.85	2.88	5	2.12
Average	4.42	5	0.58	4.57	5	0.43	3.18	5.00	1.82	3.18	5.00	1.82
4.1. Cybersecurity Identity, Access and Authorization Management	4.19	5	0.81	4.72	5	0.28	3.47	5	1.53	3.13	5	1.87
4.2. Cybersecurity Information Management and Cooperation	4.69	5	0.31	4.74	5	0.26	3.71	5	1.29	3.18	5	1.82
4.3. Cybersecurity Organization and Incident Management	4.69	5	0.31	4.91	5	0.09	3.53	5	1.47	3.14	5	1.86
Average	4.52	5	0.48	4.80	5	0.20	3.57	5.00	1.43	3.15	5.00	1.85
5.1. Cybersecurity Standards	4.72	5	0.28	4.86	5	0.14	4.58	5	0.42	4.29	5	0.71
5.2. Cybersecurity Legal and Regulatory Measures	4.50	5	0.50	4.50	5	0.50	4.50	5	0.50	4.50	5	0.50
5.3. Cybersecurity Information Privacy and Protection	4.75	5	0.25	4.84	5	0.16	4.31	5	0.69	3.47	5	1.53
Average	4.66	5	0.34	4.73	5	0.27	4.46	5.00	0.54	4.08	5.00	0.92

For the institution in the information technology sector, cybersecurity strategy, risk, and policy has the most significant gap of 0.88; cybersecurity culture, education, and workforce has the second most significant gap of 0.70; cybersecurity infrastructure has the third most significant gap of 0.58; cybersecurity identity, information and organization has the fourth most significant gap of 0.48; and cybersecurity standards, legislation, regulation and protection has the fifth most significant gap of 0.34.

For the institution in the finance sector, cybersecurity culture, education, and workforce has the most significant gap of 0.94; cybersecurity strategy, risk, and policy has the most significant gap of 0.54; cybersecurity infrastructure has the third most significant gap of 0.43; cybersecurity standards, legislation, regulation and protection has the fourth most significant gap of 0.27; and cybersecurity identity, information, and organization has the fifth most significant gap of 0.20.

For the institution in the energy sector, cybersecurity culture, education, and workforce has the most significant gap of 2.20; cybersecurity infrastructure has the second most significant gap of 1.82; cybersecurity identity, information and organization has the third most significant gap of 1.43; cybersecurity strategy, risk, and policy has the most significant gap of 1.38; and cybersecurity standards, legislation, regulation and protection has the fifth most significant gap of 0.54.

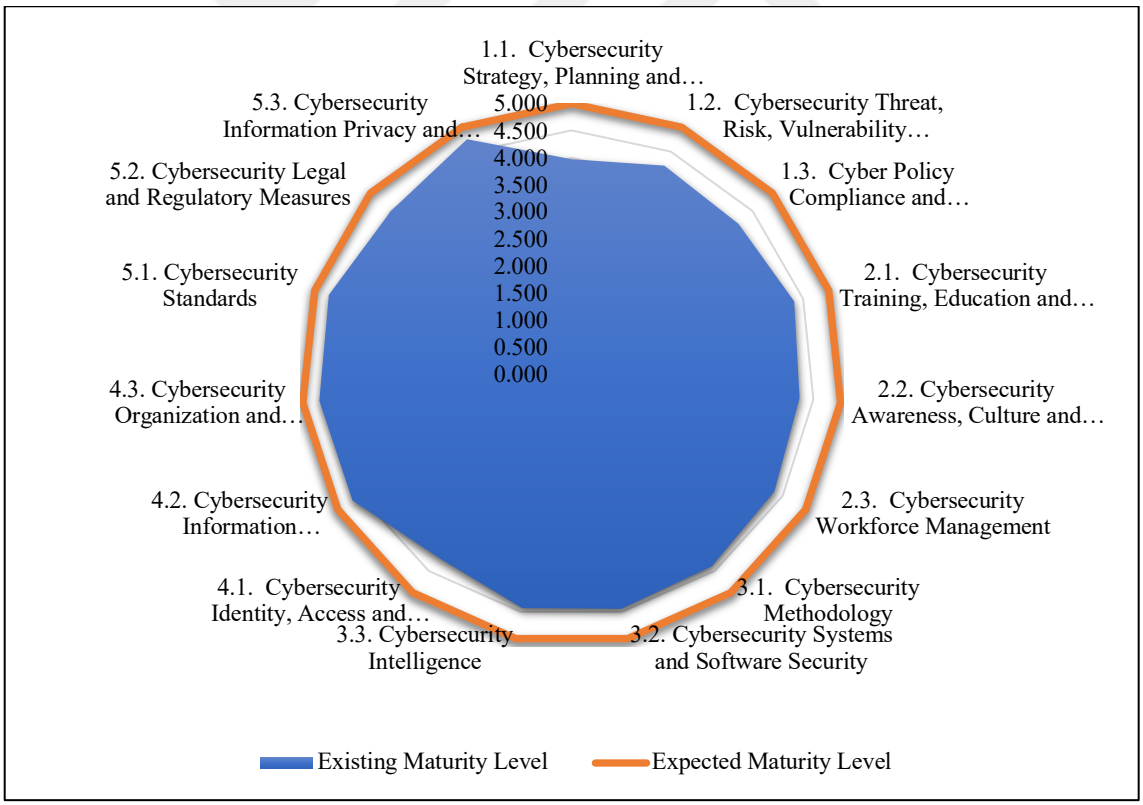

Figure 5.20: The gap analysis for the institution in the IT sector

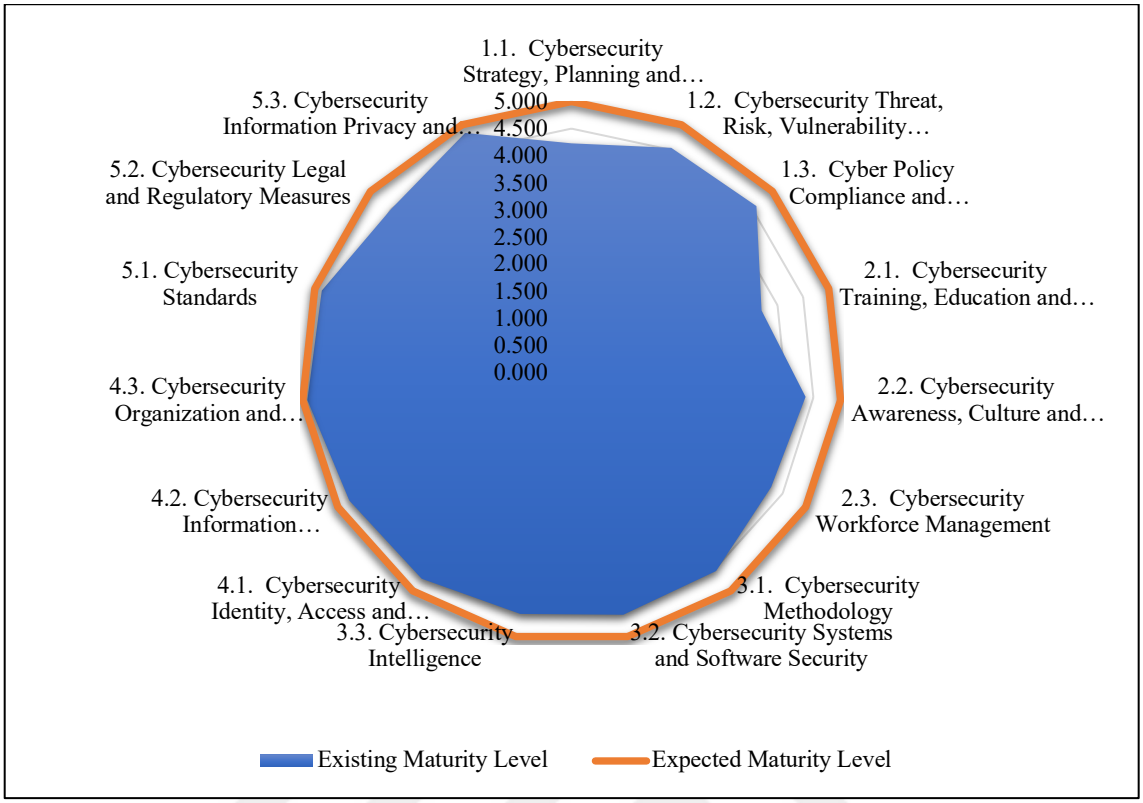

Figure 5.21: The gap analysis for the institution in the finance sector

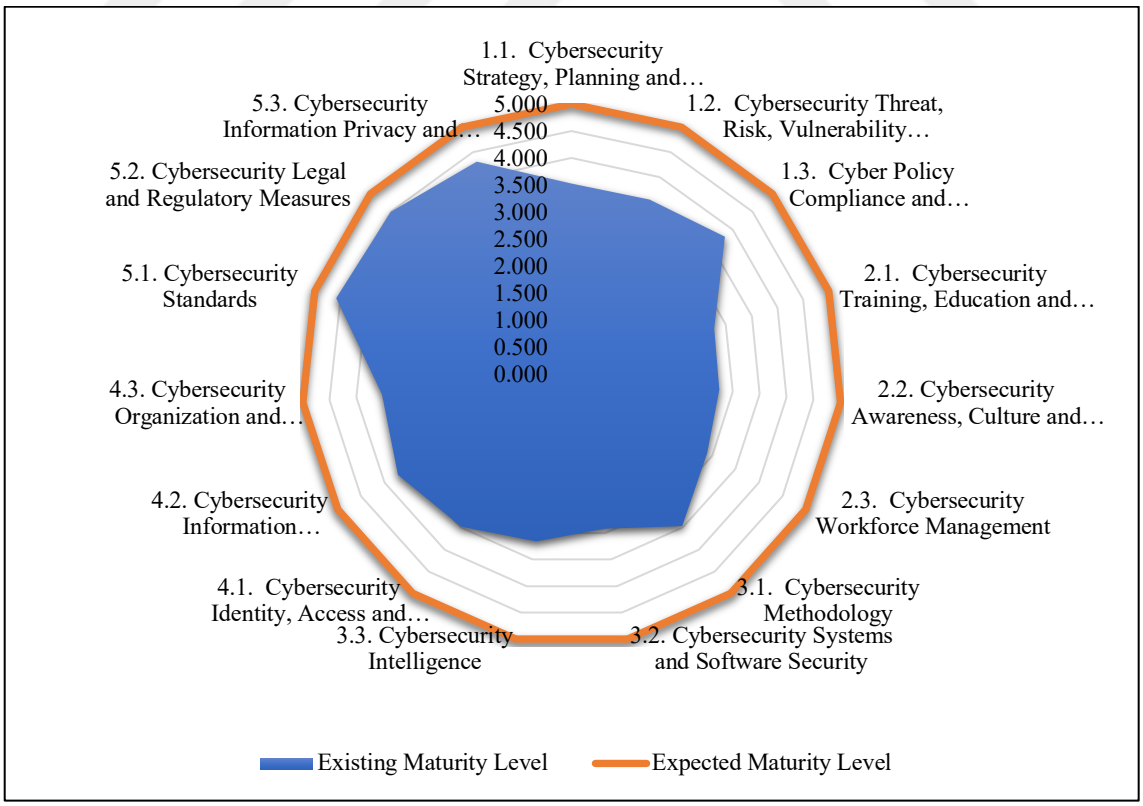

Figure 5.22: The gap analysis for the institution in the energy sector

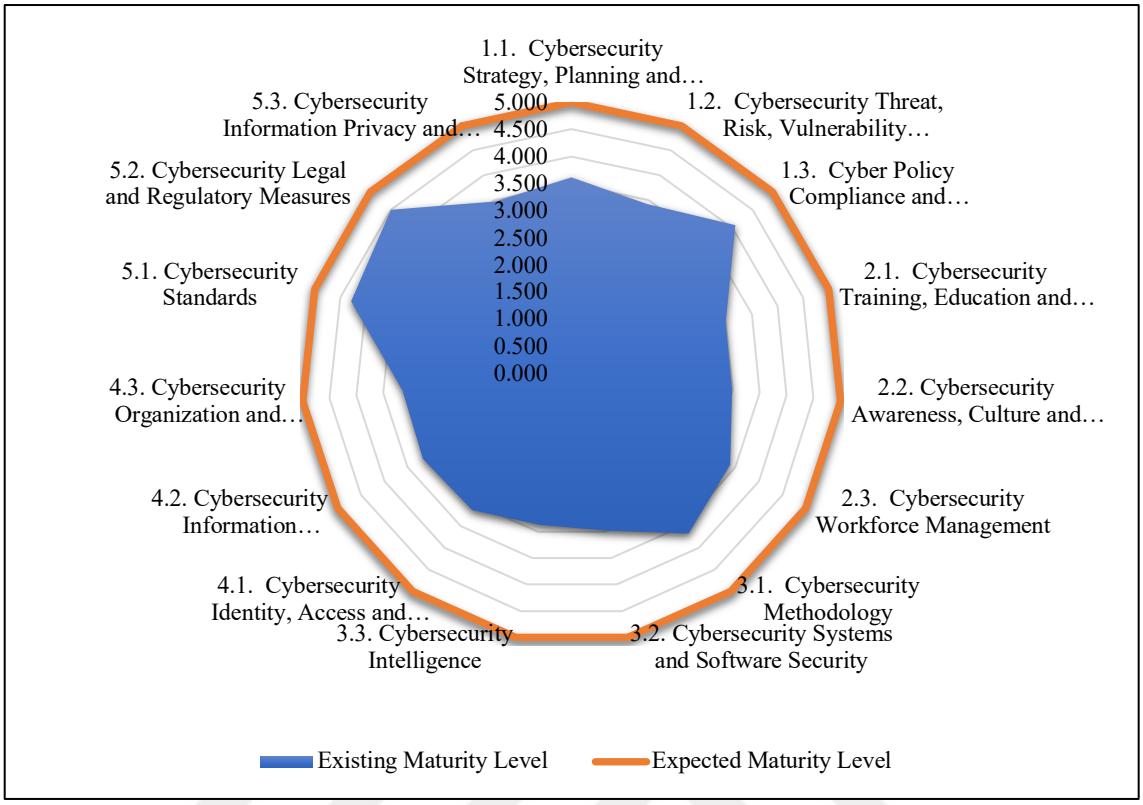

Figure 5.23: The gap analysis for the institution in the health sector

For the institution in the health sector, cybersecurity culture, education, and workforce has the most significant gap of 1.89; cybersecurity identity, information and organization has the second most significant gap of 1.85; cybersecurity infrastructure has the third most significant gap of 1.82; cybersecurity strategy, risk, and policy has the fourth most significant gap of 1.33; and cybersecurity standards, legislation, regulation and protection has the fifth most significant gap of 0.92.

5.8 Cybersecurity Roadmap for Public Institutions' DGT

Based on the cybersecurity maturity assessment of public institutions that has been done, the gap maturity levels are found for the cybersecurity maturity factors. As a result of the gap analysis of public institutions, recommendations are prepared after comparing what should be done with the institutions' ongoing cybersecurity processes. These recommendations can be used to improve the cybersecurity maturity level of public institutions. These recommendations should also align with the broader sectoral development objectives and national visions.

To facilitate the implementation of specific remediation or mitigation plans and subsequent measurement of their outcomes it is important for the recommended actions to follow quality criteria, such as specificity (the recommendation should be clear and detailed about the specific actions to be implemented and goals to achieve), responsibility (the recommendation should identify responsible owners and accountable entities), and measurability. It is advisable to link each recommendation to a specific Factor (and, thus, link it to a Dimension as well). Different Action Plans are possible since more than one way to improve cybersecurity maturity typically exists (The World Bank, 2023.

Total cybersecurity can never be "achieved." Instead, an organization's cybersecurity program is a risk-based, necessary business process that requires constant, ongoing efforts at all levels. To create successful improvements in cybersecurity, a utility needs to create an action plan that outlines clear steps for achieving a goal. The action plans serve as a guide. This study provides insight into valuable and effective strategies for improved cybersecurity, but the success of any project lies in its execution (Gartner, 2019).

The action plans for the public institutions are provided in Figures 5.24, 5.25, 5.26, and 5.27.

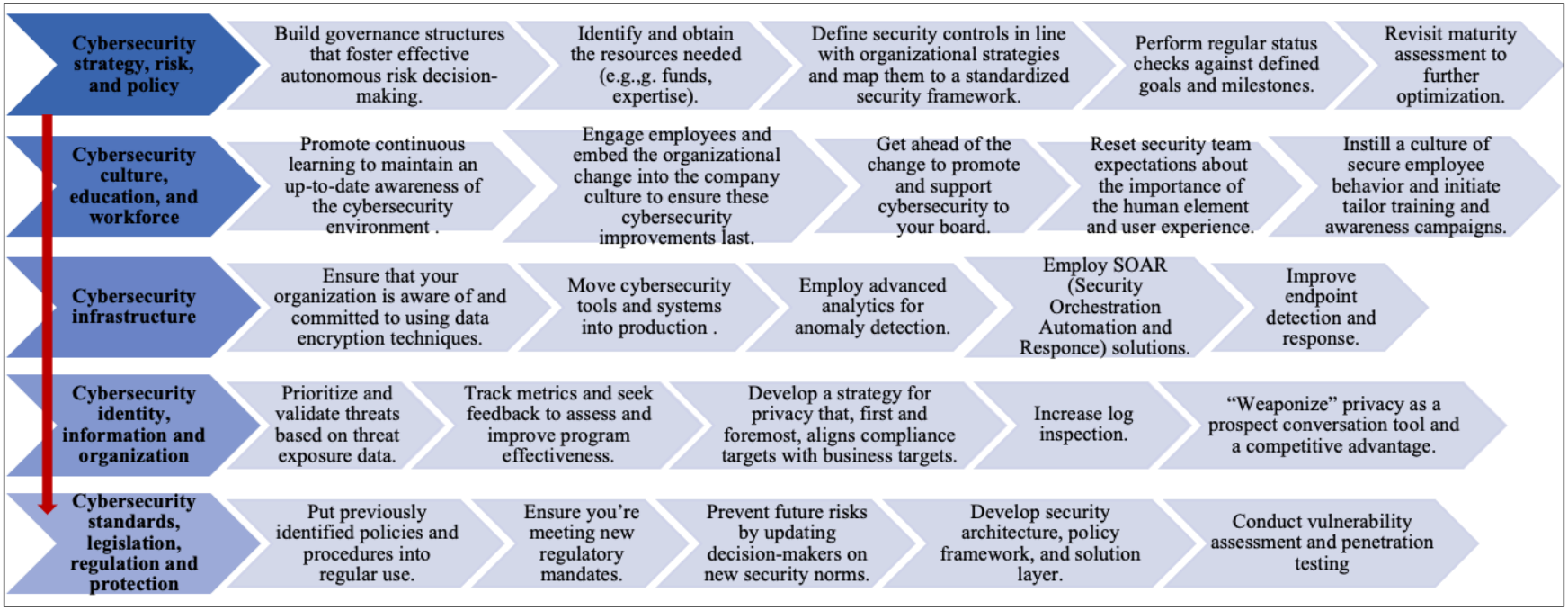

Figure 5.24: Action plans for the institution in the IT sector based on (Gartner, 2019, 2021, 2023a, 2023b; Office of the Under Secretary of Defense For Acquisition, 2003; Splunk, 2023)

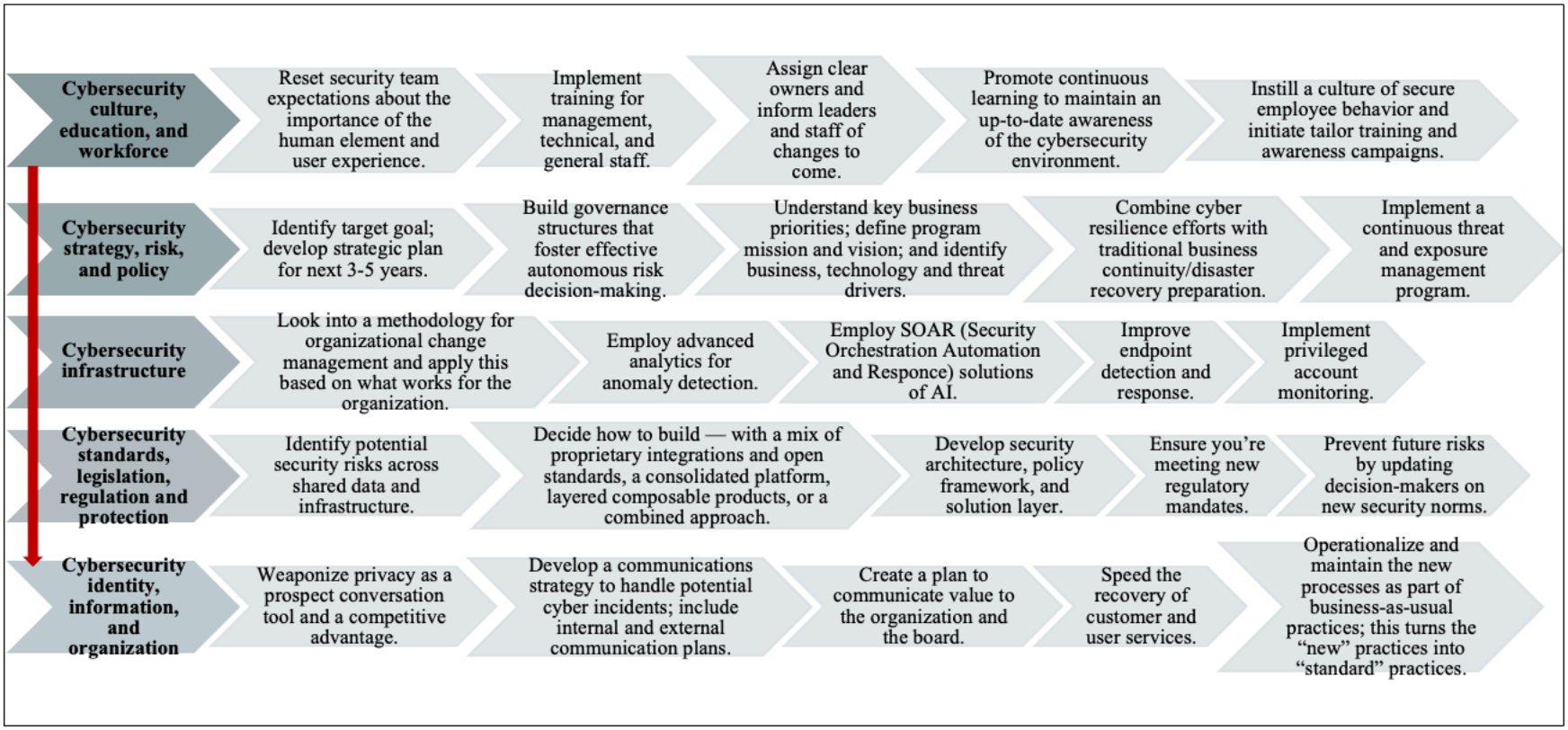

Figure 5.25: Action plans for the institution in the finance sector based on (Gartner, 2019, 2021, 2023a, 2023b; Office of the Under Secretary of Defense For Acquisition, 2003; Splunk, 2023)

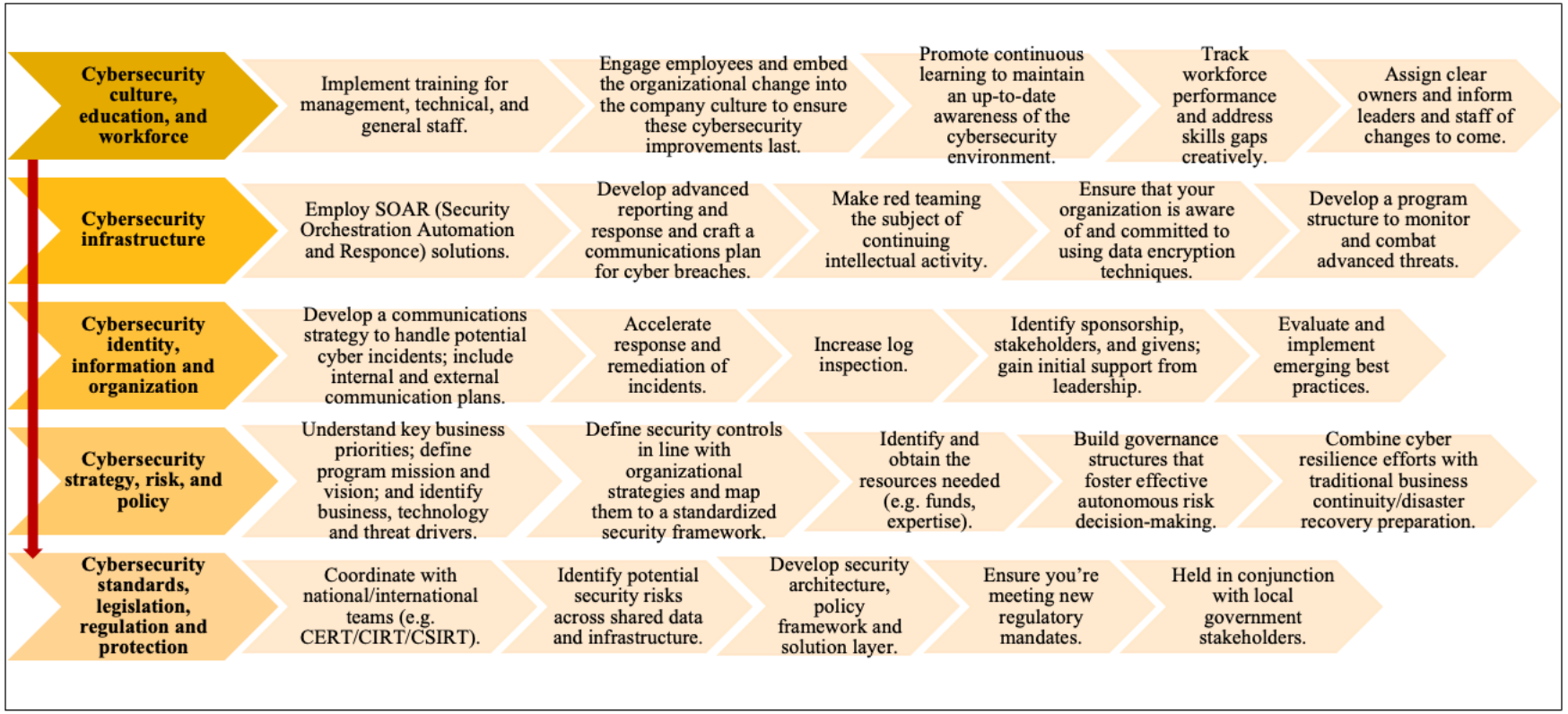

Figure 5.26: Action plans for the institution in the energy sector based on (Gartner, 2019, 2021, 2023a, 2023b; Office of the Under Secretary of Defense For Acquisition, 2003; Splunk, 2023)

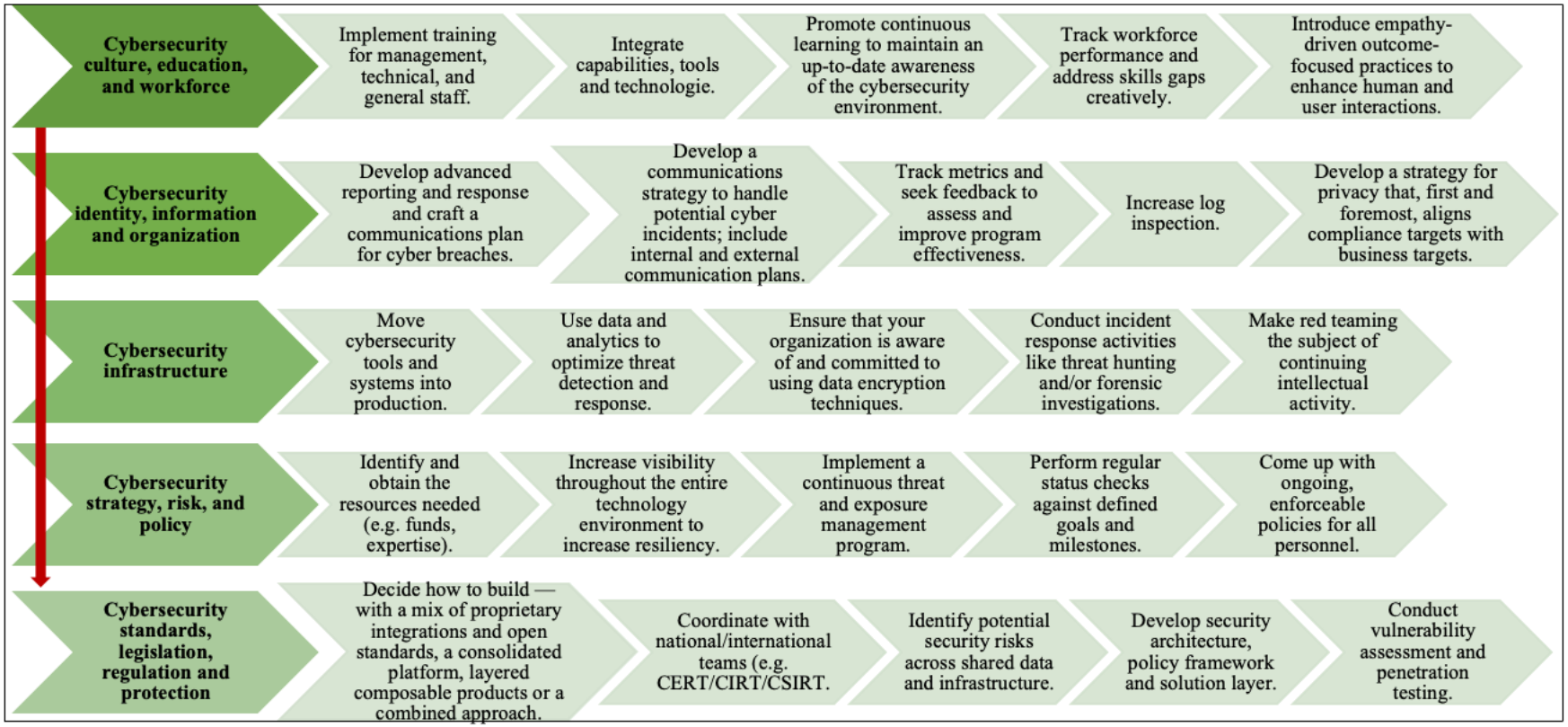

Figure 5.27: Action plans for the institution in the health sector based on (Gartner, 2019, 2021, 2023a, 2023b; Office of the Under Secretary of Defense For Acquisition, 2003; Splunk, 2023)

5.9 Concluding Remarks on Cybersecurity Maturity Assessment

A relevant cybersecurity program is essential for constructing a secure environment for the private and public sectors. In this context, organizations should measure their cybersecurity maturity levels. Cybersecurity maturity models help organizations realize these assessments.

In the related literature, a few papers provided cybersecurity maturity models. The subject has been examined in more detail in industry reports than in academic papers. This study has focused on reviewing existing cybersecurity maturity models to propose a new one. For this reason, this study systematically reviews studies on the cybersecurity maturity model and proposes a cybersecurity maturity model that guides organizations in assessing themselves. The multifaceted structure of these studies reveals a necessity to develop research in this field by systematically analyzing the existing studies.

In the related literature, a few papers provided cybersecurity roadmaps. This study has focused on proposing cybersecurity action plans based on the gaps between the institutions' existing cybersecurity maturity levels and their target cybersecurity maturity levels. For this reason, this study uses the findings of the cybersecurity maturity model assessment of four public institutions. This research proposes a generic cybersecurity action plans based on industry reports and expert opinions. Then, the most appropriate action plans for the public institutions are determined based on necessity regarding their cybersecurity maturity level gaps.

6. CONCLUSION AND PERSPECTIVES

The conclusions and perspectives from this thesis are provided in this chapter. Then, the limitations of thesis study are presented. Finally, future research directions are suggested based on the findings and limitations of the thesis.

6.1 Conclusions on DG

This thesis aimed to model and analyze the DG for an efficient, accountable, and transparent DGT. Thus, the purpose of this research was to model and analyse the DG framework with integrated methodologies to obtain an accessible, effective, and accountable DG. The DG subject is examined by conducting a systematic literature survey with the science mapping approach. At the end of the literature survey, the DG definition is clarified, the research directions are proposed.

Then, the digital transformation of governments is investigated based on three dimensions. In this context, the success and risk factors of the DGT are modeled and analyzed using the CM approach under the HFLTS GDM environment. The causal relationships between success and risk factors are considered in this approach with the utilization of the cognitive map approach. The HFLCM technique allowed a more straightforward representation of experts' judgments of the concept values and causal influences between the concepts. In the Digital Citizenship Improvement, the citizen side of the DGT is examined by proposing fourteen success/risk factors. In the Digital Technology Improvement, the technological infrastructure of DGT is examined based on thirteen success/risk factors. In the Digital Service Improvement, the services provided by governments are examined by fourteen success/risk factors. The most central factors are determined, and scenarios are conducted to observe the dynamic structure of the DG environment.

According to the results of the DG literature survey, industry reports, DGT analysis, and scenario analyses, this study was focused on cybersecurity for public institutions. A Cybersecurity Maturity Model (CMM) is proposed based on a detailed literature survey, industry reports, and advising experts. The cybersecurity maturity levels of public institutions are analyzed using the incomplete HFPRs and AHP method in GDM with Bonferroni means operator environment. An incomplete HFPR-AHP method is employed to deal with incomplete preferences provided by experts, and a case study for public institutions in Türkiye is provided to illustrate the usability of the proposed method. Cybersecurity action plans are proposed based on the gaps between the institutions' existing cybersecurity maturity levels and their target cybersecurity maturity levels. For this reason, this study uses the cybersecurity maturity model assessment findings of four public institutions. First, this research proposes a generic cybersecurity action plan based on industry reports and expert opinions. Then, public institutions' most appropriate action plans are determined based on necessity regarding their cybersecurity maturity level gaps.

The contributions of this thesis can be listed as:

(1) This study is the first attempt to examine the DG literature using the science mapping methodology by presenting the state-of-the-art DG, classifying the publications with science mapping,

(2) A novel success/risk factors framework for analyzing the DGT framework with an HFLCM approach is proposed,

(3) The HFLCM technique with the fuzzy envelope technique under the GDM environment is presented for the first time,

(4) Scenario analysis is conducted to analyze the DGT framework comprehensively,

(5) A new CMM with five levels, five dimensions, 15 factors, and 60 sub-factors is proposed for public institutions,

(6) A research methodology based on an incomplete HFPR-AHP method with a GDM approach with the HFL Bonferroni means operator is presented for the first time,

(7) A generic cybersecurity action plan and a research methodology based on a gap analysis are proposed for public institutions,

(8) A case study for public institutions in Türkiye is provided to illustrate the usability of the proposed CMM.

6.2 Limitations and Future Research Directions

Within the scope of the thesis, the DG framework was modeled and analyzed. Focusing on the technology dimension and specifically the cybersecurity dimension, roadmaps, and action plans were presented to increase the security of DGT of government institutions. Just as every study has areas open to improvement, this thesis also has limitations and potential areas open to progress. These areas can be summarized as follows:

- One of the limitations is conducting studies based on experts' subjective evaluations based on their knowledge and experience.
- Another limitation of this thesis is the focus on public institutions in Türkiye, which may limit the generalizability of the findings.
- Limitations of this study include assuming that the factors in the proposed CMM are independent of each other. Thus, the AHP method with incomplete HFPRs is used when calculating the weights.

Accordingly, the future research directions are proposed:

- In future studies, it may be considered to increase the number of the experts.
- Future research directions could include expanding the study by applying the methodology to different types of institutions to increase the generalizability of the findings.
- Finally, methods such as ANP or DEMATEL may be applied to the proposed approach considering the relationships between the factors in the CMM wherein the results can be compared with the obtained results.

REFERENCES

Abdel-Basset, M., Gamal, A., Moustafa, N., Abdel-Monem, A., & El-Saber, N. (2021). A Security-by-Design Decision-Making Model for Risk Management in Autonomous Vehicles. *IEEE Access*, *9*, 107657–107679. https://doi.org/10.1109/ACCESS.2021.3098675

Abushark, Y. B., Khan, A. I., Alsolami, F., Almalawi, A., Alam, M. M., Agrawal, A., Kumar, R., & Khan, R. A. (2022). Cyber Security Analysis and Evaluation for Intrusion Detection Systems. *Computers, Materials and Continua*, *72*(1), 1765–1783. https://doi.org/10.32604/cmc.2022.025604

Acar, C., Beskese, A., & Temur, G. T. (2018). Sustainability analysis of different hydrogen production options using hesitant fuzzy AHP. *International Journal of Hydrogen Energy*, *43*(39), 18059–18076. https://doi.org/https://doi.org/10.1016/j.ijhydene.2018.08.024

Accenture. (2020). *Cybersecurity Behavior Assessment*.

Action Aid. (2023). Good Governance and Citizen Participation. **URL:***https://morethanprojects.actionaid.it/en/good-governance-and-citizen-participation/*

Addo, A. (2022). Information technology and public administration modernization in a developing country: Pursuing paperless clearance at Ghana customs. *Information Systems Journal*, *32*(4), 819–855. https://doi.org/10.1111/isj.12371

Akinsanya, O. O., Papadaki, M., & Sun, L. (2020). Towards a maturity model for health-care cloud security (M2HCS). *Information and Computer Security*, *28*(3), 321–345. https://doi.org/10.1108/ICS-05-2019-0060

Akram, M. S., Malik, A., Shareef, M. A., & Awais Shakir Goraya, M. (2019). Exploring the interrelationships between technological predictors and behavioral mediators in online tax filing: The moderating role of perceived risk. *Government Information Quarterly*. https://doi.org/10.1016/j.giq.2018.12.007

Aktas, A., & Kabak, M. (2018). A Hybrid Hesitant Fuzzy Decision-Making Approach for Evaluating Solar Power Plant Location Sites. *Arabian Journal for Science and Engineering*, *44*. https://doi.org/10.1007/s13369-018-3604-5

Al Sulaimani, Ahmed Hamed Abdullah and Ozuem, W. (2022). Understanding the role of transparency, participation, and collaboration for achieving open digital government goals in Oman. *Transforming Government: People, Process and Policy*, *16*, 595–612.

Alarabiat, A., Soares, D., & Estevez, E. (2021). Determinants of citizens' intention to engage in government-led electronic participation initiatives through Facebook. *Government Information Quarterly*, *38*(1), 101537.

Alcaide–Muñoz, L., Rodríguez–Bolívar, M. P., Cobo, M. J., & Herrera–Viedma, E. (2017). Analysing the scientific evolution of e-Government using a science mapping approach. *Government Information Quarterly*, *34*(3), 545–555.

Alenezi, M., Agrawal, A., Kumar, R., & Khan, R. A. (2020). Evaluating Performance of Web Application Security through a Fuzzy Based Hybrid Multi-Criteria Decision-Making Approach: Design Tactics Perspective. *IEEE Access*, *8*, 25543–25556. https://doi.org/10.1109/ACCESS.2020.2970784

Alharbi, A., Seh, A. H., Alosaimi, W., Alyami, H., Agrawal, A., Kumar, R., & Khan, R. A. (2021). Analyzing the impact of cyber security related attributes for intrusion detection systems. *Sustainability (Switzerland)*, *13*(22), 1–19. https://doi.org/10.3390/su132212337

Aliyu, A., Maglaras, L., He, Y., Yevseyeva, I., Boiten, E., Cook, A., & Janicke, H. (2020). A holistic cybersecurity maturity assessment framework for higher education institutions in the United Kingdom. *Applied Sciences (Switzerland)*, *10*(10), 1–14. https://doi.org/10.3390/app10103660

Al-Karaki, J. N., Gawanmeh, A., & El-Yassami, S. (2020). GoSafe: On the practical characterization of the overall security posture of an organization information system using smart auditing and ranking. *Journal of King Saud University - Computer and Information Sciences*, *xxxx*. https://doi.org/10.1016/j.jksuci.2020.09.011

Alladi, T., Chamola, V., & Zeadally, S. (2020). Industrial Control Systems: Cyberattack trends and countermeasures. *Computer Communications*, *155*(December 2019), 1–8. https://doi.org/10.1016/j.comcom.2020.03.007

Allan, A., Perkins, E., & Scholtz, Tom, G. (2009). *Gartner Identity and Access Management Program Maturity Model* (Issue October).

Almamari, M. (2016). *The Role of Organisational Culture in Digital Government Implementation. Exploring the Relationship between Public Sector Organisational Culture and the Implementation of Digital Government in Oman*. The University of Bradford Open Access.

Almansoori, A., Al-Emran, M., & Shaalan, K. (2023). Exploring the Frontiers of Cybersecurity Behavior: A Systematic Review of Studies and Theories. *Applied Sciences (Switzerland)*, *13*(9). https://doi.org/10.3390/app13095700

Al-Matari, O. M. M., Helal, I. M. A., Mazen, S. A., & Elhennawy, S. (2021). Adopting security maturity model to the organizations' capability model. *Egyptian Informatics Journal*, *22*(2), 193–199. https://doi.org/10.1016/j.eij.2020.08.001

Almomani, I., Ahmed, M., & Maglaras, L. (2021). Cybersecurity maturity assessment framework for higher education institutions in Saudi Arabia. *PeerJ Computer Science*, *7*, e703. https://doi.org/10.7717/peerj-cs.703

Al-Muftah, H., Weerakkody, V., Rana, N. P., Sivarajah, U., & Irani, Z. (2018). Factors influencing e-diplomacy implementation: Exploring causal relationships using interpretive structural modelling. *Government Information Quarterly*. https://doi.org/10.1016/j.giq.2018.03.002

Alshallaqi, M. (2022). The complexities of digitization and street-level discretion: a socio-materiality perspective. *Public Management Review*, 1–23.

AL-Shehry, A. M. (2008). Transformation towards E-government in The Kingdom of Saudi Arabia: Technological and Organisational Perspectives. *Technology*, *August*, 265.

Alvarenga, A., Matos, F., Godina, R., & Matias, J. C. O. (2020). Digital transformation and knowledge management in the public sector. *Sustainability (Switzerland)*, *12*(14). https://doi.org/10.3390/su12145824

Anass, R., Saliha, A., & Ounsa, R. (2020). A concept & compliance study of security maturity models with ISO 21827. *ICEIS 2020 - Proceedings of the 22nd International Conference on Enterprise Information Systems*, *2*(Iceis), 385–392. https://doi.org/10.5220/0009569703850392

Andersen, K. N., Medaglia, R., Vatrapu, R., Henriksen, H. Z., & Gauld, R. (2011). The forgotten promise of e-government maturity: Assessing responsiveness in the digital public sector. *Government Information Quarterly*, *28*(4), 439–445.

Andreasson, A., Artman, H., Brynielsson, J., & Franke, U. (2021). A Census of Swedish Public Sector Employee Communication on Cybersecurity during the COVID-19 Pandemic. *2021 International Conference on Cyber Situational Awareness, Data Analytics and Assessment, CyberSA 2021*, 1–8. https://doi.org/10.1109/CyberSA52016.2021.9478241

Ashaye, O. O. (2014). *Evaluating the Implementation of E-Government in Developing Countries : the Case of Nigeria* (Issue April). http://bura.brunel.ac.uk/handle/2438/8751

Ashaye, O. R., & Irani, Z. (2019). The role of stakeholders in the effective use of e-government resources in public services. *International Journal of Information Management*, *49*, 253–270. https://doi.org/10.1016/J.IJINFOMGT.2019.05.016

Ashok, M., Madan, R., Joha, A., & Sivarajah, U. (2022). Ethical framework for Artificial Intelligence and Digital technologies. *International Journal of Information Management*, *62*, 102433. https://doi.org/10.1016/J.IJINFOMGT.2021.102433

Atoum, I., & Otoom, A. (2016). Effective belief network for cyber security frameworks. *International Journal of Security and Its Applications*, *10*(4), 221–228. https://doi.org/10.14257/IJSIA.2016.10.4.21

Avanzi, D. da S., Foggiatto, A., dos Santos, V. A., Deschamps, F., & de Freitas Rocha Loures, E. (2017). A framework for interoperability assessment in crisis management. *Journal of Industrial Information Integration*, *5*, 26–38. https://doi.org/10.1016/j.jii.2017.02.004

Axelrod, R. (1976). *Structure of decision: The cognitive maps of political elites*. Princeton university press.

Ayağ, Z., & Samanlioglu, F. (2020). A hesitant fuzzy linguistic terms set-based AHP-TOPSIS approach to evaluate ERP software packages. *International Journal of Intelligent Computing and Cybernetics*. https://doi.org/10.1108/IJICC-07-2020-0079

Baheer, B. A., Lamas, D., & Sousa, S. (2020). A Systematic Literature Review on Existing Digital Government Architectures: State-of-the-Art, Challenges, and

Prospects. *Administrative Sciences*, *10*(2), 25. https://doi.org/10.3390/admsci10020025

Bahuguna, A., Bisht, R. K., & Pande, J. (2019). Assessing cybersecurity maturity of organizations: An empirical investigation in the Indian context. *Information Security Journal*, *28*(6), 164–177. https://doi.org/10.1080/19393555.2019.1689318

Baikloy, E., Praneetpolgrang, P., & Jirawichitchai, N. (2020). Development of cyber resilient capability maturity model for cloud computing services. *TEM Journal*, *9*(3), 915–923. https://doi.org/10.18421/TEM93-11

Baldini, G. (2022). Detection of cybersecurity spoofing attacks in vehicular networks with recurrence quantification analysis. *Computer Communications*, *191*(October 2021), 486–499. https://doi.org/10.1016/j.comcom.2022.05.021

Barcevičius, E., Cibaitė, G., Codagnone, C., Gineikytė, V., Klimavičiūtė, L., Liva, G., Matulevič, L., Misuraca, G., & Vanini, I. (2019). Exploring Digital Government transformation in the EU. In *Publications Office of the European Union, Luxembourg*. https://doi.org/doi:10.2760/17207

Barnes, B., & Daim, T. (2022). Information Security Maturity Model for Healthcare Organizations in the United States. *IEEE Transactions on Engineering Management*, 1–12. https://doi.org/10.1109/TEM.2021.3139836

Başar, A. (2016). Hesitant Fuzzy Pairwise Comparison for software cost estimation: A case study in Turkey. *Turkish Journal of Electrical Engineering and Computer Sciences*, *25*. https://doi.org/10.3906/elk-1604-45

Batur Sir, G. D., & Sir, E. (2021). Pain Treatment Evaluation in COVID-19 Patients with Hesitant Fuzzy Linguistic Multicriteria Decision-Making. *Journal of Healthcare Engineering*, *2021*. https://doi.org/10.1155/2021/8831114

Beg, I., & Rashid, T. (2013). TOPSIS for hesitant fuzzy linguistic term sets. *International Journal of Intelligent Systems*, *28*. https://doi.org/10.1002/int.21623

Beliakov, G., James, S., Mordelová, J., Rückschlossová, T., & Yager, R. R. (2010). Generalized Bonferroni mean operators in multi-criteria aggregation. *Fuzzy Sets and Systems*, *161*(17), 2227–2242. https://doi.org/10.1016/j.fss.2010.04.004

Beliakov, Gleb., Calvo, T., & Pradera, Ana. (2007). Aggregation functions : a guide for practitioners. Springer-Verlag.

Benz, M., & Chatterjee, D. (2020). Calculated risk? A cybersecurity evaluation tool for SMEs. *Business Horizons*, *63*(4), 531–540. https://doi.org/10.1016/j.bushor.2020.03.010

Bhol, S. G., Mohanty, J. R., & Pattnaik, P. K. (2020). Cyber Security Metrics Evaluation Using Multi-criteria Decision-Making Approach BT - Smart Intelligent Computing and Applications. In S. C. Satapathy, V. Bhateja, J. R. Mohanty, & S. K. Udgata (Eds.), *Smart Innovation, Systems and Technologies* (pp. 665–675). Springer Singapore.

Bitzer, M., Häckel, B., Leuthe, D., Ott, J., Stahl, B., & Strobel, J. (2023). Managing the Inevitable – A Maturity Model to Establish Incident Response Management Capabilities. *Computers and Security*, *125*, 103050. https://doi.org/10.1016/j.cose.2022.103050

Boccardo, D. R., Bento, L. M. S., & Costa, F. H. (2021). Towards a practical information security maturity evaluation method focused on people, process and technology. *2021 IEEE International Workshop on Metrology for Industry 4.0 and IoT, MetroInd 4.0 and IoT 2021 - Proceedings*, 721–726. https://doi.org/10.1109/MetroInd4.0IoT51437.2021.9488471

Bojanić, D., Vulić, I., Ristić, V., & Marček, J. (2020). Designing cybersecurity management bodies in strategic planning: application of hybrid analysis. *Advances in Economics, Business and Management Research*, *108*(Senet), 259–265. https://doi.org/10.2991/senet-19.2019.43

Boltürk, E., Onar, S., Öztayşi, B., Kahraman, C., & Goztepe, K. (2016). Multi-Attribute Warehouse Location Selection in Humanitarian Logistics Using Hesitant Fuzzy AHP. *International Journal of the Analytic Hierarchy Process*, *8*, 271–298. https://doi.org/10.13033/ijahp.v8i2.387

Bozkurt, Y., Rossmann, A., Konanahalli, A., & Pervez, Z. (2023). Toward Urban Data Governance: Status-Quo, Challenges, and Success Factors. *IEEE Access*, *11*(August), 85656–85677. https://doi.org/10.1109/ACCESS.2023.3302835

Bright, J., Margetts, H. Z., Wang, N., & Hale, S. A. (2015). Explaining Usage Patterns in Open Government Data: The Case of Data.Gov.UK. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.2613853

Büyüközkan, G., & Güler, M. (2020). Analysis of companies' digital maturity by hesitant fuzzy linguistic MCDM methods. *Journal of Intelligent & Fuzzy Systems*, *38*(1), 1119–1132.

Büyüközkan, G., Karabulut, Y., & Mukul, E. (2018). A novel renewable energy selection model for United Nations' sustainable development goals. *Energy*, *165*, 290–302. https://doi.org/https://doi.org/10.1016/j.energy.2018.08.215

Büyüközkan, G., Mukul, E., & Kongar, E. (2020). Health tourism strategy selection via SWOT analysis and integrated hesitant fuzzy linguistic AHP-MABAC approach. *Socio-Economic Planning Sciences*, 100929. https://doi.org/10.1016/j.seps.2020.100929

Büyüközkan, G., & Vardaloglu, Z. (2012). Analyzing of CPFR success factors using fuzzy cognitive maps in retail industry. *Expert Systems with Applications*, *39*(12), 10438–10455. https://doi.org/10.1016/j.eswa.2012.02.014

Camci, A., Temur, G., & Beskese, A. (2018). CNC router selection for SMEs in woodwork manufacturing using hesitant fuzzy AHP method. *Journal of Enterprise Information Management*, *31*, 0. https://doi.org/10.1108/JEIM-01-2018-0017

Camgöz Akdağ, H., & Menekşe, A. (2023). Cybersecurity Framework Prioritization for Healthcare Organizations Using a Novel Interval-Valued Pythagorean Fuzzy CRITIC BT - Intelligent Systems in Digital Transformation: Theory and Applications. In C. Kahraman & E. Haktanır (Eds.), *Lecture Notes in Networks and Systems* (pp. 241–266). Springer International Publishing. https://doi.org/10.1007/978-3-031-16598-6_11

Carias, J. F., Arrizabalaga, S., Labaka, L., & Hernantes, J. (2021). Cyber Resilience Self-Assessment Tool (CR-SAT) for SMEs. *IEEE Access*, *9*, 80741–80762. https://doi.org/10.1109/ACCESS.2021.3085530

Cäsar, M., Pawelke, T., Steffan, J., & Terhorst, G. (2022). A survey on Bluetooth Low Energy security and privacy. *Computer Networks*, *205*(December 2021), 108712. https://doi.org/10.1016/j.comnet.2021.108712

Castilla, R., Pacheco, A., & Franco, J. (2023). Digital Government: Mobile Applications and Their Impact on Access to Public Information. *SSRN Electronic Journal*, *22*, 101382. https://doi.org/10.2139/ssrn.4341247

Çevik Onar, S., Büyüközkan, G., Öztayşi, B., & Kahraman, C. (2016). A new hesitant fuzzy QFD approach: An application to computer workstation selection. *Applied Soft Computing*, *46*, 1–16. https://doi.org/https://doi.org/10.1016/j.asoc.2016.04.023

Chapman, T. A., & Reithel, B. J. (2021). Perceptions of Cybersecurity Readiness among Workgroup IT Managers. *Journal of Computer Information Systems*, *61*(5), 438–449. https://doi.org/10.1080/08874417.2019.1703224

Chen, L., & Aklikokou, A. K. (2020). Determinants of E-government Adoption: Testing the Mediating Effects of Perceived Usefulness and Perceived Ease of Use. *International Journal of Public Administration*, *43*(10), 850–865. https://doi.org/10.1080/01900692.2019.1660989

Chen, Y., Bretschneider, S., Stritch, J. M., Darnall, N., & Hsueh, L. (2022). E-procurement system adoption in local governments: the role of procurement complexity and organizational structure. *Public Management Review*, *24*(6), 903–925.

Chen, Y. C., & Lee, J. (2018). Collaborative data networks for public service: governance, management, and performance. *Public Management Review*, *20*(5), 672–690. https://doi.org/10.1080/14719037.2017.1305691

Choi, H., Chung, C., & Cho, Y. (2022). Changes in planning approach: a comparative study of digital government policies in South Korea and Denmark. *European Planning Studies*, *0*(0), 1–20. https://doi.org/10.1080/09654313.2022.2132787

Choi, Y., Lee, H., & Irani, Z. (2018). Big data-driven fuzzy cognitive map for prioritising IT service procurement in the public sector. *Annals of Operations Research*, *270*(1–2), 75–104. https://doi.org/10.1007/s10479-016-2281-6

CISA. (2021). Zero Trust Maturity Model. In *CISA* (Issue June).

Clarke, A. (2020). Digital government units: what are they, and what do they mean for digital era public management renewal? *International Public Management Journal*, *23*(3), 358–379. https://doi.org/10.1080/10967494.2019.1686447

CLC. (2018). *Foundation for Technology and the City : Foundation for a Smart Nation*. **URL:***https://www.clc.gov.sg/docs/default-source/urban-systems-studies/uss-technology-and-the-city.pdf*

CMM, N. (2021). *Cybersecurity Capacity Maturity*. *Cmm*.

CMMI. (2017). *Capability Maturity Model Integration*.

Çoban, V., & Onar, S. Ç. (2017a). Analysis of Solar Energy Generation Capacity Using Hesitant Fuzzy Cognitive Maps. *International Journal of Computational Intelligence Systems*, *10*(1), 1149–1167. https://doi.org/10.2991/ijcis.2017.10.1.76

Çoban, V., & Onar, S. Ç. (2017b). Modeling renewable energy usage with hesitant Fuzzy cognitive map. *Complex & Intelligent Systems*, *3*(3), 155–166. https://doi.org/10.1007/s40747-017-0043-y

Cobo, M. J., López-Herrera, A. G., Herrera-Viedma, E., & Herrera, F. (2011). Science mapping software tools: Review, analysis, and cooperative study among tools. *Journal of the American Society for Information Science and Technology*, *62*(7), 1382–1402.

Coelho, T. R., Pozzebon, M., & Cunha, M. A. (2022). Citizens influencing public policy-making: Resourcing as source of relational power in e-participation platforms. *Information Systems Journal*, *32*(2), 344–376. https://doi.org/10.1111/isj.12359

Çolak, M., & Kaya, İ. (2017). Prioritization of renewable energy alternatives by using an integrated fuzzy MCDM model: A real case application for Turkey. *Renewable and Sustainable Energy Reviews*, *80*, 840–853. https://doi.org/https://doi.org/10.1016/j.rser.2017.05.194

Çolak, M., Kaya, İ., Özkan, B., Budak, A., & Karaşan, A. (2020). A multi-criteria evaluation model based on hesitant fuzzy sets for blockchain technology in supply chain management. *Journal of Intelligent & Fuzzy Systems*, *38*, 935–946. https://doi.org/10.3233/JIFS-179460

Country Tool Kit. (2020). Feedbak Mechanisms. **URL:***https://countytoolkit.devolution.go.ke/resource/feedback-mechanisms*

Daim, T., Lai, K. K., Yalcin, H., Alsoubie, F., & Kumar, V. (2020). Forecasting technological positioning through technology knowledge redundancy: Patent citation analysis of IoT, cybersecurity, and Blockchain. *Technological Forecasting and Social Change*, *161*(September), 120329. https://doi.org/10.1016/j.techfore.2020.120329

David, A., Yigitcanlar, T., Li, R. Y. M., Corchado, J. M., Cheong, P. H., Mossberger, K., & Mehmood, R. (2023). Understanding Local Government Digital Technology Adoption Strategies: A PRISMA Review. In *Sustainability (Switzerland)* (Vol. 15, Issue 12). Multidisciplinary Digital Publishing Institute (MDPI). https://doi.org/10.3390/su15129645

Dawes, S. S., Vidiasova, L., & Parkhimovich, O. (2016). Planning and designing open government data programs: An ecosystem approach. *Government Information Quarterly*, *33*(1), 15–27.

De Blasio, E., & Selva, D. (2016). Why Choose Open Government? Motivations for the Adoption of Open Government Policies in Four European Countries. *Policy and Internet*, *8*(3), 225–247. https://doi.org/10.1002/poi3.118

De Bruin, R., & Von Solms, S. H. (2016). Modelling Cyber Security Governance Maturity. *International Symposium on Technology and Society, Proceedings*, *2016-March*, 1–8. https://doi.org/10.1109/ISTAS.2015.7439415

de Neira, A. B., Kantarci, B., & Nogueira, M. (2023). Distributed denial of service attack prediction: Challenges, open issues and opportunities. *Computer Networks*, *222*(December 2022), 109553. https://doi.org/10.1016/j.comnet.2022.109553

Deloitte. (2022). *Government Trends in 2022*.

Deloitte. (2014). Cyber security: everybody's imperative. *Deloitte Advisory*, 16.

Deloitte. (2019). *Behavior-first government transformation*. **URL:***https://www2.deloitte.com/us/en/insights/economy/covid-19/behavioral-science-in-government-transformation.html*

Deloitte. (2021). *Government Trends in 2021*.

Drivas, G., Chatzopoulou, A., Maglaras, L., Lambrinoudakis, C., Cook, A., & Janicke, H. (2020). A NIS Directive Compliant Cybersecurity Maturity Assessment Framework. *Proceedings - 2020 IEEE 44th Annual Computers, Software, and Applications Conference, COMPSAC 2020*, 1641–1646. https://doi.org/10.1109/COMPSAC48688.2020.00-20

Dudley, E., Lin, D.-Y., Mancini, M., & Ng, J. (2015). *Implementing a citizen-centric approach to delivering government services*. *July*, 3–9.

Durman, O., Durman, M., Topalova, E., Grytsak, L., & Zhiliaieva, O. (2021). An economic model to assess the effectiveness of economic cooperation between Ukraine and international non-government organization. *Journal of Eastern European and Central Asian Research*, *8*(1), 62–80. https://doi.org/10.15549/jeecar.v8i1.640

Economic Commission for Latin America and the Caribbean (ECLAC). (2021). *Digital technologies for a new future*.

Edwards, M. M. (2018). *Identifying Factors Contributing Towards Information Security Maturity in an Organization. Doctoral dissertation.* Nova Southeastern University. Retrieved from NSUWorks, College of Engineering and Computing (Issue 1027).

EIF. (2017). European Interoperability Framework. In *White Pages*. https://doi.org/10.2799/78681

Ekinci, Ö. (2021). *Smart Government Transformation : Opportunities , Challenges and Change Management Strategies* (Issue May). University of Ljubljana.

El-Haddadeh, R., Weerakkody, V., Osmani, M., Thakker, D., & Kapoor, K. K. (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

ElKheshin, S. A. (2016). Determinants of E-Government Services Adoption in Developing Countries (Egypt). *Phd Thesis*, 1–237.

Elsheikh, Y., Alqasrawi, Y., & Azzeh, M. (2022). On obtaining a stable vote ranking methodology for implementing e-government strategies. *Journal of King Saud University - Computer and Information Sciences*, *34*(6), 3379–3392. https://doi.org/10.1016/j.jksuci.2020.11.035

Eom, S. J., & Lee, J. (2022). Digital government transformation in turbulent times: Responses, challenges, and future direction. In *Government Information Quarterly* (Vol. 39, Issue 2). Elsevier Ltd. https://doi.org/10.1016/j.giq.2022.101690

Erdoğan, M., Karaşan, A., Kaya, İ., Budak, A., & Çolak, M. (2020). A fuzzy based MCDM methodology for risk evaluation of cyber security technologies. *Advances in Intelligent Systems and Computing*, *1029*, 1042–1049. https://doi.org/10.1007/978-3-030-23756-1_123

Ernst and Young. (2022). *How can government workers and technology align to serve future citizens?* **URL:**https://assets.ey.com/content/dam/ey-sites/ey-com/en_gl/topics/government-and-public-sector/ey-digital-state-workforce-report.pdf

Erzhenin, R. V. (2018). Russian e-government: Review of scientific publications and research. In *Public Administration Issues* (Vol. 2018, Issue 3, pp. 205–228).

ESCAP. (2021). *Digital government and transformation*. https://repository.unescap.org/bitstream/handle/20.500.12870/4515/ESCAP-2021-MN-Digital-government-transformation.pdf?sequence=1&isAllowed=y

EuroControl. (2017). *ATM Cybersecurity Maturity Model Level 1* (Issue October).

European Commission. (2021). *2030 Digital Compass: the European way for the Digital Decade*.

European Commission. (2022a). Digital Economy and Society Index 2022: Methodological Note. *Clinical Epigenetics*, 1–14.

European Commission. (2022b). *eGovernment Benchmark 2022 Synchronising Digital Governments Analyze the Future*.

Ferreira, J., Claver, P., Pereira, P., & Thomaz, S. (2020). Remote Working and the Platform of the Future. In *BCG* (Issue October).

Gaehtgens, F., Hoover, J., Teixeira, H., Neiva, C., Kelley, M., Ruddy, M., & Hevesi, P. (2022). *Gartner, Top Strategic Technology Trends for 2022: Cybersecurity Mesh*.

Gao, H., Ju, Y., Zeng, X. J., & Zhang, W. (2021). Satisfaction-driven consensus model for social network MCGDM with incomplete information under probabilistic linguistic trust. *Computers and Industrial Engineering*, *154*(May 2020), 107099. https://doi.org/10.1016/j.cie.2021.107099

Garba, A. A., Siraj, M. M., & Othman, S. H. (2020). An explanatory review on cybersecurity capability maturity models. *Advances in Science, Technology and Engineering Systems*, *5*(4), 762–769. https://doi.org/10.25046/AJ050490

Gartner. (2019). *Public Power Cybersecurity Roadmap*.

Gartner. (2021). *IT Roadmap for Cybersecurity Excerpt*.

Gartner. (2023a). *Gartner's Top Cybersecurity Predictions 2023-2024*.

Gartner. (2023b). *Top 3 Strategic Priorities for Security and Risk Management Leaders Leadership Vision for 2023*.

Gholami Mehrabadi, M., Kassaee, M., & Arabsorkhi, A. (2019). A novel maturity model for MSSP assessment. *International Journal of Information and Communication Technology Research*, *11*(1), 57–70.

Gil-García, J. R. (2004). Information technology policies and standards: A comparative review of the states. *Journal of Government Information*, *30*(5–6), 548–560. https://doi.org/10.1016/j.jgi.2004.10.001

Gil-Garcia, J. R., Dawes, S. S., & Pardo, T. A. (2018). Digital government and public management research: finding the crossroads. *Public Management Review*, *20*(5), 633–646. https://doi.org/10.1080/14719037.2017.1327181

Gil-Garcia, J. R., & Flores-Zúñiga, M. (2020). Towards a comprehensive understanding of digital government success: Integrating implementation and adoption factors. *Government Information Quarterly*, *37*(4). https://doi.org/10.1016/j.giq.2020.101518

Gil-Garcia, J. R., Gasco-Hernandez, M., & Pardo, T. A. (2020). Beyond Transparency, Participation, and Collaboration? A Reflection on the Dimensions of Open Government. *Public Performance and Management Review*, *43*(3), 483–502. https://doi.org/10.1080/15309576.2020.1734726

Gil-Garcia, J. R., Pardo, T. A., & Gasco-Hernandez, M. (2020). *Beyond Smart and Connected Governments*. Springer.

Gimenez-Aguilar, M., de Fuentes, J. M., Gonzalez-Manzano, L., & Arroyo, D. (2021). Achieving cybersecurity in blockchain-based systems: A survey. *Future Generation Computer Systems*, *124*, 91–118. https://doi.org/10.1016/j.future.2021.05.007

Giuca, O., Popescu, T. M., Popescu, A. M., Prostean, G., & Popescu, D. E. (2021). A survey of cybersecurity risk management frameworks. In *Advances in Intelligent Systems and Computing: Vol. 1221 AISC*. https://doi.org/10.1007/978-3-030-51992-6_20

Gjaltema, J., Biesbroek, R., & Termeer, K. (2020). From government to governance…to meta-governance: a systematic literature review. *Public Management Review*, *22*(12), 1760–1780. https://doi.org/10.1080/14719037.2019.1648697

Gong, Y., Yang, J., & Shi, X. (2020). Towards a comprehensive understanding of digital transformation in government: Analysis of flexibility and enterprise architecture. *Government Information Quarterly*, *37*(3). https://doi.org/10.1016/j.giq.2020.101487

Gou, X., Xu, Z., & Liao, H. (2017). Multiple criteria decision making based on Bonferroni means with hesitant fuzzy linguistic information. *Soft Computing*, *21*(21), 6515–6529. https://doi.org/10.1007/s00500-016-2211-1

Gourisetti, S. N. G., Mylrea, M., & Patangia, H. (2020). Cybersecurity vulnerability mitigation framework through empirical paradigm: Enhanced prioritized gap analysis. *Future Generation Computer Systems*, *105*(2), 410–431. https://doi.org/10.1016/j.future.2019.12.018

GovNet. (2023). *GovNet*. https://blog.govnet.co.uk/technology/what-is-the-definition-of-organisational-culture-in-the-public-sector

Greco, M., Locatelli, G., & Lisi, S. (2017). Open innovation in the power & energy sector: Bringing together government policies, companies' interests, and academic essence. *Energy Policy*, *104*(November 2016), 316–324. https://doi.org/10.1016/j.enpol.2017.01.049

Guenduez, A. A., Oberli, M., Schedler, K., Tomczak, T., & Singler, S. (2018). *Smart Government Success Factors. Swiss Yearbook of Administrative Sciences, 9 (1), 96–110*. https://doi.org/10.5334/ssas.124

Güler, M., & Büyüközkan, G. (2023). A Survey of Digital Government: Science Mapping Approach, Application Areas, and Future Directions. *Systems*, *11*(12), 563. https://doi.org/10.3390/systems11120563

Gupta Gourisetti, N., Mylrea, M., & Patangia, H. (2019). Application of rank-weight methods to blockchain cybersecurity vulnerability assessment framework. *2019 IEEE 9th Annual Computing and Communication Workshop and Conference, CCWC 2019*, 206–213. https://doi.org/10.1109/CCWC.2019.8666518

Gupta, S., & Gupta, S. (2017). Modeling economic system using fuzzy cognitive maps. *International Journal of System Assurance Engineering and Management*, *8*(s2), 1472–1486. https://doi.org/10.1007/s13198-017-0616-6

Haneem, F., Kama, N., Taskin, N., Pauleen, D., & Abu Bakar, N. A. (2019). Determinants of master data management adoption by local government organizations: An empirical study. *International Journal of Information Management*, *45*, 25–43. https://doi.org/10.1016/J.IJINFOMGT.2018.10.007

Hasan, M., Maarop, N., Naswir, R. Y., Samy, G. N., Magalingam, P., Yaácob, S., & Daud, S. M. (2018). A proposed conceptual success model of citizen-centric digital government in Malaysia. *Journal of Fundamental and Applied Sciences*, *10*(2S), 35–46.

Hasan, S., Ali, M., Kurnia, S., & Thurasamy, R. (2021). Evaluating the cyber security readiness of organizations and its influence on performance. *Journal of Information Security and Applications*, *58*, 102726. https://doi.org/10.1016/j.jisa.2020.102726

Hassan, M. H., & Lee, J. (2019). Policymakers' perspective about e-Government success using AHP approach: Policy implications towards entrenching Good Governance in Pakistan. *Transforming Government: People, Process and Policy*, *13*(1), 93–118. https://doi.org/10.1108/TG-03-2018-0017

Hussain, M. (2017). *M-government Implementation : A Comparative Study between a Developed and a Developing Country*. *August*.

Iakovidis, D. K., & Papageorgiou, E. (2011). Intuitionistic Fuzzy Cognitive Maps for Medical Decision Making. *IEEE Transactions on Information Technology in Biomedicine*, *15*(1), 100–107. https://doi.org/10.1109/TITB.2010.2093603

IDB. (2020). *Environmental and Social Policy Framework*.

Idzi, F. M., & Gomes, R. C. (2022). Digital governance: government strategies that impact public services. *Global Public Policy and Governance*, *2*(4), 427–452. https://doi.org/10.1007/s43508-022-00055-w

Institute for Government. (2021). *Digital government during the coronavirus crisis*.

Ionescu, A. M., Clipa, A. M., Turnea, E. S., Clipa, C. I., Bedrule-Grigoruță, M. V., & Roth, S. (2022). the Impact of Innovation Framework Conditions on Corporate Digital Technology Integration: Institutions As Facilitators for Sustainable Digital Transformation. *Journal of Business Economics and Management*, *23*(5), 1037–1059. https://doi.org/10.3846/jbem.2022.17039

Janowski, T. (2015). Digital government evolution: From transformation to contextualization. *Government Information Quarterly*, *32*(3), 221–236. https://doi.org/10.1016/J.GIQ.2015.07.001

Janssen, M., Rana, N. P., Slade, E. L., & Dwivedi, Y. K. (2018). Trustworthiness of digital government services: deriving a comprehensive theory through interpretive structural modelling. *Public Management Review*, *20*(5), 647–671. https://doi.org/10.1080/14719037.2017.1305689

Jaquire, V., & Von Solms, S. (2017). Developing a cyber counterintelligence maturity model for developing countries. *2017 IST-Africa Week Conference, IST-Africa 2017*, *Cci*, 1–8. https://doi.org/10.23919/ISTAFRICA.2017.8102288

Jiang, S., Jiang, S., He, W., Qin, F., & Cheng, Q. (2020). Multiple Attribute Group Decision-Making Based on Power Heronian Aggregation Operators under Interval-Valued Dual Hesitant Fuzzy Environment. *Mathematical Problems in Engineering*, *2020*. https://doi.org/10.1155/2020/2080413

Jin, F., Zhang, Y., Garg, H., Liu, J., & Chen, J. (2022). Evaluation of small and medium-sized enterprises' sustainable development with hesitant fuzzy linguistic group decision-making method. *Applied Intelligence*, *52*(5), 4940–4960. https://doi.org/10.1007/s10489-021-02372-9

Jmila, H., & Khedher, M. I. (2022). Adversarial machine learning for network intrusion detection: A comparative study. *Computer Networks*, *214*(April). https://doi.org/10.1016/j.comnet.2022.109073

Juno Risk Solutions. (2015). *Cybersecurity Best Practices Guide For IIROC Dealer Members*. 1–53.

Kalhoro, S., Rehman, M., Ponnusamy, V., & Shaikh, F. B. (2021). Extracting key factors of cyber hygiene behaviour among software engineers: A systematic literature review. *IEEE Access*, *9*, 99339–99363. https://doi.org/10.1109/ACCESS.2021.3097144

Kam, H. J., Ormond, D. K., Menard, P., & Crossler, R. E. (2022). That's interesting: An examination of interest theory and self-determination in organisational cybersecurity training. *Information Systems Journal*, *32*(4), 888–926. https://doi.org/10.1111/isj.12374

Karabacak, B., Yildirim, S. O., & Baykal, N. (2016). A vulnerability-driven cyber security maturity model for measuring national critical infrastructure protection preparedness. *International Journal of Critical Infrastructure Protection*, *15*, 47–59. https://doi.org/10.1016/j.ijcip.2016.10.001

Karokola, G., Kowalski, S., & Yngström, L. (2011). Towards an information security maturity model for secure e-Government services: A stakeholders view. *Proceedings of the 5th International Symposium on Human Aspects of Information Security and Assurance, HAISA 2011*, 58–73.

Katie Terrell Hanna. (2023). *What is gap analysis?* https://www.techtarget.com/searchcio/definition/gap-analysis

Kaya, T., Sağsan, M., Medeni, T., Medeni, T., & Yıldız, M. (2020). Qualitative analysis to determine decision-makers' attitudes towards e-government services in a De-Facto state. *Journal of Information, Communication and Ethics in Society*. https://doi.org/10.1108/JICES-05-2019-0052

Kaya, T., Sağsan, M., Yıldız, M., Medeni, T., & Medeni, T. (2020). Citizen Attitudes Towards E-Government Services. *International Journal of Public Administration in the Digital Age*, *7*(1), 17–32. https://doi.org/10.4018/ijpada.2020010102

Khatib, H., Lee, H., Suh, C., & Weerakkody, V. (2019). e-Government systems success and user acceptance in developing countries: The role of perceived support quality.

Asia Pacific Journal of Information Systems, *29*(1), 1–34. https://doi.org/10.14329/apjis.2019.29.1.1

Kim, T. H., Hong, G. H., & Park, S. C. (2008). Developing an intelligent web information system for minimizing information gap in government agencies and public institutions. *Expert Systems with Applications*, *34*(3), 1618–1629. https://doi.org/10.1016/j.eswa.2007.01.041

Kitchenham, B. (2004). Procedures for performing systematic reviews. *Keele, UK, Keele University*, *33*(2004), 1–26.

Kosko, B. (1986). Fuzzy cognitive maps. *International Journal of Man-Machine Studies*, *24*(1), 65–75.

Kosko, B., & Burgess, J. C. (1998). *Neural networks and fuzzy systems*. Acoustical Society of America.

Kour, R., & Karim, R. (2020). Cybersecurity workforce in railway: its maturity and awareness. *Journal of Quality in Maintenance Engineering*, *27*(3), 453–464. https://doi.org/10.1108/JQME-07-2020-0059

KPMG. (2017). *Cyber Maturity Assessment*.

KPMG International. (2021). *Modernizing Government: Global Trends*. 1–41.

Krawczyk-Sokołowska, I., & Caputa, W. (2023). Awareness of network security and customer value – The company and customer perspective. *Technological Forecasting and Social Change*, *190*(December 2022). https://doi.org/10.1016/j.techfore.2023.122430

Kritzinger, E. (2020). Improving cybersafety maturity of South African schools. *Information (Switzerland)*, *11*(10), 1–17. https://doi.org/10.3390/info11100471

Kurtul, A., Zeyveli, M. F., İnce Y., Yıldız, K., Yüce F., Yakaryılmaz, F. (2020). *Siber Güvenlik Raporu,* Bilişim İnovasyon Derneği.

Lamid, L. I., Ibrahim, I. A., Abdullahi, K. I., & Abdullahi, U. G. (2021). A Framework for Digital Government Transformation Performance Assessment and Toolkit for Developing Countries. *ACM International Conference Proceeding Series*, 203–215. https://doi.org/10.1145/3494193.3494222

Law, N., Woo, D., de la Torre, J., & Wong, G. (2018). A Global Framework of Reference on Digital Literacy Skills for Indicator 4.4.2. *Information Paper N°51*, *51*, 146.

Lee, J., Kim, B. J., Park, S. J., Park, S., & Oh, K. (2018). Proposing a value-based digital government model: Toward broadening sustainability and public participation. *Sustainability (Switzerland)*, *10*(9). https://doi.org/10.3390/su10093078

Li, E., Chen, Q., Zhang, X., & Zhang, C. (2023). Digital Government Development, Local Governments' Attention Distribution and Enterprise Total Factor Productivity: Evidence from China. *Sustainability (Switzerland)*, *15*(3). https://doi.org/10.3390/su15032472

Li, H., & Kostka, G. (2022). Accepting but not engaging with it: Digital participation in local government-run social credit systems in China. *Policy and Internet*, *14*(4), 845–874. https://doi.org/10.1002/poi3.316

Li, J., Niu, L., Chen, Q., & Wang, Z. (2021). Approaches for multicriteria decision-making based on the hesitant fuzzy best-worst method. *Complex & Intelligent Systems*, *7*(5, SI), 2617–2634. https://doi.org/10.1007/s40747-021-00406-w

Li, J., Niu, L., Chen, Q., Wang, Z., & Li, W. (2022). Group decision making method with hesitant fuzzy preference relations based on additive consistency and consensus. *Complex & Intelligent Systems*. https://doi.org/10.1007/s40747-021-00585-6

Li, J., Ye, J., Niu, L., Chen, Q., & Wang, Z. (2022). Decision-making models based on satisfaction degree with incomplete hesitant fuzzy preference relation. *Soft Computing*, *26*(7), 3129–3145. https://doi.org/10.1007/s00500-021-06635-y

Li, L., He, W., Xu, L., Ash, I., Anwar, M., & Yuan, X. (2019). Investigating the impact of cybersecurity policy awareness on employees' cybersecurity behavior. *International Journal of Information Management*, *45*(February 2018), 13–24. https://doi.org/10.1016/j.ijinfomgt.2018.10.017

Li, Y., & Shang, H. (2020). Service quality, perceived value, and citizens' continuous-use intention regarding e-government: Empirical evidence from China. *Information and Management*, *57*(3). https://doi.org/10.1016/j.im.2019.103197

Liao, H., Qin, R., Gao, C., Wu, X., Hafezalkotob, A., & Herrera, F. (2019). Score-HeDLiSF: A score function of hesitant fuzzy linguistic term set based on hesitant degrees and linguistic scale functions: An application to unbalanced hesitant fuzzy linguistic MULTIMOORA. *Information Fusion*, *48*, 39–54. https://doi.org/10.1016/j.inffus.2018.08.006

Liu, H., & Rodríguez, R. M. (2014). A fuzzy envelope for hesitant fuzzy linguistic term set and its application to multicriteria decision making. *Information Sciences*, *258*, 220–238. https://doi.org/10.1016/J.INS.2013.07.027

Liu, J., Huang, C., Song, J., Du, P., Jin, F., & Chen, H. (2021). Group decision making based on the modified probability calculation method and DEA cross-efficiency with probabilistic hesitant fuzzy preference relations. *Computers & Industrial Engineering*, *156*. https://doi.org/10.1016/j.cie.2021.107262

Liu, X., Wang, Z., Zhang, S., & Liu, J. (2019). A novel approach to fuzzy cognitive map based on hesitant Fuzzy sets for modeling risk impact on electric power system. *International Journal of Computational Intelligence Systems*, *12*(2), 842–854. https://doi.org/10.2991/ijcis.d.190722.001

Liu, Y., Li, H., Kostakos, V., Goncalves, J., Hosio, S., & Hu, F. (2014). An empirical investigation of mobile government adoption in rural China: A case study in Zhejiang province. *Government Information Quarterly*, *31*(3), 432–442. https://doi.org/10.1016/j.giq.2014.02.008

Loft, P., He, Y., Yevseyeva, I., & Wagner, I. (2022). CAESAR8: An agile enterprise architecture approach to managing information security risks. *Computers and Security*, *122*, 102877. https://doi.org/10.1016/j.cose.2022.102877

Long, Y., & Gil-Garcia, J. R. (2020). The cost of citizen access to government services in China: A survey of eight common services in all provinces. *ACM International Conference Proceeding Series*, *20*, 319–321. https://doi.org/10.1145/3396956.3396999

Lu, Y., Xu, Y., Huang, J., Wei, J., & Herrera-Viedma, E. (2022). Social network clustering and consensus-based distrust behaviors management for large-scale group decision-making with incomplete hesitant fuzzy preference relations. *Applied Soft Computing*, *117*. https://doi.org/10.1016/j.asoc.2021.108373

Luna-Reyes, L. F., Andersen, D. F., Black, L. J., & Pardo, T. A. (2021). Sensemaking and social processes in digital government projects. *Government Information Quarterly*, *38*(2), 101570.

Macas, M., Wu, C., & Fuertes, W. (2022). A survey on deep learning for cybersecurity: Progress, challenges, and opportunities. *Computer Networks*, *212*(February), 109032. https://doi.org/10.1016/j.comnet.2022.109032

Magoutas, B., & Mentzas, G. (2010). SALT: A semantic adaptive framework for monitoring citizen satisfaction from e-government services. *Expert Systems with Applications*, *37*(6), 4292–4300. https://doi.org/10.1016/j.eswa.2009.11.071

Mahmood, M., Weerakkody, V., & Chen, W. (2019). The influence of transformed government on citizen trust: insights from Bahrain. *Information Technology for Development*, *25*(2), 275–303. https://doi.org/10.1080/02681102.2018.1451980

Mahundu, F. G. (2015). *E-Governance In The Public Sector: a Case Study of the Central Admission System in Tanzania*.

Makki, A. A., & Alqahtani, A. Y. (2022). Modeling the Barriers Surrounding Digital Government Implementation: Revealing Prospect Opportunities in Saudi Arabia. *Sustainability (Switzerland)*, *14*(23). https://doi.org/10.3390/su142315780

Malatji, M., Marnewick, A., & von Solms, S. (2020). Validation of a socio-technical management process for optimising cybersecurity practices. *Computers and Security*, *95*, 101846. https://doi.org/10.1016/j.cose.2020.101846

Malodia, S., Dhir, A., Mishra, M., & Bhatti, Z. A. (2021). Future of e-Government: An integrated conceptual framework. *Technological Forecasting and Social Change*, *173*(December 2020), 121102. https://doi.org/10.1016/j.techfore.2021.121102

Margetts, H., & Naumann, A. (2017). Government as a platform: What can Estonia show the world. In *Research paper, University of Oxford*. ospi.es

Marican, M. N. Y., Razak, S. A., Selamat, A., & Othman, S. H. (2023). Cyber Security Maturity Assessment Framework for Technology Startups: A Systematic Literature Review. *IEEE Access*, *11*(November 2022), 5442–5452. https://doi.org/10.1109/ACCESS.2022.3229766

Markinos, A., Papageorgiou, E., Stylios, C., & Gemtos, T. (2007). Introducing Fuzzy Cognitive Maps for decision making in precision agriculture. *Precision Agriculture 2007 - Papers Presented at the 6th European Conference on Precision Agriculture, ECPA 2007*, 223–231.

Matheus, R., & Janssen, M. (2020). A Systematic Literature Study to Unravel Transparency Enabled by Open Government Data: The Window Theory. *Public Performance and Management Review*, *43*(3), 503–534. https://doi.org/10.1080/15309576.2019.1691025

Matheus, R., Janssen, M., & Janowski, T. (2021). Design principles for creating digital transparency in government. *Government Information Quarterly*, *38*(1), 101550. https://doi.org/10.1016/j.giq.2020.101550

Mattioli, R., & Moulinos, Konstantinos, E. (2015). Analysis of ICS-SCADA Cyber Security Maturity Levels in Critical Sectors. In *Enisa*.

McDaniel, S. (2022). *E-Governance in Urban Planning: Use and management of websites in Puget Sound planning offices*. University of Washington.

McKinsey & Company. (2020). *A government blueprint to adapt the ecosystem to the future of work*. **URL:***https://www.mckinsey.com/industries/public-sector/our-insights/a-government-blueprint-to-adapt-the-ecosystem-to-the-future-of-work*

McKinsey &Company. (2022). *Transforming government in a new era* (Issue September). **URL:***https://www.mckinsey.com/industries/public-sector/our-insights/transforming-government-in-a-new-era*

Meijer, K. (2019). *Designing a co-creation tool for an innovation platform in the Dutch e-Government.*

Meng, F.-Y., Tang, J., Pedrycz, W., & An, Q.-X. (2021). Optimal Interaction Priority Calculation From Hesitant Fuzzy Preference Relations Based on the Monte Carlo Simulation Method for the Acceptable Consistency and Consensus. *IEEE Transactions On Cybernetics*, *51*(12), 5871–5882. https://doi.org/10.1109/TCYB.2019.2962095

Merigó, J. M., Cancino, C. A., Coronado, F., & Urbano, D. (2016). Academic research in innovation: a country analysis. *Scientometrics*, *108*, 559–593.

Mi, X., Wu, X., Tang, M., Liao, H., Al-Barakati, A., Altalhi, A. H., & Herrera, F. (2019). Hesitant Fuzzy Linguistic Analytic Hierarchical Process With Prioritization, Consistency Checking, and Inconsistency Repairing. *IEEE Access*, *7*, 44135–44149. https://doi.org/10.1109/ACCESS.2019.2908701

Microsoft. (2018). *The Digital Transformation of Government*. https://info.microsoft.com/rs/157-GQE-382/images/EN-CNTNT-ebook-TheDigitalTransformationofGovernment.pdf

Moher, D., Altman, D. G., & Tetzlaff, J. (1996). PRISMA (Preferred Reporting items for systematic reviews and Meta-Analyses). *Guidelines for Reporting Health Research: A User's Manual*, *1999*, 250.

Moreira, F. R., Da Silva Filho, D. A., Nze, G. D. A., De Sousa Junior, R. T., & Nunes, R. R. (2021). Evaluating the Performance of NIST's Framework Cybersecurity Controls through a Constructivist Multicriteria Methodology. *IEEE Access*, *9*, 129605–129618. https://doi.org/10.1109/ACCESS.2021.3113178

Morris, D., Madzudzo, G., & Garcia-Perez, A. (2020). Cybersecurity threats in the auto industry: Tensions in the knowledge environment. *Technological Forecasting and Social Change*, *157*(May 2019), 120102. https://doi.org/10.1016/j.techfore.2020.120102

Mourtada, R., Felden, F., Bruehwiler, R., & Joykutty, T. (2022). *Digital Government Transformation in the Middle East*. *August*.

Mousavi, S. M., Gitinavard, H., & Siadat, A. (2014). A new hesitant fuzzy analytical hierarchy process method for decision-making problems under uncertainty. *IEEE International Conference on Industrial Engineering and Engineering Management*, *2015-Janua*(x), 622–626. https://doi.org/10.1109/IEEM.2014.7058713

Mujali Al-rawahna, A. S., Chen, S.-C., & Hung, C.-W. (2018). The Barriers of E-Government Success : An Empirical Study from Jordan. *International Journal of Managing Public Sector Information and Communication Technologies*, *9*(2), 01–18. https://doi.org/10.5121/ijmpict.2018.9201

Multi-State Information Sharing & Analysis Center. (2016). Nationwide Cyber Security Review Assesment. In *U.S. Department of Homeland Security under*.

Muronga, K., Herselman, M., Botha, A., & Da Veiga, A. (2019). An Analysis of Assessment Approaches and Maturity Scales used for Evaluation of Information Security and Cybersecurity User Awareness and Training Programs: A Scoping Review. *2nd International Conference on Next Generation Computing Applications 2019, NextComp 2019 - Proceedings*. https://doi.org/10.1109/NEXTCOMP.2019.8883535

Ndlovu, N., Ochara, N. M., & Martin, R. (2022). Influence of digital government innovation on transformational government in resource-constrained contexts. *Journal of Science and Technology Policy Management*. https://doi.org/10.1108/JSTPM-11-2021-0173

Newman, J., Mintrom, M., & O'Neill, D. (2022). Digital technologies, artificial intelligence, and bureaucratic transformation. *Futures*, *136*(April 2021), 102886. https://doi.org/10.1016/j.futures.2021.102886

Nikaj, B. (2017). *From No-government to E-government state-building in post-conflict situations*. https://www.merit.unu.edu/training/theses/NIKAJ.pdf

NIST Cybersecurity Framework Team. (2018). *Framework for improving critical infrastructure cybersecurity* (Vol. 535).

Noor, U., Anwar, Z., Altmann, J., & Rashid, Z. (2020). Customer-oriented ranking of cyber threat intelligence service providers. *Electronic Commerce Research and Applications*, *41*(February), 100976. https://doi.org/10.1016/j.elerap.2020.100976

Oe, H., Yamaoka, Y., & Hideshima, E. (2016). How to support decision making of local government in prioritising policy menu responding to citizens' views: An exploratory study of text mining approach to attain cognitive map based on citizen survey data. *Lecture Notes in Business Information Processing*, *250*, 202–216. https://doi.org/10.1007/978-3-319-32877-5_15

OECD. (2020). The OECD Digital Government Policy Framework : Six dimensions of a Digital Government. *Public Governance Policy Papers*, *02*, 1–40. https://www.oecd-ilibrary.org/governance/the-oecd-digital-government-policy-framework_f64fed2a-en;jsessionid=XhJD9gaDdxvdGv3T4xLK-28I.ip-10-240-5-68

OECD. (2022). Good Practice Principles for Data Ethics in the Public Sector. *Organisation for Economic Co-Operation and Development*, 1–16.

OECD. (2023). *Digital Government Review of Türkiye* (OECD Digital Government Studies). OECD. https://doi.org/10.1787/3958d102-en

Office of the Under Secretary of Defense For Acquisition, T. and L. W. (2003). *The Role and Status of DoD Red Teaming Activities*.

Omar, A., Weerakkody, V., & Daowd, A. (2020). Studying Transformational Government: A review of the existing methodological approaches and future outlook. *Government Information Quarterly*. https://doi.org/10.1016/j.giq.2020.101458

OPDC. (2018). *Government Innovation Lab in Thailand*.

Orlovsky, S. A. (1978). Decision-making with a fuzzy preference relation. *Fuzzy Sets and Systems*, *1*(3), 155–167. https://doi.org/10.1016/0165-0114(78)90001-5

Osman, I. H., Anouze, A. L., Irani, Z., Al-Ayoubi, B., Lee, H., Balc, A., Medeni, T. D., & Weerakkody, V. (2014). COBRA framework to evaluate e-government services:

A citizen-centric perspective. *Government Information Quarterly*, *31*(2), 243–256. https://doi.org/10.1016/j.giq.2013.10.009

Osman, I. H., Anouze, A. L., Irani, Z., Al-Ayoubi, B., Lee, H., Balcı, A., Medeni, T. D., & Weerakkody, V. (2014). COBRA framework to evaluate e-government services: A citizen-centric perspective. *Government Information Quarterly*, *31*(2), 243–256. https://doi.org/10.1016/j.giq.2013.10.009

Osman, I. H., Anouze, A. L., Irani, Z., Lee, H., Medeni, T. D., & Weerakkody, V. (2019). A cognitive analytics management framework for the transformation of electronic government services from users' perspective to create sustainable shared values. *European Journal of Operational Research*. https://doi.org/10.1016/j.ejor.2019.02.018

Öztayşi, B., Çevik, S., Seker, S., & Kahraman, C. (2019). Water treatment technology selection using hesitant Pythagorean fuzzy hierachical decision making. *Journal of Intelligent & Fuzzy Systems*, *37*, 1–18. https://doi.org/10.3233/JIFS-181538

Papageorgiou, E. I., & Iakovidis, D. K. (2013). Intuitionistic Fuzzy Cognitive Maps. *IEEE Transactions on Fuzzy Systems*, *21*(2), 342–354. https://doi.org/10.1109/TFUZZ.2012.2214224

Patergiannaki, Z., & Pollalis, Y. (2023). E-Government maturity assessment: Evidence from Greek municipalities. *Policy and Internet*, *15*(1), 6–35. https://doi.org/10.1002/poi3.317

Pérez-Morote, R., Pontones-Rosa, C., & Núñez-Chicharro, M. (2020). The effects of e-government evaluation, trust and the digital divide in the levels of e-government use in European countries. *Technological Forecasting and Social Change*, *154*(March), 119973. https://doi.org/10.1016/j.techfore.2020.119973

Petter, S., DeLone, W., & McLean, E. (2008). Measuring information systems success: models, dimensions, measures, and interrelationships. *European Journal of Information Systems*, *17*, 236–263.

Piscopo, A., Siebes, R., & Hardman, L. (2017). Predicting Sense of Community and Participation by Applying Machine Learning to Open Government Data. *Policy and Internet*, *9*(1), 55–75. https://doi.org/10.1002/poi3.145

Polireddi, N. S. A., & Sekhar, K. R. (2023). Improved fuzzy-based MCDM–TOPSIS model to find and prevent the financial system vulnerability and hazards in real time. *Soft Computing*, *2*. https://doi.org/10.1007/s00500-023-08318-2

Porrúa, M., & Contreras B, I. (2020). *Cybersecurity: risks, progress, and the way forward in Latin America and the Caribbean* (Vol. 1).

Porumbescu, G. A., Cucciniello, M., & Gil-Garcia, J. R. (2020). Accounting for citizens when explaining open government effectiveness. *Government Information Quarterly*. https://doi.org/10.1016/j.giq.2019.101451

Priyadarshini, I., Kumar, R., Sharma, R., Singh, P. K., & Satapathy, S. C. (2021). Identifying cyber insecurities in trustworthy space and energy sector for smart grids. *Computers and Electrical Engineering*, *93*(May), 107204. https://doi.org/10.1016/j.compeleceng.2021.107204

Puron-Cid, G., Luna, D. E., Picazo-Vela, S., Gil-Garcia, J. R., Sandoval-Almazan, R., & Luna-Reyes, L. F. (2022). Improving the assessment of digital services in government websites: Evidence from the Mexican State government portals ranking. *Government Information Quarterly*, *39*(1). https://doi.org/10.1016/j.giq.2021.101589

Putra, A. P. G., Humani, F., Zakiy, F. W., Shihab, M. R., & Ranti, B. (2020). Maturity assessment of cyber security in the workforce management domain: A case study in bank indonesia. *2020 International Conference on Information Technology Systems and Innovation, ICITSI 2020 - Proceedings*, 89–94. https://doi.org/10.1109/ICITSI50517.2020.9264982

PwC. (2021). *Building a digital government Seven trends in digital government*. www.pwc.com/ca/digitalgovernment

PwC. (2022). *The Journey to Digital Government*. 207–224.

Rabii, A., Assoul, S., Ouazzani Touhami, K., & Roudies, O. (2020). Information and cyber security maturity models: a systematic literature review. *Information and Computer Security*, *28*(4), 627–644. https://doi.org/10.1108/ICS-03-2019-0039

Rajan, R., Rana, N. P., Parameswar, N., Dhir, S., Sushil, & Dwivedi, Y. K. (2021). Developing a modified total interpretive structural model (M-TISM) for organizational strategic cybersecurity management. *Technological Forecasting and Social Change*, *170*(January), 120872. https://doi.org/10.1016/j.techfore.2021.120872

Ramon Gil-Garcia, J., Chengalur-Smith, I. S., & Duchessi, P. (2007). Collaborative e-Government: Impediments and benefits of information-sharing projects in the public

sector. *European Journal of Information Systems*, *16*(2), 121–133. https://doi.org/10.1057/palgrave.ejis.3000673

Re, B. (2010). *Quality of (Digital) Services in e-Government*.

Rea-Guaman, A. M., San Feliu, T., Calvo-Manzano, J. A., & Sanchez-Garcia, I. D. (2017). Comparative study of cybersecurity capability maturity models. *Communications in Computer and Information Science*, *770*, 100–113. https://doi.org/10.1007/978-3-319-67383-7_8

REBIT. (2017). Cyber Security Maturity Model (CMM). In *REBIT*.

Ren, Z., Xu, Z., & Wang, H. (2019). The Strategy Selection Problem on Artificial Intelligence With an Integrated VIKOR and AHP Method Under Probabilistic Dual Hesitant Fuzzy Information. *IEEE Access*, *7*, 103979–103999. https://doi.org/10.1109/access.2019.2931405

Results, F. S. (2022). *Information Security Maturity Report 2022*.

Riadi, I., Yanto, I. T. R., & Handoyo, E. (2020). Analysis of academic service cybersecurity in university based on framework COBIT 5 using CMMI. *IOP Conference Series: Materials Science and Engineering*, *821*(1). https://doi.org/10.1088/1757-899X/821/1/012003

Roberts, R. (2016). *Measuring Cybersecurity Readiness : The Cybersecurity Maturity Model What is a Cybersecurity Maturity Model ?*

Rodríguez, R. M., Martinez, L., & Herrera, F. (2011). Hesitant fuzzy linguistic term sets for decision making. *IEEE Transactions on Fuzzy Systems*, *20*(1), 109–119.

Rodriguez-Repiso, L., Setchi, R., & Salmeron, J. L. (2007). Modelling IT projects success with Fuzzy Cognitive Maps. *Expert Systems with Applications*, *32*(2), 543–559. https://doi.org/10.1016/j.eswa.2006.01.032

Saaty, T. L. (1990). How to make a decision: the analytic hierarchy process. *European Journal of Operational Research*, *48*(1), 9–26.

Sahu, K., Alzahrani, F. A., Srivastava, R. K., & Kumar, R. (2021). Evaluating the impact of prediction techniques: Software reliability perspective. *Computers, Materials and Continua*, *67*(2), 1471–1488. https://doi.org/10.32604/cmc.2021.014868

Salmeron, J. L. (2010). Modelling grey uncertainty with Fuzzy Grey Cognitive Maps. *Expert Systems with Applications*, *37*(12), 7581–7588. https://doi.org/https://doi.org/10.1016/j.eswa.2010.04.085

Salustri, A. (2022). A Multidimensional Analysis of the Municipalities of the Italian Small Islands. *Sustainability (Switzerland)*, *14*(16). https://doi.org/10.3390/su14169871

Santos, R. M., Gallardo, A. A., & Aguirre, J. A. (2021). Reference Model to Identify the Maturity Level of Cyber Threat Intelligence on the Dark Web. *Smart Innovation, Systems and Technologies*, *201*, 161–172. https://doi.org/10.1007/978-3-030-57548-9_15

Sapraz, M. (2023). *An E-Government Design Science Research in Sri Lanka* (Issue 23). Stockholm University.

Schlatt, V., Guggenberger, T., Schmid, J., & Urbach, N. (2023). Attacking the trust machine: Developing an information systems research agenda for blockchain cybersecurity. *International Journal of Information Management*, *68*(December 2020), 102470. https://doi.org/10.1016/j.ijinfomgt.2022.102470

Schumacher, A., Erol, S., & Sihn, W. (2016). A Maturity Model for Assessing Industry 4.0 Readiness and Maturity of Manufacturing Enterprises. *Procedia CIRP*, *52*, 161–166. https://doi.org/10.1016/j.procir.2016.07.040

Sepúlveda Estay, D. A., Sahay, R., Barfod, M. B., & Jensen, C. D. (2020). A systematic review of cyber-resilience assessment frameworks. *Computers and Security*, *97*. https://doi.org/10.1016/j.cose.2020.101996

Serna Patiño, A. M., & Giraldo Ramírez, D. P. (2019). A technological analysis of Colombia's cybersecurity capacity: a systemic perspective from an organizational point of view. *Ingeniería Solidaria*, *15*(28), 1–30.

Shaked, A., Tabansky, L., & Reich, Y. (2021). Incorporating Systems Thinking into a Cyber Resilience Maturity Model. *IEEE Engineering Management Review*, *49*(2), 110–115. https://doi.org/10.1109/EMR.2020.3046533

Sheikh, Z. A., Singh, Y., Singh, P. K., & Ghafoor, K. Z. (2022). Intelligent and secure framework for critical infrastructure (CPS): Current trends, challenges, and future scope. *Computer Communications*, *193*(July), 302–331. https://doi.org/10.1016/j.comcom.2022.07.007

Shemshadi, A., Shirazi, H., Toreihi, M., & Tarokh, M. J. (2011). A fuzzy VIKOR method for supplier selection based on entropy measure for objective weighting. *Expert Systems with Applications*, *38*(10), 12160–12167. https://doi.org/https://doi.org/10.1016/j.eswa.2011.03.027

Shen, Y., Cheng, Y., & Yu, J. (2022). From recovery resilience to transformative resilience: How digital platforms reshape public service provision during and post COVID-19. *Public Management Review*. https://doi.org/10.1080/14719037.2022.2033052

Shi-Kupfer, K., & Ohlberg, M. (2019). *China's Digital Rise*. **URL:***https://merics.org/en/report/chinas-digital-rise*

Shokry, M., Awad, A. I., Abd-Ellah, M. K., & Khalaf, A. A. M. (2022). Systematic survey of advanced metering infrastructure security: Vulnerabilities, attacks, countermeasures, and future vision. *Future Generation Computer Systems*, *136*, 358–377. https://doi.org/10.1016/j.future.2022.06.013

Simonofski, A., Zuiderwijk, A., Clarinval, A., & Hammedi, W. (2022). Tailoring open government data portals for lay citizens: A gamification theory approach. *International Journal of Information Management*, *65*(July 2021), 102511. https://doi.org/10.1016/j.ijinfomgt.2022.102511

Smith, K. J., Dhillon, G., & Carter, L. (2021). User values and the development of a cybersecurity public policy for the IoT. *International Journal of Information Management*, *56*(March 2020), 102123. https://doi.org/10.1016/j.ijinfomgt.2020.102123

Software Engineering Institute. (2010). *CMMI for Development, Version 1.3* (Issue November).

Sonje, S. A., Pawar, R. S., & Shukla, S. (2023). Assessing Blockchain-Based Innovation for the "Right to Education" Using MCDA Approach of Value-Focused Thinking and Fuzzy Cognitive Maps. *IEEE Transactions on Engineering Management*, *70*(5), 1945–1965. https://doi.org/10.1109/TEM.2021.3128192

Splunk. (2023). *Global research: How leading organizations engage the entire business to build resilience Security 2023*.

Spruit, M., & Roeling, M. (2014). ISFAM: The information security focus area maturity model. *ECIS 2014 Proceedings - 22nd European Conference on Information Systems*, 0–15.

Srdjevic, B., Srdjevic, Z., & Lakicevic, M. (2019). Urban greening and provisioning of ecosystem services within hesitant decision making framework. *Urban Forestry & Urban Greening*, *43*, 126371. https://doi.org/https://doi.org/10.1016/j.ufug.2019.126371

Srimuang, C., Cooharojananone, N., Tanlamai, U., & Chandrachai, A. (2018). Development of an open government data assessment model: user-centric approach to identify the weighted components in Thailand. *International Journal of Electronic Governance*, *10*(3), 276–295. https://doi.org/10.1504/IJEG.2018.095952

Srinivas, J., Das, A. K., & Kumar, N. (2019). Government regulations in cyber security: Framework, standards and recommendations. *Future Generation Computer Systems*, *92*, 178–188. https://doi.org/10.1016/j.future.2018.09.063

Sterrenberg, G., & L'Espoir Decosta, P. (2023). Identifying the crucial factors of e-government success from the perspective of Australian citizens living with disability using a public value approach. *Government Information Quarterly*, *March*, 101813. https://doi.org/10.1016/j.giq.2023.101813

Stylios, C. D., & Groumpos, P. P. (1999). Mathematical formulation of fuzzy cognitive maps. *Proceedings of the 7th Mediterranean Conference on Control and Automation*, *June 1999*, 2251–2261.

Sun, L., Dong, H., & Liu, A. X. (2018). Aggregation functions considering criteria interrelationships in fuzzy multi-criteria decision making: state-of-the-art. *IEEE Access*, *6*, 68104-68136.

Taherdoost, H. (2022). Understanding Cybersecurity Frameworks and Information Security Standards—A Review and Comprehensive Overview. *Electronics (Switzerland)*, *11*(14). https://doi.org/10.3390/electronics11142181

Tangi, L., Janssen, M., Benedetti, M., & Noci, G. (2021). Digital government transformation: A structural equation modelling analysis of driving and impeding factors. *International Journal of Information Management*, *60*(April), 102356. https://doi.org/10.1016/j.ijinfomgt.2021.102356

The World Bank. (2022). *GovTech Maturity Index Trends in Public Sector Digital Transformation*. *December*.

The World Bank. (2023). *Sectoral Cybersecurity Maturity Model*.

Tiller, R., De Kok, J. L., Vermeiren, K., Richards, R., Van Ardelan, M., & Bailey, J. (2016). Stakeholder perceptions of links between environmental changes to their socio-ecological system and their adaptive capacity in the region of Troms, Norway. *Frontiers in Marine Science*, *3*(DEC), 1–16. https://doi.org/10.3389/fmars.2016.00267

Tissir, N., El Kafhali, S., & Aboutabit, N. (2021). Cybersecurity management in cloud computing: semantic literature review and conceptual framework proposal. *Journal of Reliable Intelligent Environments*, *7*(2), 69–84. https://doi.org/10.1007/s40860-020-00115-0

Tokerud, S. (2022). *Designing the Extended Zero Trust Maturity Model*.

Tolman, E. C. (1948). Cognitive maps in rats and men. *Psychological Review*, *55*(4), 189.

Torbacki, W. (2021). A hybrid mcdm model combining danp and promethee ii methods for the assessment of cybersecurity in industry 4.0. *Sustainability (Switzerland)*, *13*(16). https://doi.org/10.3390/su13168833

Torra, V. (2010). Hesitant fuzzy sets. *International Journal of Intelligent Systems*, *25*(6), 529–539.

Tüysüz, F., & Şimşek, B. (2017). A hesitant fuzzy linguistic term sets-based AHP approach for analyzing the performance evaluation factors: an application to cargo sector. *Complex & Intelligent Systems*, *3*(3), 167–175. https://doi.org/10.1007/s40747-017-0044-x

Tüysüz, F., & Yıldız, N. (2020). A novel multi-criteria analysis model for the performance evaluation of bank regions: an application to Turkish agricultural banking. *Soft Computing*, *24*(7), 5289–5311. https://doi.org/10.1007/s00500-019-04279-7

Ungkap, P., & Daengsi, T. (2022). Cybersecurity Awareness Modeling Associated with Influential Factors Using AHP Technique: A Case of Railway Organizations in Thailand. *2022 International Conference on Decision Aid Sciences and Applications, DASA 2022*, 1359–1362. https://doi.org/10.1109/DASA54658.2022.9765092

United Nations. (2022a). *E-Government Survey 2022*. **URL:***https://publicadministration.un.org/en/*

United Nations. (2022b). *E-Government Survey 2022, The Future of Digital Government*.

US DoD. (2020). Cybersecurity maturity model certification. In *Department of Defense: Vol. DM* (Issues 19–0824).

US DoE. (2019). *Cybersecurity Capability Maturity Model (C2M2)* (Issue June).

Vaccari, L., Posada, M., Boyd, M., & Santoro, M. (2021). Apis for eu governments: A landscape analysis on policy instruments, standards, strategies and best practices. *Data*, *6*(6), 1–20. https://doi.org/10.3390/data6060059

van Eck, N. J., & Waltman, L. (2014). Visualizing Bibliometric Networks. In *Measuring Scholarly Impact* (pp. 285–320). Springer International Publishing. https://doi.org/10.1007/978-3-319-10377-8_13

Varela-Vaca, Á. J., Rosado, D. G., Sánchez, L. E., Gómez-López, M. T., Gasca, R. M., & Fernández-Medina, E. (2021). CARMEN: A framework for the verification and diagnosis of the specification of security requirements in cyber-physical systems. *Computers in Industry*, *132*. https://doi.org/10.1016/j.compind.2021.103524

Vicente Aceituno Canal, I. (2007). *ISM3 1.0.*

Wang, K., Zhao, N., He, Q., & Xu, J. (2021). A quality analysis method for three-dimensional model in aircraft structural parts design. *Advances in Mechanical Engineering*, *13*(3), 1–16. https://doi.org/10.1177/16878140211008045

Wang, S., Liu, Q., Yuksel, S., & Dincer, H. (2019). Hesitant Linguistic Term Sets-Based Hybrid Analysis for Renewable Energy Investments. *IEEE Access*, *7*, 114223–114235. https://doi.org/10.1109/access.2019.2935427

Wang, Y., Lo, H., Zhang, Q., & Xue, Y. (2006). How technological capability influences business performance: An integrated framework based on the contingency approach. *Journal of Technology Management in China*, *1*(1), 27–52.

Wang, Z., Liu, H., Li, T., Zhou, L., & Zhou, M. (2023). The Impact of Internet Use on Citizens' Trust in Government: The Mediating Role of Sense of Security. *Systems*, *11*(1), 1–19. https://doi.org/10.3390/systems11010047

Weerakkody, V., El-Haddadeh, R., Sivarajah, U., Omar, A., & Molnar, A. (2019). A case analysis of E-government service delivery through a service chain dimension. *International Journal of Information Management*, *47*(November), 233–238. https://doi.org/10.1016/j.ijinfomgt.2018.11.001

Weerakkody, V., Irani, Z., Lee, H., Hindi, N., & Osman, I. (2014). A review of the factors affecting user satisfaction in electronic government services. *International Journal of Electronic Government Research (IJEGR)*, *10*(4), 21–56.

Weerakkody, V., Irani, Z., Lee, H., Hindi, N., & Osman, I. (2016). Are U.K. Citizens Satisfied With E-Government Services? Identifying and Testing Antecedents of Satisfaction. *Information Systems Management*, *33*(4), 331–343. https://doi.org/10.1080/10580530.2016.1220216

Weerakkody, V., Irani, Z., Lee, H., Osman, I., & Hindi, N. (2015). E-government implementation: A bird's eye view of issues relating to costs, opportunities, benefits

and risks. *Information Systems Frontiers*, *17*(4), 889–915. https://doi.org/10.1007/s10796-013-9472-3

Weerakkody, V., Janssen, M., & Dwivedi, Y. K. (2011). Transformational change and business process reengineering (BPR): Lessons from the British and Dutch public sector. *Government Information Quarterly*, *28*(3), 320–328. https://doi.org/10.1016/J.GIQ.2010.07.010

WEF. (2023). *Digital Transition Framework: An action plan for public-private collaboration*. *January*.

William D. Eggers, Jason Manstof, Pankaj Kamleshkumar Kishnani, J. B. (2021). Seven Pivots for Government's Digital Transformation. *Deloitte Insights*.

Wilson, C., & Mergel, I. (2022). Overcoming barriers to digital government: mapping the strategies of digital champions. *Government Information Quarterly*, *39*(2), 101681. https://doi.org/10.1016/j.giq.2022.101681

Wirnsperger, Peter; Yildiz, M. (2017). *Deloitte: A new approach to Cyber Security Secure. Vigilant. Resilient.™*.

Wu, Y., Tao, Y., Deng, Z., Zhou, J., Xu, C., & Zhang, B. (2020). A fuzzy analysis framework for waste incineration power plant comprehensive benefit evaluation from refuse classification perspective. *Journal of Cleaner Production*, *258*, 120734. https://doi.org/https://doi.org/10.1016/j.jclepro.2020.120734

Xia, M., & Xu, Z. (2011). Hesitant fuzzy information aggregation in decision making. *International Journal of Approximate Reasoning*, *52*(3), 395–407. https://doi.org/10.1016/j.ijar.2010.09.002

Xia, M., & Xu, Z. (2013). Managing hesitant information in gdm problems under fuzzy and multiplicative preference relations. In *International Journal of Uncertainty, Fuzziness and Knowlege-Based Systems* (Vol. 21, Issue 6). https://doi.org/10.1142/S0218488513500402

Xia, M., Xu, Z., & Zhu, B. (2013). Geometric Bonferroni means with their application in multi-criteria decision making. *Knowledge-Based Systems*, *40*, 88–100. https://doi.org/10.1016/j.knosys.2012.11.013

Xu, Z., & Yager, R. R. (2011). Intuitionistic fuzzy bonferroni means. *IEEE Transactions on Systems, Man, and Cybernetics, Part B: Cybernetics*, *41*(2), 568–578. https://doi.org/10.1109/TSMCB.2010.2072918

Xu, K., & Xu, J. (2019). A Direct Consistency Improvement Method for the Probability-Hesitant Analytic Hierarchy Process. *IEEE Access*, *7*, 9445–9458. https://doi.org/10.1109/ACCESS.2019.2891286

Xu, Y., Liu, S., Wang, J., & Shang, X. (2022). Consensus checking and improving methods for AHP with q-rung dual hesitant fuzzy preference relations. *Expert Systems With Applications*, 117902. https://doi.org/10.1016/j.eswa.2022.117902

Yager, R. R. (2009). On generalized Bonferroni mean operators for multi-criteria aggregation. *International Journal of Approximate Reasoning*, *50*(8), 1279–1286. https://doi.org/10.1016/j.ijar.2009.06.004

Yigit Ozkan, B., & Spruit, M. (2019). A Questionnaire Model for Cybersecurity Maturity Assessment of Critical Infrastructures. In *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics): Vol. 11398 LNCS*. Springer International Publishing. https://doi.org/10.1007/978-3-030-12085-6_5

Yigit Ozkan, B., Spruit, M., Wondolleck, R., & Burriel Coll, V. (2020). Modelling adaptive information security for SMEs in a cluster. *Journal of Intellectual Capital*, *21*(2), 235–256. https://doi.org/10.1108/JIC-05-2019-0128

Yigit Ozkan, B., van Lingen, S., & Spruit, M. (2021). The Cybersecurity Focus Area Maturity (CYSFAM) Model. *Journal of Cybersecurity and Privacy*, *1*(1), 119–139. https://doi.org/10.3390/jcp1010007

Yıldız, N., & Tüysüz, F. (2019). A hybrid multi-criteria decision making approach for strategic retail location investment: Application to Turkish food retailing. *Socio-Economic Planning Sciences*, *68*, 100619. https://doi.org/https://doi.org/10.1016/j.seps.2018.02.006

Young, M. M. (2022). The impact of technological innovation on service delivery: social media and smartphone integration in a 311 system. *Public Management Review*, *24*(6), 926–950.

Yun, Y., & Jung, H. Y. (2021). Impacts of public medical insurance reforms on households: An application of fuzzy cognitive map for scenario evaluation. *Soft Computing*, *25*(12), 7947–7956. https://doi.org/10.1007/s00500-021-05617-4

Zadeh, L. A. (1965). Fuzzy sets. *Information and Control*, *8*(3), 338–353. https://doi.org/10.1016/S0019-9958(65)90241-X

Zaidan, A. A., Alsattar, H. A., Qahtan, S., Deveci, M., Pamucar, D., & Hajiaghaei-Keshteli, M. (2023). Uncertainty Decision Modeling Approach for Control Engineering Tools to Support Industrial Cyber-Physical Metaverse Smart Manufacturing Systems. *IEEE Systems Journal*, *PP*, 1–12. https://doi.org/10.1109/JSYST.2023.3266842

Zandieh, M., & Aslani, B. (2019). A hybrid MCDM approach for order distribution in a multiple-supplier supply chain: A case study. *Journal of Industrial Information Integration*, *16*(August), 100104. https://doi.org/10.1016/j.jii.2019.08.002

Zhang, Y., Xu, L., & Lu, Z. (2022). Research on policy diffusion mechanism of Government Procurement of Public Services based on an MFCM. *Kybernetes*. https://doi.org/10.1108/K-01-2022-0082

Zhang, Z., Kou, X., & Dong, Q. (2018). Additive consistency analysis and improvement for hesitant fuzzy preference relations. *Expert Systems With Applications*, *98*, 118–128. https://doi.org/10.1016/j.eswa.2018.01.016

Zhang, Z., Wang, C., & Tian, X. (2015). Multi-criteria group decision making with incomplete hesitant fuzzy preference relations. *Applied Soft Computing*, *36*, 1–23. https://doi.org/10.1016/j.asoc.2015.06.047

Zhu, B., & Xu, Z. (2013a). Regression Methods For Hesitant Fuzzy Preference Relations. *Technological and Economic Development of Economy*, *19*(1, SI), S214–S227. https://doi.org/10.3846/20294913.2014.881430

Zhu, B., & Xu, Z. (2014). Analytic hierarchy process-hesitant group decision making. *European Journal of Operational Research*, *239*(3), 794–801. https://doi.org/https://doi.org/10.1016/j.ejor.2014.06.019

Zhu, B., & Xu, Z. S. (2013b). Hesitant fuzzy Bonferroni means for multi-criteria decision making. *Journal of the Operational Research Society*, *64*(12), 1831–1840. https://doi.org/10.1057/jors.2013.7

Zhu, B., Xu, Z., Zhang, R., & Hong, M. (2016). Hesitant analytic hierarchy process. *European Journal of Operational Research*, *250*(2), 602–614. https://doi.org/https://doi.org/10.1016/j.ejor.2015.09.063

Zivanovic, Jasmina, I. (2018). *IBM security strategy* (Issue October).

Zou, Q., Mao, Z., Yan, R., Liu, S., & Duan, Z. (2023). Vision and reality of e-government for governance improvement: Evidence from global cross-country panel data.

Technological Forecasting and Social Change, *194*(March 2022), 122667. https://doi.org/10.1016/j.techfore.2023.122667

APPENDICES

Appendix A.

Table A.1: Evaluation of DM1 about the digital citizenship improvement

	DCI1	DCI2	DCI3	DCI4	DCI5	DCI6	DCI7	DCI8	DCI9	DCI10	DCI11	DCI12	DCI13	DCI14	DCI
DCI1		Between H and P	Between L and M	Between L and M	At least VH		Negatively between M and H		Between M and H	At most L	Between H and P	Negatively between M and H	Negatively between M and H	Between H and P	Between M and H
DCI2	Between L and M			Between H and P				Between M and H	At most L	Between H and P			Negatively between L and M	At least P	Between H and P
DCI3		At least P		Negatively between M and H		Between H and P	Negatively at most L	At least VH	Between L and M		Between L and M		Negatively between L and M	At least VH	
DCI4		Between L and M	Between M and H							At least VH	Between M and VH			Between L and M	
DCI5		At least VH		Between H and P		At least VH	Between H and P		Between L and M		Between M and VH	Negatively between M and H	Between H and P		
DCI6	Between H and P	At least P							Between M and H		Between L and M			Between H and P	Between M and H
DCI7		Negatively between H and P	Negatively at least VH	Between M and H				Negatively at least VH			Negatively between L and M			Negatively at least VH	
DCI8		At least VH	Between M and H				Negatively between H and P				Between L and M		Negatively between H and P	At least VH	Between M and H
DCI9	At least VH				Between L and M							Negatively between L and M			
DCI10		At least P	At least VH	Negatively between M and H		Between M and H	Negatively between L and M	Between M and H			Between M and H		Negatively between L and M	Between H and P	

Table A.1: Evaluation of DM1 about the digital citizenship improvement (*continue*)

	DCI1	DCI2	DCI3	DCI4	DCI5	DCI6	DCI7	DCI8	DCI9	DCI10	DCI11	DCI12	DCI13	DCI14	DCI
DCI11		Between H and P	Between M and H	Between M and H			Negatively between L and M	Between M and H		At least VH			Negatively between L and M	Between L and M	Between H and P
DCI12	Negatively between H and P	Negatively at least VH			Negatively between L and M				Negatively between H and P		Negatively at least VH			Negatively at least VH	
DCI13		Negatively between H and P	Negatively at least VH	Between M and H				Negatively at least VH			Negatively between M and H			Negatively at least VH	
DCI14		At least P						At least VH							Between M and H
DCI															

Table A.2: Evaluation of DM2 about the digital citizenship improvement

	DCI1	DCI2	DCI3	DCI4	DCI5	DCI6	DCI7	DCI8	DCI9	DCI10	DCI11	DCI12	DCI13	DCI14	DCI
DCI1		Between M and VH	At most L	Between M and H	At least P		Negatively between L and M		Between L and M	At most L	Between M and VH	Negatively between M and H	Negatively between M and H	Between M and VH	Between H and P
DCI2	At most L			Between H and P				Between M and H	At most L	Between H and P			Negatively between L and M	At least P	Between H and P
DCI3		At least P		Negatively between M and H		Between M and VH	Negatively at most L	At least VH	Between L and M		Between L and M		Negatively between L and M	At least VH	
DCI4		Between M and H	Between L and M							At least VH	Between M and VH			Between L and M	
DCI5		At least P		Between M and VH		At least VH	Between H and P		Between L and M		Between M and VH	Negatively between M and H	Between H and P		
DCI6	Between M and VH	At least P							Between M and H		Between M and H			Between H and P	Between M and H
DCI7		Negatively between H and P	Negatively at least VH	Between M and H				Negatively at least H			Negatively between L and M			Negatively at least VH	
DCI8		At least VH	Between M and H				Negatively between H and P				Between L and M		Negatively between H and P	At least H	Between M and H
DCI9	At least P				Between L and M							Negatively between L and M			
DCI10		At least P	At least H	Negatively between M and H		Between M and H	Negatively between L and M	Between M and H			Between M and H		Negatively between L and M	Between H and P	

Table A.2: Evaluation of DM2 about the digital citizenship improvement (*continue*)

	DCI1	DCI2	DCI3	DCI4	DCI5	DCI6	DCI7	DCI8	DCI9	DCI10	DCI11	DCI12	DCI13	DCI14	DCI
DCI11		Between H and P	Between M and H	Between M and H			Negatively between L and M	Between M and H		At least VH			Negatively between L and M	Between L and M	Between H and P
DCI12	Negatively between H and P	Negatively at least H			Negatively at most L				Negatively between H and P		Negatively at least VH			Negatively at least VH	
DCI13		Negatively between H and P	Negatively at least VH	Between M and H				Negatively at least VH			Negatively between M and H			Negatively at least VH	
DCI14		At least P						At least VH							Between H and P
DCI															

Table A.3: Evaluation of DM3 about the digital citizenship improvement

	DCI1	DCI2	DCI3	DCI4	DCI5	DCI6	DCI7	DCI8	DCI9	DCI10	DCI11	DCI12	DCI13	DCI14	DCI
DCI1		Between H and P	Between L and M	Between L and M	At least VH		Negatively between M and H		Between M and H	At most L	Between H and P	Negatively between M and H	Negatively between M and H	Between H and P	Between M and H
DCI2	Between L and M			Between H and P				Between M and H	At most L	Between H and P			Negatively between L and M	At least P	Between H and P
DCI3		At least P		Negatively between M and H		Between H and P	Negatively at most L	At least VH	Between L and M		Between L and M		Negatively between L and M	At least VH	
DCI4		Between L and M	Between M and H							At least VH	Between M and VH			Between L and M	
DCI5		At least VH		Between H and P		At least VH	Between H and P		Between L and M		Between M and VH	Negatively between M and H	Between H and P		
DCI6	Between H and P	At least P							Between M and H		Between L and M			Between H and P	Between M and H
DCI7		Negatively between H and P	Negatively at least VH	Between M and H				Negatively at least VH			Negatively between L and M			Negatively at least VH	
DCI8		At least VH	Between M and H				Negatively between H and P				Between L and M		Negatively between H and P	At least VH	Between M and H
DCI9	At least VH				Between L and M							Negatively between L and M			
DCI10		At least P	At least VH	Negatively between M and H		Between M and H	Negatively between L and M	Between M and H			Between M and H		Negatively between L and M	Between H and P	

Table A.3: Evaluation of DM3 about the digital citizenship improvement (*continue*)

	DCI1	DCI2	DCI3	DCI4	DCI5	DCI6	DCI7	DCI8	DCI9	DCI10	DCI11	DCI12	DCI13	DCI14	DCI
DCI11		Between H and P	Between M and H	Between M and H			Negatively between L and M	Between M and H		At least VH			Negatively between L and M	Between L and M	Between H and P
DCI12	Negatively between H and P	Negatively at least VH			Negatively between L and M				Negatively between H and P		Negatively at least VH			Negatively at least VH	
DCI13		Negatively between H and P	Negatively at least VH	Between M and H				Negatively at least VH			Negatively between M and H			Negatively at least VH	
DCI14		At least P						At least VH							Between M and H
DCI															

Table A.4: Evaluation of DM1 about the digital technology improvement

	DTI1	DTI2	DTI3	DTI4	DTI5	DTI6	DTI7	DTI8	DTI9	DTI10	DTI11	DTI12	DTI13	DTI
DTI1							Between M and H	Between M and H				Between L and M		Between M and H
DTI2			Between H and P			Between M and H	Between M and H							
DTI3	Negatively at most L	At least VH			At least VH	At least VH	Between M and H	At least VH	Between H and P			Between L and M		At least P
DTI4		Between H and P	At least VH		Between H and P	At most L		Between M and H				Between H and P	Negatively at least VH	Between M and H
DTI5		Between H and P	At least VH	At least VH		At least VH	Between L and M	Between H and P				Between H and P	Negatively at least VH	Between M and H
DTI6	Between M and H		At least H	Between L and M	At least P		Between H and P	Between L and M		Negatively between L and M				
DTI7	Negatively between L and M		Negatively at least H	Between L and M	Between L and M	Between L and M		At least VH			Between L and M		Negatively between H and P	Between M and H
DTI8	Negatively between L and M		Between M and VH	Between M and H	Between M and H		Between H and P					Between M and H	Negatively between M and H	Between M and H
DTI9			At least VH	Between H and P	Between M and H						At least VH	At least P		
DTI10			Negatively at most L		Negatively between M and H	Negatively between M and H	Between L and M							
DTI11				Between L and M	Between L and M	Negatively between L and M						Between H and P	Negatively at least VH	
DTI12			Between M and H	At least VH	Between L and M	Between L and M			At least VH		Between H and P		Negatively between H and P	Between H and P
DTI13				Negatively between L and M		Negatively between H and P	Negatively between M and H	Negatively between L and M						
DTI														

Table A.5: Evaluation of DM2 about the digital technology improvement

	DTI1	DTI2	DTI3	DTI4	DTI5	DTI6	DTI7	DTI8	DTI9	DTI10	DTI11	DTI12	DTI13	DTI
DTI1							Between M and H	Between M and H				At most L		Between M and H
DTI2			Between H and P			Between M and H	Between M and H							
DTI3	Negatively at most L	At least VH			At least VH	At least P	Between M and H	At least VH	Between H and P			At most L		At least P
DTI4		At least H	At least VH		Between H and P	At most L		Between M and H				Between H and P	Negatively at least VH	Between H and P
DTI5		Between H and P	At least VH	At least VH		At least VH	Between L and M	Between H and P				Between H and P	Negatively at least VH	Between H and P
DTI6	Between H and P		At least H	Between L and M	At least P		Between H and P	Between L and M		Negatively between L and M				
DTI7	Negatively at most L		Negatively at least H	Between L and M	Between L and M	Between L and M		At least P			Between L and M		Negatively between H and P	Between M and H
DTI8	Negatively between L and M		Between M and VH	Between M and H	Between M and H		Between H and P					Between M and H	Negatively between M and H	Between M and H
DTI9			At least VH	Between H and P	Between M and H						At least H	At least P		
DTI10			Negatively at most L		Negatively between M and H	Negatively between M and H	At most L							
DTI11				Between L and M	Between M and H	Negatively between L and M						Between H and P	Negatively at least VH	
DTI12			Between M and H	At least VH	Between M and H	Between L and M			At least H		Between H and P		Negatively between H and P	Between H and P
DTI13				Negatively between L and M		Negatively between H and P	Negatively between M and H	Negatively between L and M						
DTI														

Table A.6: Evaluation of DM3 about the digital technology improvement

	DTI1	DTI2	DTI3	DTI4	DTI5	DTI6	DTI7	DTI8	DTI9	DTI10	DTI11	DTI12	DTI13	DTI
DTI1							Between M and H	Between M and H				Between L and M		Between M and H
DTI2			Between H and P			Between M and H	Between M and H							
DTI3	Negatively at most L	At least VH			At least VH	At least VH	Between M and H	At least VH	Between H and P			Between L and M		At least P
DTI4		Between H and P	At least VH		Between H and P	At most L		Between M and H				Between H and P	Negatively at least VH	Between M and H
DTI5		Between H and P	At least VH	At least VH		At least VH	Between L and M	Between H and P				Between H and P	Negatively at least VH	Between M and H
DTI6	Between M and H		At least H	Between L and M	At least P		Between H and P	Between L and M		Negatively between L and M				
DTI7	Negatively between L and M		Negatively at least H	Between L and M	Between L and M	Between L and M		At least VH			Between L and M		Negatively between H and P	Between M and H
DTI8	Negatively between L and M		Between M and VH	Between M and H	Between M and H		Between H and P					Between M and H	Negatively between M and H	Between M and H
DTI9			At least VH	Between H and P	Between M and H						At least VH	At least P		
DTI10			Negatively at most L		Negatively between M and H	Negatively between M and H	Between L and M							
DTI11				Between L and M	Between L and M	Negatively between L and M						Between H and P	Negatively at least VH	
DTI12			Between M and H	At least VH	Between L and M	Between L and M			At least VH		Between H and P		Negatively between H and P	Between H and P
DTI13				Negatively between L and M		Negatively between H and P	Negatively between M and H	Negatively between L and M						
DTI														

Table A.7: Evaluation of DM1 about the digital service improvement

	DSI1	DSI2	DSI3	DSI4	DSI5	DSI6	DSI7	DSI8	DSI9	DSI10	DSI11	DSI12	DSI13	DSI14	DSI
DSI1		Between H and P	At least VH		At least VH		Between H and P	Between H and P	At least VH		Between L and M	Between H and P	Between L and M		Between H and P
DSI2	At least VH		At least VH					Between M and H	Between H and P		Negatively between L and M				Between M and H
DSI3	At least VH	At least VH			Between H and P		At least VH	At least VH	At least VH		Negatively between M and H	At least VH	Between H and P	Between M and H	Between H and P
DSI4	Between M and H	Between M and H	At least H		Between M and VH		Between L and M			Between L and M					
DSI5	At least VH		At least VH				At least VH	Between H and P	Between H and P		Negatively between L and M	Between H and P	Between H and P	Between L and M	
DSI6	Between M and H	Between M and H	At least VH		Between M and VH		Between M and H				Negatively between M and H	At least VH		Between L and M	Between M and H
DSI7								Between L and M	Between M and H				Between M and H		
DSI8	Negatively between L and M	Negatively between L and M	Negatively at least H		Negatively at least H					Negatively between M and H					
DSI9	Negatively between L and M	Negatively between L and M	Negatively between M and VH		Negatively between M and VH										
DSI10			Between L and M	Between M and H	Between L and M	Between H and P					Negatively between M and H	Between M and H	Between M and H	At least VH	

Table A.7: Evaluation of DM1 about the digital service improvement (*continue*)

	DSI1	DSI2	DSI3	DSI4	DSI5	DSI6	DSI7	DSI8	DSI9	DSI10	DSI11	DSI12	DSI13	DSI14	DSI
DSI11	Negatively between L and M		Negatively between H and P		Negatively between L and M										
DSI12	At most L	At most L	Between H and P		Between H and P	At most L				At most L	Negatively between H and P		Between L and M		Between M and H
DSI13			Between H and P		Between M and H		At least VH	Between M and H	Between L and M		Negatively between L and M	Between M and H		Between H and P	
DSI14	Between L and M		Between H and P		Between M and H	Between H and P	Between L and M			At least P	Negatively between M and H	At least VH	Between M and H		Between H and P
DSI1		Between H and P	At least VH		At least VH		Between H and P	Between H and P	At least VH		Between L and M	Between H and P	Between L and M		

Table A.8: Evaluation of DM2 about the digital service improvement

	DSI1	DSI2	DSI3	DSI4	DSI5	DSI6	DSI7	DSI8	DSI9	DSI10	DSI11	DSI12	DSI13	DSI14	DSI
DSI1		Between H and P	At least P		At least VH		Between H and P	Between H and P	At least VH		Between L and M	Between H and P	Between L and M		Between M and VH
DSI2	At least P		At least P					Between M and H	Between H and P		Negatively between L and M				Between M and H
DSI3	At least VH	At least VH			Between H and P		At least H	At least VH	At least VH		Negatively between M and H	At least VH	Between H and P	Between M and H	Between H and P
DSI4	Between L and M	Between M and H	Between H and P		Between M and VH		Between L and M			At most L					
DSI5	At least VH		At least VH				At least H	Between H and P	At least H		Negatively between L and M	Between H and P	Between H and P	At most L	
DSI6	Between M and H	Between M and H	At least VH		Between M and VH		Between M and H				Negatively between M and H	At least VH		At most L	Between M and H
DSI7								Between L and M	Between M and H				Between M and H		
DSI8	Negatively between L and M	Negatively between L and M	Negatively at least H		Negatively at least H					Negatively between M and H					
DSI9	Negatively between L and M	Negatively between L and M	Negatively between M and VH		Negatively between M and VH										
DSI10			Between L and M	Between M and H	Between L and M	Between H and P					Negatively between M and H	Between M and H	Between M and H	At least VH	

Table A.8: Evaluation of DM2 about the digital service improvement (*continue*)

	DSI1	DSI2	DSI3	DSI4	DSI5	DSI6	DSI7	DSI8	DSI9	DSI10	DSI11	DSI12	DSI13	DSI14	DSI
DSI11	Negatively between L and M		Negatively between H and P		Negatively between M and H										
DSI12	Between L and M	At most L	Between H and P		Between H and P	At most L				At most L	Negatively between H and P		Between L and M		Between M and H
DSI13			Between H and P		Between M and H		At least VH	Between M and H	Between L and M		Negatively between L and M	Between M and H		Between H and P	
DSI14	Between L and M		Between H and P		Between M and H	Between H and P	Between L and M			At least P	Negatively between M and H	At least VH	Between M and H		Between M and VH
DSI1															

Table A.9: Evaluation of DM3 about the digital service improvement

	DSI1	DSI2	DSI3	DSI4	DSI5	DSI6	DSI7	DSI8	DSI9	DSI10	DSI11	DSI12	DSI13	DSI14	DSI
DSI1		Between H and P	At least VH		At least VH		Between H and P	Between H and P	At least VH		Between L and M	Between H and P	Between L and M		Between H and P
DSI2	At least VH		At least VH					Between M and H	Between H and P		Negatively between L and M				Between M and H
DSI3	At least VH	At least VH			Between H and P		At least VH	At least VH	At least VH		Negatively between M and H	At least VH	Between H and P	Between M and H	Between H and P
DSI4	Between M and H	Between M and H	At least H		Between M and VH		Between L and M			Between L and M					
DSI5	At least VH		At least VH				At least VH	Between H and P	Between H and P		Negatively between L and M	Between H and P	Between H and P	Between L and M	
DSI6	Between M and H	Between M and H	At least VH		Between M and VH		Between M and H				Negatively between M and H	At least VH		Between L and M	Between M and H
DSI7								Between L and M	Between M and H				Between M and H		
DSI8	Negatively between L and M	Negatively between L and M	Negatively at least H		Negatively at least H					Negatively between M and H					
DSI9	Negatively between L and M	Negatively between L and M	Negatively between M and VH		Negatively between M and VH										
DSI10			Between L and M	Between M and H	Between L and M	Between H and P					Negatively between M and H	Between M and H	Between M and H	At least VH	

Table A.9: Evaluation of DM3 about the digital service improvement (*continue*)

	DSI1	DSI2	DSI3	DSI4	DSI5	DSI6	DSI7	DSI8	DSI9	DSI10	DSI11	DSI12	DSI13	DSI14	DSI
DSI11	Negatively between L and M		Negatively between H and P		Negatively between L and M										
DSI12	At most L	At most L	Between H and P		Between H and P	At most L				At most L	Negatively between H and P		Between L and M		Between M and H
DSI13			Between H and P		Between M and H		At least VH	Between M and H	Between L and M		Negatively between L and M	Between M and H		Between H and P	
DSI14	Between L and M		Between H and P		Between M and H	Between H and P	Between L and M			At least P	Negatively between M and H	At least VH	Between M and H		Between H and P
DSI1															

Table A.10: Adjacency matrix about all of the success/risk factors for DGT

	DCI1	DCI2	DCI3	DCI4	DCI5	DCI6	DCI7	DCI8	DCI9	DCI10	DCI11	DCI12	DCI13	DCI14	DCI
DCI1	0.00	0.42	0.00	0.00	0.00	0.75	0.00	0.00	0.89	0.00	0.00	0.00	0.00	0.00	0.00
DCI2	0.75	0.00	0.94	0.42	0.89	0.94	-0.75	0.89	0.00	0.94	0.00	0.00	0.00	0.00	0.00
DCI3	0.58	0.00	0.00	0.58	0.00	0.00	-0.89	0.58	0.00	0.89	0.00	0.00	0.00	0.00	0.00
DCI4	0.58	0.75	-0.58	0.00	0.75	0.00	0.58	0.00	0.00	-0.58	0.00	0.00	0.00	0.00	0.00
DCI5	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.42	0.00	0.00	0.00	0.00	0.00	0.00
DCI6	0.00	0.00	0.75	0.00	0.89	0.00	0.00	0.00	0.00	0.58	0.00	0.00	0.00	0.00	0.00
DCI7	-0.42	0.00	-0.18	0.00	0.75	0.00	0.00	-0.75	0.00	-0.42	0.00	0.00	0.00	0.00	0.00
DCI8	0.58	0.58	0.89	0.00	0.00	0.00	-0.89	0.00	0.00	0.58	0.00	0.00	0.00	0.00	0.00
DCI9	0.00	0.18	0.42	0.00	0.42	0.58	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
DCI10	0.89	0.75	0.00	0.89	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
DCI11	0.00	0.00	0.42	0.58	0.58	0.42	-0.42	0.42	0.00	0.58	0.00	0.00	0.00	0.00	0.00
DCI12	0.00	0.00	0.00	0.00	-0.58	0.00	0.00	0.00	-0.42	0.00	0.00	0.00	0.00	0.00	0.00
DCI13	-0.42	-0.42	-0.42	0.00	0.75	0.00	0.00	-0.75	0.00	-0.42	0.00	0.00	0.00	0.00	0.00
DCI14	0.42	0.94	0.89	0.42	0.00	0.75	-0.89	0.89	0.00	0.75	0.00	0.00	0.00	0.00	0.00
DCI	0.75	0.75	0.00	0.00	0.00	0.58	0.00	0.58	0.00	0.00	0.00	0.00	0.00	0.00	0.00
DTI1	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
DTI2	0.00	0.00	0.00	0.00	0.58	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
DTI3	0.00	0.00	0.00	0.00	0.75	0.58	0.89	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
DTI4	0.75	0.00	0.00	0.58	0.00	0.00	0.00	0.00	0.00	0.89	0.00	0.00	0.00	0.00	0.00
DTI5	0.58	0.00	0.00	0.58	0.00	0.00	0.00	0.00	0.00	0.75	0.00	0.00	0.00	0.00	0.00
DTI6	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.42	0.00	0.00	0.00	0.00	0.00
DTI7	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
DTI8	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
DTI9	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.75	0.00	0.00	0.00	0.00	0.00
DTI10	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
DTI11	0.75	0.00	0.00	0.58	0.00	0.00	0.00	0.00	0.00	0.58	0.00	0.00	0.00	0.00	0.00
DTI12	0.42	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.58	0.00	0.00	0.00	0.00	0.00
DTI13	0.00	0.00	0.00	0.00	0.00	-0.75	0.58	-0.89	-0.58	-0.89	0.00	0.00	0.00	0.00	0.00
DTI	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
DSI1	0.75	0.00	0.00	0.75	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
DSI2	0.75	0.00	0.00	0.75	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
DSI3	0.58	0.75	0.00	0.00	0.00	0.75	0.00	0.89	0.00	0.00	0.00	0.00	0.00	0.00	0.00
DSI4	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
DSI5	0.00	0.75	0.00	0.00	0.00	0.75	0.00	0.75	0.00	0.00	0.00	0.00	0.00	0.00	0.00
DSI6	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
DSI7	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
DSI8	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
DSI9	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
DSI10	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.58	0.00	0.00	0.00	0.00	0.00	0.00	0.00
DSI11	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
DSI12	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
DSI13	0.00	0.00	0.00	0.00	0.00	0.00	0.75	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
DSI14	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
DSI	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00

Table A.10: Adjacency matrix about all of the success/risk factors for DGT (*continue*)

	DCI1	DCI2	DCI3	DCI4	DCI5	DCI6	DCI7	DCI8	DCI9	DCI10	DCI11	DCI12	DCI13	DCI14	DCI	DTI1	DTI2	DTI3	DTI4	DTI5	DTI6	DTI7	DTI8	DTI9	DTI10	DTI11	DTI12	DTI13	DTI	DSI1	DSI2	DSI3	DSI4	DSI5	DSI6	DSI7	DSI8	DSI9	DSI10	DSI11	DSI12	DSI13	DSI14	DSI
DCI1	0.00	-0.75	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
DCI2	0.75	0.00	-0.89	0.00	-0.42	0.00	0.00	0.00	-0.75	0.00	-0.89	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	-0.89	-0.75	0.00	0.00	0.00	0.89	0.00	0.00	0.00	-0.75	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
DCI3	0.75	0.00	0.00	-0.89	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	-0.89	0.00	0.00	0.00	0.75	0.89	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
DCI4	0.00	0.00	0.58	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.58	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
DCI5	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
DCI6	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
DCI7	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
DCI8	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
DCI9	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
DCI10	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
DCI11	0.00	-0.89	0.00	0.00	0.00	0.00	0.00	0.00	-0.75	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
DCI12	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
DCI13	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
DCI14	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
DCI	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
DTI1	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
DTI2	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
DTI3	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
DTI4	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
DTI5	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
DTI6	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
DTI7	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
DTI8	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
DTI9	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
DTI10	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
DTI11	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
DTI12	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
DTI13	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
DTI	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
DSI1	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
DSI2	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
DSI3	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
DSI4	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
DSI5	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
DSI6	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
DSI7	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
DSI8	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
DSI9	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
DSI10	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
DSI11	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
DSI12	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
DSI13	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
DSI14	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
DSI	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00

Table A.10: Adjacency matrix about all of the success/risk factors for DGT (*continue*)

	DCI1	DCI2	DCI3	DCI4	DCI5	DCI6	DCI7	DCI8	DCI9	DCI10	DCI11	DCI12	DCI	DTI1	DTI2	DTI3	DTI4	DTI5	DTI6	DTI7	DTI8	DTI9	DTI10	DTI11	DTI12	DTI13	DTI	DSI1	DSI2	DSI3	DSI4	DSI5	DSI6	DSI7	DSI8	DSI9	DSI10	DSI11	DSI12	DSI13	DSI14	DSI
DTI1	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	-0.42	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	-0.58	0.00	-0.58	0.00	0.00	0.00	0.00	0.00	0.58	0.00	0.00	0.00	0.00
DTI12	0.00	0.75	0.75	0.58	0.00	0.00	0.00	0.00	0.00	0.00	0.42	0.00	0.00	0.00	0.00	0.58	0.89	0.42	0.42	0.89	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.75	0.58	0.75	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
DTI11	0.00	0.58	0.58	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.42	0.00	-0.42	0.00	0.00	0.00	0.00	0.75	0.00	-0.89	0.00	0.00	0.42	0.75	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
DTI10	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	-0.18	0.00	-0.58	-0.58	0.42	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	-0.58	0.00	0.00	0.00	0.00	0.00	0.00	0.00
DTI9	0.00	0.42	0.75	0.00	0.00	0.00	0.00	0.00	0.00	0.89	0.42	0.00	0.00	0.00	0.00	0.89	0.75	0.58	0.00	0.00	0.00	0.00	0.00	0.89	0.94	0.00	0.00	0.89	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.89	0.00	0.00	0.58	0.00	0.00	0.00
DTI8	0.00	0.58	0.75	0.00	0.00	0.00	0.00	0.00	0.00	0.75	0.00	0.00	0.00	-0.42	0.00	0.58	0.58	0.58	0.00	0.75	0.00	0.00	0.00	0.00	0.58	-0.58	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.94	0.00	0.00	0.00	0.00	0.00	0.00	0.00
DSI1	0.00	0.75	0.89	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.89	0.75	0.00	0.89	0.00	0.75	0.75	0.89	0.00	0.75	0.42	0.00	0.00	0.75
DSI2	0.00	0.75	0.75	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.89	0.00	0.89	0.00	0.00	0.00	0.00	0.58	0.75	0.00	0.00	0.75	0.00	0.00	0.00
DSI3	0.00	0.58	0.75	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
DSI4	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.58	0.75	0.00	0.58	0.00	0.42	0.00	0.00	0.42	0.00	0.00	0.00	0.00	0.00
DSI5	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
DSI6	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
DSI7	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
DSI8	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
DSI9	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
DSI10	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
DSI11	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
DSI12	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
DSI13	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
DSI14	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
DSI	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00

Table A.10: Adjacency matrix about all of the success/risk factors for DGT (*continue*)

	DSI5	DSI6	DSI7	DSI8	DSI9	DSI10	DSI11	DSI1	DSI13	DSI14	DSI
DCI1	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
DCI2	0.58	0.00	0.00	0.00	0.00	0.00	-0.58	0.00	0.00	0.89	0.00
DCI3	0.42	0.00	0.00	0.00	0.00	0.00	-0.75	0.00	0.00	0.75	0.00
DCI4	0.00	0.00	0.00	0.00	0.00	0.00	-0.75	0.00	0.00	0.00	0.00
DCI5	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
DCI6	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
DCI7	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
DCI8	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
DCI9	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
DCI10	0.58	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
DCI11	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
DCI12	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
DCI13	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
DCI14	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.75	0.00
DCI	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
DTI1	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
DTI2	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.75	0.00	0.00
DTI3	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.89	0.00	0.00
DTI4	0.89	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
DTI5	0.75	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
DTI6	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
DTI7	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
DTI8	0.00	0.00	0.00	-0.58	0.00	0.00	0.00	0.00	0.00	0.00	0.00
DTI9	0.00	0.00	0.00	0.00	-0.58	0.00	0.00	0.00	0.00	0.00	0.00
DTI10	0.00	0.00	0.00	0.58	0.00	0.00	0.00	0.00	0.00	0.00	0.00
DTI11	0.00	0.75	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
DTI12	0.00	0.58	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
DTI13	-0.42	0.00	0.00	0.00	0.00	0.00	0.75	0.00	0.00	0.00	0.00
DTI	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
DSI1	0.89	0.58	0.00	-0.42	-0.42	0.00	-0.42	0.18	0.00	0.42	0.00
DSI2	0.00	0.58	0.00	-0.42	-0.42	0.00	0.00	0.18	0.00	0.00	0.00
DSI3	0.89	0.89	0.00	-0.75	-0.58	0.42	-0.75	0.75	0.75	0.75	0.00
DSI4	0.00	0.00	0.00	0.00	0.00	0.58	0.00	0.00	0.00	0.00	0.00
DSI5	0.00	0.58	0.00	-0.75	-0.58	0.42	-0.42	0.75	0.58	0.58	0.00
DSI6	0.00	0.00	0.00	0.00	0.00	0.75	0.00	0.18	0.00	0.75	0.00
DSI7	0.89	0.58	0.00	0.00	0.00	0.00	0.00	0.00	0.89	0.42	0.00
DSI8	0.75	0.00	0.42	0.00	0.00	0.00	0.00	0.00	0.58	0.00	0.00
DSI9	0.75	0.00	0.58	0.00	0.00	0.00	0.00	0.00	0.42	0.00	0.00
DSI10	0.00	0.00	0.00	-0.58	0.00	0.00	0.00	0.18	0.00	0.94	0.00
DSI11	-0.42	-0.58	0.00	0.00	0.00	-0.58	0.00	-0.75	-0.42	-0.58	0.00
DSI12	0.75	0.00	0.58	0.00	0.00	0.58	0.00	0.42	0.58	0.89	0.00
DSI13	0.75	0.00	0.00	0.00	0.00	0.89	0.00	0.00	0.75	0.58	0.00
DSI14	0.42	0.58	0.00	0.00	0.00	0.00	0.00	0.58	0.00	0.00	0.00
DSI	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00

Table A.11: The results of the scenarios

	0. Scenario	1. Scenario		2. Scenario		3. Scenario		4. Scenario		5. Scenario		6. Scenario	
Concepts	**Concept's value**	**Changes**	**Results**	**Changes**	**Results**	**Changes**	**Results**	**Changes**	**Results**	**Changes**	**Results**	**Changes**	**Results**
DCI1	0.947		0.924	-1.000	-1.000		0.943	1.000	1.000		0.930		0.799
DCI2	1.000		0.955	-1.000	-1.000		1.000	1.000	1.000		0.990	-1.000	-1.000
DCI3	1.000		0.070	-1.000	-1.000		0.997	1.000	1.000		0.263	-1.000	-1.000
DCI4	0.941		0.967	-1.000	-1.000		0.877	1.000	1.000		0.982		0.977
DCI5	0.892		0.872	-1.000	-1.000		0.886	1.000	1.000		0.876		0.867
DCI6	0.956		0.861	-1.000	-1.000		0.956	1.000	1.000		0.887		0.480
DCI7	0.038		0.877	1.000	1.000		0.039	-1.000	-1.000		0.853		0.160
DCI8	0.998		0.311	-1.000	-1.000		0.998	1.000	1.000		0.421		0.772
DCI9	0.952		0.904	-1.000	-1.000		0.948	1.000	1.000		0.916		0.774
DCI10	1.000		0.236	-1.000	-1.000		0.999	1.000	1.000		0.336	-1.000	-1.000
DCI11	0.995		0.767	-1.000	-1.000		0.994	1.000	1.000		0.822		0.930
DCI12	0.057		0.358	1.000	1.000		0.161	-1.000	-1.000		0.320		0.068
DCI13	0.020		0.816	1.000	1.000		0.020	-1.000	-1.000		0.768		0.296
DCI14	1.000		0.940	-1.000	-1.000		0.998	1.000	1.000		0.965		0.823
DTI1	0.523	-1.000	-1.000		0.521		0.523	-1.000	-1.000	-1.000	-1.000		0.518
DTI2	0.991	-1.000	-1.000		0.986		0.958	-1.000	-1.000	-1.000	-1.000		0.992
DTI3	1.000	-1.000	-1.000		0.997		0.998	-1.000	-1.000	-1.000	-1.000		1.000
DTI4	1.000	-1.000	-1.000		0.991		0.994	-1.000	-1.000	-1.000	-1.000		1.000
DTI5	1.000	-1.000	-1.000		0.996		0.993	-1.000	-1.000	-1.000	-1.000		1.000
DTI6	0.981	-1.000	-1.000		0.935		0.980	-1.000	-1.000	-1.000	-1.000		0.956

Table A.11: The results of the scenarios (*continue*)

Concepts	Concept's value	Changes	Results	Changes	Results	Changes	Results	Changes	Results	Changes	Results	Changes	Results
DTI7	0.990	-1.000	-1.000		0.965		0.989	-1.000	-1.000	-1.000	-1.000		0.990
DTI8	0.985	-1.000	-1.000		0.958		0.983	-1.000	-1.000	-1.000	-1.000		0.985
DTI9	0.965	-1.000	-1.000		0.570		0.965	-1.000	-1.000	-1.000	-1.000		0.832
DTI10	0.707	-1.000	-1.000		0.712		0.707	-1.000	-1.000	-1.000	-1.000		0.709
DTI11	0.996	-1.000	-1.000		0.757		0.984	-1.000	-1.000	-1.000	-1.000		0.986
DTI12	1.000	-1.000	-1.000		0.986		0.997	-1.000	-1.000	-1.000	-1.000		0.999
DTI13	0.000	1.000	1.000		0.611		0.003	1.000	1.000	1.000	1.000		0.003
DSI1	1.000		0.730		0.999	-1.000	-1.000		0.790	1.000	1.000		1.000
DSI2	0.998		0.928		0.929	-1.000	-1.000		0.943	1.000	1.000		0.998
DSI3	1.000		0.992		0.940	-1.000	-1.000		1.000	1.000	1.000		1.000
DSI4	0.797		0.792		0.676	-1.000	-1.000		0.799	1.000	1.000		0.785
DSI5	1.000		0.930		0.950	-1.000	-1.000		0.993	1.000	1.000		0.999
DSI6	0.930		0.928		0.856	-1.000	-1.000		0.931	1.000	1.000		0.925
DSI7	1.000		0.933		1.000	-1.000	-1.000		0.938	1.000	1.000		1.000
DSI8	1.000		0.564		1.000	1.000	1.000		0.589	-1.000	-1.000		1.000
DSI9	1.000		0.711		1.000	1.000	1.000		0.736	-1.000	-1.000		1.000
DSI10	0.980		0.935		0.105	-1.000	-1.000		0.994	1.000	1.000		0.880
DSI11	0.012		0.036		0.108	1.000	1.000		0.020	-1.000	-1.000		0.040
DSI12	0.999		0.992		0.996	-1.000	-1.000		0.993	1.000	1.000		0.999
DSI13	0.997		0.996		0.998	-1.000	-1.000		0.943	1.000	1.000		0.997
DSI14	0.993		0.992		0.896	-1.000	-1.000		0.992	1.000	1.000		0.990

Table A.11: The results of the scenarios (*continue*)

	0. Scenario	7. Scenario		8. Scenario		9. Scenario		10. Scenario		11. Scenario		12. Scenario	
Concepts	**Concept's value**	**Changes**	**Results**	**Changes**	**Results**	**Changes**	**Results**	**Changes**	**Results**	**Changes**	**Results**	**Changes**	**Results**
DCI1	0.947		0.946		0.947		0.876		0.947		0.947		0.876
DCI2	1.000		1.000		1.000	-1.000	-1.000		1.000		1.000	-1.000	-1.000
DCI3	1.000		0.999		1.000		1.000		1.000		1.000		1.000
DCI4	0.941		0.953		0.940		0.742		0.949		0.940		0.787
DCI5	0.892		0.891		0.892		0.883		0.892		0.892		0.883
DCI6	0.956		0.956		0.956		0.956		0.956		0.956		0.956
DCI7	0.038		0.292		0.038		0.039		0.175		0.038		0.187
DCI8	0.998		0.969		0.998		0.993		0.983		0.998		0.937
DCI9	0.952		0.951		0.952		0.928		0.952		0.952		0.928
DCI10	1.000		1.000		1.000		1.000		1.000		1.000		1.000
DCI11	0.995		0.994		0.995		0.994		0.994		0.995		0.992
DCI12	0.057		0.075		0.057		0.060		0.058		0.057		0.062
DCI13	0.020		0.189		0.020		0.047		0.120		0.020		0.284
DCI14	1.000		0.999		1.000		0.997		1.000		1.000		0.996
DTI1	0.523		0.642		0.523		0.523		0.632		0.523		0.632
DTI2	0.991		0.345		0.989		0.991		0.948		0.991		0.953
DTI3	1.000	-1.000	-1.000		1.000		1.000	-1.000	-1.000		1.000	-1.000	-1.000
DTI4	1.000	-1.000	-1.000		0.994		1.000		1.000		1.000		1.000
DTI5	1.000	-1.000	-1.000		0.993		1.000		1.000		1.000		0.998
DTI6	0.981		0.212		0.981		0.981		0.883		0.981		0.883

Table A.11: The results of the scenarios (*continue*)

Concepts	Concept's value	Changes	Results	Changes	Results	Changes	Results	Changes	Results	Changes	Results	Changes	Results
DTI7	0.990		0.689		0.990		0.990		0.965		0.990		0.965
DTI8	0.985		0.167		0.985		0.985		0.911		0.985		0.911
DTI9	0.965		0.844		0.966		0.964		0.846		0.965		0.840
DTI10	0.707		0.778		0.703		0.707		0.717		0.706		0.716
DTI11	0.996		0.995		0.996		0.996		0.996		0.996		0.995
DTI12	1.000		0.974		1.000		1.000		0.999		1.000		0.999
DTI13	0.000		0.016		0.001		0.000		0.000		0.001		0.001
DSI1	1.000		0.998	-1.000	-1.000		1.000		1.000		1.000		1.000
DSI2	0.998		0.998		0.944		0.998		0.998		0.987		0.985
DSI3	1.000		1.000	-1.000	-1.000		1.000		1.000	-1.000	-1.000	-1.000	-1.000
DSI4	0.797		0.797		0.797		0.797		0.797		0.797		0.797
DSI5	1.000		0.997	-1.000	-1.000		1.000		1.000		1.000		0.999
DSI6	0.930		0.930		0.925		0.930		0.930		0.929		0.929
DSI7	1.000		0.996		0.937		1.000		0.998		0.998		0.987
DSI8	1.000		0.971		0.975		1.000		0.999		0.999		0.994
DSI9	1.000		0.985		0.968		1.000		0.999		0.999		0.995
DSI10	0.980		0.979		0.978		0.980		0.979		0.979		0.978
DSI11	0.012		0.012		0.048		0.012		0.012		0.039		0.039
DSI12	0.999		0.999		0.849		0.999		0.999		0.993		0.993
DSI13	0.997		0.992		0.824		0.997		0.991		0.985		0.964
DSI14	0.993		0.992		0.937		0.993		0.992		0.976		0.975

Appendix B.

Table B.1: Existing research about CMM in academic papers

Authhor(s)	Model Name	# of Maturity Dimensions / # of Maturity Levels	Type of Model	Field of Application	Assessment Method	Application Method	Evaluation Criteria Basis	Dimensions	Levels	Numeric Calculation (Y/N)	Cooperation
(Bitzer et al., 2023)	IRM3	4/3	Generic	IT	Self-assessment	Design science research	-	1. Organization, 2. Human 3. Tools 4. Processes	1. Class A 2. Class B 3. Class C	Y	-
(Barnes & Daim, 2022)	-	5/-	Generic	Healthcare	Self-assessment/ 3rd party assisted	Hierarchical decision model, case study	-	1. Organizational Support 2. Policies and Standards 3. Awareness and Training 4. Information Security Technical Hygiene 5. Mitigation of External Threats	-	N	Healthcare Organizations-USA
(Loft et al., 2022)	CAESAR 8	8/5	Generic	-	Self-assessment	Questionnaire, case study	-	1. External factors 2. Security governance 3. Business process 4. Information assets 5. Technology infrastructure 6. Human factors 7. Management influence 8. Enterprise architecture	1. Level 1- The business 2. Level 2- Business change 3. Level 3- Security impact 4. Level 4- Security Strategy 5. Level 5- Optimization	Y	Metropolitan Police Service-U.K.

Table B.1: Existing research about CMM in academic papers (*continue*)

Authhor(s)	Model Name	# of Maturity Dimensions/ # of Maturity Levels	Type of Model	Field of Application	Assessment Method	Application Method	Evaluation Criteria Basis	Dimensions	Levels	Numeric Calculation (Y/N)	Cooperation
(Srinivas et al., 2019)	-	3/5	Specific	-	Self-assessment/3rd party assisted	Linear regression, path analysis	CEAT, CMM	1. Education 2. Awareness 3. Training	1. Start-up 2. Formative 3. Established 4. Strategic 5. Dynamic	Y	-
(Tokerud, 2022)	-	8/3	Generic		Self-assessment	Design science research	Zero Trust maturity model	1. Identity and Access management 2. Change Management 3. Asset Management 4. Incident Management 5. Supply Chain Management 6. Data Governance and Protection 7. Employee Awareness and Training 8. IS Culture	1. Level 1 2. Level 2 3. Level 3	Y	-
(Al-Matari et al., 2021)	-	4/6	Generic	SMEs	Self-assessment/3rd party assisted	Questionnaire	ISM3	1. General 2. Strategic 3. Tactical 4. Operational	1. Nonexistent 2. Ad hoc 3. Repeatable 4. Defined 5. Managed 6. Optimized	Y	Retirement organization, Telcom - Yemen

Table B.1: Existing research about CMM in academic papers (*continue*)

Authhor(s)	Model Name	# of Maturity Dimensions/ # of Maturity Levels	Type of Model	Field of Application	Assessment Method	Application Method	Evaluation Criteria Basis	Dimensions	Levels	Numeric Calculation	Cooperation
(Almomani et al., 2021)	SCMAF	16/5	Specific	Higher education	Self-assessment	Questionnaire	ECC, CRF, HCYMAF	-	1. Initial 2. Managed 3. Defined 4. Quantitively Managed 5. Optimized	Y	Higher Education Institutes-Saudi Arabia
(Andreasson et al., 2021)	-	-	Specific	Government	3rd party assisted	Interviews, questionnaire	-	-	-	Y	Government Agencies-Sweden
(Boccardo et al., 2021)	-	6/3	Generic	General	Self-assessment	Questionnaire, spreadsheet	CIS Controls, NIST, BMIS	1. Control of hardware assets 2. Control of software assets 3. Continuous vulnerability management 4. Controlled use administrative privileges 5. Secure configuration 6. Maintenance, monitoring and analysis of audit logs	1. People 2. Process 3. Technology	Y	Industry 4.0 Organization

Table B.1: Existing research about CMM in academic papers (*continue*)

Authhor(s)	Model Name	# of Maturity Dimensions/ # of Maturity Levels	Type of Model	Field of Application	Assessment Method	Application Method	Evaluation Criteria Basis	Dimensions	Levels	Numeric Calculation	Cooperation
(Chapman & Reithel, 2021)	PACRM	14/-	Generic	Public universities	Self-assessment	Qualitative Interviews, path analysis	CIS, ISO, NIST	-	-	Y	Public universities- USA
(S. Hasan et al., 2021)	-	3/-	Generic	General	Self-assessment	Technology-organization-environment framework, survey	-	1. Technological 2. Organizational 3. Environmental	-	N	-
(Santos et al., 2021)	-	3/5	Specific	Dark Web	Self-assessment	Questionnaire	CAT-FFIEC, COBIT 2019	1. Identification 2. Diagnostics 3. Deployment	1. Initial 2. Basic 3. Normal 4. Advanced 5. Optimal	Y	Insurance company - Peru
(Shaked et al., 2021)	ProGRESS	4/4	Generic	General	Self-assessment	Workshops, questionnaire	-	1. Organization 2. Process 3. Workforce 4. Tools 5. Compliance	1. Level 1 2. Level 2 3. Level 3 1. Level 4	N	-
(Tissir et al., 2021)	CSCMM	5/-	Specific	Cloud Security	Self-assessment	Systematic review	ISO 27001, ISO 27017, ISO27032, NIST	1. Leadership and planning 2. Risk management process 3. Implementation and operation 4. Performance and evaluation 5. Improvement	-	N	-

Table B.1: Existing research about CMM in academic papers (*continue*)

Authhor(s)	Model Name	# of Maturity Dimensions/ # of Maturity Levels	Type of Model	Field of Application	Assessment Method	Application Method	Evaluation Criteria Basis	Dimensions	Levels	Numeric Calculation	Cooperation
(Yigit Ozkan et al., 2021)	CYSFAM	2/12	Generic	General	Self-assessment	Design science research	ISFAM	1. Technical 2. Organizational	-	Y	Bank – Western European
(Al-Karaki et al., 2020)	GoSafe	5/4	Generic	General	Self-assessment/3rd party assisted	Online survey, pre-audit tool, security index rating	ISO 27001	1. Legal 2. Technical 3. Organizational 4. Capacity building 5. Cooperation	1. Collection 2. Processing 3. Analysis 4. Reporting	Y	-
(Aliyu et al., 2020)	HCYMAF	3/5	Specific	Higher education	3rd party assisted	Interviews	CMMI	1. Identify 2. Protect & detect 3. Respond & recover	1. Initial 2. Managed 3. Defined 4. Quantitively Managed 5. Optimized	N	Higher Education Institutes-UK
(Anass et al., 2020)	CCSMM	4/3	Specific	Government	Self-assessment/3rd party assisted	Audit tool	ISO 21827, CCSMM, MMISS-SME	1. Awareness 2. Information Sharing 3. Policies 4. Planning	1. Initial 2. Established 3. Self-Assessed 4. Integrated 5. Vanguard	N	-
(Baikloy et al., 2020)	-	6/5	Specific	Cloud Computing Services	Self-assessment	Online survey, AHP	NIST, ISF, CERT, CMMI	1. Identify 2. Protect 3. Detect 4. Respond 5. Recover 6. Dependability	1. Initial 2. Managed 3. Defined 4. Optimized 5. Resilient	Y	Cloud Service Companies

Table B.1: Existing research about CMM in academic papers (*continue*)

Authhor(s)	Model Name	# of Maturity Dimensions/ # of Maturity Levels	Type of Model	Field of Application	Assessment Method	Application Method	Evaluation Criteria Basis	Dimensions	Levels	Numeric Calculation	Cooperation
(Benz & Chatterjee, 2020)	NIST CSF	5/5	Generic	SMEs	Self-assessment	Online survey	NIST	1. Identify (ID) 2. Protect (PR) 3. Detect (DE) 4. Respond (RS) 5. Recover (RC)	1. None 2. Reactive 3. Formalizing 4. Repeatable 5. Role model	Y	SMEs
(Drivas et al., 2020)	CMAF	3/6	Generic	National infrastructures	Self-assessment/3rd party assisted	-	-	1. Identification 2. Protection 3. Reaction	1. Incomplete 2. Initial 3. Basic 4. Advanced 5. Effective 6. Efficient	N	-
(Gourisetti et al., 2020)	CyFER	5/5	Generic	General	Self-assessment/3rd party assisted	Enhanced prioritized gap analysis	NIST	1. Identify (ID) 2. Protect (PR) 3. Detect (DE) 4. Respond (RS) 5. Recover (RC)	1. MIL0 2. MIL1 3. MIL2 4. MIL3 5. MIL4	Y	Industrial control systems
(Kritzinger, 2020)	360safe	4/-	Specific	Schools	Self-assessment	Online survey, Cronbach's alpha	UK 360safe measuring tool	1. Policy and Leadership 2. Infrastructure 3. Education Standards and inspection	-	Y	Schools – South Africa

Table B.1: Existing research about CMM in academic papers (*continue*)

Authhor(s)	Model Name	# of Maturity Dimensions/ # of	Type of Model	Field of Applicatio n	Assessment Method	Application Method	Evaluation Criteria Basis	Dimensio ns	Levels	Numeric Calculation	Cooperation
(Malatji et al., 2020)	-	3/5	Generic	General	Self-assessment	Survey, interview	COBIT5	1. Functions 2. People 3. Tasks	1. Haphazard 2. Basic 3. Formalized processes 4. Measurable outcome 5. Optimizing	N	-
(Putra et al., 2020)	-	5/3	Specific	Workforce Management	Self-assessment	Case study methodology	C2M2	1. Assign Cybersecurity Responsibilities 2. Develop Cybersecurity Workforce 3. Implement Workforce Controls 4. Increase Cybersecurity Awareness 5. Management Activities	1. MIL0 2. MIL1 3. MIL2 4. MIL3 6. MIL4	Y	Bank - Indonesia
(Riadi et al., 2020)	-	6/5	Specific	Universities	Self-assessment	Capability maturity model integration (CMMI)method	DSS05 domain of COBIT 5	-	1. Initial 2. Managed 3. Defined 4. Quantitively Managed 5. Optimized	Y	Ahmad Dahlan University - Indonesia

Table B.1: Existing research about CMM in academic papers (*continue*)

Authhor(s)	Model Name	# of Maturity Dimensions/ # of Maturity Levels	Type of Model	Field of Application	Assessment Method	Application Method	Evaluation Criteria Basis	Dimensions	Levels	Numeric Calculation	Cooperation
(Yigit Ozkan et al., 2020)	CA-ISFAM	4/12	Generic	SMEs	Self-assessment	Design science research	ISFAM	1. Organizational 2. Technical 3. Organizational and technical 4. Support	-	Y	SMEs – Port of Rotterdam
(Akinsanya et al., 2020)	M2HCS	5/4	Specific	Healthcare cloud security	3rd party assisted	Case Study/ Survey	CMM, ISFAM, CSCMM, NHS NIMM, HIN CMM	1. Incident response management 2. Identity and access management 3. Enterprise risk management 4. Personnel security 5. Physical security	1. Level 1 2. Level 2 3. Level 3 4. Level 4	Y	NHS Trust University Teaching Hospital
(Bahuguna et al., 2019)	-	6/-	Generic	Government	3rd party assisted	Questionnaire, workshop	GCI	1. Cybersecurity Initiatives, Challenges and Priorities for the entity 2. Legal and regulatory Measures 3. Technical Measures 4. Organizational and Policy Measures 5. Capacity Building and Awareness 6. Cooperation, Information Sharing	-	Y	Indian Organizations

Table B.1: Existing research about CMM in academic papers (*continue*)

Authhor(s)	Model Name	# of Maturity Dimensions/ # of Maturity Levels	Type of Model	Field of Application	Assessment Method	Application Method	Evaluation Criteria Basis	Dimensions	Levels	Numeric Calculation	Cooperation
(Gholami Mehrabadi et al., 2019)	-	4/5	Specific	Managed Security Service Providers	Self-assessment/3rd party assisted	Multi-model analysis	ISM3, C2M2, PRISMA, ISF, FFIEC	1. Organizational 2. Financial 3. Environment 4. Technology	1. Initial 2. Formed 3. Defined 4. Managed 5. Optimized	N	Managed Security Service Providers - Iran
(Gupta Gourisetti et al., 2019)	CyFER	5/5	Generic	General	Self-assessment/3rd party assisted	Prioritized gap analysis	NIST, C2M2	1. Identify (ID) 2. Protect (PR) 3. Detect (DE) 4. Respond (RS) 5. Recover (RC)	1. MIL0 2. MIL1 3. MIL2 4. MIL3 5. MIL4	Y	Blockchain
(Yigit Ozkan & Spruit, 2019)	-	-	Specific	Identity Management and Access Control	Self-assessment	Questionnaire model	ISO27002, ETSI TR 103 305	1. -	1. -	N	-

Table B.1: Existing research about CMM in academic papers (*continue*)

Authhor(s)	Model Name	# of Maturity Dimensions/ # of Maturity	Type of Model	Field of Application	Assessment Method	Application Method	Evaluation Criteria Basis	Dimensions	Levels	Numeric Calculation	Cooperation
(Kour & Karim, 2020)	R-C2M2	10/5	Specific	Railways	Self-assessment	Questionnaire	C2M2	1. Risk management 2. Asset, change, configuration management 3. Identity and access management 4. Threat and vulnerability management 5. Situational awareness 6. Information sharing and communication 7. Event and incident response, continuity of operations 8. Supply chain and external dependencies management 9. Workforce management 10. Cybersecurity program management	2. MIL0 3. MIL1 4. MIL2 5. MIL3 MIL4	Y	Railway organizations
(Jaquire & Von Solms, 2017)	CCIMM	6/4	Specific	Developing countries	Self-assessment /3rd party assisted	Dashboards	-	1. Structures 2. People 3. Processes/Techniques 4. Technologies 5. Legal/policies 6. Training/Skills development	1. Level 0 2. Level 1 3. Level 2 4. Level 3	N	-

Table B.1: Existing research about CMM in academic papers (*continue*)

Authhor(s)	Model Name	# of Maturity Dimensions/ # of Maturity Levels	Type of Model	Field of Application	Assessment Method	Application Method	Evaluation Criteria Basis	Dimensions	Levels	Numeric	Cooperation
(Karabacak et al., 2016)	-	-	Specific	National infrastructures	3rd party assisted	Delphi survey	CCSMM, NCSecM, Cyber Readiness Index, Global Cybersecurity Index	-	-	Y	Critical Infrastructures - Türkiye
(De Bruin & Von Solms, 2016)	CSGMM	5/4	Generic	General	Self-assessment	Dashboards	-	1. Capability 2. Contingency 3. Capacity building 4. Conformance 5. Threat	1. Level 1 2. Level 2 3. Level 3 4. Level 4	N	-
(Spruit & Roeling, 2014)	ISFAM	4/5	Generic	General	Self-assessment /3rd party assisted	Questionnaire	CMM	1. Organizational 2. Technical 3. Organizational and technical 4. Support	1. Initial (A-E) 2. Repeatable (A-E) 3. Defined (A-E) 4. Managed (A-E) 5. Optimized (A-E)	Y	Telcom - Netherlands
(Karokola et al., 2011)	eGMM	5/5	Specific	e-Government	Self-assessment /3rd party assisted	Soft systems methodology	ISO- ISM3	1. Web-presence 2. Interaction 3. Transaction 4. Transformation 5. Continuous improvement	1. Undefined 2. Defined 3. Managed 4. Controlled 5. Optimized	N	-

Table B.2: Existing research about CMM on industry reports

Study	Model Name	# of Maturity Dimensions/ # of Maturity Levels	Type of Model	Field of Application	Assessment Method	Application Method	Evaluation Criteria Basis	Dimensions	Levels
CISO (Results, 2022)	CISO-CMM	4/5	Generic	General	Self-assessment/3rd party assisted	Questionnaire, survey	CMM	1. Culture 2. Technology 3. Risk 4. People	1. Initial 2. Repeatable 3. Defined 4. Managed 5. Optimizing
(CMM, 2021)	CMM for Nations	5/5	Specific	Government	Self-assessment/3rd party assisted	Questionnaire, survey	-	1. Cybersecurity Policy and Strategy 2. Cybersecurity Culture and Society 3. Building Cybersecurity Knowledge and Capabilities 4. Legal and Regulatory Frameworks 5. Standards and Technologies	1. Start-up 2. Formative 3. Established 4. Strategic 5. Dynamic
(CISA, 2021)	Zero Trust Maturity Model	5/3	Specific	Government	Self-assessment/3rd party assisted	Questionnaire, survey	NIST SP 800-207	1. Identity 2. Device 3. Network/Environment 4. Application Workload 5. Data	1. Traditional 2. Advanced 3. Optimal

Table B.2: Existing research about CMM on industry reports (*continue*)

Study	Model Name	# of Maturity Dimensions/ # of Maturity Levels	Type of Model	Field of Application	Assessment Method	Application Method	Evaluation Criteria Basis	Dimensions	Levels
(Ferreira et al., 2020)	BCG Maturity Model	6/4	Specific	Remote Working	Self-assessment/3rd party assisted	Questionnaire, survey	-	1. Vision RW models 2. Practices and routines 3. Trust-based management 4. Leadership and culture 5. Technology solutions 6. Coaching and training	1. Reluctant 2. Passives 3. Performers 4. Leaders
(Porrúa & Contreras B, 2020)	Cybersecurity Capacity Maturity Model (CMM)	5/5	Generic	Governments	Self-assessment/3rd party assisted	Questionnaire	Global Cyber Security Capacity Centre	1. Cybersecurity Policy and Strategy 2. Cyberculture and society 3. Cybersecurity Education, Training, and Skills 4. Legal and Regulatory Frameworks 5. Standards, Organizations, and Technologies	1. Startup 2. Formative 3. Established 4. Strategic 5. Dynamic
(EuroControl, 2017)	ATM cybersecurity maturity model	6/5	Specific	Air Navigation Service Providers	Self-assessment	Scoring form, questionnaire	NIST, ISO27001	1. Lead and Govern 2. Identify 3. Protect 4. Detect 5. Respond Recover	1. Non-existent 2. Partial 3. Defined 4. Assured Adaptive

Table B.2: Existing research about CMM on industry reports (*continue*)

Study	Model Name	# of Maturity Dimensions/ #	Type of Model	Field of Application	Assessment Method	Application Method	Evaluation Criteria Basis	Dimensions	Levels
(US DoD, 2020)	Cybersecurity Maturity Model Certification (CMMC)	17/5	Specific	Defense Industrial Base Contractors	3rd party assisted	Questionnaire	NIST SP 800-171, FIPS	1. Access Control 2. Asset Management 3. Audit and Accountability 4. Awareness and Training 5. Configuration Management 6. Identification and Authentication 7. Incident Response 8. Maintenance 9. Media Protection 10. Personnel Security 11. Physical Protection 12. Recovery 13. Risk Management 14. Security Assessment 15. Situational Awareness 16. System Communications and Protection 17. System and Information Integrity	1. Performed 2. Documented 3. Managed 4. Reviewed 5. Optimizing

Table B.2: Existing research about CMM on industry reports (*continue*)

Study	Model Name	# of Maturity Dimensions/ #	Type of Model	Field of Application	Assessment Method	Application Method	Evaluation Criteria Basis	Dimensions	Levels
(US DoE, 2019)	C2M2 (Cybersecurity Capacity Maturity Model) version 2.0 (Developed in 2012, updated in 2014 and 2019)	10/4	Generic	General	Self-assessment	Workshop	ES-C2M2 (Electricity Subsector Cybersecurity Capability Maturity Model) version 1.0	1. Risk Management 2. Asset, Change, and Configuration Management 3. Identity and Access Management 4. Threat and Vulnerability Management 5. Situational Awareness 6. Event and Incident Response 7. Supply Chain and External Dependencies Management 8. Workforce Management 9. Cybersecurity Architecture 10. Cybersecurity Program Management	1. Maturity Indicator Level 1 (MIL0) 2. MIL1 3. MIL2 4. MIL3
(CMMI, 2017)	Capability Maturity Model Integration	3/5	Generic	General	Self-assessment	Dashboard, scoring form,	ISO, NIST, ISC, COBIT 5.0	1. People 2. Process 3. Technology	1. Performed 2. Managed 3. Defined 4. Quantitively Managed 5. Optimized

Table B.2: Existing research about CMM on industry reports (*continue*)

Study	Model Name	# of Maturity Dimensions/ #	Type of Model	Field of Application	Assessment Method	Application Method	Evaluation Criteria Basis	Dimensions	Levels
(Zivanovic, Jasmina, 2018)	IBM Security Immune System	7/3	Generic	General	Self-assessment/3rd party assisted	Questionnaire	-	1. Security Orchestration and Analytics 2. Fraud Protection 3. Identity and Access Management 4. Application Security 5. Endpoint Protection 6. Network Protection 7. Mobile Security	1. Prove compliance 2. Stop threats 3. Grow business
(NIST Cybersecurity Framework Team, 2018)	NIST CSF (Cybersecurity Framework) (Developed in 2014, updated in 2017 and 2018)	5/4	Generic	General	Self-assessment	Questionnaire	NIST 800-53, FIPS, COBIT 5.0, ISO 27000	1. Identify (ID) 2. Protect (PR) 3. Detect (DE) 4. Respond (RS) 5. Recover (RC)	1. Tier 1: Partial 2. Tier 2: Risk Informed 3. Tier 3: Repeatable 4. Tier 4: Adaptive
(Wirnsperger, Peter; Yildiz, 2017)	Deloitte's CIC (Cyber Intelligence Center)	4/3	Generic	General	Self-assessment/3rd party assisted	Questionnaire	-	1. Cyber Strategy 2. Cyber Secure 3. Cyber Vigilant 4. Cyber Resilient	1. Advice 2. Implement 3. Manage

Table B.2: Existing research about CMM on industry reports (*continue*)

Study	Model Name	# of Maturity Dimensions/ # of Maturity	Type of Model	Field of Application	Assessment Method	Application Method	Evaluation Criteria Basis	Dimensions	Levels
(KPMG, 2017)	Cyber maturity assessment	6/3	Generic	General	Self-assessment/3rd party assisted	Questionnaire	International information security standards	1. Leadership and Governance 2. Human Factors 3. Information Risk Management 4. Business Continuity and Crisis Management 5. Operation and Technology 6. Legal and Compliance	1. Benchmarking against relevant peers 2. Industry average 3. Good practices
(REBIT, 2017)	Cyber Security Maturity Model (CMM)	5/5	Generic	General	Self-assessment	Questionnaire, spreadsheet	NIST, COBIT 5.0, ISO 27000	1. Security Management 2. Infrastructure Management 3. Cybersecurity Engineering 4. Delivery Channels 5. Situational Awareness	1. Initializing 2. Developing 3. Operating 4. Managing 5. Optimizing

Table B.2: Existing research about CMM on industry reports (*continue*)

Study	Model Name	# of Maturity Dimensions/ # of Maturity	Type of Model	Field of Application	Assessment Method	Application Method	Evaluation Criteria Basis	Dimensions	Levels
(Multi-State Information Sharing & Analysis Center, 2016)	Nationwide Cyber Security Review	5/7	Generic	Governments	Self-assessment/3rd party assisted	Questionnaire	NIST	1. Identify 2. Protect 3. Detect 4. Respond 5. Recover	1. Not performed 2. Informally performed 3. Documented policy 4. Partially documented standards and/or procedures 5. Risk formally accepted & implementation in process 6. Tested and verified 7. Optimized
(Mattioli & Moulinos, Konstantinos, 2015)	ICS-SCADA Cyber Security Maturity Assessment Model	3/5	Generic	Governments	3rd party assisted	Interviews	-	1. Legislation 2. Support 3. Local Conditions	1. Basic 2. Developing 3. Established 4. Advanced 5. Leading
(Software Engineering Institute, 2010)	CMMI-DEV (Capability Maturity Model Integration for Development)	3/5	Generic	General	3rd party assisted	Questionnaire	CMMI	1. Support 2. Process Management 3. Engineering	1. Initial 2. Managed 3. Defined 4. Quantitively Managed 5. Optimizing

Table B.2: Existing research about CMM on industry reports (*continue*)

Study	Model Name	# of Maturity Dimensions/ # of Maturity Levels	Type of Model	Field of Application	Assessment Method	Application Method	Evaluation Criteria Basis	Dimensions	Levels
(Allan et al., 2009)	Identity and Access Management Maturity Model	6/5	Generic	General	Self-assessment/3rd party assisted	Questionnaire	-	1. Governance 2. Organization 3. Vision and Strategy 4. Processes 5. Architecture and Infrastructure Design 6. Business Value	1. Initial 2. Developing 3. Defined 4. Managed 5. Optimized
(Vicente Aceituno Canal, 2007)	Information Security Management Maturity Model (ISM3 1.0.)	3/5	Generic	General	Self-assessment	Questionnaire	CMMI, ISO 9001:200	1. Strategic Management 2. Tactical Management 3. Operational Management	1. Level 0 2. Level 1 3. Level 2 4. Level 3 5. Level 4

Table B.3: The CMM Questionnaire

Dimensions	Factors	Questions
1. Cybersecurity Strategy, Risk and Policy	**1.1. Cybersecurity Strategy, Planning and Transformation**	Q1: In your experience, do you agree that your organization has an effective cybersecurity strategy?
		Q2: In your experience, do you agree that your organization has effectively achieved cybersecurity program integration with business needs?
		Q3: In your experience, do you agree that your organization has a sufficient budget allocated for cybersecurity?
		Q4: In your experience, do you agree that your organization has a holistic approach about cybersecurity transformation?
	1.2. Cybersecurity Threat, Risk, Vulnerability Management and Resiliency	Q5: In your experience, do you agree that your organization has an effective threat management framework for potential cyber threats?
		Q5: In your experience, do you agree that your organization has a risk-aware work culture related to cybersecurity?
		Q7: In your experience, do you agree that your organization has effective cybersecurity vulnerability management?
		Q8: In your experience, do you agree that your organization has the ability to adapt to and counter threats (cybersecurity resiliency)?
	1.3. Cyber Policy Compliance and Governance	Q9: In your experience, do you agree that your organization has effectively formulated a cybersecurity program policy?
		Q10: In your experience, do you agree that the organization has effectively implemented cybersecurity governance structures?
		Q11: In your experience, do you agree that the organization realizes regular cybersecurity policy internal/external audits?
		Q12: In your experience, do you agree that the organization comply with information security standards?
2. Cybersecurity Culture, Education and Workforce	**2.1. Cybersecurity Training, Education and Skills**	Q13: In your experience, do you agree that the organization gives regular training in cybersecurity tools and techniques to its personnel?
		Q14: In your experience, do you agree that the organization has innovation, research and development programs?
		Q15: In your experience, do you agree that the top level in the organization demonstrates commitment to cybersecurity?

Table B.3: The CMM Questionnaire (*continue*)

Dimensions	Factors	Questions
		Q16: In your experience, do you agree that the organization effectively ensures continuous improvements in security skills of employees related to cybersecurity?
	2.2. Cybersecurity Awareness, Culture and Capacity Building	Q17: In your experience, do you agree that the organization realizes practical exercises in awareness training that are aligned with current threat scenarios and provide feedback to individuals involved in the training?
		Q18: In your experience, do you agree that the organization have an organization-wide cyber-focused mindset and cyber-conscious culture?
		Q19: In your experience, do you agree that the organization has a security team committed to cybersecurity?
		Q20: In your experience, do you agree that the organization develops the necessary skills, knowledge, and technical capabilities to detect, prevent, and respond to cyber-attacks?
	2.3. Cybersecurity Workforce Management	Q21: In your experience, do you agree that the organization has successfully identified the appropriate experts and policymakers in government, private sector and academia?
		Q22: In your experience, do you agree that the organization has defined security roles related to cybersecurity?
		Q23: In your experience, do you agree that the organization has effective ways for cybersecurity workforce screening for certifications and promotions?
		Q24: In your experience, do you agree that the organization has hired skilled security practitioners related to cybersecurity?
3. Cybersecurity Infrastructure	**3.1. Cybersecurity Methodology**	Q25: In your experience, do you agree that the organization is aware of and committed to using data encryption techniques?
		Q26: In your experience, do you agree that the organization configuring, monitoring, maintaining a firewall, and managing its infrastructure?
		Q27: In your experience, do you agree that the organization's physical assets such as servers, routers, switches, and other network devices are protected from potential cyber threats?
		Q28: In your experience, do you agree that the organization employs a enterprise cybersecurity architecture by ensuring that all areas of the organization are protected against potential cyber threats?
	3.2. Cybersecurity Systems and Software Security	Q29: In your experience, do you agree that the organization creates a continuous control environment by employing Software Development Life Cycle (SDCL)?
		Q30: In your experience, do you agree that the organization is aware of and committed to using virus protection software to protect its systems and applications ?

Table B.3: The CMM Questionnaire (*continue*)

Dimensions	Factors	Questions
		Q31: In your experience, do you agree that the organization is aware of and committed to continuously monitoring security alerts to detect cyber-attacks on its network?
		Q32: In your experience, do you agree that the organization implements a good governance model and architecture to enable cloud and mobile security?
	3.3. Cybersecurity Intelligence	Q33: In your experience, do you agree that the organization has effectively formulated an advanced threat response strategy for cybersecurity?
		Q34: In your experience, do you agree that the organization simulates a DDoS attack using various tools and techniques for DDoS testing?
		Q35: In your experience, do you agree that the organization has effectively tracked the signs of threats in the area of cybersecurity, and it is aware of being prepared to respond to potential attacks?
		Q36: In your experience, do you agree that the organization simulates a comprehensive cyber-attack that tests the organization's prevention, detection, and response mechanisms (i.e., red-teaming)?
4. Cybersecurity Identity, Information and Organization	**4.1. Cybersecurity Identity, Access and Authorization Management**	Q37: In your experience, do you agree that the organization protect its sensitive data and resources from unauthorized access and data breaches by identity management and access control?
		Q38: In your experience, do you agree that the organization effectively provides two or multi factor identification to access a system or application to prevent unauthorized access?
		Q39: In your experience, do you agree that the organization authenticate or verify the identities of those users, processes or devices, as a prerequisite to allowing access to organizational information systems?
		Q40: In your experience, do you agree that the organization automate the process of generating and distributing reports?
	4.2. Cybersecurity Information Management and Cooperation	Q41: In your experience, do you agree that the organization has effective preemptive knowledge of cybersecurity to manage information and data consistently?
		Q42: In your experience, do you agree that the organization prioritizes the protection of privacy and confidentiality of sensitive data?
		Q43: In your experience, do you agree that the organization effectively cooperate with stakeholders and agencies for cybersecurity?
		Q44: In your experience, do you agree that the organization put collaborative efforts and interactions between countries or international organizations to achieve common cybersecurity goals?

Table B.3: The CMM Questionnaire (*continue*)

Dimensions	Factors	Questions
	4.3. Cybersecurity Organization and Incident Management	Q45: In your experience, do you agree that the organization establishes standard workflows of cybersecurity procedures?
		Q46: In your experience, do you agree that the organization ensure that they follow the latest security guidelines by comparing with the best practices?
		Q47: In your experience, do you agree that the organization employs a business continuity plan to minimize the impact of any disruption and ensure that the organization can continue to operate with as little disruption as possible?
		Q48: In your experience, do you agree that the organization implements cybersecurity incident management (i.e., real-time logging and inspection) to develop a response to malicious events?
5. Cybersecurity Standards, Legislation, Regulation and Protection	**5.1. Cybersecurity Standards**	Q49: In your experience, do you agree that the organization endorses cooperation and coordination with national/international teams (e.g., CERT/CIRT/CSIRT)?
		Q50: In your experience, do you agree that the organization follows standards (i.e., ISO/IEC 27001:2013/SOC2) for enhancing the organization's cybersecurity?
		Q51: In your experience, do you agree that the organization employs pentest and social engineering tests for reducing the organization's cybersecurity failures?
		Q52: In your experience, do you agree that the organization has cybersecurity certifications?
	5.2. Cybersecurity Legal and Regulatory Measures	Q53: In your experience, do you agree that the organization employs legal compliance roadmap is to minimize legal and regulatory risk?
		Q54: In your experience, do you agree that your organization has specified any cybercrime legislations, rule or act?
		Q55: In your experience, do you agree that the organization's cybersecurity program and capabilities align to government regulations?
		Q56: In your experience, do you agree that the organization has constructed a formal/informal cooperation framework to combat cybercrime?
	5.3. Cybersecurity Information Privacy and Protection	Q57: In your experience, do you agree that your organization has effective system for cyber security related data collection, analysis, classification, and ownership?
		Q58: In your experience, do you agree that the organization protects and encrypts sensitive information according to the international data protection laws?
		Q59: In your experience, do you agree that the organization implements policies and procedures to control the flow of data both within and outside an organization to minimize the risk of data breaches, theft, or loss?

BIOGRAPHICAL SKETCH

Merve Güler Kesmez received her high school education at Florya Tevfik Ercan Anatolian High School and graduated as the first-ranking graduate in 2011. She obtained her B.S. in the Industrial Engineering Department of Galatasaray University as the first-ranking graduate in 2016. Since February 2017, she has been working as a research assistant in the Industrial Engineering Department of Galatasaray University. She received her M.S. in Industrial Engineering at the Institute of Science of Galatasaray University in 2018.

Her areas of interest include smart systems, digital transformation, digital government, cybersecurity, logistics and supply chain management, multi-criteria decision making, and the application of fuzzy sets and their extensions. She has published several papers and many proceeding papers in the field of Engineering.

PUBLICATION

Güler, M., & Büyüközkan, G. (2023). A Survey of Digital Government: Science Mapping Approach, Application Areas, and Future Directions. Systems, 11(12), 563. https://doi.org/10.3390/systems11120563