OPEN UNIVERSITY OF KENYA

MASTER'S THESIS

Developing a Digital Forensic Readiness Framework for Incident Response in Smart City Ecosystems: A Case Study of Konza Technopolis, Kenya

Timothy Kosgei
SCHOOL OF SCIENCE

A Master's Thesis Submitted in Partial Fulfilment of the Requirements for the Award of the Master of Science in Cybersecurity and Digital Forensics of the Open University of Kenya.

OPEN UNIVERSITY OF KENYA

OCTOBER 2026

DECLARATION

I declare that this research thesis is my original work and that it has not been presented at any institution for examination. No part of this proposal may be reproduced without the prior written permission of the author and/or the Open University of Kenya.

Signature:  Date: 16/10/2026

Candidate full name: Timothy Kosgei

Reg. No.: **ST63/80222/2024**

This research thesis has been submitted for examination with my approval as the appointed University supervisor.

Signature:  Date: 16/10/2026

Dr. Peter Ngaira

Department of Computing and Informatics

Open University of Kenya

DEDICATION

I dedicate this project thesis to my family for their unwavering love, encouragement, prayers, and support, which have been a constant source of motivation and inspiration. Their sacrifices, patience, and belief in me gave me the courage to pursue and complete this project successfully.

Special appreciation goes to my supervisor Dr. Peter Ngaira whose guidance, advice, and encouragement contributed greatly to the accomplishment of this work. His support and positive influence played a significant role in shaping this academic journey.

To the entire department of Computing and Informatics, school of Science and Technology Lecturers for the wonderful training and valuable knowledge imparted to me through class work.

Above all, I return much thanks to the Almighty God for creating an enabling environment throughout the writing of this Thesis.

ACKNOWLEDGEMENTS

My sincere thanks to my supervisor Dr. Peter Ngaira for his ideal supervision, constructive criticism, professional counselling, patience, for the support and motivation he gave me throughout the course of my project. His knowledge, encouragement and effort have been key to the direction and quality of this work.

I would like to express my gratitude to my colleagues and friends for their cooperation, support, intelligent talks and positive contributions during this academic journey. Your assistance and teamwork were helpful in enriching my thoughts and keeping my enthusiasm.

I appreciate the institution (OUK) for providing a perfect environment for studying, the facilities for study, and knowledge and skills enhancement in cyber security and digital forensics. The commitment and enthusiasm of faculty and staff.

Finally, I would like to express my gratitude to my family for their constant encouragement and support during my studies.

ABSTRACT

Smart cities are becoming increasingly reliant on a network of interconnected digital infrastructure, such as Internet of Things devices, cloud-based platforms, communication systems, and data-driven services, which are all prone to cybersecurity and digital evidence issues. This study examined perceived digital forensic readiness for incident response within Konza Technopolis, Kenya, and developed a context-specific framework for strengthening forensic-ready incident response in smart city ecosystems. This study used a post-positivist embedded mixed-methods case study approach. Data were gathered using purposive sampling techniques, resulting in 109 respondents from ICT operations, cybersecurity, incident response, governance and similar functions. The quantitative data were analysed with descriptive statistics, Pearson correlation and multiple linear regression and open-ended data were analysed thematically.

The results indicated an average score of 3.852 on a scale of 1 to 5 for the overall perceived digital forensic readiness, with 63.3% of the respondents giving a very high to high rating. The highest mean was for logging and monitoring (M = 3.979), and the lowest mean score was for staff preparedness (M = 3.731), which came out as the top priority for improvement. Technological, organisational and environmental factors positively correlated with perceived readiness. In the original regression model, technological factors ($\beta = 0.527$, $p < .001$, 95% CI [0.352, 0.634]) and organisational factors ($\beta = 0.347$, $p < .001$, 95% CI [0.185, 0.430]) showed significant independent associations, while environmental factors were not statistically significant after the other predictors were considered ($\beta = 0.102$, $p = .160$, 95% CI [-0.040, 0.240]). The model accounted for 84.5% of the variation in perceived readiness. Since some predictor items correlated conceptually with the readiness measures, caution was taken in interpreting these findings and they were subsequently analyzed using sensitivity analysis.

A Digital Forensic Readiness Framework was created that centres around three enabling domains – technological, organisational and environmental – and five operational readiness areas – logging and monitoring, digital evidence preservation, incident reporting and escalation, governance and coordination, and staff preparedness and capability. This framework was implemented using a web-based assessment tool built with Node.js, Next.js and Cloudflare Workers. To demonstrate the potential applicability in practice, the tool has been used to calculate the readiness scores for the data used from the Konza Technopolis and to identify readiness gaps and prioritisation of the areas for readiness improvement. The study was limited by its reliance on self-reported perceptions, a single-case cross-

sectional design, purposive sampling and the absence of independent external validation of the framework and tool.

TABLE OF CONTENTS

DECLARATION *1*

DEDICATION *2*

ACKNOWLEDGEMENTS *3*

ABSTRACT *4*

TABLE OF CONTENTS *6*

LIST OF TABLES *9*

LIST OF FIGURES *10*

CHAPTER 1 INTRODUCTION *1*

1.1 Background of the Study **1**

1.2 Statement of the Problem **3**

1.3 Objectives of the Study **4**

1.3.1 General Objective 4

1.3.2 Specific Objectives 4

1.4 Research Questions **5**

1.5 Hypothesis **5**

1.6 Significance of the Study **6**

1.7 Scope of the Study **6**

1.8 Limitations of the Study **7**

CHAPTER 2 LITERATURE REVIEW *8*

2.1 Introduction **8**

2.2 Theoretical Review **8**

2.2.1 Socio – Technical System Theory 8

2.2.2 Technology- organization – Environment (TOE) Framework 9

2.2.3 Digital Forensic Readiness perspective 11

2.3 Empirical Review **12**

2.3.1 Smart City Ecosystems and Digital Infrastructure 12

2.3.2 Cybersecurity in Smart City Environments 13

2.3.3 Digital Forensic Readiness in Smart and Connected Environments 15

2.3.4 Cybersecurity Governance, Incident response, and Policy Environment 16

2.4 Theoretical Framework **19**

2.5 Conceptual Framework **20**

2.6 Research Gap **21**

CHAPTER 3 RESEARCH METHODOLOGY *23*

3.1 Introduction **23**

3.2 Research Philosophy and Design **23**

3.3 Study Area **24**

3.4 Target Population and Sampling Design **25**

3.5 Data Collection Instrument 26
3.6 Data Collection Procedure 27
3.7 Data Preparation and Construction of Study Variables 27
3.8 Validity and Reliability 28
3.9 Data Analysis 29
3.9.1 Descriptive Analysis 29
3.9.2 Correlation Analysis 30
3.9.3 Multiple Linear Regression 30
3.9.4 Regression Diagnostics 30
3.9.5 Qualitative Analysis 31
3.9.6 Framework Development 32
3.10 Analysis by Research Objective 33
3.11 Ethical Considerations 33
CHAPTER 4 DATA ANALYSIS, RESULTS AND DISCUSSION 35
4.1 Introduction 35
4.2 Response Rate 35
4.3 Demographic Characteristics of Respondents 35
4.3.1 Current Role or Designation 36
4.3.2 Functional Area 37
4.3.3 Years of Experience in Current Role 37
4.3.4 Highest Level of Education 38
4.3.5 Level of Involvement in ICT Operations, Cybersecurity or Incident Response 39
4.3.6 Previous Experience in Handling or Reporting Cyber Incidents 39
4.4 Descriptive Statistics 41
4.4.1 Reliability Analysis 41
4.4.2 Descriptive Statistics for Digital Forensic Readiness Components 42
4.4.3 Descriptive Statistics for Technological, Organisational and Environmental Factors 43
4.4.4 Overall Perceived Level of Digital Forensic Readiness 44
4.4.5 Weakest Digital Forensic Readiness Component 45
4.4.6 Priority Areas for Improvement 45
4.5 Diagnostic and Assumption Tests 46
4.5.1 Normality of Residuals 46
4.5.2 Multicollinearity 47
4.5.3 Linearity 47
4.5.4 Homoscedasticity 47
4.6 Findings for Objective 1 49
4.6.1 Logging and Monitoring Practices 49
4.6.2 Digital Evidence Preservation 50
4.6.3 Incident Reporting Procedures 50
4.6.4 Governance and Coordination Arrangements 51
4.6.5 Staff Preparedness for Evidential Handling 52
4.6.6 Technological, Organisational and Environmental Factors 53
4.6.7 Inferential Analysis 56
4.6.8 Measurement Overlap and Sensitivity Analysis 58
4.6.9 Summary of Technological, Organisational and Environmental Findings 59
4.7 Findings for Objective 2 60
4.7.1 Challenges and Readiness Gaps 60

4.7.2 Current Incident Response Process 62
4.7.3 Suggested Improvements to Digital Forensic Readiness 63
4.7.4 Proposed Digital Forensic Readiness Framework 64

4.8 Findings for Objective 3 67
4.8.1 Web-Based Digital Forensic Readiness Assessment Tool 67
4.8.2 Identification of Readiness Gaps and Improvement Priorities 69
4.8.3 Practical Applicability of the Framework 70
4.8.4 Summary of Findings for Objective 3 71

4.9 Discussion of Findings 72
4.9.1 Discussion of Findings for Objective 1 72
4.9.2 Discussion of Findings for Objective 2 75
4.9.3 Discussion of Findings for Objective 3 76

CHAPTER 5 SUMMARY, CONCLUSIONS AND RECOMMENDATIONS 79

5.1 Introduction 79

5.2 Summary of Findings 79
5.2.1 Summary for Objective 1 79
5.2.2 Summary for Objective 2 80
5.2.3 Summary for Objective 3 80

5.3 Conclusions 81

5.4 Recommendations 82
5.4.1 Recommendations for Practice and Policy 82
5.4.2 Recommendations for Further Research 83

5.5 Contribution to Knowledge 84

REFERENCES 85

APPENDICES 88

Appendix A: Research Instruments 88

Appendix B: Introductory Letter 89

Appendix C: Ethical Approval (NACOSTI Permit) 91

Appendix D: Research Timeline and Budget Details 93

Appendix E: Turnitin Similarity Report 94

Appendix F: Supervisor Approval Form 95

LIST OF TABLES

Table 2.1 Theoretical Framework 19
Table 3.1 Analysis by Research Objective 33
Table 4.1Response Rate 35
Table 4.2 : Distribution of Respondents by Functional Area 37
Table 4.3:Distribution of Respondents by Highest Level of Education 38
Table 4.4:Level of Involvement in ICT Operations, Cybersecurity or Incident Response 39
Table 4.5:Reliability Analysis of Study Constructs 41
Table 4.6:Descriptive Statistics for Digital Forensic Readiness Components 43
Table 4.7: Descriptive Statistics for Factors Affecting Digital Forensic Readiness 43
Table 4.8: Normality Test for Regression Residuals 47
Table 4.9: Multicollinearity Test 47
Table 4.10: Linearity Test 47
Table 4.11:Homoscedasticity Test 48
Table 4.12: Independence of Errors Test 48
Table 4.13: Logging and Monitoring Practices 49
Table 4.14: Digital Evidence Preservation Practices 50
Table 4.15: Incident Reporting Procedures 51
Table 4.16: Governance and Coordination Arrangements 51
Table 4.17: Staff Preparedness for Evidential Handling 52
Table 4.18: Technological Factors Affecting Digital Forensic Readiness 53
Table 4.19: Organisational Factors Affecting Digital Forensic Readiness
Table 4.20: Environmental Factors Affecting Digital Forensic Readiness
Table 4.21: Correlation between TOE Factors and Digital Forensic Readiness 56
Table 4.22: Multiple Regression Model Summary 57
Table 4.23: Regression Coefficients for Factors Affecting Digital Forensic Readiness 57
Table 4.24: Summary of Hypothesis Decisions 58

LIST OF FIGURES

Figure 2.1 Conceptual Framework 21
Figure 4.1Respondents by Current Role 36
Figure 4.2:Distribution of Respondents by Years of Experience 38
Figure 4.3:Participation in Handling or Reporting Cyber Incidents 39
Figure 4.4: Formal Training in Cybersecurity, Incident Response or Digital Evidence Handling
Figure 4.5:Overall Perceived Level of Digital Forensic Readiness 44
Figure 4.6: Perceived Weakest Component of Digital Forensic Readiness 45
Figure 4.7: Priority Areas for Improving Digital Forensic Readiness 46
Figure 4.8: Current Incident Response at Konza Technopolis 62
Figure 4.9: Creation of a New Organisational Digital Forensic Readiness Assessment 68
Figure 4.10: Web-Based Digital Forensic Readiness Assessment Interface 69
Figure 4.11: Overview Dashboard of Digital Forensic Readiness at Konza Technopolis 69
Figure 4.12: Digital Forensic Readiness Gap and Priority Analysis 71
Figure 4.13: Web-Based Digital Forensic Readiness Assessment Process **Error! Bookmark not defined.**

ABBREVIATIONS AND ACRONYMS

Acronym	Definition
AI	Artificial Intelligence
DFR	Digital Forensic Readiness
ICT	Information and Communication Technology
IoT	Internet of Things
IS	Information Systems
IT	Information Technology
ITU	International Telecommunication Union
KoTDA	Konza Technopolis Development Authority
KE-CIRT/CC	Kenya Computer Incident Response Team – Coordination Centre
MSc	Master of Science
NACOSTI	National Commission for Science, Technology and Innovation
NIST	National Institute of Standards and Technology
OUK	Open University of Kenya
SIEM	Security Information and Event Management
SPSS	Statistical Package for the Social Sciences
STS	Socio-Technical Systems
TOE	Technology–Organisation–Environment

CHAPTER 1 INTRODUCTION

1.1 Background of the Study

Smart cities have become a global concept that is part of a larger digital transformation plan, which seeks to optimize urban efficiency, sustainability, governance, and quality of life (Carro-Suárez et al., 2023). Smart cities depend on the communication, connectivity, integration and support of digital technologies such as Internet of Things (IoT) devices, cyber physical systems, cloud platforms, data analytics and connected communication networks for various functions, including transport, utilities, public safety, health and administrative services. According to the National Institute of Standards and Technology (NIST), the smart city is driven by the use of Cyber Physical Systems and Internet of Things (IoT) technologies that integrate devices, applications, infrastructure and people in various sectors, which serve to enhance service provision and economic productivity of the city (NIST, 2016).

Along with the growth and complexity of smart city ecosystems, their exposure to cybersecurity threats also increases (Forestiero et al., 2023). The same systems that support real-time data exchange, automation and intelligent decision-making may introduce vulnerabilities through device diversity, weak configuration, inadequate authentication, insecure integration and dependence on cloud-based infrastructure. The National Institute of Standards and Technology has emphasised the need for cybersecurity requirements, guidance and supporting controls throughout the lifecycle of IoT products and the environments in which they operate (Fagan et al., 2026). In a smart city, it is crucial to note that the vulnerabilities have cascading impacts, as disruption to the interdependent digital systems can impact critical services.

In addition to digital forensics readiness, the need for assault prevention also exists in the context of smart cities. Digital forensic readiness is the degree to which an organization or system is prepared to detect, gather, preserve and use digital evidence to support investigations after cyber events (Sibe & Kaunert, 2024). In increasingly networked systems like smart cities, forensic readiness is critical because incidents might involve multiple devices, platforms, actors and data sources scattered across different infrastructure layers. Lack of sufficient documentation, retention, chain-of-custody protocols and governance mechanisms make effective investigation of incidents, determination of cause, support for accountability and reinforcement of future resilience difficult. Recent studies on digital forensic readiness in smart and circular

cities further underlines the growing relevance of forensic preparedness in complex IoT-driven urban ecosystems (Kuku et al., 2025).

In Africa, smart city development is taking place in the broader African continental drive for digital transformation, digital infrastructure growth, innovation and e-governance(Das et al., 2026). The fundamental pillars for socio-economic transformation as identified in the African Union's Digital Transformation Strategy for Africa are digital infrastructure, digital innovation, policy and regulation and digital skills(African Union,2020). At the same time, the region faces major cyber concerns as reliance on digital technology expands. INTERPOL's 2024 African Cyberthreat Assessment Report outlines the size and changing nature of cyber threats across Africa, while the ITU's 2024 Global Cybersecurity Index indicates that many countries have progressed with national cybersecurity strategies, with Africa achieving significant advances in this domain. The changes suggest that the design of Africa's smart city initiatives needs to be innovative and service-efficient but also cyber-resilient and event-ready.

This is the Kenyan experience of a digital plan and cybersecurity need. Kenya has put in place a National Cybersecurity Strategy for 2022–2027 to improve national cyber resilience, governance, cooperation and capacity development. The cyber governance in Kenya is largely shaped by the National KE-CIRT/CC, which leads the country's response to cyber threats and the Computer Misuse and Cybercrimes (Critical Information Infrastructure and Cybercrime Management) Regulations 2024, which offer a more holistic approach to cybercrime governance and critical information infrastructure management. The Communications Authority of Kenya is still recording a high rate of cyber threat incidents, highlighting the importance of cybersecurity readiness in the country's evolving digital landscape.

Konza Technopolis is strategically located in this national setting. Konza Technopolis is an official flagship project of the Government of Kenya under Vision 2030 and is being developed as a scientific park, region of innovation and smart city aimed at putting Kenya as a major technological hub. It is a sustainable city, digitally driven, with state-of-the-art infrastructure, that use ICT to establish an internationally competitive smart city and thriving innovation ecosystem. Konza's ecosystem boasts of sophisticated digital infrastructure including communication networks, cloud services and the Konza National Data Centre, a safe and reliable facility servicing government and enterprise users. As these digital assets grow, the importance of

cybersecurity governance, cyber resilience and digital forensic preparation becomes clearer.

While Konza Technopolis is being touted as Kenya's smart city, there is little to no empirical evidence in the public domain to assess its readiness to handle incident response and digital evidence after the event of a cyber incident. It is a critical gap especially in the Kenyan and African environment as smart city research has been aimed at innovation, infrastructure and digital growth rather than readiness for post-incident investigation and evidential preservation. In this context, this study aims at evaluating the current digital forensic readiness in incident response in Konza Technopolis and presenting a framework for enhancing digital forensic readiness in the emerging smart city ecosystems.

1.2 Statement of the Problem

The smart city technology, which has been developing rapidly, has brought with it a host of interconnected digital systems like Internet of Things (IoT) devices, cloud platforms, sensors and data-driven infrastructure to support urban services and governance. The technologies not only boost efficiency and service delivery but also add multiple points of vulnerability to complex digital ecosystems, thereby increasing the threat landscape in cyberspace. The research has revealed that the cyber risks to smart cities' infrastructures are more severe than the threats of traditional forms of cities due to the large number of connected devices, variety of systems, and frequent exchange of sensitive data on networks (Allam & Jones, 2020; Sicari et al., 2015). The impact of cyber breaches, such as disruption to services, data breaches and compromises to city systems and infrastructure, can be more far-reaching and potentially devastating in cities where they become more connected with technology.

However, existing research indicates that there are still shortfalls in many smart city projects in terms of post-incident investigations and handling of digital evidence, especially in emerging economies. Digital Forensic readiness means the capability of systems or organizations to proactively gather, save and control digital evidence which facilitates the effective investigation of cyber incidents (Rowlingson, 2004) (Rowlingson, 2004; Behl & Behl, 2017).

In smart city environments, such readiness depends not only on technical protection, but also on the existence of logging and monitoring practices, digital evidence preservation mechanisms, incident reporting procedures, governance and coordination

arrangements, and staff preparedness for evidential handling. Where these elements are weak, organisations may struggle to investigate cyber incidents effectively, support accountability, and implement corrective action (Kitchin, 2016; Zhang et al., 2022)..

In Africa, the drive for digital transformation and smart city development has opened up new avenues of opportunity but has also identified inadequacies in the institutional readiness to manage cyber incidents. Although several African countries have made progress in national cybersecurity strategies, the available literature suggests that digital systems often remain vulnerable due to weak institutional coordination, limited technical capacity and underdeveloped mechanisms for post-incident investigation and evidence preservation (African Union Commission & Symantec, 2016; ITU, 2023). Consequently, most of the attention in developing contexts is on prevention and protection, and the forensic preparation for incident response is significantly less.

Empirical data on the status of digital forensic readiness for incident response (IR) is limited in the context of Konza Technopolis, the flagship smart city under the Vision 2030 of the Government of the Republic of Kenya. Although Konza is being developed as a digitally enabled urban ecosystem, it is not yet clear whether the systems and institutional arrangements necessary for logging, evidence preservation, incident reporting, coordination, and staff preparedness are adequately in place. Without such evidence, stakeholders may lack a clear basis for strengthening post-incident investigation capacity and evidential preparedness within the smart city environment. There is therefore a need to assess digital forensic readiness for incident response in Konza Technopolis and to develop a framework for strengthening this capability in smart city ecosystems.

1.3 Objectives of the Study

1.3.1 General Objective

i. To develop a digital forensic readiness framework for incident response in smart city ecosystems, using Konza Technopolis, Kenya as a case study.

1.3.2 Specific Objectives

i. To assess the current state of digital forensic readiness and evaluate the technological, organisational and environmental factors affecting incident response at Konza Technopolis.

ii. To develop a digital forensic readiness framework for strengthening incident response in smart city ecosystems based on the empirical findings from Konza Technopolis.

iii. To evaluate the practical applicability of the developed digital forensic readiness framework in assessing readiness, identifying gaps and prioritising improvements for incident response in smart city ecosystems.

1.4 Research Questions

1. What is the current state of digital forensic readiness at Konza Technopolis, and how do technological, organisational and environmental factors affect incident response readiness?
2. What digital forensic readiness framework can be developed to strengthen incident response in smart city ecosystems based on the empirical findings from Konza Technopolis?
3. To what extent is the developed digital forensic readiness framework practically applicable in assessing readiness, identifying gaps and prioritising improvements for incident response in smart city ecosystems?

1.5 Hypothesis

1. H01: Technological factors do not significantly influence digital forensic readiness for incident response in Konza Technopolis.
2. H02: Organisational factors do not significantly influence digital forensic readiness for incident response in Konza Technopolis.
3. H03: Environmental factors do not significantly influence digital forensic readiness for incident response in Konza Technopolis.
4. Technological, organisational and environmental factors do not jointly have a significant influence on digital forensic readiness for incident response in Konza Technopolis.

1.6 Significance of the Study

This study provided evidence that can support government institutions and policymakers involved in Kenya's smart city and digital transformation agenda. By examining digital forensic readiness within Konza Technopolis, the study identified areas of strength and weakness in relation to incident response, digital evidence handling, governance and organisational preparedness. The results can be beneficial for further enhancement of cybersecurity governance, better preparedness for cyber incidents, and more resilient smart city digital infrastructure.

The study had also significance in the context of Konza Technopolis and technology partners developing and managing smart city services. It showed through the practical examples the lack of preparedness of staff, governance and coordination, incident reporting, evidence preservation and technical integration. The results offer a foundation for enhancing the way incidents are handled and the associated digital evidence management and operational arrangements to facilitate effective forensic investigation. The proposed framework and web-based assessment tool also offer a real-world way to measure readiness, establish priorities for improvement over time, and identify gaps.

Academically, the study adds to the body of evidence related to digital forensic readiness in an African smart city setting, which is very scarce.
It also presented a context dependent framework, which includes technological, organizational and environmental aspects in operational readiness elements for incident response. The study thus contributes to the current knowledge about cybersecurity, digital forensics, and the readiness of smart cities and serves as a benchmark for further research on cybersecurity in digitally enabled environments.

1.7 Scope of the Study

The study focused on digital forensic readiness in the context of incident response in the smart city environment of Konza Technopolis. It covered five key areas of readiness; logging and monitoring, digital evidence preservation, incident reporting and escalation, governance and coordination, and staff preparedness and capability to manage digital evidence.

The case study was Konza Technopolis, while respondents who participated in the research were those involved in ICT operations, cyber security, incident response, governance and related digital infrastructure functions. So the study was geared towards how ready was the organisation to accept, collect, control and use digital evidence if a cyber incident occurred.

In the terms of this research, the plan considers reviewing literature that is related to the study. The concept of this study is to review the literature related to the study in the context of smart city cybersecurity and digital forensic readiness in smart city ecosystems.

1.8 Limitations of the Study

The study relied mainly on respondents' perceptions of digital forensic readiness collected through a structured questionnaire. The findings therefore reflect how participants assessed existing practices and capabilities rather than an independent technical verification of the systems themselves. The study did not directly inspect system logs, evidence repositories, chain-of-custody records or technical configurations to confirm whether the reported practices were consistently implemented in practice. This was particularly relevant given the sensitivity of cybersecurity and incident-response information within the study environment.

The research was also limited to a single case, Konza Technopolis and used purposive sampling to reach respondents with relevant knowledge of ICT, cybersecurity, governance and incident response. Although this ensured that participants had experience relevant to the study, the sample was dominated by ICT-related personnel, which may have given greater weight to technical perspectives than to other organisational functions. In addition, the study was cross-sectional and captured readiness at one point in time. The use of the same questionnaire to measure both digital forensic readiness and the technological, organisational and environmental factors may also have introduced common-method bias and contributed to stronger observed relationships between the variables.

Last but not least, the study designed and implemented the proposed Digital Forensic Readiness Framework using a web-based assessment tool, but it lacked independent testing in other smart city or organization contexts. The practical applicability was demonstrated with the use of Konza Technopolis assessment, but with larger and diverse sample size for other environments and repeated assessments over time, its wider applicability and robustness could be established. Those limitations should not detract from the results and the proposed framework and should be considered as the context in which the results and proposed framework should be interpreted.

CHAPTER 2 LITERATURE REVIEW

2.1 Introduction

The literature review presented in this chapter is the process of assessing and analyzing the literature in the field of cybersecurity and digital forensic readiness in smart city ecosystems. It examines the theoretical perspectives that inform the study, synthesizes empirical studies on cybersecurity, digital forensic readiness, and smart city governance, and highlights the gaps that justify the present research. The chapter also presents the theoretical framework, conceptual framework, and research gap that guide the study.

2.2 Theoretical Review

This section discusses the key theories that underpin the study. The anchor theory for this study is Socio-Technical Systems Theory. The supporting theoretical perspectives discussed in this section are the Technology–Organisation–Environment (TOE) Framework and the Digital Forensic Readiness perspective.

2.2.1 Socio – Technical System Theory

Socio-Technical Systems Theory originated in the 1950s from the work of Eric Trist and Ken Bamforth at the Tavistock Institute in London(Abbas & Michael, 2025). The theory emerged as a response to highly mechanistic approaches to work organisation, particularly the Tayloristic view that technology and people could be treated as separate elements in production systems. Instead, the theory proposed that organisations function best when technology and people are viewed as interdependent parts of one system. Early socio-technical thinking was also influenced by open systems ideas, which emphasized that organisations operate within broader environmental conditions rather than in isolation(Bednar & Welch, 2020).

The theory explains organisational effectiveness as the outcome of interaction between the social subsystem and the technical subsystem, operating within a wider environment. The social subsystem includes people, relationships, roles, values, and organisational structures, while the technical subsystem includes tools, technologies, skills, and work processes. The theory's core principle is joint optimisation, meaning that neither the social nor the technical side should be designed independently of the other. Trist later argued that attempts to optimise either side alone would lead to sub-optimisation of the whole system.

The theory was later applied more directly to information systems research by Bostrom & Heinen (1977) who argued that many information systems failures arise because technical design is separated from organisational and human realities. Their contribution was due to their role in bringing the concept of socio-technical thinking to the study of information systems and showing that the success of the system is dependent more than anything on the extent to which the system matches the organisational structure, work practice and needs of the user, and thus the theory is useful for the examination of complex digital systems.
But the importance does not end here – take a look at all the cybersecurity efforts that have been done recently. For instance, Mahmood et al. (2024) have proposed that Cybersecurity is a complex social, technical, political, economic and environmental subsystem problem, not just technical. Socio-technological Systems Theory can be used in the study because cybersecurity and digital forensic preparedness in Konza Technopolis is a socio-technological problem and hence requires both social and technological solutions. The readiness is part of a smart city, which encompasses not only the pieces of technology (sensors, networks, cloud platform, monitoring tools) but also governance, institutional aspects, people and staff capacity, reporting and proving. Hence, the theory offers an informative framework to look at synergies of technical controls with organizational structures and their impact on the level of cybersecurity and cyber forensic preparedness for the Konza smart city ecosystem. Although Socio-Technical Systems Theory provides a solid basis for understanding the interaction between people, organisational processes and technology, its general nature can make it difficult to use alone when a study requires clearly defined categories for analysis (Baxter & Sommerville, 2011). In this study, the idea helps to demonstrate that factors other than technological infrastructure affect cybersecurity and digital forensic readiness. However, it provides little direction on the structuring and analysis of the specific circumstances affecting preparedness. This implies that theory has to be complemented with theories and frameworks that provide a more explicit analytical structure, particularly with respect to technological, organisational and external issues.

2.2.2 Technology- organization – Environment (TOE) Framework

Tornatzky & Fleischer (1990) created a Technology – Organisation – Environment (TOE) Framework to explain the adoption and implementation of technological innovation in organizations. The concept shows that adoption is influenced by three

interrelated settings namely the technology context, the organizational context and the environmental context. The technological context is about the characteristics and availability of relevant technologies, the organisational context is about internal structures, resources and managerial processes and the environmental context is about external pressures like regulation, institutional demands and the broader operating environment (Baker, 2012).

The power of the TOE Framework is that it allows the structuring of a complex problem into analytically manageable domains. As Baker (2012) explains it is a flexible and generic paradigm, which helps to explain why it has been used across various domains of information systems study. TOE is still being used in more recent studies as it captures internal and external variables that affect technology-related decisions in new digital contexts. Anomah (2025) applied the TOE Framework in his study of institutional readiness and capacity for AI adoption in public audit institutions in developing countries to demonstrate how technological capacity, organisational preparedness, and environmental conditions collectively influence digital adoption in public-sector environments. The continuous use illustrates that the paradigm remains important for study in digital governance and change today, especially in the developing nation contexts.

The framework plays critical role in the present study because the three factors also have an influence on the cybersecurity and digital forensic readiness in Konza Technopolis. Technologically, readiness could depend on having the capability to provide safe systems, surveillance systems, logs of incidents, and digital evidence management. The range of organisational issues that may be considered include governance processes, plans for managing cyber-security, skills of staff, and plans for incident response. The readiness statement is also likely to be shaped by the legal, regulatory and policy landscape of digital infrastructure and smart city operations, from an environmental point of view, in Kenya. The TOE Framework is therefore an important framework to study the impact of these various factors in the Konza smart city ecosystem when it comes to preparing.

While the framework is useful in arranging preparation factors, the paradigm has several limitations. Its greatest strength is its elasticity but this flexibility can also make it hypothetically wide. The TOE Framework has not significantly developed since its first development (Baker, 2012), as researchers choose to adapt the categories of the TOE Framework to their own contexts rather than refine the theory itself. Thus, while

the framework is helpful in categorising preparation criteria, it does not offer a detailed explanation of how these aspects interact in highly specialised situations, such as cybersecurity investigation and digital evidence preparedness. Thus, the TOE Framework is a useful tool in this study to structure the technological, organisational and environmental factors on preparation, but it is better utilized in conjunction with a perspective that more directly addresses digital forensic preparedness.

2.2.3 Digital Forensic Readiness perspective

Digital forensic preparedness is the proactive ability of an organisation to improve its capability to gather, retain and use digital evidence, while at the same time reducing the expense and interruption of an investigation when a cyber incident occurs. This perspective is best shown by Rowlingson (2004) who moved from the reactive digital inquiry to the pre-emptive model of digital investigation in anticipation of its use as evidence. In this respect, forensic preparation is more than the digital forensics of the past; it is about preparedness before an occurrence, such as procedures for logging, evidence retention, procedural control and organisational coordination (Rowlingson, 2004).

This perspective is crucial to this study since cybersecurity in a smart city setting does not stop at preventing or detecting attacks. Accidents can affect many devices, platforms/services, and cause effects in many layers of infrastructure in a complex digital ecosystem like Konza Technopolis. Therefore, the state of digital preparedness is critical to determining whether an organisation is prepared to respond to an incident and to retain digital evidence to be used in an inquiry, for accountability, and for remedial measures. Recent research on forensic readiness in networked systems demonstrates that forensic readiness depends not only on technical capacity but also on management processes, legal issues, standardization and human aspects (Friedl & Pernul, 2024a).

Within this study's theoretical framework, the digital forensic readiness perspective is a supplement to the two previous hypotheses. According to Sociotechnical Systems Theory, preparedness in Konza Technopolis is a function of the interplay between technological systems and the social and organisational systems in which they operate. The TOE Framework is then used to systematically examine these influences by technical, organisational and environmental factors. The digital forensic preparation approach provides a singular aspect, by defining the meaning of preparedness as applied to digital evidence, investigation and post incident accountability. Thus it offers

operational dimension to the forensic component of the study and helps explain the kind of preparation the proposed framework is seeking to strengthen(Rowlingson, 2004).

The approach is pertinent to the study but the key limitation is that it is mostly concerned with evidential preparedness and does not completely explain the larger technological, organisational and environmental circumstances that shape overall readiness in a smart city ecosystem. So it is more beneficial when used together with more general theories explaining system interaction and contextual preparedness. This study does not employ the framework as an independent theory but rather as an additional lens to enhance the examination of digital forensic preparation inside the cybersecurity environment of Konza Technopolis.

2.3 Empirical Review

2.3.1 Smart City Ecosystems and Digital Infrastructure

Smart city ecosystems are generally considered to be urban environments in which digital infrastructure, data systems and interconnected technologies are embedded in the management and provision of city services. In empirical terms, this infrastructure often includes IoT devices, sensor networks, communication systems, cloud platforms, and data-driven applications that support sectors such as transport, energy, health, waste management, and public administration(Sanchez-Gallegos et al., 2025). Recent studies show that these technologies are no longer treated as isolated tools, but as interdependent components of a wider digital ecosystem that supports real-time monitoring, automation, and decision-making in urban environments. Zaman et al. (2024) shows that IoT has become central to the development and management of smart cities, while Salih et al. (2025) similarly observes that IoT technologies now form a foundational layer of smart city infrastructure because of their ability to support continuous data exchange across city functions.

A consistent finding across the literature is that the value of smart city infrastructure lies in its interconnectivity, but this same interconnectivity also increases system complexity. Bhardwaj et al. (2024) through text mining and semantic analysis of global smart city and IoT research, identify infrastructure integration, interoperability, and security as recurring issues in smart city development. Their findings show that smart city ecosystems should be seen as layered digital environments in which devices, platforms and governance systems are continuously interlinked, as opposed to operating separately. This is important because in such environments, digital risks

rarely remain contained in a single system. The common infrastructure and interdependency of services is a likely the source of digital risks.

Empirical studies also show that digital infrastructures in smart cities are not only technical but also depend on various governance and implementation factors. Tan & Taeihagh (2020) conducted an exhaustive study of smart city governance in developing countries and found it to be more than just technology—requiring a series of legal, regulatory, human and institutional reforms to take place simultaneously. In developing countries, the typical constraints on infrastructure goals are related to governance problems, limited implementation capacity and questionable control environments. As it is relevant to new smart city scenarios where the concept may be mature but the operational maturity is still to be reached.

The findings in this study are based on these empirical findings. The concept of Konza Technopolis is a smart city with digital technologies whose operational and utility will rely on the interoperability of its infrastructure, data and smart technologies. The literature suggests that it is important to draw inferences on Konza as a complex digital ecosystem before considering any assessment of readiness, rather than one of individual technologies. This sets the stage for the next paragraph on the specific cybersecurity issues that are present in a smart city.

2.3.2 Cybersecurity in Smart City Environments

With the development of smart cities emphasized on smart infrastructures, including Internet of Things (IoT) devices, sensors, communication grid, cloud platforms, and service-oriented infrastructures including data systems, Cyber Security is recognized as an essential issue in smart city environments. These technologies boost efficiency, automation, and service delivery but also expand the types of potential vulnerabilities available because there are multiple points of exposure in as interdependent a system as these technologies. Under such conditions, the malfunction of one function can result in closure or other consequences to several related functions, which means that the issue of cybersecurity becomes extremely relevant not only in terms of technology but also in governance and resilience (Almeida, 2023).

This is confirmed by Kim et al. (2023). Considering all of the differences in smart cities, the authors found that cybersecurity challenges are tightly associated with system heterogeneity, large-scale connectivity, and using IoT-based infrastructure. Some of the most highly-rated concerns regarding cybersecurity were smart homes, IoT systems and

urban digital services. The 'Internet of Things' network is one of the most influential components of vulnerable smart city environments and is growing in size at an increasing rate. In addition, the difficulties of smart cyber security were identified as factors attributed to that the systems' setups are not safe, access controls are not secure, there's a lack of system standardization, and interfacing systems is fragmented. The results show that cyber threat is also entrenched in the architecture of smart cities' interconnections, and not just a matter of technologies.

The interlinkages to critical key urban systems exacerbate cyber-security issues in smart cities, as demonstrated in the literature. If these smart transport public services are connected to other public services such as the smart surveillance services, which utilize similar technology platforms and digital networks, there would be a cascade of risks according to Demertzi et al. (2023). These results shift the attention from protecting individual subsystems to the more abstract problem of the propagation of cyber risk effects across an interdependent urban infrastructure. In this respect, the security of a smart city relies on the effectiveness of single controls, as well as the security of the larger digital ecosystem.

Further, as described in the literature, governance and institutional coordination also is as important as the technical protection to address a smart city's cybersecurity. The authors of the systematic review on security in smart cities from Laufs et al. (2020), pointed out that in addition to technology-based protections, security in smart city environments is influenced by code of conduct, governing frameworks, and arrangements, characteristics of public safety, and institutional collaboration. Their research highlights that the most frequent areas of vulnerability in cybersecurity are frequently the consequences of having disorganized responsibilities, insufficient monitoring and oversight practices, and the lack of an effective connection between the technical operations and organizational decision making. Therefore, from a smart cities perspective, Cyber Security can be viewed as a technical and governance issue, as its effectiveness relies heavily on the governance model that underpins the institutions for managing, overseeing, and coordinating digital protection.

The smart city cybersecurity programs are focused on prevention rather than a response to an incident. Kim et al. (2023) have noted that while there has been an extensive increase in the number of studies working on the cybersecurity in smart cities, cyber forensics and post incident investigations lag considerably behind. This gap is important because it shows that many smart city systems can be more resilient to attacks

than to the safeguarding of evidence and investigation and giving them more responsibility after it has happened. The empirical research therefore leads to a wider gap between securing smart city infrastructure and guaranteeing readiness to manage the whole lifecycle of cyber incidents.

Technological interdependence of the smart city environment, the exposure of smart city technology and the governance capacity and resilience of connected services are all critical to the cyber security of the smart city environment. They also emphasize the need to understand the connectedness of the elements in smart city systems, and the fact that cybersecurity has to be perceived beyond the limit of what is merely a technical function. As an alternative, it would be better to view this as part of a broader evaluation of ecosystem preparedness, coordination and continuity.

2.3.3 Digital Forensic Readiness in Smart and Connected Environments

The preparedness of digital forensics means the level of capability of an organization to identify, preserve, and use digital evidence in case of a cyber-attack. This idea was fully elaborated by Rowlingson, who argued that an organization must be ready for the evidential implications of any cyber event prior to its occurrence. In this sense, the potential usefulness of evidence in later proceedings is not simply a matter of evidence being retrieved technologically but also of arrangements that have been taken beforehand that will enable it to be used when required, including the logging, retention, documentation and procedural control of evidence (Rowlingson, 2004).

In the smart and connected environments, this risk is more noticeable as the potential evidence is spread across different devices, communication levels and cloud-based services. These environments differ from traditional information systems in that they are characterised by device heterogeneity, constant data flow, and interdependence between digital components. Practically speaking, this means that evidential traces can be fractured, volatile or held in several technical layers, therefore making the post-incident investigation more difficult if the proper preparedness procedures are not already in place.

This change from reactive investigation to advance preparedness is reflected in recent empirical research . In their analysis of IoT forensic readiness, Friedl & Pernul (2024) identify five broad criteria that shape readiness in connected environments, including legal aspects, standardisation approaches, technology resources and procedures, management processes, and human factors. The significance of their analysis is that it

demonstrates that forensic readiness is not merely a technological issue. But it depends on the interplay of technical capability, institutional procedure and organizational capacity. This is especially significant for smart city settings, in which the complexity of interrelated systems demands technological and procedural preparation.

Ariffin & Ahmad (2021) also assessed the indicators of maturity and readiness of digital forensic inquiry in the era of Industry 4.0 from the organisational perspective. The assessment emphasizes on the importance of the chain of custody, the maturity of the procedure, the capability development, and preparedness of the institutions in the current framework to handle digital investigations. The significance of this conclusion is that the readiness of organisations needs to be assessed against the structures, skills and processes they have in place which will make them effective in an inquiry and not whether forensic tools are being made available.

Moreover, the evidential landscape in connected environments is complex, and so are the device-level forensic studies. Eichhorn & Pugliese (2024) examined smart relays and companion IoT applications and found that pertinent forensic artefacts may be recovered from the devices themselves as well as the affiliated mobile applications and vendor cloud servers. They found that a key challenge in securely networking systems is that future evidence is rarely scarce in one place. Rather, it may be scattered across local devices, applications and remote platforms and thus will require previous provisions for identification, access and preservation.

Based on the results, readiness in digital forensic is not just the ability to investigate after the incident in smart and connected environments. It must include forward-looking mechanisms to assure evidence and technical/technological organisational consistency and cooperation. This is very essential in a smart city context such as Konza Technopolis where cyber attacks may impact various services and leave digital footprints on a number of interconnected systems. Therefore, empirical studies validate the necessity of conceptualizing readiness in those contexts as more than the ability to respond to situations but as the capability to preserve/discover digital evidence timely and in a procedurally correct manner.

2.3.4 Cybersecurity Governance, Incident response, and Policy Environment

Cybersecurity of smart city environments is not only about technical solutions but also on governance structures, response mechanisms, and a regulatory framework within which digital systems operate. The effectiveness of cyber security measures in complex urban ecosystems depends on the distribution of tasks, on mechanisms of reporting and

responding to incidents and on existing mechanisms of coordination, supervision, and recovery of action in institutions. Therefore, governance and policies have been the key in the understanding to form and maintain cybersecurity and digital forensic readiness. Technology exposure is not the only factor that poses security issues in smart city contexts; in addition, fragmented institutional systems pose security risks. When studying the security in smart cities, Laufs et al. (2020) identified the governance structures, surveillance techniques, public safety systems and institutional coordination as shaping the security in smart urban environments as much as technical protection.

They discover that the places where their cybersecurity weaknesses are most often found are where responsibilities are spread across multiple areas, the oversight is weak, and technical operations are not aligned with the organisational decision-making. It implies that cybersecurity in smart cities should be treated as an institutional issue, rather than a technical one.

One of the concerns for smart city cybersecurity is the ability to recover after an event. In the study of cybersecurity and cyber forensics in smart cities, Kim et al. (2023) observed that most existing literature focus more on the prevention and protection aspects rather than the post-incident response, cyber forensics, and evidentiary readiness. The imbalance is large because it implies that the smart city systems are more resilient to attacks than they are to investigate attacks, retaining evidence, and holding accountable for attacks after they have happened. Thus, there is a gap between cyber security as protection and cyber security as a more general ability to respond and recover.

The way governance and response are put into practice is affected by legal and regulatory settings. Based on a systematic review of smart city governance in developing countries, Tan & Taeihagh (2020) highlighted that smart city roll out requires more than technology investments; it requires supportive legal, regulatory and institutional changes as well. While their research does not focus exclusively on cybersecurity, the insights gained are applicable to the debate on the need for explicit policy directions, legal powers and institutionalized governance processes to assist institutional arrangements and to assure the functioning of digital systems. This is a proof that the technical preparedness of the field for Cyber security can be enhanced by regulatory guidance provided to the field with regards to accountability, compliance and institutional response.

Examples of the importance of this broader governance environment include Kenya's policy landscape. The National Cybersecurity Strategy 2022-2027 in Kenya seeks to

create national cyber-resilience by focusing on the four pillars of the strategy which are protection of critical information infrastructure, multi-stakeholder co-ordination, incident response and capacity building. The Computer Misuse and Cybercrimes framework and the tools for it, also offer a statutory ground for cyber governance, cyber response, and cyber responsibility. The changes indicate that the readiness of cyber security in the digital environment of Kenyan smart city systems should be viewed as an integral part of organisational practice and the broader regulatory environment in which organisational practice is embedded.

This means that there is a direct relationship between Cybersecurity governance, incident response and policy support with the readiness of the smart city ecosystems. Governance structures define the distribution of responsibility, incident response systems define the action taken on a cyber incident, and policy frameworks provide power and direction for coordinated action. The concerns are critical in Konza Technopolis where the digital infrastructure is expected to serve various services and stakeholders in an integrated urban setting.

2.4 Theoretical Framework

Table 2.1 Theoretical Framework

Theory 1: Socio-Technical Systems Theory *(Bostrom & Heinen, 1977))*	**Theory 2 [TOE Framework]** *(Tornatzky & Fleischer, 1990)*	**Theory 3: Digital Forensic Readiness Perspective** *(Rowlingson, 2004)*
UNDERPINNING THEORIES ***Core Propositions*** ● *Cybersecurity and forensic readiness are shaped by both technical and social-organisational factors.* ● *Readiness is influenced by technological, organisational, and environmental conditions.* ● *Effective preparedness includes prior arrangements for digital evidence preservation and investigation.* ***Application to This Study*** ● *Socio-Technical Systems Theory helps the understanding of Konza as a socio-technical smart city ecosystem.* ● *TOE directs the analysis of readiness elements that influence cybersecurity and digital forensic readiness.* ● *The forensic part of the study and the creation of the proposed framework are informed by the Digital Forensic Readiness approach* ***Theoretical Contribution*** ● *It requires a socio-technical and organisational readiness and forensic preparedness approach in a smart city context of Kenya.* ● *Boosts their joint engagement in cybersecurity and digital forensics preparation activities in Konza Technopolis.*		

2.5 Conceptual Framework

The conceptual framework provides an explanation of how the conditions surrounding Konza Technopolis could impact its digital forensic readiness for incident response. The study is based on the Technology–Organization–Environment (TOE) model and divides the conditions into three categories: technological, organizational and environmental. The study does not consider these as 'readiness outcomes' but rather, as conditions which may impede or assist an organization in being ready and responding to incidents in a forensically appropriate manner. Technologically, readiness is impacted by the greater technical context of all digital systems. This includes system interoperability, interplatform integration, technical resources available and systems set up for investigations. They are in addition to organizational factors, such as management support, use of resources, institutional policies, definitions of roles, and organizational arrangements that support incident response. Further external factors like the requirements of regulation, the national cybersecurity policy, compliance requirements and directives of relevant institutions influence the technological and organizational situation.

These enabling conditions are seen as independent constructs in this study, and digital forensic readiness is seen as the dependent construct in this study. The five operational dimensions of readiness are: logging and monitoring; digital evidence preservation; incident reporting and escalation; governance and coordination; preparedness and capability of staff. These dimensions were used to express readiness in action and are thus conceptually separated from conditions that could affect readiness.

The framework thus provides a visual representation of how technological, organisational and environmental factors are related to digital forensic readiness for incident response. These relationships are illustrated in the study hypotheses, the first one being about technological factors, the second about organisational factors and the third about environmental factors. Results of the empirical relationships were then used to support the creation of the final Digital Forensic Readiness Framework and its practical evaluation using the web-based assessment tool.

Figure 2.1 Conceptual Framework

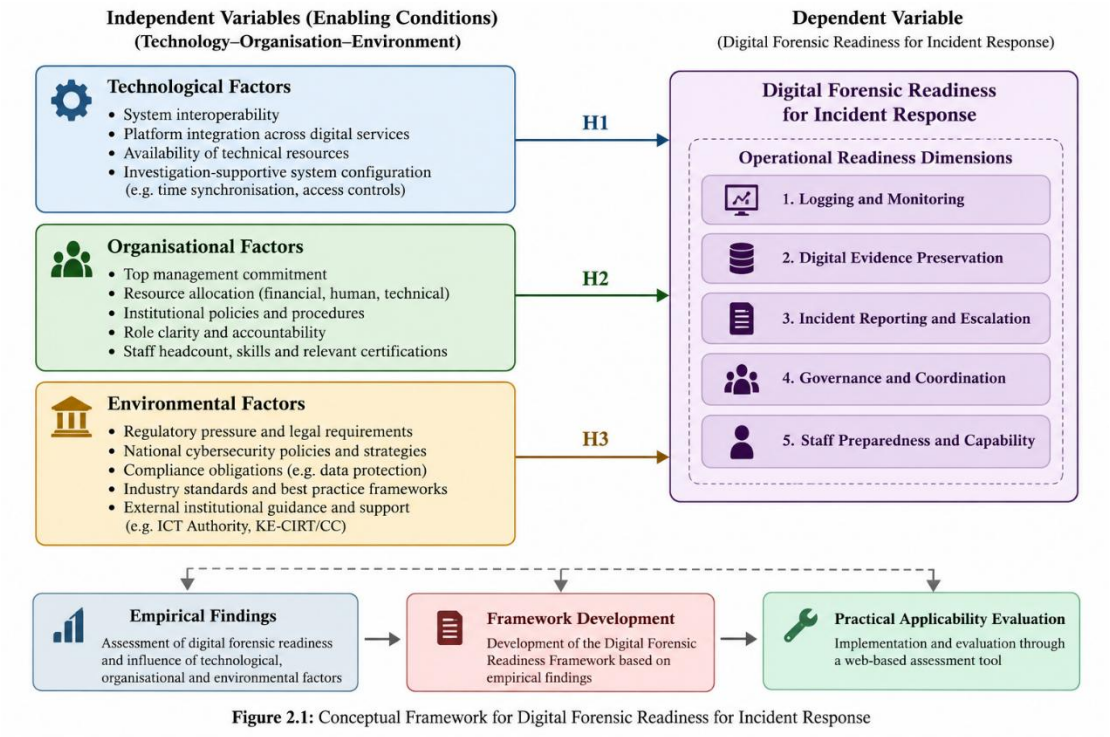


Figure 2.1: Conceptual Framework for Digital Forensic Readiness for Incident Response

2.6 Research Gap

Smart city literature reviewed indicates that cybersecurity is one of the key challenges faced by smart city research in the era of digital interconnected cities. Some existing research has focused on vulnerabilities related to dependence on IoT, infrastructure integration, governance failures, and smart city ecosystem complexity. This research is further supported by the fact that scholarly research is becoming increasingly focused on a digital forensic readiness, especially in connected environments where digital evidence may be spread over various devices, networks, applications, and cloud platforms. These two lines of research have mostly been conducted in isolation so far, however, and there has been very little work done to connect the dots between smart city cyber security and digital forensic readiness for incident response.

A theoretical gap exists in the limited combined application of socio-technical, organisational readiness, and digital forensic perspectives to the study of incident response preparedness in smart city ecosystems. Much of the literature treats cybersecurity, governance, and forensic readiness as separate issues, yet the present study argues that they are closely interconnected within complex smart city environments.

An empirical gap is also evident. Although there is growing international literature on smart city cybersecurity, there remains limited empirical evidence on digital forensic

readiness for incident response within emerging smart city environments in Sub-Saharan Africa. In Kenya, available evidence is stronger at the level of national cyber policy, cyber threat reporting, and digital transformation than at the level of operational readiness within specific smart city systems. In particular, there is limited empirical evidence on whether Konza Technopolis is adequately prepared in relation to logging and monitoring, digital evidence preservation, incident reporting procedures, governance and coordination, and staff preparedness for evidential handling after cyber incidents.

A methodological gap can further be identified in that many existing studies rely on conceptual reviews, threat mapping, or broad discussions of smart city security, with relatively less emphasis on structured readiness assessment within a specific smart city case. This severely limits the context knowledge and comprehension of the effect of technological, organizational and environmental factors on the digital forensic readiness to respond to incidents in reality.

This study aims to close these gaps and to evaluate the current readiness of digital forensics tools in incident response in Konza Technopolis and to formulate a context-specific framework to enhance the capability of digital forensics tools in smart city environment.

CHAPTER 3 RESEARCH METHODOLOGY

3.1 Introduction

This chapter presents the methodology used to investigate digital forensic readiness for incident response within Konza Technopolis. It describes the research philosophy and design, study area, target population and sampling procedure, data collection instrument and procedure, data preparation and management, validity and reliability procedures, and the quantitative and qualitative techniques used to analyse the data. The chapter also provides the explanation about the incorporation of the outcomes of various analytical phases with each other to support the development of the digital forensic readiness framework.

3.2 Research Philosophy and Design

This study adopted a post-positivist research paradigm. This was fitting as the research aimed to determine the state of digital forensic readiness through quantitative measures and employing statistics that also accounted for the readiness of an organisation's practices and governance arrangements and staff experiences, which were not fully quantified. Post-positivism was thus appropriate for the integration of empirical measurement and contextual interpretation (Creswell & Creswell, 2018). The empirical part of the study was based on an embedded mixed-methods case study design, following from this philosophical standpoint. In the context of a smart city, the study focused on one case in Konza Technopolis, where the scope of digital forensic readiness in the context of a smart city is well-defined in terms of the context of the organisation, namely the processes of cybersecurity, governance, infrastructure and incident-response. The case study design therefore allowed the phenomenon to be examined within its real-world setting (Yin, 2018).

The quantitative strand was used as a major component of the study and was used to examine the five dimensions of digital forensic readiness, as well as the impact of technological, organisational and environmental factors. The qualitative strand was included in the same questionnaire with open-ended questions to elicit more information about readiness gaps, incident-response practices, and areas for improvement. This resulted in a quantitative design, where qualitative evidence was used as a supportive part of the design (Creswell & Plano Clark, 2018).

Two strands were woven together as they were interpreting and developing the framework. The main strengths, weaknesses and statistical relationships were identified via quantitative findings, while the open-ended responses helped explain the operational challenges behind those findings. The combined evidence was then synthesised to identify the practical requirements that informed the Digital Forensic Readiness Framework.

The framework-development stage was informed by Design Science Research principles, which emphasise the development and evaluation of practical artefacts that address identified organisational problems (Hevner et al., 2004; Peffers et al., 2007). The empirical research results guided the framework structure, which was then transformed to an assessment tool on the web.

This web-based tool was used to assess the framework's practicality by exploring whether it could measure the readiness dimensions outlined in the framework and calculate overall and dimension-level scores, and by identifying areas of weakness and pointing to areas that could be targeted for improvement. This gave a preliminary evaluation of the practical use and further validation across other organisations and smart city environments was set as an area for further study.

3.3 Study Area

The study was carried out at Konza Technopolis in Kenya, a smart city being built with the use of communication networks, cloud services and Konza National Data Centre. These systems generate and share a great deal of digital information in interconnected systems, which brings with it the challenge of cybersecurity and digital evidence in incident response.

Konza is a smart city ecosystem but the functions of institutions studied were those associated with operations of ICTs, cybersecurity, digital infrastructure and incident response and governance. The sampling frame was thus not all actors in the external ecosystem (e.g., vendors, tenants, utility providers or public institutions) involved in these functions but only those who had first-hand experience of them. Konza offered an adequate environment to discuss the effects of technological, organizational and environmental conditions on digital forensic readiness in a new smart city environment. The results, however, should be analyzed at the institutional level represented by the respondents, and not at the level of the broader Konza smart city ecosystem.

3.4 Target Population and Sampling Design

The target population consisted of about 200 staff members that are important in the planning, management, operation, security and governance of digital systems in Konza Technopolis. This comprised ICT officers, system administrators, cybersecurity and incident response officers, managers and supervisors, governance personnel, and those who work with digital infrastructure and functions. The number of personnel which were relevant to the institutional functions included in the study were taken as the population estimate.

Purposive sampling was used to identify respondents with knowledge or experience relevant to cybersecurity, digital systems, governance, incident response or digital infrastructure. So, eligibility was determined by the relevance of the role of a respondent rather than by random selection from the larger population. No stratification by role was applied because the study sought informed responses from personnel with relevant institutional knowledge rather than proportional representation of occupational groups. As a result, the sample was not intended to support statistical generalisation to all actors within the wider Konza smart city ecosystem (Saunders et al., 2019).

With an estimated population of 200 and a 5% precision level, the computation was:

$$n = N / [1 + N(e^2)] \quad (3.1)$$

Where n represents the required sample size, N represents the target population and e represents the acceptable margin of error.

Using an estimated population of 200 and a 5% precision level, the computation was:

$$n = \frac{200}{1 + 200(0.05^2)} = \frac{200}{1 + 200(0.0025)} = \frac{200}{1.5} = 133.3 (3.2)$$

The sample size for the target population was thus rounded up to 133 respondents. This calculation was used to determine how many samples were to be collected and not as a basis for sampling with probabilities. A total of 109 respondents completed the questionnaire, or 82.0% of the 133 individuals targeted.

Eligibility is extended beyond direct involvement in operational ICT, cybersecurity or incident response. It also featured respondents who work in governance, management, and related digital infrastructure functions where their roles provided relevant knowledge of the institutional environment. This explains why three respondents who reported no direct involvement in ICT operations, cybersecurity or incident response were retained

in the analysis. The majority of respondents, however, had at least some level of involvement in these operational areas.

3.5 Data Collection Instrument

Structured questionnaire was used to gather primary data. The instrument was selected because it allowed comparable information to be collected across the main dimensions of digital forensic readiness and provided data suitable for both descriptive and inferential analysis (Saunders et al., 2019). Timothy Kosgei 2026 Thesis

The questionnaire consisted mainly of closed-ended statements measured on a five-point Likert scale ranging from 1 = Strongly Disagree to 5 = Strongly Agree. The items assessed five aspects of digital forensic readiness: logging and monitoring; digital evidence preservation; incident reporting and escalation; governance and coordination; and staff preparedness and capability. Other items captured technological, organisational and environmental factors developed based on the Technology–Organisation–Environment paradigm. Open-ended questions were also used to elicit the opinions of respondents regarding the gaps in readiness, practices in incident response and areas for improvement.

The questionnaire item was created based on the study goals, the theoretical framework and the literature studies on the digital forensic readiness reviewed in Chapter Two. This allowed for the instrument to be anchored to the primary constructs studied and to keep a connection between the research questions, variables and measures so examined.This questionnaire was conducted in English using Google Forms to the eligible respondents in Konza Technopolis. The coded responses to the closed-ended items were submitted to statistical analysis and the open-ended items were left in the text for thematic analysis.

3.6 Data Collection Procedure

The eligible respondents comprising the personnel involved in activities of ICT, cybersecurity, governance, digital infrastructure and incident response within Konza Technopolis were interviewed during the month of September 2026. The questionnaire was sent via Google forms. Before completing the questionnaire, participants were informed about the purpose of the study, the voluntary nature of participation and the confidentiality of their responses. Respondents were elected based on the relevance of their role to the study areas, namely in ICT operations, cybersecurity, governance, digital infrastructure and incident response. The questionnaire link was sent to employees involved in these positions and follow-up reminders were sent throughout the data collection period to encourage employees to complete the questionnaire.

After the data was collected, 109 responses were kept for analysis at the end of the data collection period. The five-point Likert Scale was used to code closed-ended items, and responses to open-ended items were kept in textual form and analysed thematically. Data was then screened for completeness, appropriate response range, consistency and for any duplicate entries prior to statistical analysis.

3.7 Data Preparation and Construction of Study Variables

Data collected was cleaned prior to analysis. Responses were checked for missing data, incorrect responses, duplicate responses, and inconsistencies. Likert-scale responses were coded numerically from 1 to 5. Values not within the range of acceptable answer were not inserted with estimated values, but were considered missing. Only those observations that met the criteria for the variable(s) needed for each procedure were used in the analyses.

Multiple questionnaire statements were used to measure the major study constructs, which resulted in composite scores. For a construct consisting of k items, the composite score for respondent i was calculated as:

$$C_i = (\Sigma_{j=1}^{k} X_{ij}) / k \quad (3.3)$$

where C_i is the composite score for respondent i, X_{ij} is the respondent's rating on item j, and k is the number of valid items included in the construct.

Composite scores were generated for Logging and Monitoring, Digital Evidence Preservation, Incident Reporting and Escalation, Governance and Coordination, Staff Preparedness and Capability, Technological Factors, Organisational Factors and Environmental Factors. Constructing composite measures was appropriate because

each of these concepts was measured by a number of related questionnaire items, therefore they were each being measured as an underlying dimension.

The overall Digital Forensic Readiness score was constructed from the five operational readiness dimensions as:

$$DFR = (LM + DEP + IR + GC + SP) / 5 \quad (3.4)$$

where LM represents Logging and Monitoring, DEP represents Digital Evidence Preservation, IR represents Incident Reporting and Escalation, GC represents Governance and Coordination, and SP represents Staff Preparedness and Capability.

3.8 Validity and Reliability

The questionnaire items were developed from the study objectives, theoretical framework and constructs identified in the literature. This helped maintain a clear connection between the concepts examined in the study and the questions used to measure them. The five digital forensic readiness dimensions and the technological, organisational and environmental factors were each represented by several related items rather than by single questions. However, no formal content-validity index or pilot-based expert assessment was undertaken; therefore, validity was considered primarily in terms of theoretical and conceptual alignment.

Internal consistency was assessed using Cronbach's alpha because each study construct was measured using multiple Likert-scale items intended to represent the same underlying concept (Field, 2018). The coefficient was calculated as:

$$\alpha = [k / (k - 1)] [1 - (\Sigma\sigma_i^2 / \sigma_t^2)] \quad (3.5)$$

where k represents the number of items in the scale, σ_i^2 represents the variance of an individual item and σ_t^2 represents the variance of the total scale score. A Cronbach's alpha coefficient of approximately 0.70 or above was considered acceptable for internal consistency.

Because the study measured several closely related constructs, particular attention was also given to the distinction between the independent factors and the digital forensic readiness dimensions. Cronbach's alpha was used to assess consistency within each construct, but it does not by itself demonstrate that the constructs are empirically distinct. This issue was therefore considered when interpreting the correlation and regression findings, especially where strong relationships were observed between the predictor and outcome variables

3.9 Data Analysis

Quantitative data were analysed mainly using IBM SPSS Statistics. SPSS was used for data management, descriptive statistics, reliability analysis, Pearson correlation, multiple linear regression and the associated regression diagnostics (Field, 2018).

The questionnaire items were measured on a five-point Likert scale and were therefore ordinal at the individual-item level. Item-level means were used to describe response patterns, while the main inferential analyses were based on multi-item composite scores representing the study constructs. Each of these composite measures was judged acceptable, as they were based on a number of related items, and the internal consistency of each item was checked before further analysis.

The data from the open-ended items of the questionnaire was analysed qualitatively, thematically, in NVivo. The analysis was concentrated on recurrent patterns in terms of gaps in readiness, incident-response practices and proposed improvements. The qualitative findings have been used as a context to the quantitative results, and have informed the practical needs of the Digital Forensic Readiness Framework.

3.9.1 Descriptive Analysis

Descriptive statistics were applied mainly for the first research objective of examining the current state of the digital forensic readiness. Categorical data was summarised using frequencies and percentages, and Likert scale responses and composite readiness variables were summarised using means and standard deviations.

The following percentage distribution calculations were made:

$$P = (f / N) \times 100 \quad (3.6)$$

where P is the percentage, f is the frequency within a category and N is the total number of valid responses.

The arithmetic mean was calculated as:

$$\bar{x} = (\Sigma_{i=1}^{n} x_i) / n \quad (3.7)$$

while the standard deviation was calculated as:

$$s = \sqrt{[\Sigma_{i=1}^{n}(x_i - \bar{x})^2 / (n - 1)]} \quad (3.8)$$

These statistics were appropriate because they enabled the study to describe both the central tendency and variation in respondents' assessments of the different readiness dimensions.

3.9.2 Correlation Analysis

Pearson's product-moment correlation coefficient was used to examine the strength and direction of the bivariate relationship between Technological Factors, Organisational Factors, Environmental Factors and Digital Forensic Readiness.

The coefficient was expressed as:

$$r = \Sigma[(x_i - \bar{x})(y_i - \bar{y})] / \sqrt{\{\Sigma(x_i - \bar{x})^2 \, \Sigma(y_i - \bar{y})^2\}} \quad (3.9)$$

Pearson correlation was appropriate because the analysis involved continuous composite measures and sought to determine whether changes in each TOE dimension were associated with corresponding changes in Digital Forensic Readiness. Statistical significance was evaluated at the 5% level (Field, 2018).

3.9.3 Multiple Linear Regression

Multiple linear regression was used to assess the simultaneous influence of technological, organisational and environmental factors on Digital Forensic Readiness. The method was appropriate because the study examined one continuous dependent variable in relation to several predictor variables and sought to estimate the independent contribution of each predictor while holding the others constant (Field, 2018; Tabachnick & Fidell, 2019).

The regression model was specified as:

$$DFR_i = \beta_0 + \beta_1 TECH_i + \beta_2 ORG_i + \beta_3 ENV_i + \varepsilon_i \quad (3.10)$$

where DFR_i represents Digital Forensic Readiness, $TECH_i$ represents Technological Factors, ORG_i represents Organisational Factors, ENV_i represents Environmental Factors, β_0 is the regression constant, β_1 to β_3 are the regression coefficients, and ε_i represents the error term.

The coefficient of determination, R^2, was used to estimate the proportion of variation in Digital Forensic Readiness explained collectively by the predictors:

$$R^2 = 1 - (SSResidual / SSTotal) \quad (3.11)$$

The overall model was evaluated using the F-test, while the statistical significance of individual predictor coefficients was assessed using t-tests. Hypothesis decisions were made at a significance level of $\alpha = 0.05$.

3.9.4 Regression Diagnostics

Diagnostic tests were undertaken before interpreting the regression model to assess whether the underlying assumptions were adequately satisfied. Normality of residuals was examined using the Shapiro-Wilk test, while multicollinearity among predictors

was assessed using tolerance and the Variance Inflation Factor (Field, 2018; Tabachnick & Fidell, 2019).

The Variance Inflation Factor was calculated as:

$$VIF_j = 1 / (1 - R_j^2) \quad (3.12)$$

with tolerance calculated as:

$$Tolerance_j = 1 - R_j^2 \quad (3.13)$$

Homoscedasticity was examined using the Breusch-Pagan test, while independence of residuals was assessed using the Durbin-Watson statistic:

$$DW = \Sigma_{t=2}^{n}(e_t - e_{t-1})^2 / \Sigma_{t=1}^{n} e_t^2 \quad (3.14)$$

Model specification was additionally examined using the Ramsey RESET test. These diagnostic procedures were applied to support the validity of the regression estimates before hypothesis testing.

3.9.5 Qualitative Analysis

Open-ended questionnaire responses were analysed using thematic analysis following the general approach outlined by Braun and Clarke (2006). The analysis focused on respondents' views of readiness gaps, operational challenges, incident-response practices and suggested improvements. This was appropriate as it enabled the same ideas to be recognised in multiple responses and grouped together in coherent themes.

The researcher, first, read the responses to familiarize herself with the data and then gave first impressions of codes to common themes or problems. Individual codes were aggregated into larger categories and then developed into themes which illustrated patterns of relevance to the study goals. A codebook was kept to document the codes, definitions of the codes and the themes to which they were linked. The themes were checked to see if they matched with themes of the original responses.

The qualitative findings were summarised using theme frequencies and verbatim quotations to increase the transparency. These findings were then compared with the quantitative results to provide additional explanation of the observed readiness gaps and to identify practical requirements that informed the development of the Digital Forensic Readiness Framework.

3.9.6 Framework Development

The Digital Forensic Readiness Framework was developed from the empirical findings of the study together with the theoretical perspectives that guided the research. The process started with the main readiness strengths, weaknesses and influencing factors identified from the quantitative analysis and then the findings were compared with the findings from the qualitative analysis of operational challenges, incident-response practices and suggested improvements. The results of these findings were translated into framework requirements and were correlated with each other and with the components in a traceability matrix. The information on weaknesses of staff preparedness informed the staff capability component, gaps in evidence handling informed the digital evidence preservation component, and the findings on technological, organisational and environmental informed the enabling conditions of the framework.

This framework combined three enabling domains (technological, organisational and environmental factors), and five operational readiness areas (logging and monitoring, digital evidence preservation, incident reporting and escalation, governance and coordination, staff preparedness and capability). These components were integrated with the incident-response lifecycle and a continuous improvement process that involved assessment, gap identification, prioritisation and reassessment.

To implement the framework, a web-based digital forensic readiness assessment tool, built with Next.js and Node.js, was created. These technologies were chosen due to their ability to help create a modern, responsive web application that includes interface and server-side functionality. The app translated the framework into structured assessment items and automated dimension-level and overall readiness scores. The application was deployed using Cloudflare Workers and stored in the Cloudflare environment, enabling the tool to be accessible without the need for a dedicated on-premises server while providing a lightweight and scalable solution.

The practical applicability of the framework was then examined through the implemented tool using the Konza Technopolis assessment data. The framework was evaluated to see if it was a measurable readiness to be translated.

3.10 Analysis by Research Objective

Table 3.1 summarises the analytical approach used for each research objective and shows the relationship between the study variables, analytical methods and tools.

Table 3.1 Analysis by Research Objective

Research Objective	Variables / Evidence	Analysis Method	Tool
1. Assess the current state of digital forensic readiness	Logging and Monitoring; Digital Evidence Preservation; Incident Reporting and Escalation; Governance and Coordination; Staff Preparedness	Frequencies, percentages, means, standard deviations, composite scores and thematic analysis	IBM SPSS Statistics and thematic analysis
2. Evaluate technological, organisational and environmental factors affecting readiness	Technological Factors, Organisational Factors, Environmental Factors and Digital Forensic Readiness	Pearson correlation, multiple linear regression, hypothesis testing and regression diagnostics	IBM SPSS Statistics
3. Develop a digital forensic readiness framework	Quantitative findings, qualitative themes, readiness gaps, incident-response processes and theoretical constructs	Integration and synthesis of empirical and theoretical findings	Framework development and web-based implementation

3.11 Ethical Considerations

Ethical principles were observed throughout the study. Participation was voluntary, and respondents were informed about the purpose of the research before completing the questionnaire. Informed consent was obtained from all participants, and respondents were advised that the information collected would be used for academic purposes. The study was undertaken after obtaining the required institutional and regulatory approvals, including the OUK ethics clearance, NACOSTI research licence and authorisation from the Konza Technopolis Development Authority (KoTDA). The relevant approvals were included as appendices.

Throughout data collection, analysis and reporting confidentiality and anonymity were maintained. The study did not require respondents to provide personally identifying information, and access to the research data was restricted to the researcher. Data were handled in accordance with the Data Protection Act, 2019, particularly the principles of purpose limitation, data minimisation, confidentiality and secure handling of personal

information. Because of the limited number of respondents in some functional groups, findings were generally presented in summary form, and detailed cross tabulations were not included that might have allowed identification of the individuals in their role.

Extra effort was made to present the results of the organisation through web-based Digital Forensic Readiness assessment tool. For an organisation as a whole the tool showed readiness scores and organisational responses aggregated together but not individual responses. No respondent-level information or identifiable personal data were presented through the dashboard. When the Konza Technopolis name was applied in the study to illustrate the assessment findings, only a summarized and summarized version of the findings already presented in the study was displayed, thus minimizing the possibility of revealing sensitive operational or individual information.

CHAPTER 4 DATA ANALYSIS, RESULTS AND DISCUSSION

4.1 Introduction

This chapter presents the analysis, results and discussion of the data collected on digital forensic readiness for incident response within Konza Technopolis. It presents the response rate and respondent characteristics, descriptive statistics for the study variables, diagnostic tests, findings according to the three research objectives, and hypothesis testing using correlation and multiple regression analysis. The chapter concludes with a discussion of the findings in relation to the study objectives, theoretical framework and existing empirical literature.

4.2 Response Rate

The study targeted 133 respondents from an estimated population of approximately 200 personnel involved in ICT operations, cybersecurity, incident response, governance and related functions within Konza Technopolis. A total of 109 completed questionnaires were received and retained for analysis, giving a response rate of 82.0% based on the targeted sample. The remaining 24 targeted participants did not respond, representing 18.0%.as shown in Table 4.1.

Table 4.1Response Rate

Response Category	**Frequency**	**Percentage (%)**
Completed questionnaires	109	82.0
Non-response	24	18.0
Total targeted sample	133	100.0

The 82.0% response rate therefore relates to the 133 respondents who were targeted for participation and not to the entire estimated population. Relative to the estimated population of 200 personnel, the 109 completed responses represented 54.5%.

Although the achieved response provided sufficient data for the analyses undertaken in the study, the characteristics of the 24 non-respondents were not available. It was therefore not possible to establish whether non-response was concentrated within particular specialist or functional groups. This creates a possibility of non-response bias and is taken into account when interpreting the findings.

4.3 Demographic Characteristics of Respondents

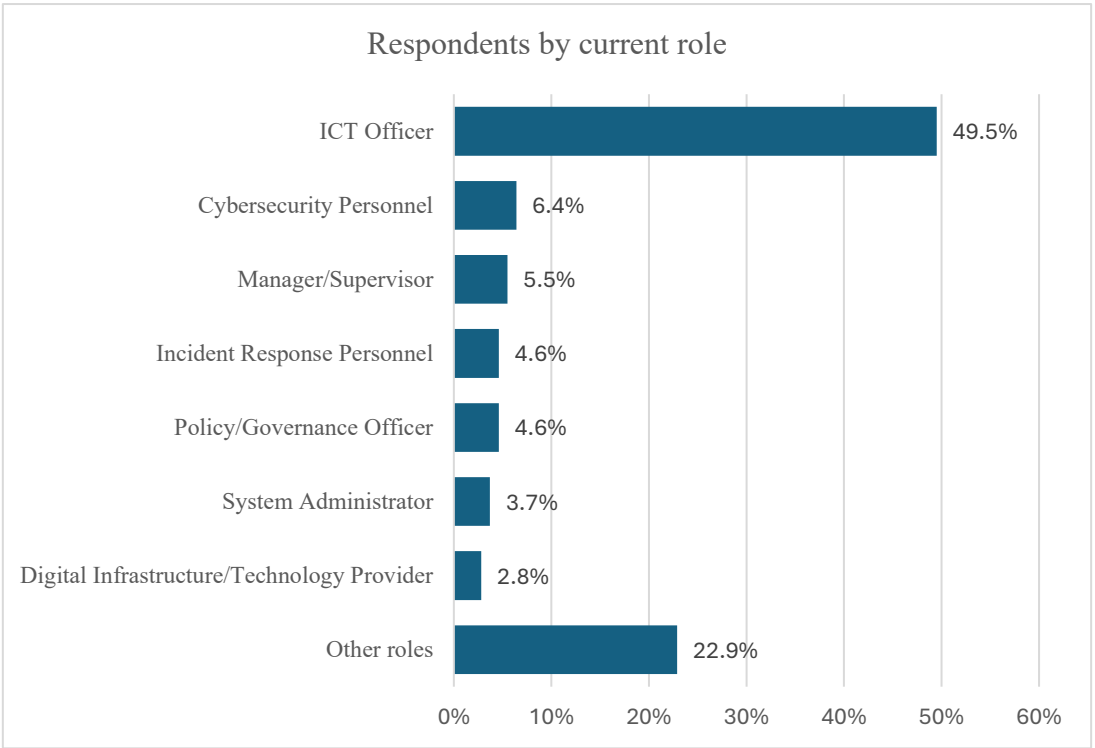
The demographic information of the respondents was analyzed to help to interpret the findings of the study. The analysis considered respondents' current role, years of

experience in their current role, highest level of education, level of involvement in ICT operations, cybersecurity or incident response, previous participation in handling or reporting cyber incidents, and formal training in relevant areas.

4.3.1 Current Role or Designation

Respondents came from a range of technical, managerial, governance and operational roles within Konza Technopolis. The largest group were the ICT Officers, which accounted for 54 respondents (49.5%). This was followed by cybersecurity personnel at 7 (6.4%), managers or supervisors at 6 (5.5%), incident response personnel at 5 (4.6%), policy or governance officers at 5 (4.6%), system administrators at 4 (3.7%), and digital infrastructure or technology providers at 3 (2.8%). Twenty-five others (22.9%) were in a variety of other technical, engineering, administrative and operational positions.

Figure 4.1Respondents by Current Role



The distribution indicates that the achieved sample was skewed towards general ICT roles while respondents with specific designations in cybersecurity or incident response were a smaller proportion. It is important to consider this when analysing the readiness results, as most of the readiness assessments include the opinion of employees involved in the digital environment, but not necessarily in incident response or related to digital evidence.

Respondents from governance, infrastructure, management and other operational functions are included at the same time, highlighting the broader organisational context and the implementation of digital forensic readiness.

4.3.2 Functional Area

RThe respondents were selected from different functional areas of Konza Technopolis. ICT accounted for the largest proportion, with 51 respondents (46.8%), followed by Infrastructure/Technical Services with 17 (15.6%) and Operations with 11 (10.1%). Ten respondents (9.2%) were from Cybersecurity, six (5.5%) were from Governance/Management and four (3.7%) were from Incident Response. The other 10 respondents (9.2%) were from other functional areas.

Table 4.2 : Distribution of Respondents by Functional Area

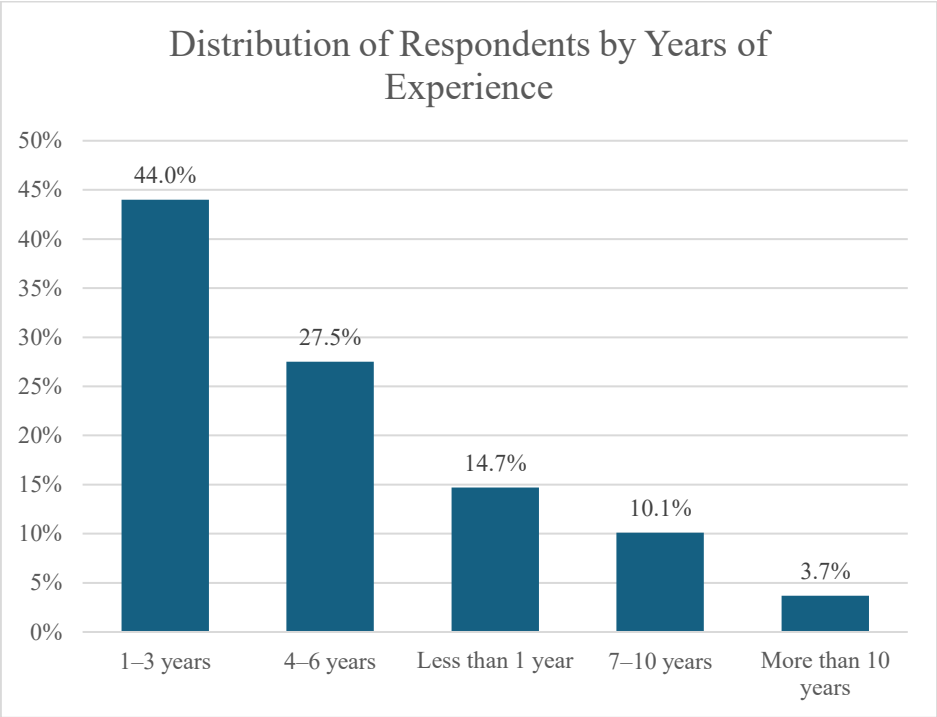
Functional Area	Frequency	Percentage (%)
ICT	51	46.8
Infrastructure/Technical Services	17	15.6
Operations	11	10.1
Cybersecurity	10	9.2
Governance/Management	6	5.5
Incident Response	4	3.7
Other functional areas	10	9.2
Total	**109**	**100.0**

As seen in the distribution, ICT and technical roles were the most prevalent with a larger percentage of people in these roles, followed by cybersecurity and incident response. This is relevant to the findings as many of the readiness assessments are a reflection of the wider organisational and technical landscape and not the opinion of specialist incident-response personnel alone.

4.3.3 Years of Experience in Current Role

Most respondents (71.5%) had between one and six years of experience in their current roles, while 14.7% had less than one year and 13.8% had more than six years, as shown in Figure 4.2

Figure 4.2:Distribution of Respondents by Years of Experience



This indicates that most respondents had sufficient exposure to their current organisational roles and operating environments to provide informed views on cybersecurity, incident response and digital forensic readiness practices within Konza Technopolis.

4.3.4 Highest Level of Education

Most respondents had attained university-level education. Bachelor's degree holders formed the largest group, with 75 respondents (68.8%), followed by 21 respondents (19.3%) who held a master's degree. A further 12 respondents (11.0%) had diploma-level qualifications, while one respondent (0.9%) reported a certificate as their highest level of education.

Table 4.3:Distribution of Respondents by Highest Level of Education

Education Level	**Frequency**	**Percentage (%)**
Certificate	1	0.9
Diploma	12	11.0
Bachelor's Degree	75	68.8
Master's Degree	21	19.3
Total	109	100.0

Overall, the distribution reflected that the respondents were quite well educated, with 88.1% having either a bachelor's or a master's degree. This suggests that most participants had the educational background needed to understand the technical, organisational and governance issues addressed in the study.

4.3.5 Level of Involvement in ICT Operations, Cybersecurity or Incident Response

The level of involvement in ICT operations, cybersecurity or incident response is presented in Table 4.4.

Table 4.4: Level of Involvement in ICT Operations, Cybersecurity or Incident Response

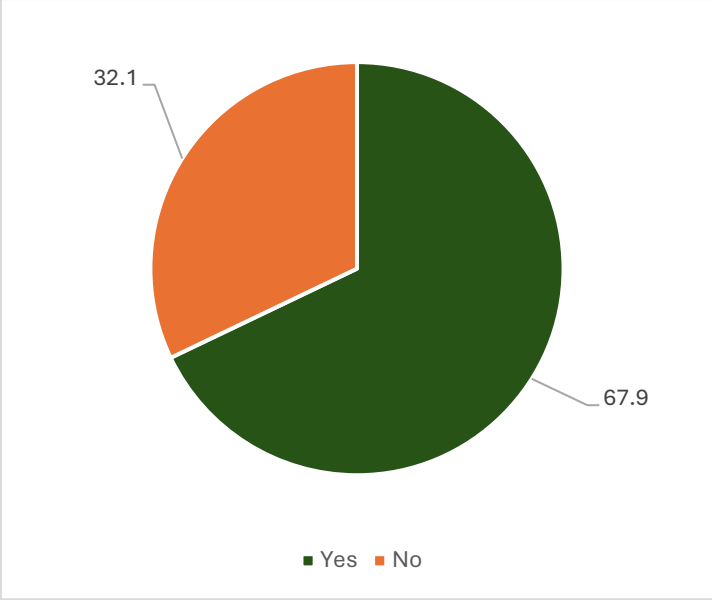
Level of Involvement	**Frequency**	**Percentage (%)**
No involvement	3	2.8
Limited to moderate involvement	53	48.6
High to very high involvement	53	48.6
Total	**109**	**100.0**

The findings show that almost all participants had some level of involvement in the relevant operational areas. 48.6% had limited to moderate involvement and another 48.6% had high to very high involvement. Only 2.8% had no involvement, indicating that the study largely captured perspectives from individuals with relevant exposure to ICT operations, cybersecurity or incident response.

4.3.6 Previous Experience in Handling or Reporting Cyber Incidents

The findings in Figure 4.3 show that 67.9% of the respondents had previous experience in handling or reporting cyber incidents, while 32.1% had no such experience.

Figure 4.3:Participation in Handling or Reporting Cyber Incidents



This implies that most of the respondents were practically exposed to the cyber incident management, which further enhanced the relevance of their thoughts on incident response processes and digital forensic readiness within Konza Technopolis.

4.3.7 Formal Training in Relevant Areas

The majority of respondents responded that they had some formal training in cybersecurity, incident response or digital evidence handling. Of the 109 respondents, 92 (84.4%) answered "Yes", while 17 (15.6%) indicated that they had not received such training.

Table 4.5: Formal Training in Cybersecurity, Incident Response or Digital Evidence Handling

Response	**Frequency**	**Percentage (%)**
Yes	92	84.4
No	17	15.6
Total	109	100.0

Among the 92 respondents who reported having received formal training, cybersecurity was the most common area, reported by 44 respondents, followed by incident response with 22 and ICT governance with 20. Only a few respondents reported having received some training in digital forensics (reported by three respondents) or evidence handling and chain of custody (two respondents), and one respondent reported training in both cybersecurity and ICT governance. This reveals a generally high level of exposure to

formal training, but largely in the general field of cybersecurity and governance, and not so much on the more specialised aspects of digital forensics and evidence handling.

4.4 Descriptive Statistics

The descriptive statistics were used for the summarization of the main study variables and for an overall picture on the digital forensic readiness in Konza Technopolis. The analysis focused on the reliability of the measurement scales, the five dimensions of digital forensic readiness, the technological, organisational and environmental factors, the overall perceived level of readiness and the areas considered weakest or most in need of improvement.

4.4.1 Reliability Analysis

Reliability analysis was conducted to assess the internal consistency of the items used to measure the study constructs. The five constructs of digital forensic readiness were: logging and monitoring, preserving digital evidence, reporting of incidents, governance and coordination, and staff preparedness. There were six items in each of these constructs. Technological, organisational and environmental constructs were each comprised of eight items.

The Cronbach's alpha values obtained in the study were between the range of 0.922 and 0.959 as presented in Table 4.6. All of these scores reflect high internal consistency, but a coefficient greater than 0.90 can also imply that some items are tapping into very similar aspects of the same construct, not different information (Streiner, 2003; Tavakol & Dennick, 2011). This meant that the high coefficients were interpreted with caution, especially as some of the questionnaire statements had a close conceptual relationship.

Table 4.6: Reliability Analysis of Study Constructs

Construct	**No. of Items**	**Cronbach's Alpha**	**Corrected Item–Total Correlation Range**	**Mean Inter-Item Correlation**
Logging and Monitoring	6	0.922	0.736–0.820	0.666
Digital Evidence Preservation	6	0.943	0.766–0.876	0.739
Incident Reporting	6	0.947	0.806–0.858	0.750
Governance and Coordination	6	0.946	0.806–0.871	0.746

Staff Preparedness	6	0.942	0.760–0.867	0.732
Technological Factors	8	0.959	0.809–0.890	0.746
Organisational Factors	8	0.958	0.806–0.873	0.740
Environmental Factors	8	0.955	0.781–0.873	0.730

Individual item–total correlations were all high (0.736 to 0.890) indicating that items within each scale were highly correlated with the scale total. The inter-item correlation also ranged from high to very high (0.666-0.750). The pattern presented with alpha values above 0.90, along with the above, indicates a high degree of similarity between some items and redundancy of some of the scales.

The scales were kept for this analysis because they had been designed to reflect a number of related issues involving each construct, and the items responded in a similar fashion. The reliability results, however, should be treated with caution as evidence of construct validity or as a definitive distinction among measures due to the high level of internal association. This issue was taken into account when interpreting the subsequent correlation and regression findings, particularly where closely related predictor and readiness constructs were involved.

4.4.2 Descriptive Statistics for Digital Forensic Readiness Components

The findings show that the mean scores for the five digital forensic readiness components ranged from **3.731 to 3.979** on the five-point scale. Logging and monitoring recorded the highest mean, while staff preparedness recorded the lowest. The overall digital forensic readiness score was **3.852**, as presented in Table 4.7.

Table 4.7: Descriptive Statistics for Digital Forensic Readiness Components

Digital Forensic Readiness Component	Mean	Standard Deviation
Logging and Monitoring	3.979	0.866
Digital Evidence Preservation	3.927	0.886
Incident Reporting	3.833	0.953
Governance and Coordination	3.814	0.944
Staff Preparedness	3.731	1.036
Overall Digital Forensic Readiness	**3.852**	**0.867**

The pattern suggests that digital forensic readiness was relatively stronger in the technical aspects concerned with generating, retaining and preserving digital evidence. The comparatively lower scores for staff preparedness, governance and coordination point to greater weaknesses in the human and organisational dimensions of readiness. Staff preparedness also recorded the largest standard deviation, suggesting greater variation in how respondents assessed staff capability across the study context.

4.4.3 Descriptive Statistics for Technological, Organisational and Environmental Factors

The three factors examined in relation to digital forensic readiness all recorded mean scores above 3.7. Technological factors had a mean score of 3.921, environmental factors 3.909, and organisational factors 3.773 as shown in Table 4.8.

Table 4.8: Descriptive Statistics for Factors Affecting Digital Forensic Readiness

Factor	Mean	Standard Deviation
Technological Factors	3.921	0.908
Environmental Factors	3.909	0.865
Organisational Factors	3.773	0.956

The results show that technological and environmental factors were rated at almost the same level, with only a very small difference between their mean scores. Organisational factors recorded a slightly lower mean than the other two factors.Overall, the findings suggest that respondents generally viewed the technological, organisational and environmental conditions surrounding digital forensic readiness positively. The comparatively lower organisational score points to areas such as management support,

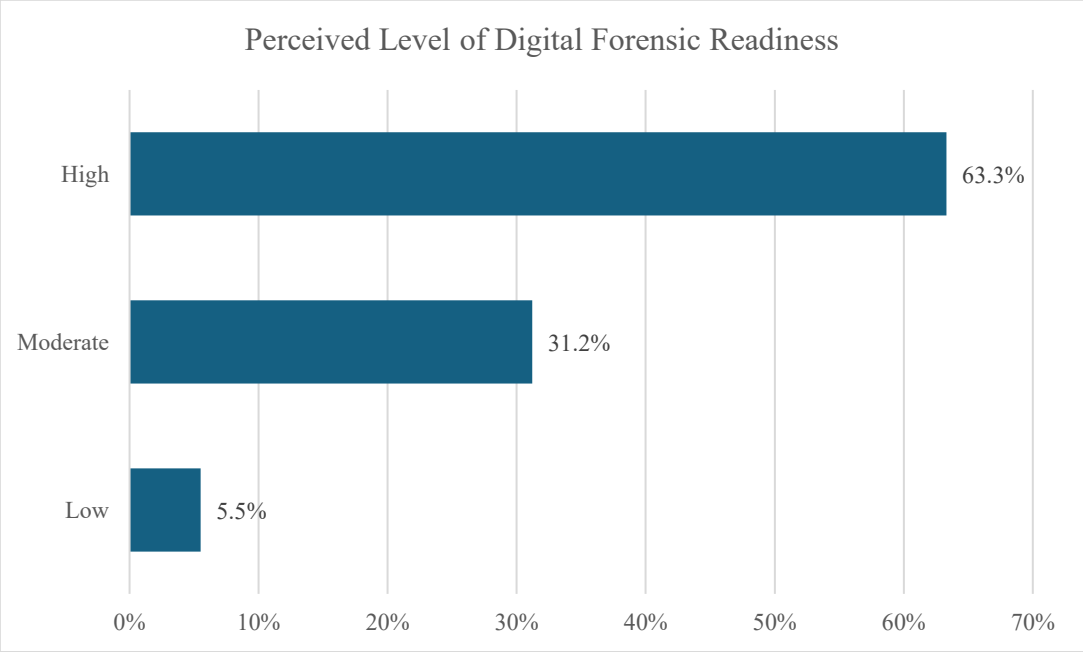
coordination, staff capability, procedures and resource allocation as possible areas requiring greater attention.

4.4.4 Overall Perceived Level of Digital Forensic Readiness

Respondents were asked to give an overall assessment of digital forensic readiness at Konza Technopolis. As shown in Figure 4.5, 63.3% gave a high or very high rating for readiness, 31.2% gave a moderate rating and 5.5% gave a low rating.

For interpretation, the study treated scores from 1.00–1.80 as very low, 1.81–2.60 as low, 2.61–3.40 as moderate, 3.41–4.20 as high and 4.21–5.00 as very high. Overall composite score of 3.852 is in the high range, when using these bands.

Figure 4.4: Overall Perceived Level of Digital Forensic Readiness



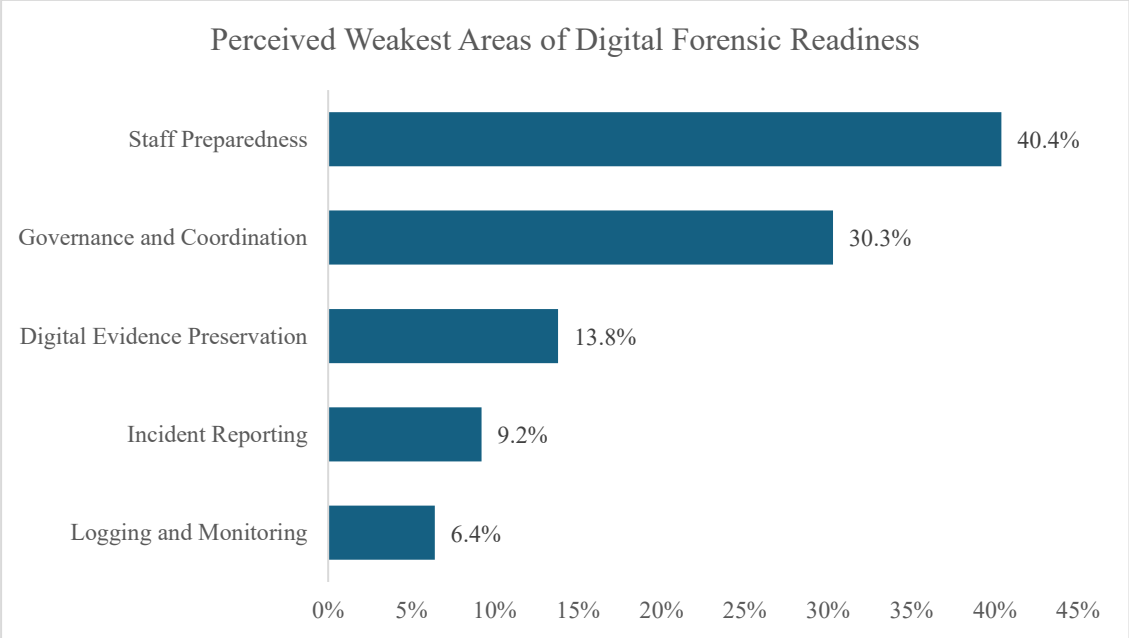
The results indicated a generally favorable attitude of the respondents towards digital forensic readiness, but this does not necessarily imply that they have the capability to conduct digital forensics. The assessment was conducted on a self-reported basis and there was no technical review or evidence-handling system review or practical exercise. This is significant because quite a few of the respondents were not digital evidence-handling specialists but instead from more general ICT and operational functions, which may have led to a different level of expertise in digital evidence and/or an bias towards the positive in how the organisation work. The overall finding that respondents generally were at high level of readiness should therefore be interpreted as being indicative of a high level of readiness, and the more detailed findings relating to staff preparedness, governance,

evidence preservation and incident reporting indicate important areas of concern. There would be a need for independent technical or documentary validation to verify the level of digital forensic readiness at Konza Technopolis.

4.4.5 Weakest Digital Forensic Readiness Component

The results indicate that preparedness of the staff is the weakest point in digital forensic readiness, with 40.4% of the responses, followed by governance and coordination with 30.3%. The area of least frequency mentioned were digital evidence preservation, incident reporting and logging and monitoring (as shown in Figure 4.5).

Figure 4.5: Perceived Weakest Component of Digital Forensic Readiness

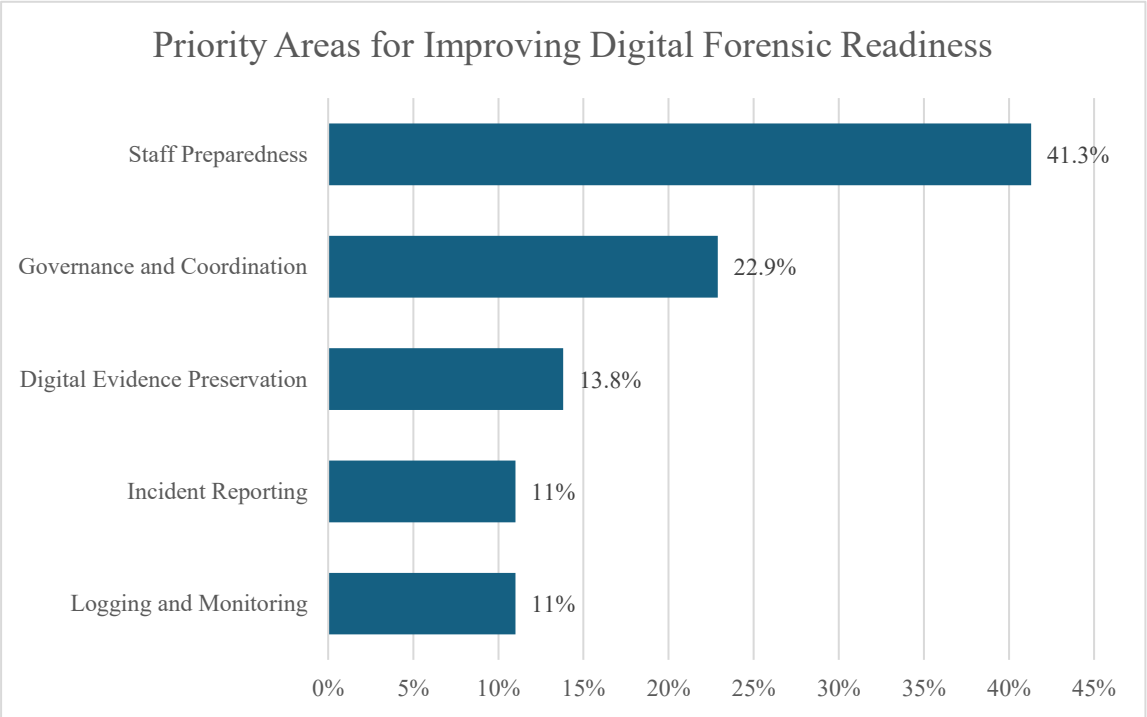


As anticipated, the pattern confirms the above descriptive findings, demonstrating that the key identified strengths were around staff skills and organisational coordination and not the technical infrastructure. Staff preparedness and governance and coordination combined made up 70.7% of the weakest areas identified, emphasising the importance of the human and organisational aspects of forensic readiness.

4.4.6 Priority Areas for Improvement

TStaff preparedness was identified as the main priority to increase digital forensic readiness at 41.3% followed by governance and coordination with 22.9%. As illustrated in Figure 4.6, digital evidence preservation took up 13.8% and incident reporting and logging and monitoring took up 11.0% respectively.

Figure 4.6: Priority Areas for Improving Digital Forensic Readiness



The prioritisation pattern indicates that respondents did not view improvements in digital forensic readiness primarily as a technology acquisition issue. Instead, the greatest emphasis was placed on strengthening staff capability and improving governance and coordination. It gives a foretaste of the need to incorporate organisational and human-capacity measures as well as technical measures in the framework that emerged from the study.

4.5 Diagnostic and Assumption Tests

The main assumptions of the model were assessed through diagnostic tests prior to the multiple regression analysis. The tests applied were normality of residuals, multicollinearity, linearity, homoscedasticity and independence of errors and were applied to the 107 complete cases available for the regression analysis.

4.5.1 Normality of Residuals

The Shapiro–Wilk test produced a statistic of 0.983 with a p-value of 0.182, indicating no statistically significant departure from normality at the 5% significance level.

Table 4.9: Normality Test for Regression Residuals

Test	Statistic	p-value	Decision
Shapiro–Wilk	0.983	0.182	Normality assumption satisfied

The result shows that the regression residuals were distributed approximately normally. This supported the use of multiple linear regression and the associated significance tests for evaluating the relationships between the study variables.

4.5.2 Multicollinearity

Multicollinearity was assessed using the Variance Inflation Factor (VIF) and tolerance statistics. The VIF values were between 3.235 and 3.835 and the tolerance values ranged from 0.261 to 0.309 as presented in Table 4.10.

Table 4.10: Multicollinearity Test

Predictor	**VIF**	**Tolerance**
Technological Factors	3.835	0.261
Organisational Factors	3.235	0.309
Environmental Factors	3.427	0.292

The values imply that the relationships of these three factors were not high enough to cause serious concern with multicollinearity. All the predictors thus had sufficient independent variation to be included in the multiple regression model.

4.5.3 Linearity

The linearity assumption was assessed using the Ramsey Regression Equation Specification Error Test (RESET). The test produced an F-statistic of 0.061 and a p-value of 0.805.

Table 4.11: Linearity Test

Test	**F-statistic**	**p-value**	**Decision**
Ramsey RESET	0.061	0.805	Linearity assumption satisfied

The non-significant result provides no evidence of substantial non-linear relationships or model specification problems. The linear regression form was therefore considered appropriate for examining the relationship between the technological, organisational and environmental factors and digital forensic readiness.

4.5.4 Homoscedasticity

Homoscedasticity was assessed using the Breusch–Pagan test. The test yielded a statistic of 3.112 with a p-value of 0.375, as shown in Table 4.11.

Table 4.12: Homoscedasticity Test

Test	**Statistic**	**p-value**	**Decision**

Breusch–Pagan	3.112	0.375	Homoscedasticity assumption satisfied

The result indicates that the variance of the residuals did not change significantly across levels of the predicted values. The regression model therefore did not show evidence of problematic heteroscedasticity, supporting the reliability of the estimated standard errors and significance tests.

4.5.5 Independence of Errors

The independence of regression errors was assessed using the Durbin–Watson statistic, which produced a value of **2.052**.

Table 4.13: Independence of Errors Test

Test	**Statistic**	**Interpretation**
Durbin–Watson	2.052	Independence assumption satisfied

A Durbin–Watson statistic close to 2 indicates little evidence of serial correlation among the residuals. The obtained value therefore suggests that the errors were sufficiently independent for the regression analysis. The diagnostic tests indicated that the main assumptions required for multiple linear regression were sufficiently met. The data were therefore considered appropriate for the inferential analyses used to evaluate the technological, organisational and environmental factors associated with digital forensic readiness.

4.6 Findings for Objective 1

The first objective focused on the current level of digital forensic readiness in Konza Technopolis with respect to the five areas of digital forensic readiness, which include logging and monitoring, digital evidence preservation, incident reporting, governance and coordination, and staff preparedness for evidential handling. The findings for each area are presented in the following subsections.

4.6.1 Logging and Monitoring Practices

The respondents generally rated the logging and monitoring at a positive level. Protection of logs from alteration or deletion had the highest mean (M = 4.073, SD = 1.007) with 73.4% indicating some agreement or strong agreement with the statement. This was followed by adequate log retention (M = 4.037, SD = 1.009) and timely detection of suspicious events (M = 4.000, SD = 0.972). The lowest ratings were recorded for the sufficiency of logs for investigations and consistency of log collection across systems, both with a mean of 3.890.

Table 4.14: Logging and Monitoring Practices

Logging and Monitoring Item	**N**	**Mean**	**SD**	**Agree/Strongly Agree (%)**
Protection of logs from alteration or deletion	109	4.073	1.007	73.4
Adequate log retention period	109	4.037	1.009	69.7
Timely detection of suspicious events	109	4.000	0.972	73.4
Maintenance of audit trails	109	3.982	1.063	67.9
Sufficient logs for investigations	109	3.890	1.074	67.9
Consistent log collection across systems	109	3.890	0.994	63.3

The positive ratings indicate that respondents overall identified existing expertise in areas of log protection, retention and event detection. At the same time, concerns were raised about fragmented or inconsistent logging across systems and the need for more centralised log management. This is consistent with the comparatively lower rating for consistent log collection across systems, where 63.3% of respondents agreed or strongly agreed.

The results thus indicate a positive attitude to logging and monitoring on the whole with some variations in logging and monitoring coverage between systems and platforms. In particular, greater consistency and integration of log collection would strengthen the availability and completeness of information needed during post-incident investigations.

4.6.2 Digital Evidence Preservation

Digital evidence preservation was generally rated favourably with the highest score being obtained for the retrieval of evidential data (M = 4.028). Other areas that were relatively strong were evidence integrity from collection (M = 3.982) and secure post-incident evidence handling (M = 3.963). Table 4.15 lists the lowest-rated aspect as the chain of custody practices (M = 3.817).

Table 4.15: Digital Evidence Preservation Practices

Digital Evidence Preservation	**Mean**
Retrieval of evidential data	4.028
Evidence integrity during collection	3.982
Secure post-incident evidence handling	3.963
Staff understanding of preservation requirements	3.936
Immediate evidence preservation mechanisms	3.835
Chain-of-custody practices	3.817

The pattern suggests that the technical aspects of preservation and retrieval of digital evidence were relatively more robust than the procedural aspects. The lower score for chain of custody practices indicates a lack of documented control of evidence during handling. This could weaken the evidential value of collected data during formal investigation.

4.6.3 Incident Reporting Procedures

Incident reporting procedures were well established, particularly in relation to clear reporting procedures **(M = 3.935)** and clear escalation procedures **(M = 3.916)**. Reporting processes were also viewed as supportive of subsequent forensic investigation (**M = 3.888**). However, timely incident reporting recorded the lowest

mean (M = 3.673), while staff knowledge of reporting channels and consistency of incident documentation each recorded a mean of **3.794**, as shown in Table 4.16.

Table 4.16: Incident Reporting Procedures

Incident Reporting Item	**Mean**
Clear incident reporting procedures	3.935
Clear escalation procedures	3.916
Reporting supports forensic investigation	3.888
Staff knowledge of reporting channels	3.794
Consistent incident documentation	3.794
Timely incident reporting	3.673

The pattern indicates that the lack of formal reporting frameworks was not the main concern, but rather the regularity and timely application of these frameworks in practice. Sometimes the information available at the beginning of an incident may be of lower quality because of delayed reporting, unsure of reporting channels and inconsistent documentation. Promptly reporting and documenting incidents is especially critical for forensic readiness, as evidence can be altered, overwritten or lost if incidents are not reported and documented promptly. These results indicate there is a need to increase operational discipline in relation to reporting timelines, documentations and awareness of staff escalation pathways.

4.6.4 Governance and Coordination Arrangements

The overall results of governance and coordination arrangements were relatively positive, the highest mean scores were registered for engagement of external stakeholders (M = 3.890). As seen in Table 4.17, clear incident response roles and evidence handling policies and procedures each had a mean of 3.826, with oversight of incident response actions having the lowest mean (M = 3.761).

Table 4.17: Governance and Coordination Arrangements

Governance and Coordination Item	**Mean**
Engagement of external stakeholders	3.890
Clear incident response roles	3.826
Evidence-handling policies and procedures	3.826

Effective interdepartmental coordination	3.807
Management support for forensic readiness	3.771
Oversight of incident response actions	3.761

The pattern indicates that the governance environment had basic structures to support incident response, but these were not equally strong across all areas. External engagement and role definition appeared relatively stronger, while internal oversight, management support and coordination were less developed. This suggests that the main governance challenge lies in ensuring that responsibilities are not only defined, but also actively coordinated, supervised and supported across the different functions involved in incident response. Weaknesses in these areas may result in fragmented decision-making, inconsistent evidence-handling practices and reduced accountability during cyber incidents.

4.6.5 Staff Preparedness for Evidential Handling

Assessment of staff preparedness showed stronger awareness than practical readiness for evidential handling. Understanding of evidence preservation recorded the highest mean (M = 3.899), while regular refresher training and awareness recorded the lowest mean (M = 3.495). Other relatively lower scores were recorded for identification of evidence sources (M = 3.725) and adequacy of staff preparedness (M = 3.734), as shown in Table 4.18.

Table 4.18: Staff Preparedness for Evidential Handling

Staff Preparedness Item	**Mean**
Understanding of evidence preservation	3.899
Training in digital evidence handling	3.771
Knowledge of evidence-handling procedures	3.761
Adequacy of staff preparedness	3.734
Identification of evidence sources	3.725
Regular refresher training and awareness	3.495

The pattern suggests that general awareness of the importance of preserving digital evidence was stronger than the practical capability required to handle evidence during

an incident.Staff capability appears not to be consistently reinforced by continuous training and by regular exposure to practice, as evidenced by the lower scores for refresher training, identification of likely evidence sources and overall preparedness. This leaves the possibility for evidence to be missed, miscollected, or mishandled in the early phases of incident response, all the while technical systems may be able to create and store evidence of relevance.

4.6.6 Technological, Organisational and Environmental Factors

Beyond the operational dimensions of readiness, the study also examined the wider conditions that may support or constrain digital forensic readiness. These were considered through the technological, organisational and environmental dimensions of the TOE framework. The findings for each factor are presented separately in the following subsections.

4.6.6.1 Technological Factors

Technological factors were generally rated positively. Logging capability recorded the highest mean score (M = 4.000, SD = 0.981), with 74.3% of respondents agreeing or strongly agreeing that the existing systems had adequate logging capabilities to support forensic investigation. Cross-platform evidence correlation recorded a mean of 3.945, while monitoring capability and secure evidence preservation each recorded a mean of 3.936. The lowest mean scores were recorded for reliable audit trails, interoperability and system configuration for investigation, each at 3.881.

Table 4.19: Technological Factors Affecting Digital Forensic Readiness

Technological Factor	**N**	**Mean**	**SD**	**Agree/Strongly Agree (%)**
Logging capabilities	109	4.000	0.981	74.3
Cross-platform evidence correlation	109	3.945	1.044	67.9
Monitoring captures useful data	109	3.936	0.984	74.3
Secure evidence preservation	109	3.936	1.048	68.8
Timely retrieval of evidence	109	3.908	1.050	68.8
Reliable audit trails	109	3.881	1.016	71.6
Interoperability supports investigations	109	3.881	1.025	67.0

Systems configured for investigation	109	3.881	1.086	68.8

The results suggest that respondents generally viewed the technological environment as supportive of forensic-ready incident response. The ratings were fairly close across the different items, although interoperability and system configuration received slightly lower scores. These areas are important in a smart city setting where investigations may involve information drawn from different devices, applications and platforms.

There were some technological items, especially those covering logging, audit trails, evidence preservation and retrieval, which were conceptually similar to the operational readiness measures discussed above. This overlap was taken into account in the inferential analysis to try and avoid the technological construct being seen as completely different from the readiness measure.

4.6.6.2 Organisational Factors

There were slightly more variations in respondents' ratings for the organisational factors. Clear policies that promotes digital forensic readiness obtained the highest mean score (M = 3.954, SD = 1.066). The mean scores for clear roles and responsibilities and supportive organisational culture for incident reporting were at 3.817 respectively. Staff training came in as the lowest of the three, with a mean of 3.624; resource allocation was the next lowest, coming in at 3.679; and management support was the next, 3.697.

Table 4.20: Organisational Factors Affecting Digital Forensic Readiness

Organisational Factor	N	Mean	SD	Agree/Strongly Agree (%)
Clear policies supporting readiness	109	3.954	1.066	69.7
Clear roles and responsibilities	109	3.817	1.073	69.7
Culture supports incident reporting	109	3.817	1.148	65.1
Internal evidence-handling procedures	109	3.807	0.995	66.1
Technical and management coordination	109	3.789	1.072	64.2
Management support	109	3.697	1.126	63.3
Adequate resource allocation	109	3.679	1.096	61.5
Staff training	109	3.624	1.129	60.6

The pattern indicates that some elements of the resources required to sustain some elements of formal arrangements were seen in a less favourable light than some of the formal

arrangements themselves. Training, resource allocation and management support received the lowest ratings within this group, pointing to areas where organisational support for forensic readiness could be strengthened.

There was also some conceptual similarity between the organisational items and the readiness dimensions examined earlier. In particular, items relating to staff training, roles and responsibilities, management support and evidence-handling procedures were closely related to staff preparedness, governance and evidence preservation. This was therefore taken into account in the later analysis of the relationship between the TOE factors and perceived digital forensic readiness.

4.6.6.3 Environmental Factors

Environmental factors were also viewed positively by respondents. Regulatory requirements encouraging forensic preparedness recorded the highest mean score (M = 4.046, SD = 0.937), with 75.2% of respondents agreeing or strongly agreeing. This was followed by the influence of compliance requirements on readiness (M = 3.991) and alignment of organisational practices with legal requirements (M = 3.945). The lowest mean score was recorded for the extent to which national laws and regulations support digital evidence handling (M = 3.771).

Table 4.21: Environmental Factors Affecting Digital Forensic Readiness

Environmental Factor	N	Mean	SD	Agree/Strongly Agree (%)
Regulatory requirements encourage preparedness	109	4.046	0.937	75.2
Compliance requirements influence readiness	109	3.991	0.918	72.5
Practices align with legal requirements	109	3.945	1.053	68.8
External collaboration supports readiness	109	3.908	0.948	71.6
Policy environment supports forensic readiness	109	3.908	0.977	73.4
External stakeholder guidance and support	109	3.908	1.014	70.6
Cybersecurity policy provides guidance	109	3.798	1.016	66.1
Laws and regulations support evidence handling	109	3.771	1.060	66.1

The ratings indicate that respondents generally recognised the role of regulation, compliance and external institutions in supporting digital forensic readiness. The lower

ratings for legal support and cybersecurity policy guidance, however, suggest that respondents were less positive about the practical guidance provided by the wider policy and regulatory environment.

The environmental items captured broad perceptions of regulation and external support rather than detailed knowledge of specific legal or technical requirements. They did not directly assess matters such as vendor obligations, access to third-party or cloud logs, cross-border data handling or compliance with particular standards. The results should therefore be understood as respondents' views of the wider regulatory and institutional environment rather than as evidence of compliance with specific legal or technical requirements.

4.6.7 Inferential Analysis

Inferential analysis was conducted to examine the relationships between the technological, organisational and environmental factors and digital forensic readiness for incident response. Pearson correlation analysis was first used to determine the direction and strength of the relationships between the study variables. Multiple linear regression was then applied to determine the independent contribution of each factor while controlling for the other predictors.

4.6.7.1 Correlation Analysis

Technological, organisational and environmental factors were all positively associated with digital forensic readiness. Technological factors recorded the strongest relationship with readiness, followed by organisational and environmental factors, as shown in Table 4.22.

Table 4.22: Correlation between TOE Factors and Digital Forensic Readiness

Factor	**Pearson Correlation (r)**	**p-value**
Technological Factors	0.889	<0.001
Organisational Factors	0.850	<0.001
Environmental Factors	0.802	<0.001

The results indicate that stronger technological, organisational and environmental conditions were associated with higher levels of digital forensic readiness. The relationships that were found for technological and organisational factors in particular

indicate that preparation is closely related to the technological capabilities that can be used to enable digital evidence, and the organisational arrangements in which these capabilities are applied.

While environmental factors also showed a strong positive relationship with digital forensic readiness, correlation analysis does not determine whether each factor makes an independent contribution when the other factors are considered simultaneously. This was examined further using multiple regression analysis.

4.6.7.2 Multiple Regression Analysis

Multiple linear regression was conducted to examine the combined and independent contribution of technological, organisational and environmental factors to digital forensic readiness. The model was statistically significant, **$F(3,103) = 187.230$, $p < 0.001$**, and explained **84.5%** of the variation in digital forensic readiness, with an **R^2 of 0.845** and an **adjusted R^2 of 0.841**.

Table 4.23: Multiple Regression Model Summary

Model Statistic	**Value**
R^2	0.845
Adjusted R^2	0.841
F-statistic	187.230
Degrees of Freedom	3, 103
p-value	<0.001
N	107

The model indicates that the three factors jointly accounted for a substantial proportion of the variation in digital forensic readiness. The individual regression coefficients are presented in Table 4.24.

Table 4.24 presents the regression coefficients of the factors affecting digital forensic readiness.

Predictor	**B**	**Standardised β**	**t**	**p-value**
Technological Factors	0.493	0.527	6.937	<0.001
Organisational Factors	0.307	0.347	4.976	<0.001

Environmental Factors	0.100	0.102	1.415	0.160

Technological factors contributed the most independently to the digital forensic readiness, followed by organisational factors. The relationships with both variables were statistically significant when all other variables were controlled. This shows that better technological competence and organisational setup were each found to be independently correlated with greater readiness.

But environmental factors failed to show a statistically significant independent contribution when technological and organisational factors were taken out of the equation. This is different from the correlation results, which found that environmental factors had a strong positive relationship with readiness. It appears that the environmental dimension of digital forensic readiness can act through and/or overlap the technological and organisational conditions in the smart city environment.

4.6.7.3 Summary of Hypothesis Decisions

The results of regression were employed to draw decisions for the three null hypotheses which were stated in the study. All the hypotheses were tested at 5% level of significance.

Table 4.25: Summary of Hypothesis Decisions

Hypothesis	**p-value**	**Decision**
H_{01}: Technological factors do not significantly influence digital forensic readiness for incident response	<0.001	Reject H_{01}
H_{02}: Organisational factors do not significantly influence digital forensic readiness for incident response	<0.001	Reject H_{02}
H_{03}: Environmental factors do not significantly influence digital forensic readiness for incident response	0.160	Fail to reject H_{03}

The results provide evidence that technological and organisational factors were significant predictors of digital forensic readiness, while the independent contribution of environmental factors was not statistically significant within the multivariate model. Environmental conditions nevertheless remained relevant to the wider readiness context because of their strong bivariate association with digital forensic readiness.

4.6.8 Measurement Overlap and Sensitivity Analysis

A review of the measurement items showed that some of the technological and organisational indicators were closely related to the operational dimensions used to

measure digital forensic readiness. For example, technological items on logging, audit trails, evidence preservation and evidence retrieval were similar to items already included under logging and monitoring and digital evidence preservation. A similar pattern was evident within the organisational construct, where training, role clarity, management support and evidence-handling procedures were also reflected in the readiness measures. This similarity could increase the strength of the relationships observed in the correlation and regression analysis.

An additional sensitivity analysis was therefore conducted using indicators that were more clearly distinguishable from the operational readiness measures. The reduced technological measure retained system interoperability, system configuration for investigation and cross-platform evidence correlation. Within the organisational construct, resource allocation was retained as the clearest antecedent that did not directly repeat a readiness dimension. Environmental measures were retained, while recognising the broad way in which it had been operationalised.

The reduced model remained statistically significant, $F(3,103) = 99.35$, $p < .001$, and explained 74.3% of the variation in perceived digital forensic readiness ($R^2 = .743$, adjusted $R^2 = .736$). Technological conditions remained significantly associated with readiness ($B = .445$, $\beta = .504$, $p < .001$), while environmental factors also made a significant independent contribution ($B = .315$, $\beta = .320$, $p = .001$). Resource allocation did not make a statistically significant independent contribution after the other factors were considered ($B = .073$, $\beta = .093$, $p = .229$).

The explanatory power of the model reduced from $R^2 = .845$ in the original analysis to $R^2 = .743$ after the most direct overlaps were removed. This suggests that some similarity regarding some of the original predictor and readiness items helped to bolster the initial relationships. The technical association was however still apparent after the adjustment. The organisational result needs extra care, as only one clearly identified organisational indicator could be kept from the previous questionnaire, the environmental result should be interpreted based on the wide perceptual measurement for the environmental construct.

4.6.9 Summary of Technological, Organisational and Environmental Findings

Overall, technological and environmental factors were rated similarly (mean score of 3.921 and 3.909 respectively), and organised factors had a slightly lower mean of 3.773. In the

organisational dimension, the areas that had lower scores included staff training, resource allocation and management support.

The expanded sensitivity analysis also revealed that some overlap between some of the predictors and readiness items contributed to the very high relationships found in the original inferential model. Following the removal of the most obvious overlaps, there was still a strong relationship between technological conditions and perceived readiness and a more complex relationship between the interpretation of organisation and environment and perceived readiness. The results were taken into consideration with the operational readiness results in determining the areas brought forward to develop the Digital Forensic Readiness Framework.

4.7 Findings for Objective 2

The second aim aimed to create a digital forensic readiness framework for digital incident response readiness in smart city ecosystems, driven by the empirical experiences of Konza Technopolis. Four primary areas that arose from the study have been used to inform the framework development: challenges and readiness gaps, current incident response process, proposed areas for improvement, and application of the results of the study to the proposed Digital Forensic Readiness Framework.

4.7.1 Challenges and Readiness Gaps

The thematic analysis identified the ability of the staff, logging and technical infrastructure, the preservation of evidence, governance and coordination, general legal and regulatory environment as the key challenges in digital forensic readiness at Konza Technopolis. These themes were identified through the comments made by the respondents in the challenges they faced, gaps they saw and institutional/policy issues that impacted incident response. The theme frequencies overlap, as respondents were able to mention more than one issue.

Table 4.26: Main Challenges and Readiness Gaps Identified by Respondents

Theme	**Main Issues Raised**	**Respondents Mentioning Theme (n)**	**Illustrative Response**
Staff capability and training	Skills gaps, limited practical forensic training, staff awareness and preparedness	64	"Lack of proper staff training and clear policies for incident response."

Logging, monitoring and technical infrastructure	Fragmented logging, inconsistent monitoring, limited centralisation and technical resources	61	“There are gaps in centralized logging and continuous monitoring.”
Evidence preservation and chain of custody	Preservation procedures, chain of custody, documentation and evidence integrity	57	“Weak evidence preservation procedures.”
Governance, coordination and procedures	Role clarity, reporting, escalation, management support, coordination and formal procedures	57	“Lack of an end to end framework for managing incident response.”
Legal, regulatory and privacy issues	Data protection, admissibility, privacy, compliance and information sharing	40	“Data protection, evidence admissibility, privacy requirements, and institutional policies can affect the collection, preservation, and sharing of digital evidence.”

The most common concern mentioned was staff capability. The weaknesses noted by the respondents were practical forensic skills, the need for ongoing refresher training and limited knowledge about evidence-handling needs. This is the difference between knowing about cybersecurity and knowing how to identify, save and preserve digital evidence in the event of a cyber incident. Especially at the beginning of an incident response, evidence that could be relevant may be accidentally changed, overlooked or lost.

There was also a high prevalence of technical and evidence-handling issues. Insatisfactory logging, inadequate centralisation of logging monitoring and insufficient evidence preservation were identified as issues. The Chain of Custody process, documentation and secure handling of evidential data were also noted. In the context of a smart city, information can be stored on various systems, devices and platforms, making it more challenging to create an accurate and comprehensive incident record.

Another theme which was often mentioned was governance and co-ordination. The participants talked about unclear responsibilities, poor reporting and escalation processes, lack of management support and difficulties in coordinating the various aspects of incident response. Legal/regulatory issues were also raised such as data protection, privacy and evidence admissibility & compliance. The results reveal that digital forensic readiness is not only a technical skill, but also has to rely on clear responsibilities, effective coordination

and institutional guidance that enables to manage evidence consistently in incident response.

4.7.2 Current Incident Response Process

Respondents were requested to write their typical procedure for the detection of a cyber incident. They described in various ways and some common steps were observed. The most frequently cited activities were detection or identification of the incident, reporting or escalation to the appropriate ICT or cybersecurity team, initial assessment, containment or isolation of the system, investigation and final documentation/remediation.

Reporting and escalation being done consistently was the most common feature of the responses, as was detection and identification. A few respondents also spoke of containment, investigation, evidence preservation, recovery, and post incident documentation, but they were not as frequently mentioned. Many responses were short, or expressed uncertainty about the incident-response process, which indicates that the incident-response process may not be uniformly understood across all the respondents.

From these consistent descriptions, a simplified view of the incident-response process was developed: figure 4.7.

Figure 4.7: Current Incident Response at Konza Technopolis



This sequence should not be interpreted as the official procedure or standard operating procedure for KoTDA incidents and/or responses. This is a researcher synthesis of the patterns found when reviewing the responses to the questionnaire. The study did not analyze an institutional incident-response plan or SOP to ensure that this sequence is the one that is formally designed.

The responses also show that evidence preservation was not consistently mentioned as a distinct step in the incident-response process. It matters to digital forensic readiness because evidence could be needed to be identified and protected during the very early stages of an

incident and not when the incident is contained or when it is being investigated. This study's framework thus included explicit identification of evidence preservation throughout the incident-response lifecycle.

4.7.3 Suggested Improvements to Digital Forensic Readiness

Responses indicated a variety of suggestions and improvement strategies to enhance the digital forensic readiness at Konza Technopolis. The most frequently cited recommendations related to staff capability, governance and procedures, evidence preservation and technical integration of logging and monitoring. Frequencies for the improvements in Table 4.27 overlap because some respondents could identify two or more improvements.

Table 4.27: Suggested Improvements to Digital Forensic Readiness

Theme	Main Improvements Suggested	Respondents Mentioning Theme (n)	Illustrative Response
Staff capability and practical training	Regular training, refresher programmes, incident-response exercises, awareness and practical forensic skills	62	"Continuous training."
Governance, procedures and coordination	Clear policies, defined responsibilities, reporting and escalation procedures, management support and coordination	49	"Develop clear incident response and evidence preservation procedures."
Evidence preservation and chain of custody	Evidence collection and preservation procedures, chain of custody, documentation and secure evidence handling	43	"Having clear policies and evidence preservation methods."
Logging, monitoring and technical integration	Centralised logging, SIEM, improved monitoring, forensic tools and integration across systems	40	"Strengthening centralized logging/SIEM, forensic capabilities, evidence preservation procedures, staff training, and incident response processes."
Legal and regulatory alignment	Alignment with legal requirements, privacy, compliance obligations and relevant standards	16	"Establish strong governance and policy framework."

There were many suggestions for improving staff development. Participants expressed a need for periodic training, refresher courses and hands-on practice to improve staff proficiency in the field of potential evidence sources, preservation of digital evidence and

the proper procedures in incident response. This is consistent with the earlier observation that readiness of staff, including refresher training and practical readiness, was one of the less strong aspects of the readiness assessment.

There was also a significant focus on improved governance and on more consistent procedures. Participants recommended the improvement of the clarity of responsibility, increase in coordination between teams, more structured reporting and escalation procedures, and more support for management. The following recommendations identify a need to understand and apply the responsibilities for responding to incidents consistently and not just as a formal process.

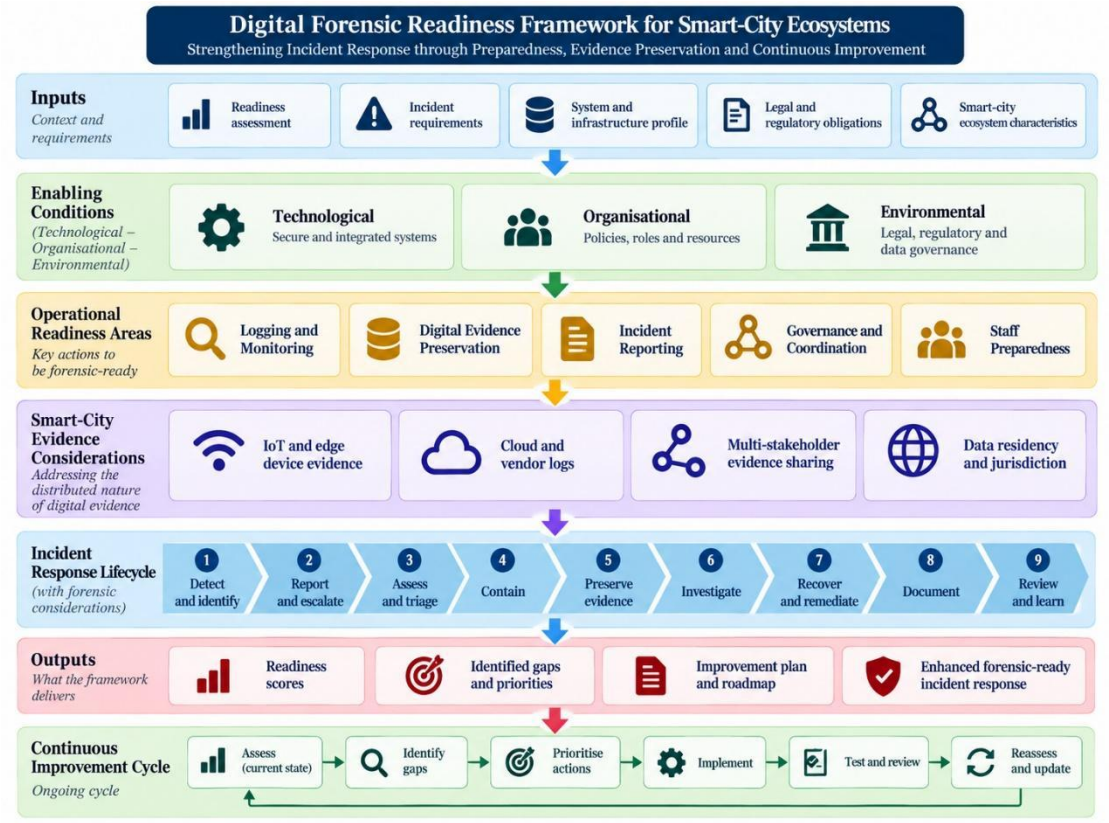
These organisational issues were closely related to the technical ones. Participants highlighted an increased focus on centralised logging and monitoring, a more robust capability to handle SIEM, access to the right forensic capabilities, and integration of systems. Evidence preservation also was often cited, with a need for the standardisation of evidence collection and preservation procedures, including identification, collection, preservation, documentation, storage and transfer of digital evidence. The maintenance of evidence integrity and traceability would be improved if evidence was maintained during the incident-response process through practices.

Another, albeit less significant, subset of responses concerned legal/regulatory alignment. The following are general suggestions for data protection, privacy, compliance and consistency of institutional procedures with relevant legal and regulatory requirements. The recommendations made in relation to the suggested improvements went beyond technology and emphasized the importance of building staff capability, operational procedures, governance and other institutional arrangements that would facilitate digital forensic readiness.

4.7.4 Proposed Digital Forensic Readiness Framework

The findings from the study and reviewed approaches in Chapter Two have been used to develop the Digital Forensic Readiness Framework. The strengths and gaps of logging and monitoring, evidence preservation, incident reporting, governance and coordination, staff preparedness and technological, organisational and environmental conditions were identified during the readiness assessment. The results of these findings were converted to actionable needs to improve forensic-ready incident response.

Table 4.28: Digital Forensic Readiness Framework for Smart-City Ecosystems



The framework starts with the most significant inputs that influence readiness, such as assessment results, identified deviations, requirements for responding to incidents, system and infrastructure attributes, legal and regulatory obligations, and the smart city environment. These link to three enabling domains: technological, organisational and environmental conditions. Together, these conditions support five operational readiness areas: logging and monitoring, digital evidence preservation, incident reporting and escalation, governance and coordination, and staff preparedness and capability.

The framework is also inspired by the smart city concept, understanding that digital evidence can be spread across various devices in the IoT, edge systems, cloud applications, and platform and system applications operated by external providers. It therefore contains data requirements, such as volatile data, access to cloud logs and vendor logs, sharing evidence with multiple stakeholders, data residency, cross-operator jurisdiction and chain of custody.

There is a connection between forensic readiness and the incident-response lifecycle – detection and reporting, assessment, containment, evidence preservation, investigation,

recovery, documentation and post-incident review. This means that evidence is taken into account at every part of the response process and not just at the investigation phase.

The framework uses four maturity levels—Initial, Developing, Established and Optimised—to show how consistently readiness practices are implemented. These levels are supported by indicators such as log coverage, retention, chain-of-custody records, reporting timelines, staff-training coverage and third-party evidence-access arrangements. The framework also includes a continuous improvement cycle of assessment, gap identification, prioritisation, implementation, testing and reassessment.

Table 4.29: Traceability of Study Findings to Framework Components

Study Finding	**Framework Response**
Low staff preparedness and limited refresher training	Regular training, practical exercises and competency assessment
Weaknesses in timely incident reporting	Defined reporting timelines and escalation procedures
Lower ratings for chain-of-custody practices	Formal evidence-preservation and chain-of-custody procedures
Fragmented or inconsistent logging	Centralised logging, time synchronisation and event correlation
Governance and coordination gaps	Clear responsibilities, oversight and interdepartmental coordination
Legal, privacy and compliance concerns	Alignment with legal, regulatory and data-protection requirements
Distributed smart-city evidence sources	IoT, cloud, vendor and cross-operator evidence-access arrangements

The framework was informed by Rowlingson's forensic readiness approach, ISO/IEC 27043 and more recent work on forensic readiness in IoT and interconnected environments. Its contribution lies in combining these foundations with the TOE enabling conditions, the readiness dimensions identified in the study, the incident-response lifecycle and smart-city-specific evidence requirements.

The framework was operationalised through the web-based assessment tool developed in the study. The tool generated readiness scores, highlighted weaker areas and supported prioritisation of improvement needs. However, the framework was not independently validated through expert review, Delphi assessment or testing in a

second organisation. Its evaluation in this study should therefore be understood as an initial assessment of practical applicability rather than external validation.

4.8 Findings for Objective 3

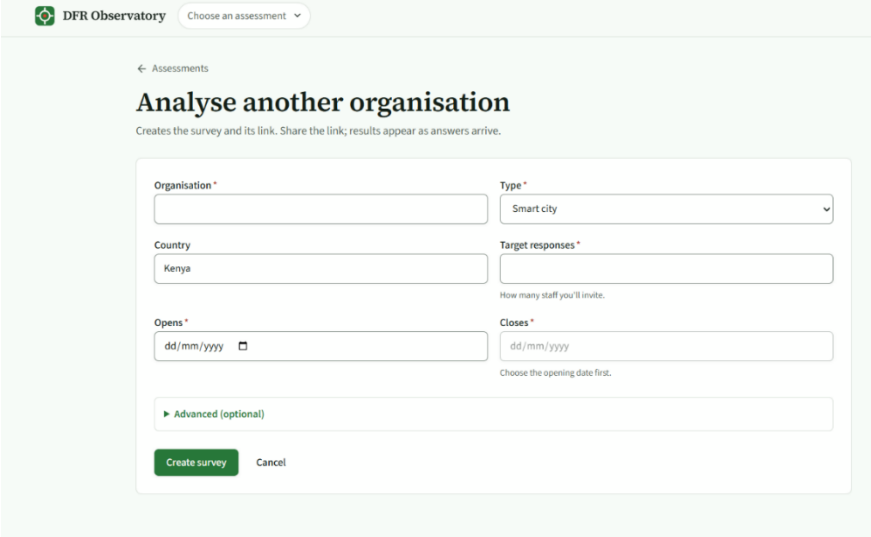
The third objective evaluated the practical applicability of the developed Digital Forensic Readiness Framework in assessing readiness, identifying gaps and prioritising improvements for incident response. The evaluation examined how the framework was implemented in a working assessment process via the web based tool and if the outputs of the assessment process could be used practically to interpret organisational readiness.

4.8.1 Web-Based Digital Forensic Readiness Assessment Tool

For that, a web-based digital forensic readiness assessment and deployment tool was created. The application converts the framework into a real assessment process that an organisation can use to gather responses, derive readiness scores, determine weak points and pinpoint priorities for change. The first case that was applied through the Konza Technopolis assessment.

The app uses Next.js, Node.js and Cloudflare Workers for deployment inside the Cloudflare environment. Details like the organisation name, organisation type, country, target number of respondents and assessment period enable the creation of a new assessment.

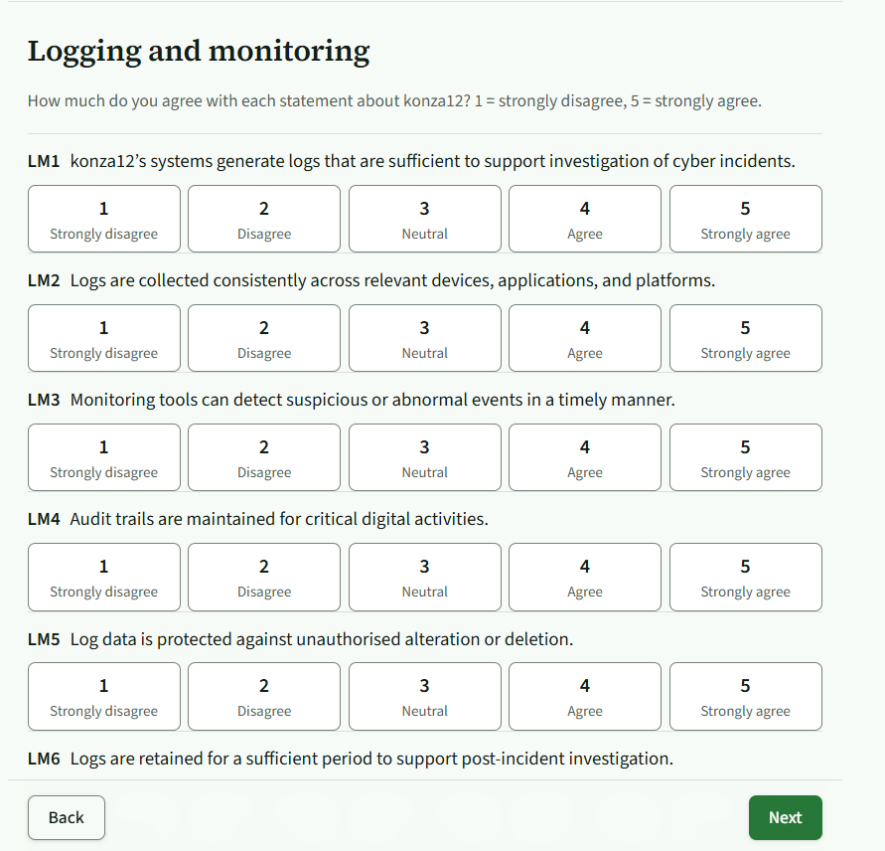
Figure 4.8: Creation of a New Organisational Digital Forensic Readiness Assessment



After an assessment is developed, a structured questionnaire is completed regarding the five areas of operational readiness: logging and monitoring, digital evidence preservation, incident reporting/escalation, governance and coordination, and staff

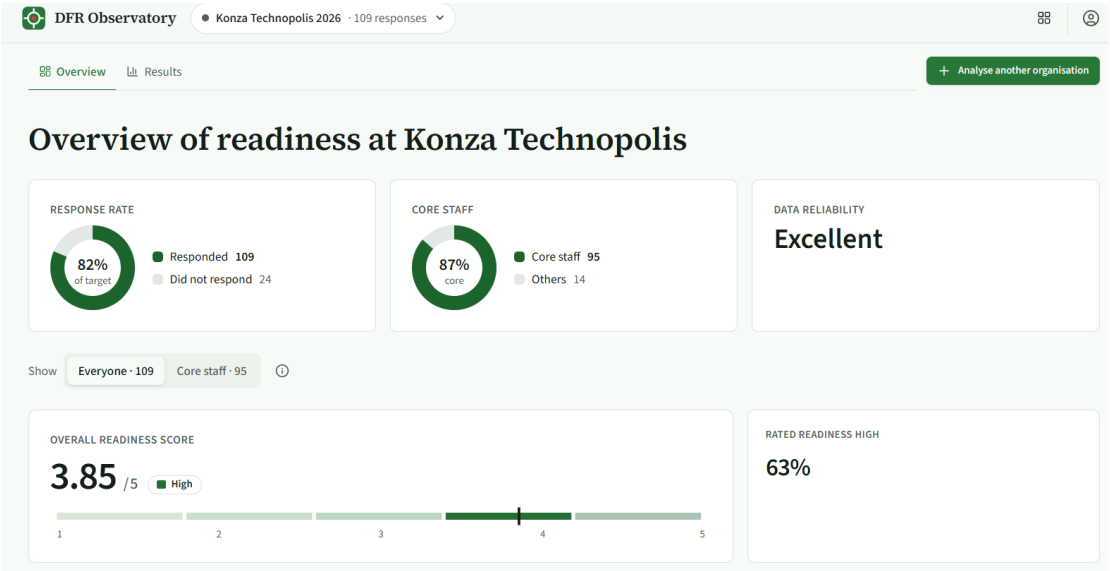
preparedness/capability. The assessment also takes into account the technological, organisational and environmental aspects of digital forensic readiness. Items are measured with a 5-point Likert scale (1 = Strongly Disagree, 5 = Strongly Agree).

Figure 4.9: Web-Based Digital Forensic Readiness Assessment Interface



The application collates submitted responses into dimension-level and an overall digital forensic readiness scores. For interpretation, scores from 1.00–1.80 are classified as Very Low, 1.81–2.60 as Low, 2.61–3.40 as Moderate, 3.41–4.20 as High and 4.21–5.00 as Very High. With these thresholds, the overall Konza Technopolis score is in the High band (3.852).

Figure 4.10: Overview Dashboard of Digital Forensic Readiness at Konza Technopolis



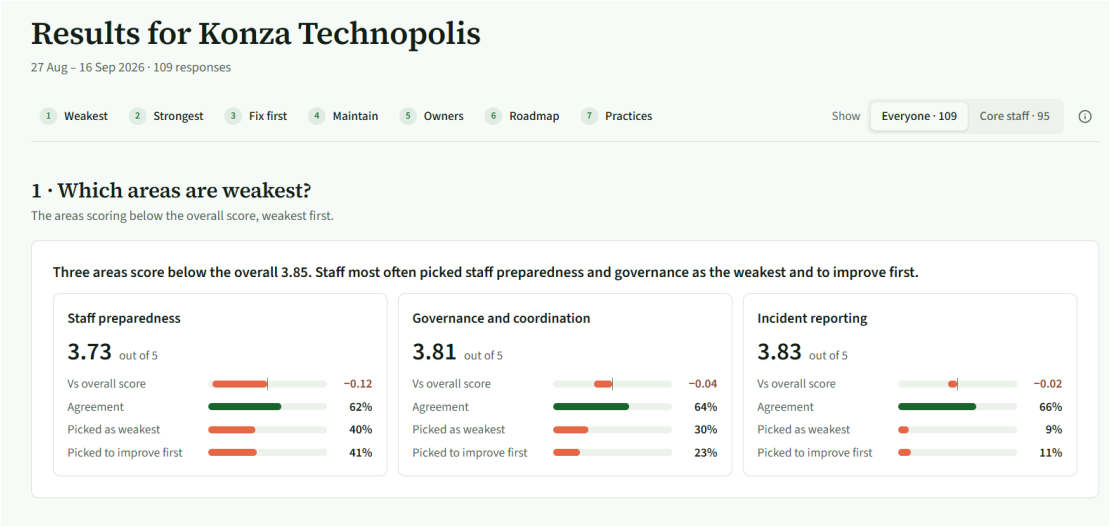
The tool was developed to be used to report on the assessment results at the organisational level and not as individual respondent profiles. The dashboard consolidates the overall readiness score, scores for the various readiness dimensions, areas identified as needing improvement and the priorities for improvement identified by respondents. This allows to shift from individual questionnaire answers to a wider organisational preparedness profile.

4.8.2 Identification of Readiness Gaps and Improvement Priorities

The next aspect of practical applicability was whether the tool could assist to identify weaker areas and demonstrate where efforts for improvement should be focused. The dashboard compares the readiness dimensions with the overall organisational score and also incorporates respondents' views on which areas they considered weakest and which should be prioritised.

Staff preparation was identified as the most common weak area and the top priority for improvement in the Konza Technopolis assessment. The roles of governance and coordination were also identified, as were digital evidence preservation, incident reporting and logging and monitoring, by some respondents. These findings were corroborated by the more detailed results which identified issues relating to refresher training, timely reporting and governance oversight and chain-of-custody.

Figure 4.11: Digital Forensic Readiness Gap and Priority Analysis



Presenting gaps and priorities together makes the dashboard more useful for decision-making because it shows not only where readiness is comparatively weaker, but also which areas respondents believe should receive attention first. This directly connects assessment results and prioritisation of corrective action.

4.8.3 Practical Applicability of the Framework

The framework was applied to the data for the Konza Technopolis and resulted in their translation into a real assessment process. The tool provided dimension-level and overall readiness scores, identified areas of weakness and assisted development of improvement priorities. This illustrated how it was possible to apply the framework to describe readiness, but also to organise the findings to enable practical interpretation and decision making.

The framework also offers a point of reference for subsequent evaluation. Once improvement measures have been put in place, a review of the readiness dimensions can occur to see if the gaps noted have been addressed or if new concerns have arisen. This helps to sustain the continuous improvement aspect of the framework by making a connection between assessment, gap identification, corrective action and reassessment.

This study was based on an evaluation conducted in case of Konza Technopolis. There was no formal usability test or independent expert validation or use in a second organisation of the framework and web-based tool. The results must therefore be interpreted as signaling initial practical applicability in the context of the study, and not external validation or provision of proof of transferability to other smart city contexts.

4.8.4 Summary of Findings for Objective 3

The findings for Objective 3 showed that the developed Digital Forensic Readiness Framework could be operationalised through the web-based assessment tool to produce dimension-level and overall readiness scores, identify weaker areas and highlight improvement priorities.In the Konza Technopolis assessment, areas that needed more attention included staff preparedness, governance and coordination and incident reporting, where the need to increase the preparedness of staff was clearly identified to be a priority for improvement.

The tool also showed the capabilities of the framework to facilitate a repeatable assessment process with connection of readiness measurement, gap identification and prioritisation of corrective action. The evaluation was, however, limited to the Konza Technopolis case, and did not involve formal usability testing of it, or validation or testing in another organisation. The findings thus lend support to the initial applicability of the framework in the study context; however, further testing of the framework for broader applicability and transferability would be warranted.

4.9 Discussion of Findings

4.9.1 Discussion of Findings for Objective 1

The first goal evaluated the current readiness of digital forensic tools at Konza Technopolis in terms of logging and monitoring, digital evidence preservation, incident reporting, governance and coordination, and staff preparedness on evidential handling. The results indicated there was a positive level of preparedness, but there were significant variations in each area. Technical capacity, especially logging and monitoring and digital evidence preservation, was relatively good; staff preparedness and preparedness related to governance were weak.

It's notable that logging and monitoring had the relatively high score, as logs are essential to helping reconstruct what has happened following a cyber incident if they are available. Some of the strongest areas noted in the study included protection against alteration/deletion of logs and retention periods. This is in line with the approach of digital forensic readiness put forward by Rowlingson (2004), where pre-incident arrangements for the collection and preservation of potentially useful evidence should be made. Especially in a smart city context, preparedness plays an important role, as there may be evidential traces produced on more and more connected systems, not just on a single device or platform.

The results indicate that the provision of logs was less consistent across the systems despite this relatively positive situation. This is significant in the context of smart cities where infrastructure is characterised by heterogeneous devices, cloud services, applications and communication platforms. Eichhorn and Pugliese (2024), as reviewed in Chapter Two, found that forensic artefacts in connected environments may be distributed across local devices, mobile applications and remote cloud services. Their findings illustrate why the existence of logging capability alone is insufficient; the logs must also provide adequate coverage across different components of the digital ecosystem.

Digital evidence preservation was similarly assessed relatively positively, particularly in relation to the retrieval of evidential information and preservation of integrity during collection. However, chain-of-custody practices were comparatively weaker. This distinction is important because being ready for a forensics investigation is much more than the technical process of recovering information. The management of the evidence should also maintain the integrity, traceability and evidential value of such evidence. Ariffin and

Ahmad (2021) also claim that chain of custody and procedural maturity and institutional preparedness are important factors for forensic readiness. Thus, the current results suggest that there is a need for technical competency in evidence preservation, as well as a corresponding competency in procedure at Konza.

The same trend was observed with reporting of incidents. Formal reporting and escalation structures seemed to be in place but the actual reporting, consistent documentation and awareness of reporting procedures were relatively less effective. When it comes to digital forensic readiness, there's a significant difference between procedure and the practice of procedure. Late reporting may restrict the amount of time to preserve volatile evidence and not having any documentation may affect the sequence of events that can be reconstructed during the investigation. The findings therefore corroborate the proactive approach of Rowlingson 2004 that states that there should be a requirement for evidence beforehand rather than afterwards.

Another area identified as a need for strengthening was governance and coordination. Roles, policies and mechanisms for external engagement were identified, but management support, oversight and interdepartmental coordination were not as well evaluated. This is consistent with the results presented by Laufs et al. (2020) who have identified governance arrangements and institutional coordination as well as the connection between technical operations and organisational decision making as factors that impact smart city cybersecurity. In complex systems, there may be confusion in reporting, evidence collection, investigation and escalation as a result of lack of coordination.

Staff preparedness (in terms of refresher training) and practical preparedness and identification of possible evidence sources were identified as areas of weakness. The awareness and practical ability gap was clear: there was good awareness of the importance of evidence and this did not always equate to preparedness for evidence handling. Friedl and Pernul (2024) also list human factors, in addition to technology, procedures, management and legal concerns, as significant aspects of forensic readiness. Their role further highlights the need for a multi-faceted approach to forensic preparedness, beyond merely adopting technical infrastructure.

The results are very indicative of the underlying theory of the study, known as the Socio-Technical Systems Theory. The theory suggests that organisational effectiveness

depends on the interaction between technological and social systems rather than the optimization of independently.

In the current study, both strong logging technologies and weak evidence preservation technologies were present, along with weak governance and staff preparedness. This shows that having good technical skills is not enough to equate with equivalent forensic readiness without the development of the associated people, procedures and organizational structures.

Overall, it provides a solid technical basis for readiness for digital forensics at Konza Technopolis, which, if developed, would support the efficacy of the basis. The findings therefore substantiate a forensic readiness perspective as an holistic capability and not as a set of technical controls.

4.9.2 Discussion of Findings for Objective 2

The second goal assessed the technological, organizational and environmental factors that impact digital forensic preparedness. The results revealed positive bivariate relationships among all three factors and digital forensic readiness. The regression analysis showed that technological and organizational factors significantly contributed to readiness, however, the contribution of environmental factors was not statistically significant after the other factors were adjusted for.

Technological factors are important in a smart city that is technologically intensive. Digital forensic readiness depends on systems being capable of generating logs, maintaining audit trails, preserving relevant data and enabling evidence to be retrieved when required.This good technological outcome is aligned with the literature on connected environments, which highlights the interoperability, integration of the environment's infrastructure and the possibility of obtaining evidence distributed across the environment. Bhardwaj et al. (2024) highlight the recurring challenges of infrastructure integration, interoperability and security when building a smart city, and the research of IoT environments shows that relevant evidence can be found in multiple interconnected technical layers.

The role of organisation, however, is significant in terms of digital forensic readiness, so technology is by itself insufficient. Technical capacity will be effectively converted to operational readiness through the staff training, management support, internal procedures, resources and coordination. This finding is consistent with the Socio-Technical Systems perspective, which argues against treating technology independently from the organisational and human system within which it operates. It also aligns with the findings of Friedl and Pernul (2024) who proposed a conceptualisation of forensic readiness that includes technical resources, management processes and procedures, human factors and legal considerations.

Organisational findings also match the description results of the study. Policies and role definitions were fairly clear, but staff training, management support and resource allocation were less robust. This implies that there must also be a formal structure, which must be supported by resources, capability development and managerial commitment. Similarly,

Tan and Taeihagh (2020) state that besides the investment in technology, smart city implementation requires institutional, regulatory and human capacity.

The environmental factor is a factor that needs more careful analysis. It has a significant positive correlation with readiness, so that the more favourable the legal, regulatory and external environment, the more ready digital forensic teams were. After considering the technological and organisational factors together in the regression model, however, the environmental factor was no longer statistically significantly different from zero. This is not to say that the outside world has no effect. Instead, it seems to indicate that its impact may be mediated by or overlapping with organisational and technological arrangements.

This interpretation is a reflection of the framework of Technology, Organisation and Environment in which technology is one context, organisation is another and environment is another, but are not mutually independent. The environmental requirements are realised in the organisation sometimes by means of the policy, decision on resources, the organisation of the system configuration and governance. The results thus show that readiness could be indirectly influenced by external requirements due to the translation of external requirements that the institutions implement.

The results provide empirical evidence of the use of TOE for the digital forensic readiness within the smart city environment. They demonstrate that readiness can be affected by a variety of contextual factors, and that these factors have varying effects. Within Konza Technopolis, technological capability and organisational preparedness appear particularly important in explaining differences in readiness, while environmental conditions provide a broader enabling and regulatory context.

4.9.3 Discussion of Findings for Objective 3

The third objective sought to develop a context-specific digital forensic readiness framework for strengthening incident response in smart city ecosystems. The results of the quantitative readiness assessment as well as the quantitative TOE, and the thematic results of the operational challenges and readiness gaps, the current incident response practices and suggested actions were included in the framework.

One of the key insights underpinning the framework was that digital forensic readiness has a multi-dimensional nature. The research highlighted the problems of staff

capability, logging and monitoring, digital evidence preservation, reporting, governance, technical infrastructure and legal requirements. This fits within the established literature, which has conceptualised forensic readiness beyond mere availability of forensic technologies. Friedl and Pernul (2024) have, for instance, defined four interdependent legal, technical, procedural, management and human factors of IoT forensic readiness. Ariffin and Ahmad (2021) also point to institutional maturity and capability development and chain of custody.

This tri-dimensionality is addressed by the proposed framework, which combines three enabling domains – technological, organising and environmental – and five domains of operational readiness – logging and monitoring, evidence preservation, incident reporting and escalation, governance and coordination, staff preparedness. This is designed to embody TOE and STST. The framework does not consider technology, people and organisational arrangements as stand-alone factors; it acknowledges the interaction of these factors in influencing the identification, preservation and use of digital evidence in incident response.

Forensic readiness is another critical component of the framework, and is a requirement to be integrated into the incident response lifecycle. The study revealed that the process of detection, reporting, containment, investigation and recovery was generally discernible within the existing response process, but not always so with respect to evidence preservation and documentation throughout the process. This is in line with the argument of Rowlingson (2004) that the process of preparing a case for presentation at court ought to be proactive and in place before the event occurs. It also addresses the research gap described by Kim et al. (2023), who note that the current research on smart city cybersecurity has focussed more on the prevention and protection of cyber-attacks than focusing on the investigation and cyber forensics after an attack.

It is also crucial that the proposed continuous improvement part is not static since the smart city systems are not static. Technologies, threats, regulations and structures evolve, and a ready-to-go organization at one time might not be ready for the next. Assessment is therefore periodic to be able to identify readiness gaps, prioritise corrective actions, and reassess progress.

This element is further realised by the development of the web-based digital forensic readiness assessment tool. Through allowing staff to determine readiness based on

specific indicators and compiling these into readiness dimensions and an overall score, the application provides a mechanism through which the conceptual framework can be applied within an organisational setting. This tool also provides for repeated evaluation, thus letting organisations recognize the weaker dimensions and track the improvements over time.

This practical orientation addresses part of the research gap identified in Chapter Two, as most of the existing research was largely conceptual discussion, threat identification, and general smart city cybersecurity, while there is less evidence involved in structured forensic readiness assessment within specific smart city environment. The framework established by this study thus makes a contribution in terms of bridging the gap between theoretical and empirical results and in the sense of making an assessment-orientated approach to readiness conditions and operational incident response.

In general, the results from the study falls in line with the argument of the study which was that the digital forensic readiness in the smart city ecosystem depends on the alignment of technology, organisational capability, staff readiness, governance, evidential procedures and the overall regulatory environment. The framework suggested and its web-based assessment tool offer a structure for integrating these elements in the incident response lifecycle more effectively.

CHAPTER 5 SUMMARY, CONCLUSIONS AND RECOMMENDATIONS

5.1 Introduction

This chapter summarises the key findings of the study, presents the conclusions drawn from the three research objectives, and outlines recommendations for practice, policy and further research. It also highlights the study's contribution to knowledge on digital forensic readiness for incident response in smart city ecosystems.

5.2 Summary of Findings

This section presents a concise summary of the key findings in relation to the three research objectives. It highlights the current level of digital forensic readiness within Konza Technopolis, the technological, organisational and environmental factors associated with readiness, and the main elements that informed the development of the proposed digital forensic readiness framework and its web-based assessment tool.

5.2.1 Summary for Objective 1

The first goal was to evaluate the level of digital forensic readiness and technology, organisational and environment at Konza Technopolis with regard to incident response readiness. The overall perceived readiness score was 3.852 of 5, and 63.3% of respondents indicated their readiness was high to very high. Logging and monitoring recorded the highest mean (M = 3.979), followed by digital evidence preservation (M = 3.927), while staff preparedness recorded the lowest mean (M = 3.731). Staff preparedness was also most frequently identified as the weakest component (40.4%) and the leading priority for improvement (41.3%).

Technological and environmental factors received broadly similar ratings, with means of 3.921 and 3.909 respectively, while organisational factors recorded a lower mean of 3.773. Correlation analysis showed strong positive associations between perceived readiness and technological ($r = 0.889$, $p < .001$), organisational ($r = 0.850$, $p < .001$) and environmental factors ($r = 0.802$, $p < .001$). In the original regression model, technological ($\beta = 0.527$, $p < .001$) and organisational factors ($\beta = 0.347$, $p < .001$) remained statistically significant, while environmental factors were not significant after the other predictors were considered ($\beta = 0.102$, $p = .160$). Because some predictor items overlapped conceptually with the readiness measures, these results were interpreted cautiously and examined further through sensitivity analysis.

The findings therefore point to a generally positive perception of readiness, but with clear weaknesses in staff preparedness, timely reporting, chain-of-custody practices, governance oversight and coordination. They also show that the relationships between readiness and the TOE factors are important, but should not be interpreted as causal.

5.2.2 Summary for Objective 2

The second objective developed a Digital Forensic Readiness Framework for strengthening incident response in smart city ecosystems using the empirical findings from Konza Technopolis. The framework development was informed by the identified readiness gaps, the existing incident-response process, respondents' suggested improvements and the theoretical foundations of the study.

The framework brings together three enabling domains technological, organisational and environmental conditions with five operational readiness areas: logging and monitoring, digital evidence preservation, incident reporting and escalation, governance and coordination, and staff preparedness and capability. It also includes smart-city-specific factors, such as IoT and edge-device evidence, cloud and vendor log, multi-stakeholder evidence sharing, data residency and jurisdiction. These are all associated with the incident response lifecycle and a continuous improvement cycle of assessment, gap identification, prioritisation, implementation, testing and reassessment.

The framework is therefore not just an assessment model but guides to a structured way of enhancing forensic readiness based on the study findings. It has not, however, been independently validated by expert review and Delphi assessment or testing in another organisation.

5.2.3 Summary for Objective 3

The third goal tested the feasibility of the developed framework in assessing readiness, identifying gaps and prioritising improvements. The framework was put to action by creating a web-based assessment tool with Next.js and Node.js, and deploying it with Cloudflare Workers.

The tool was applied to the data from the Konza Technopolis and provided dimension-level and overall readiness scores, identified areas of weakness and listed the needs of the respondents for improvement. The area highlighted as a priority to address was staff preparedness, governance and coordination were identified as an area of focus as was incident reporting, evidence preservation and logging and monitoring.

The findings show that the framework could be translated into a working assessment process within the study setting. The tool also provides a basis for repeated assessment by linking readiness measurement, gap identification and prioritisation of corrective action. However, the evaluation was limited to the Konza Technopolis case and did not include formal usability testing, independent expert validation or application in a second organisation. The findings therefore support the framework's initial practical applicability, rather than external validation or proven transferability to other smart-city environments.

5.3 Conclusions

The results showed that the general attitude of the respondents towards the digital forensic readiness in Konza Technopolis was positive, but there were variations in the level of readiness in the respective areas analyzed. Logging or monitoring and preservation of digital evidence were rated higher, and staff preparedness, timely reporting of incidents, chain-of-custody practices and governance oversight and coordination were rated as weaker. This implies that technical expertise is critical but will not suffice in support of effective handling of digital evidence during the cyber incident.

Further, the study revealed that technological and organisational conditions played a special role in influencing digital forensic readiness. Technological capability contributes to the generation, retention, retrieval and correlation of relevant evidence; organisational arrangements are the foundation of technological capability and involve the presence of relevant procedures, resources, management support and staff competence. The independent impact of environmental factors, including regulation, policy and compliance issues, was less pronounced when technological and organisational factors were also taken into account.

The findings also indicate that digital forensic readiness should be a part of the whole incident-response process, not just something that is initiated after the incident. There are evidence related considerations that must be considered from the point of detection and reporting to containment, preservation, investigation, recovery, documentation and post incident review. In smart city applications, digital evidence can be spread out in interconnected systems, IoT devices, cloud platforms and other digital services, this is particularly important.

However, conclusions must be taken with the limitations of the study in mind. The findings were primarily based on the perceptions of the respondents, and not on a direct technical verification of systems, logs or evidence-handling procedures. The study was also conducted in a single case and employed a cross-sectional, purposive sample, which consisted predominantly of those with ICT related roles. Furthermore, the same questionnaire has been used to assess the predictor variables and digital forensic readiness constructs, which could have led to high correlations among some of the variables. The framework was implemented using a web-based assessment tool and tested for practical use in the Konza context but not tested and validated independently for other organisations/smart city environments.

5.4 Recommendations

The recommendations are based on the key findings and readiness gaps found in the study. Their focus is to build digital forensic readiness in Konza Technopolis, and also outreach on areas that require further investigations and validations.

5.4.1 Recommendations for Practice and Policy

3.495) were regular refresher training and awareness, and also staff preparedness was the area most commonly reported as being weak and a priority for improvement. Hence, KoTDA's ICT and cybersecurity personnel must, through practical sessions, enhance the identification, preservation and chain of custody of digital evidence, incident reporting and documentation. It should include scenario based exercises and regular reminders to ensure that staff are confident to use the procedures during real incidents.

The research also highlights some issues related to incident reporting and evidence management. The mean for timely incident reporting was comparatively low (3.673) and the mean for chain-of-custody was a high of 3.817. Accordingly, KoTDA should provide clarity on reporting timelines, incident escalation procedures, who will keep the digital evidence, transfer of evidence, and who will access it. The procedures should be re-considered and reinforced by the ICT and cybersecurity and governance functions, taking into account guidelines from relevant organizations like ICT Authority and KE-CIRT/CC.

The requirement for forensic readiness should not be limited to systems and services managed by Konza, as they exist in a smart city context. Such agreements with IoT

vendors, cloud service providers and other technology partners should specify the following requirements in the logs: availability, retention, access to relevant evidence, notification of incidents and cooperation in investigations. This will mitigate the risk of loss of critical evidence when systems or data are controlled by someone other than KoTDA.

There should also be improved governance and coordination by better assignment of responsibilities, better management oversight and coordination of ICT, cybersecurity, governance and incident response functions. Logging and monitoring needs to be enhanced through consistency in systems and better centralised correlation of info from various platforms.

Before the framework and web-based assessment tool could be adopted for regular organisational assessment, they need to be further evaluated for usability and technical evaluation. A controlled pilot would give the chance to know if the readiness information from use of the tool would be useful, if the scoring is easy to interpret, and if the identified gaps could be turned into readiness improvement action points within KoTDA.

5.4.2 Recommendations for Further Research

The research should be expanded to other smart city, critical infrastructure and digitally enabled public-sector environments in Kenya and beyond Africa to complement the assessment of digitization readiness in Konza Technopolis. Comparative studies would be useful to determine if the readiness gaps found in this study are unique to Konza or if they also occur in similar environments. It may be worthwhile to investigate the individual readiness element further in future studies, including staff capability, chain of custody, governance, and cross-platform evidence management.

The framework built in this study was tested for its applicability in the Konza Technopolis setting using its web based assessment tool. Further studies are suggested that can expand the scope of this preliminary assessment with larger, more varied samples and use longitudinal designs if available in different organizational and technological settings. These studies could assist in creating the consistency, transferability and applicability of the framework beyond the original case.

Other research should also be conducted to better assess the web-based assessment tool, especially its usability and user experience and its ability to measure improvements in organisational readiness over time. Benchmarking techniques which could enable the comparison of readiness levels across organisations or across repeated assessment periods could also be investigated in the future.

5.5 Contribution to Knowledge

This study brings empirical evidence on the perceived digital forensic readiness for incident response in Konza Technopolis. The study covers the following areas of digital evidence: logging and monitoring of digital evidence, preserving digital evidence, reporting and escalation of incidents, governance and coordination and readiness of staff; and offers empirical evidence from a smart city context in Kenya where studies into forensic readiness in this field are scarce. The contribution is thus primarily focused on the experience of these dimensions in one institutional context, rather than on making a more general statement about smart city ecosystems.

The study also helps in the application of Technology–Organisation–Environment framework in relation to digital forensic readiness. Technological and organisational factors contributed significantly with readiness on their own, whereas the environmental factors had a strong bivariate relationship with readiness, but did not retain significant values when technological and organisational factors were included together. This implies that the technological and organizational structures for the implementation of regulatory and policy conditions can affect readiness to some extent.

Another contribution is the operationalization of digital forensic readiness within five measurable dimensions and the correlation to the technological, organizational and environmental context of incident response. These dimensions then were translated into a framework and applied in a web enabled assessment tool which facilitates readiness scoring and gap identification and prioritization of areas for improvement. The contribution here is practical and methodological, in identifying how the study results can be put into practice in an evaluation-driven way but not setting up the framework as one that is completely new and fully tested.

REFERENCES

Abbas, R., & Michael, K. (2025). *Socio-Technical Theory*. https://open.ncl.ac.uk

Allam, Z., & Jones, D. S. (2020). On the coronavirus (Covid-19) outbreak and the smart city network: Universal data sharing standards coupled with artificial intelligence (ai) to benefit urban health monitoring and management. *Healthcare (Switzerland)*, *8*(1). https://doi.org/10.3390/healthcare8010046

Almeida, F. (2023). Prospects of Cybersecurity in Smart Cities. *Future Internet*, *15*(9). https://doi.org/10.3390/fi15090285

Anomah, S. (2025). Assessing the institutional readiness and capacity for AI adoption in public audit institutions in developing countries: evidence from Ghana. *Telematics and Informatics Reports*, *20*. https://doi.org/10.1016/j.teler.2025.100260

Ariffin, K. A. Z., & Ahmad, F. H. (2021). Indicators for maturity and readiness for digital forensic investigation in era of industrial revolution 4.0. *Computers & Security*, *105*, 102237. https://doi.org/10.1016/j.cose.2021.102237

Baker, J. (2012). *The Technology–Organization–Environment Framework*. 231–245. https://doi.org/10.1007/978-1-4419-6108-2_12

Baxter, G., & Sommerville, I. (2011). Socio-technical systems: From design methods to systems engineering. *Interacting with Computers*, *23*(1), 4–17. https://doi.org/10.1016/j.intcom.2010.07.003

Bednar, P. M., & Welch, C. (2020). Socio-Technical Perspectives on Smart Working: Creating Meaningful and Sustainable Systems. *Information Systems Frontiers*, *22*(2), 281–298. https://doi.org/10.1007/s10796-019-09921-1

Bhardwaj, V., Anooja, A., Vermani, L. S., Sunita, & Dhaliwal, B. K. (2024). Smart cities and the IoT: an in-depth analysis of global research trends and future directions. *Discover Internet of Things 2024 4:1*, *4*(1), 19-. https://doi.org/10.1007/s43926-024-00076-3

Bostrom, R. P., & Heinen, J. S. (1977). MIS Problems and Failures: A Socio- Technical PerspectivePart I: The Causes. *Management Information Systems Quarterly*, *1*(3), 17–32. https://doi.org/10.2307/248710

Carro-Suárez, J., Sarmiento-Paredes, S., Nava, D., Carro-Suárez, J., Sarmiento-Paredes, S., & Nava, D. (2023). Smart and Sustainable Cities: A New Urban Transformation. *Sustainable Regional Planning*. https://doi.org/10.5772/intechopen.110234

Creswell, J. W. ,. (2014). Research design : qualitative, quantitative, and mixed methods approaches /. *Research Design Pendekatan Metode Kualitatif Kuantitatif Dan Campuran*, 251–252. https://eduq.info/xmlui/handle/11515/19498

Das, D. K., Aiyetan, A. O., & Mostafa, M. M. H. (2026). Advancing Smart Cities in Africa: Barriers, Potentials, and Strategic Pathways for Sustainable Urban Transformation. *Smart Cities*, *9*(2), 38. https://doi.org/10.3390/smartcities9020038

Demertzi, V., Demertzis, S., & Demertzis, K. (2023). An Overview of Cyber Threats, Attacks and Countermeasures on the Primary Domains of Smart Cities. In *Applied Sciences (Switzerland)* (Vol. 13, Number 2). MDPI. https://doi.org/10.3390/app13020790

Eichhorn, M., & Pugliese, G. (2024). Do You “Relay” Want to Give Me Away? – Forensic Cues of Smart Relays and Their IoT Companion Apps. *Forensic Science International: Digital Investigation*, *50*, 301810. https://doi.org/10.1016/j.fsidi.2024.301810

Forestiero, A., Abd Elaziz, M., & Almeida, F. (2023). Prospects of Cybersecurity in Smart Cities. *Future Internet 2023, Vol. 15, Page 285*, *15*(9), 285. https://doi.org/10.3390/fi15090285

Fagan, M., Megas, K., Cuthill, B., Marron, J., & Hoehn, B. (2026). *Foundational cybersecurity activities for IoT product manufacturers* (NIST IR 8259 Rev. 1). National Institute of Standards and Technology.

Friedl, S., & Pernul, G. (2024a). IoT Forensics Readiness - influencing factors. *Forensic Science International: Digital Investigation*, *49*(1), 301768. https://doi.org/10.1016/j.fsidi.2024.301768

Friedl, S., & Pernul, G. (2024b). IoT Forensics Readiness - influencing factors. *Forensic Science International: Digital Investigation*, *49*(1), 301768. https://doi.org/10.1016/j.fsidi.2024.301768

Kim, K., Alshenaifi, I. M., Ramachandran, S., Kim, J., Zia, T., & Almorjan, A. (2023). Cybersecurity and Cyber Forensics for Smart Cities: A Comprehensive Literature Review and Survey. In *Sensors* (Vol. 23, Number 7). MDPI. https://doi.org/10.3390/s23073681

Kuku, O., Chrysikos, A., & Salekzamankhani, S. (2025). Preparing IoT-enabled organisations for digital forensics: model for readiness and resilience. *International Journal of Information Security 2025 24:4*, *24*(4), 170-. https://doi.org/10.1007/s10207-025-01079-z

Laufs, J., Borrion, H., & Bradford, B. (2020). Security and the smart city: A systematic review. *Sustainable Cities and Society*, *55*, 102023. https://doi.org/10.1016/j.scs.2020.102023

Mahmood, S., Chadhar, M., & Firmin, S. (2024). Addressing Cybersecurity Challenges in Times of Crisis: Extending the Sociotechnical Systems Perspective. *Applied Sciences (Switzerland)*, *14*(24). https://doi.org/10.3390/app142411610

Möller, D. P. F. (2023). NIST Cybersecurity Framework and MITRE Cybersecurity Criteria. *Advances in Information Security*, *103*, 231–271. https://doi.org/10.1007/978-3-031-26845-8_5

NIST. (2016). *Cyber-Physical Systems/Internet of Things for Smart Cities | NIST*. https://www.nist.gov/programs-projects/cyber-physical-systemsinternet-things-smart-cities

Rowlingson, R. (2004). A Ten Step Process for Forensic Readiness. In *International Journal of Digital Evidence Winter* (Vol. 2, Number 3). www.ijde.org

Salih, S., Abdelmaboud, A., Husain, O., Motwakel, A., Elshafie, H., Sharif, M., & Hamdan, M. (2025). IoT in urban development: insight into smart city applications, case studies, challenges, and future prospects. *PeerJ Computer Science*, *11*, 1–42. https://doi.org/10.7717/peerj-cs.2816

Sanchez-Gallegos, D. D., Carrizales-Espinoza, D. E., Torres-Charles, C., & Carretero, J. (2025). Smart Cities: A Systematic Review of Emerging Technologies. *Smart Cities*, *8*(5). https://doi.org/10.3390/smartcities8050173

Saunders, M., Lewis, P., & Thornhill, A. (2011a). *Research Methods for Business Students (4th edn, Vietnamese language edition)*. Hochiminh, Huong Huy. https://openresearch.surrey.ac.uk/esploro/outputs/book/Research-Methods-for-Business-Students-4th-edn-Vietnamese-language-edition/99511839402346

Saunders, M., Lewis, P., & Thornhill, A. (2011b). *Research Methods for Business Students (4th edn, Vietnamese language edition)*. Hochiminh, Huong Huy. https://openresearch.surrey.ac.uk/esploro/outputs/book/Research-Methods-for-Business-Students-4th-edn-Vietnamese-language-edition/99511839402346

Sibe, R. T., & Kaunert, C. (2024). *Digital Evidence, Digital Forensics, and Digital Forensic Readiness*. 57–83. https://doi.org/10.1007/978-3-031-54089-9_3

Sicari, S., Rizzardi, A., Grieco, L. A., & Coen-Porisini, A. (2015). Security, privacy and trust in Internet of things: The road ahead. In *Computer Networks* (Vol. 76, pp. 146–164). Elsevier B.V. https://doi.org/10.1016/j.comnet.2014.11.008

Tan, S. Y., & Taeihagh, A. (2020). Smart City Governance in Developing Countries: A Systematic Literature Review. *Sustainability 2020, Vol. 12, Page 899*, *12*(3), 899. https://doi.org/10.3390/su12030899

THE DIGITAL TRANSFORMATION STRATEGY FOR AFRICA (2020-2030). (n.d.). Retrieved www.au.int

Tornatzky, L. G., & Fleischer, Mitchell. (1990). The processes of technological innovation | SpringerLink. *D.C. Heath & Company*, 298. https://books.google.com/books/about/The_Processes_of_Technological_Innovatio.html?id=QWiwAAAAIAAJ

Yamane, T. (n.d.). *2nd hidition*.

Yin, R. K., Calvin, Y., & Mali, G. (n.d.). *61 A BOOK REVIEW: CASE STUDY Title: Case Study Research and Applications: Design and Methods (6 th ed.)*. Retrieved March 20, 2026, from https://doi.org/http://dx.doi.org/10.1563

Zaman, M., Puryear, N., Abdelwahed, S., & Zohrabi, N. (2024). A Review of IoT-Based Smart City Development and Management. *Smart Cities 2024, Vol. 7, Pages 1462-1501*, *7*(3), 1462–1501. https://doi.org/10.3390/smartcities7030061

APPENDICES

Appendix A: Research Instruments

Primary data were collected using a structured questionnaire attached below:

https://tinyurl.com/mr24sddk

Appendix B: Introductory Letter

OPEN UNIVERSITY OF KENYA

SCHOOL OF SCIENCE AND TECHNOLOGY
SCHOOL GRADUATE STUDIES COMMITTEE

REF: OUK/SGSC/PROP/ST63/80222/2024
DATE: 4th Aug 2026

Timothy Kosgei
Registration No. ST63/80222/2024
Master of Science in Cyber Security

Dear Timothy,

RE: APPROVAL OF RESEARCH PROPOSAL

We are pleased to inform you that following your successful proposal defence and completion of the corrections recommended by the panel, your research proposal titled "Developing a Digital Forensic Readiness Framework for Incident Response in Smart City Ecosystems: A Case Study of Konza Technopolis, Kenya" has been reviewed and approved by the School Graduate Studies Committee (SGSC).

You may now proceed to the data collection stage of your study, subject to the following requirements being met prior to commencement:

- Clearance from an approved Institutional Ethics Review Committee (ERC), where applicable to the nature of your study; and
- A valid research permit from the National Commission for Science, Technology and Innovation (NACOSTI).

You are advised to liaise with the SGSC office to obtain the necessary letters of introduction to support these applications.

As you progress with your research, kindly remember to regularly complete the supervision tracking and progress report forms available on the Learning Management System (LMS), as these are used to monitor and document your supervision sessions and overall progress. You are further reminded to adhere to all other applicable institutional guidelines throughout the research process, including timelines, reporting requirements, and research ethics standards of the University.

Congratulations on this achievement, and we wish you well as you proceed with your research. Please do not hesitate to contact your supervisor(s) or the undersigned should you require any support or clarification.

Yours faithfully,

Dr. Nickcy Mbuthia
Ag. Chair, School Graduate Studies Committee
School of Science and Technology
Email: graduatestudies.sst@ouk.ac.ke
This letter is issued and signed by the undersigned and does not require an institutional stamp to be valid. Its authenticity may be verified by contacting the School using the details above.

cc:
Chair, Department of Computing and Informatics
Dr. Peter Ngaira – Supervisor

"The Innovative University for Inclusive Prosperity"

OPEN UNIVERSITY OF KENYA

SCHOOL OF SCIENCE AND TECHNOLOGY
SCHOOL GRADUATE STUDIES COMMITTEE

REF: OUK/SGSC/ERC/ST63/80222/2024
DATE: 4TH AUGUST 2026

Institutional Ethics Review Committee (ERC)

Dear Sir/Madam,

RE: INTRODUCTION LETTER FOR ETHICS REVIEW CLEARANCE **Timothy Kosgei** – REG. NO. **ST63/80222/2024**

This letter serves to introduce the above-named student, a bona fide Master's student in the Master of Science in Cyber Security at the Open University of Kenya (OUK), Registration Number ST63/80222/2024.

The student presented and successfully defended a research proposal titled "Developing a Digital Forensic Readiness Framework for Incident Response in Smart City Ecosystems: A Case Study of Konza Technopolis, Kenya" under the supervision of Dr. Peter Ngaira. The student now wishes to proceed to the next stage of the study, which requires ethical review and clearance from an approved Institutional Ethics Review Committee (ERC) prior to commencement of data collection.

We kindly request your Committee to review the attached research proposal and supporting documents, and to grant the student the necessary ethical clearance to enable them to proceed with the NACOSTI research permit application and, subsequently, data collection.

The University confirms that the student is in good standing and that the study will be conducted in accordance with the ethical standards and research guidelines of the Open University of Kenya.

Kindly do not hesitate to contact the undersigned for any clarification.

Yours faithfully,

Dr. Nickcy Mbuthia
Ag. Chair, School Graduate Studies Committee
School of Science and Technology
Email: graduatestudies.sst@ouk.ac.ke
This letter is issued and signed by the undersigned and does not require an institutional stamp to be valid. Its authenticity may be verified by contacting the School using the details above.

cc:
Chair, Department of Computing and Informatics
Dr. Peter Ngaira – Supervisor

"The Innovative University for Inclusive Prosperity"

Appendix C: Ethical Approval (NACOSTI Permit)

REPUBLIC OF KENYA

NATIONAL COMMISSION FOR SCIENCE,TECHNOLOGY & INNOVATION

Ref No: **169175**

Date of Issue: **25/August/2026**

RESEARCH LICENSE



This is to Certify that Mr.. TIMOTHY KOSGEI of Open University of Kenya, has been licensed to conduct research as per the provision of the Science, Technology and Innovation Act, 2013 (Rev.2014) in Machakos on the topic: Developing a Digital Forensic Readiness Framework for Incident Response in Smart City Ecosystems: A Case Study of Konza Technopolis, Kenya. for the period ending : 25/August/2027.

License No: **NACOSTI/P/26/4195476**

169175

Applicant Identification Number

Ag. Director General
NATIONAL COMMISSION FOR SCIENCE,TECHNOLOGY & INNOVATION

Verification QR Code

NOTE: This is a computer generated License. To verify the authenticity of this document, Scan the QR Code using QR scanner application.

See overleaf for conditions

THE SCIENCE, TECHNOLOGY AND INNOVATION ACT, 2013 (Rev. 2014)
Legal Notice No. 108: The Science, Technology and Innovation (Research Licensing) Regulations, 2014

The National Commission for Science, Technology and Innovation, hereafter referred to as the Commission, was the established under the Science, Technology and Innovation Act 2013 (Revised 2014) herein after referred to as the Act. The objective of the Commission shall be to regulate and assure quality in the science, technology and innovation sector and advise the Government in matters related thereto.

CONDITIONS OF THE RESEARCH LICENSE

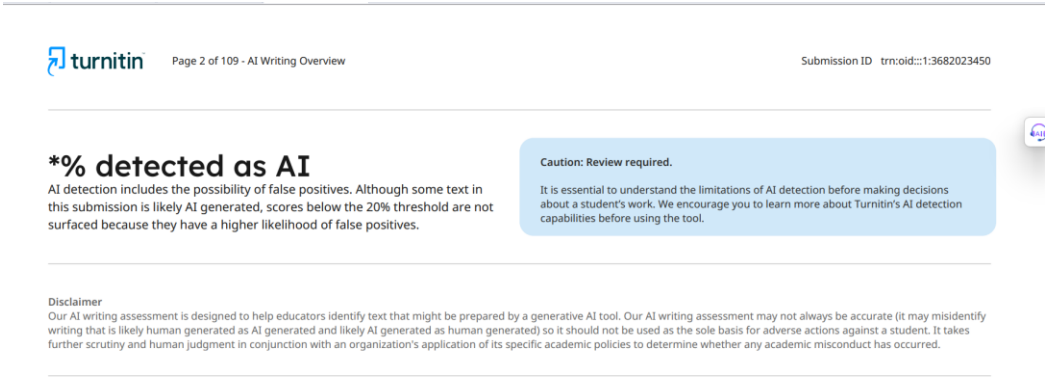
1. The License is granted subject to provisions of the Constitution of Kenya, the Science, Technology and Innovation Act, and other relevant laws, policies and regulations. Accordingly, the licensee shall adhere to such procedures, standards, code of ethics and guidelines as may be prescribed by regulations made under the Act, or prescribed by provisions of International treaties of which Kenya is a signatory to.
2. The research and its related activities as well as outcomes shall be beneficial to the country and shall not in any way;
    i. Endanger national security
    ii. Adversely affect the lives of Kenyans
    iii. Be in contravention of Kenya's international obligations including Biological Weapons Convention (BWC), Comprehensive Nuclear-Test-Ban Treaty Organization (CTBTO), Chemical, Biological, Radiological and Nuclear (CBRN).
    iv. Result in exploitation of intellectual property rights of communities in Kenya
    v. Adversely affect the environment
    vi. Adversely affect the rights of communities
    vii. Endanger public safety and national cohesion
    viii. Plagiarize someone else's work
3. The License is valid for the proposed research, location and specified period.
4. Neither the license nor any rights thereunder are transferable.
5. The Commission reserves the right to cancel the research at any time during the research period if in the opinion of the Commission the research is not implemented in conformity with the provisions of the Act or any other written law.
6. The Licensee shall inform the relevant County Director of Education, County Commissioner and County Governor before commencement of the research.
7. Excavation, filming, movement, and collection of specimens are subject to further necessary clearance from relevant Government Agencies.
8. The License does not give authority to transfer research materials.
9. The Commission may monitor and evaluate the licensed research project for the purpose of assessing and evaluating compliance with the conditions of the License.
10. The Licensee shall submit one hard copy, and upload a soft copy of their final report (thesis) onto a platform designated by the Commission within one year of completion of the research.
11. The Commission reserves the right to modify the conditions of the License including cancellation without prior notice.
12. Research, findings and information regarding research systems shall be stored or disseminated, utilized or applied in such a manner as may be prescribed by the Commission from time to time.
13. The Licensee shall disclose to the Commission, the relevant Institutional Scientific and Ethical Review Committee, and the relevant national agencies any inventions and discoveries that are of National strategic importance.
14. The Commission shall have powers to acquire from any person the right in, or to, any scientific innovation, invention or patent of strategic importance to the country.
15. Relevant Institutional Scientific and Ethical Review Committee shall monitor and evaluate the research periodically, and make a report of its findings to the Commission for necessary action.

National Commission for Science, Technology and
Innovation(NACOSTI),
Off Waiyaki Way, Upper Kabete,
P. O. Box 30623 - 00100 Nairobi, KENYA
Telephone: 020 4007000, 0713788787, 0735404245
E-mail: dg@nacosti.go.ke
Website: www.nacosti.go.ke

Appendix D: Research Timeline and Budget Details

Phase / Activity	Activity	Timeline	Estimated Cost (KES)	Justification
Phase 1:	Ethics approval, stakeholder engagement, questionnaire pilot testing	Weeks 1-3	8,000	Printing documents, communication, transport for approvals, pilot test logistics
Phase 2:	Primary data collection: Questionnaire administration to stakeholders (n - 133) at Konza Technopolis	Weeks 4 - 11	10,000	recording tools
Phase 3:	Quantitative data analysis (SPSS) and thematic analysis of qualitative responses	Weeks 12 - 14	9,000	SPSS license, cloud storage, computing resources.
Phase 4:	Cybersecurity and digital forensic readiness framework design and expert validation	Weeks 15-17	15,000	Expert validation engagement, materials, cybersecurity experts.
Phase 5:	Report writing, thesis compilation, dissemination	Weeks 18-20	7,000	Report writing, printing & binding, presentation preparation.
Contingency (10%)	Miscellaneous/ unforeseen costs	Throughout	10,000	Buffer for unexpected expenses, additional stakeholder engagement.

Appendix E: Turnitin Similarity Report



turnitin Page 2 of 109 - AI Writing Overview Submission ID trn:oid:::1:3682023450

*% detected as AI

AI detection includes the possibility of false positives. Although some text in this submission is likely AI generated, scores below the 20% threshold are not surfaced because they have a higher likelihood of false positives.

Caution: Review required.

It is essential to understand the limitations of AI detection before making decisions about a student's work. We encourage you to learn more about Turnitin's AI detection capabilities before using the tool.

Disclaimer

Our AI writing assessment is designed to help educators identify text that might be prepared by a generative AI tool. Our AI writing assessment may not always be accurate (it may misidentify writing that is likely human generated as AI generated and likely AI generated as human generated) so it should not be used as the sole basis for adverse actions against a student. It takes further scrutiny and human judgment in conjunction with an organization's application of its specific academic policies to determine whether any academic misconduct has occurred.

Appendix F: Supervisor Approval Form

OPEN UNIVERSITY OF KENYA
School of Science and Technology
Department of Computing and Informatics

RESEARCH THESIS SUPERVISOR APPROVAL FORM

Candidate Name: Timothy Kosgei

Registration Number: ST63/80222/2024

Programme: Master of Science in Cybersecurity and Digital Forensic

Thesis Title: Developing a Digital Forensic Readiness Framework for Incident Response in Smart City Ecosystems: A Case Study of Konza Technopolis, Kenya

Date of Submission: 16/10/2026

Supervisor Declaration

I confirm that I have reviewed the above-named research thesis and that it meets the minimum academic standards required for submission for examination at the Open University of Kenya. I am satisfied with:

- the clarity and significance of the research problem;
- the alignment of objectives, research questions, and methodology;
- the appropriateness of the proposed literature review;
- compliance with OUK ethical and formatting requirements.

Signature:  Date: 16/10/2026

Dr. Peter Ngaira
Department of Computing and Informatics
Open University of Kenya

Departmental Endorsement

Signature: ..... Date: .....

[Name of Chair of Department]
Chairperson, Department of Computing and Informatics
Open University of Kenya.