DEVELOPMENT OF AN INTEGRATED SECURITY MAINTENANCE TRACKING SYSTEM (ISMS) FOR SECURITY FIRMS IN NAIROBI COUNTY

MUCHIRI ESTHER WAMBUI

A THESIS SUBMITTED TO THE SCHOOL OF SCIENCE AND TECHNOLOGY IN PARTIAL FULFILLMENT FOR THE REQUIREMENT OF THE DEGREE OF MASTER OF SCIENCE IN COMPUTER INFORMATION SYSTEM AT KENYA METHODIST UNIVERSITY

JUNE 2026

DECLARATION AND RECOMMENDATION

This thesis is my original work and has not been presented in any other university.

Signed Date:

.....

ESTHER WAMBUI MUCHIRI

CIS-3-2547-2/2022

RECOMMENDATION

This Thesis has been submitted for examination with our approval as university supervisors.

Signed : Date:

.....

Mr. Patrick Kinoti

Kenya Methodist University

Signed: Date:

.....

Mr. Joel Charo

Kenya Methodist University

COPYRIGHT

©2026 Muchiri Esther Wambui

All rights Reserved. No part of this work may be reproduced or transmitted in any form by any means, electronically or mechanically, including photocopying by any information storage or retrieval media without the express permission of the author or Kenya Methodist University, on that behalf.

DEDICATION

Dedicated to my mother Tabitha Muringi and my family for their support and love throughout the whole academic journey.

ACKNOWLEDGEMENT

I would like to express my sincere gratitude to my supervisors, Mr. Patrick Kinoti and Mr. Joel Charo, for their guidance, valuable feedback, and encouragement throughout this study.

My appreciation also goes to the participating security firms in Nairobi County for their cooperation and willingness to share information that contributed significantly to this research. I am grateful to the Kenya Methodist University (KeMU) Library for providing access to relevant academic resources and guidance on acceptable research and formatting standards.

Special thanks to my classmates and colleagues, particularly Erasto Oraro, Stephen Ario, Zipporah Momanyi, Ciza Cikambazi, and Rukia Shariff, as well as many others with whom I interacted during my studies, for their support, encouragement, and insightful academic discussions. I also acknowledge the faculty and staff of the School of Computing and Informatics for their assistance and commitment to academic excellence.

I am deeply thankful to my colleagues, friends, and family for their patience, understanding, and unwavering support throughout this journey.

Above all, I thank Almighty God for His grace, strength, wisdom, and guidance, which enabled me to successfully complete this study.

ABSTRACT

The growing reliance on integrated security technologies in Kenya necessitates robust maintenance of Integrated Security Management Systems (ISMS) to ensure operational continuity and resilience. This study, guided by the Design Science Research (DSR) paradigm, drew upon General Systems Theory (GST), the Technology Acceptance Model (TAM), and Total Productive Maintenance (TPM) theory to examine maintenance practices within Nairobi's private security sector and to develop a digital ISMS Maintenance Tracking System. The system comprises modules for role-based login, client and premises management, task assignment with Service Level Agreement (SLA) tracking, automated audit logging, and email notifications, all accessible via a mobile-first interface that supports offline operation for field technicians. The target population comprised ICT managers in registered private security firms in Nairobi County. A stratified purposive sample of 90 respondents was drawn, and 63 valid responses were analyzed using descriptive statistics, correlation, and multiple regression. Findings revealed that current maintenance practices were weak and significantly negatively impacted system effectiveness ($B = -0.893$, $p < .001$). Conversely, established best practices such as preventive scheduling, accountability, and real-time monitoring showed a strong positive relationship with effectiveness ($B = 0.815$, $p < .001$). A combined model explained 75% of the variance in system effectiveness (Adj. $R^2 = 0.741$, $p < .001$), demonstrating that integrating best practices into an automated system substantially enhances performance. User Acceptance Testing (UAT) confirmed the system's efficacy, with 100% of users affirming login and notification functionality, 95% rating task assignment as very easy, and 90% describing the system as user-friendly. The study concludes that automating structured best practices can overcome the limitations of current fragmented approaches. It recommends the adoption of ISMS tracking tools aligned with ISO/IEC 27001:2022 and Kenya's Private Security Regulation Act (2016) and suggests further research into sector-wide scaling and predictive analytics integration.

TABLE OF CONTENTS

DECLARATION AND RECOMMENDATION ..... **ii**

COPYRIGHT ..... **iii**

DEDICATION ..... **iv**

ACKNOWLEDGEMENT ..... **v**

ABSTRACT ..... **vi**

LIST OF TABLES ..... **x**

LIST OF FIGURES ..... **xi**

LIST OF ABBREVIATIONS ..... **xiii**

CHAPTER ONE **1**

INTRODUCTION AND BACKGROUND TO THE STUDY **1**

1.0 Background of the study 1

1.2 Statement of the problem 7

1.3 Aim of the study 8

1.4 Main Objective 9

1.5 Specific Objectives 9

1.6 Research Questions 9

1.7 Justification of the study 10

1.8 Limitations of the study 11

1.9 Delimitations of the Study 12

1.10 Significance of the Study 13

1.11 Assumptions of the Study 16

1.12 Operational Definition of Terms 17

1.13 Summary 21

CHAPTER TWO **22**

LITERATURE REVIEW **22**

2.1 Introduction 22

2.2 Theoretical Foundations of the Study 22

2.3 Empirical Literature Review 29

2.4 Summary of research gaps 42

2.5 Conceptual framework 43

2.6 Summary 45

CHAPTER THREE 47

RESEARCH METHODOLOGY 47

3.1 Introduction 47

3.2 Research Design 47

3.3 Location of the study 48

3.4 Target Population 49

3.5 Sampling Procedure and Sample Size 50

3.6 Research Instrumentation 52

3.7 Data Collection 54

3.8 Operational Definition of Variables 56

3.9 Data Analysis 56

3.10 Summary 66

CHAPTER FOUR 68

RESULTS AND DISCUSSIONS 68

4.1 Introduction 68

4.2 Response Rate and Demographic Information 68

4.3 Current ISMS Maintenance Practices and Tracking Mechanisms 75

4.4 Best Practices in ISMS Maintenance and Tracking. 82

4.5 System Effectiveness (Dependent Variable) 90

4.6 System Analysis, Design and Architecture..... 100

4.7 System Implementation and Validation..... 117

4.8 Chapter Summary 126

CHAPTER FIVE 127

SUMMARY, CONCLUSIONS AND RECOMMENDATIONS 127

5.1 Introduction..... 127

5.2 Summary of findings 127

5.4 Conclusions..... 131

5.5 Recommendations..... 133

REFERENCES.....141

APPENDICES.....152

APPENDIX 1: RESEARCH QUESTIONNAIRE 152

APPENDIX II: SYSTEM EVALUATION CHECKLIST 155

APPENDIX III: KeMU INTRODUCTION LETTER TO NACOSTI..... 157

APPENDIX V – NACOSTI RESEARCH LICENSE 160

LIST OF TABLES

Table 2.1: Summary of Empirical Studies, Gaps, Findings, and Application 42

Table 3.1: Target Population 50

Table 3.3: Sampling of Respondents by Firm Size 52

Table 3.4: Operational Definition of Variables 56

Table 3.5: Entity Relationship Diagram Key Terms 62

Table 3.6: Integrated Tools & Technologies for ISMS 65

Table 4.1: Descriptive Statistics for Current ISMS Maintenance Practices 76

Table 4.2: Correlation between Current ISMS Maintenance Practices 78

Table 4.3: Regression Model Summary Analysis 79

Table 4.4: ANOVA Test Results 80

Table 4.5: Regression Coefficients Test Results 81

Table 4.6: Descriptive Statistics for Recognized Best Practices 83

Table 4.7: Correlation test results 85

Table 4.8: Regression Model Summary Results 86

Table 4.9: Anova Analysis Results 87

Table 4.10: Regression Coefficient Test Results 88

Table 4.11: Descriptive Statistics for System Effectiveness 90

Table 4.12: Multiple Linear Regression Results 93

Table 4.13: ANOVA Results for Multiple Regression 96

Table 4.14: Joint Regression coefficients Results 98

Table 4.15: Consolidated User Responses on System Usability 122

Table 4.16: Functional Testing Results 124

LIST OF FIGURES

Figure 2.1: Constructs of General Systems Theory Applied to ISMS Maintenance 24

Figure 2.2: Constructs of the Technology Acceptance Model 26

Figure 2.3: Total Productive Maintenance Theory 28

Figure 2.4: Conceptual Framework 44

Figure 3.1: Study Location - Nairobi County Map..... 49

Figure 3.2: System Architecture/Data Flow Diagram (DFD)..... 60

Figure 3.3: Flowchart illustrating the core maintenance task workflow 61

Figure 3.4: Entity-Relationship Diagram (ERD) 62

Figure 4.1: Gender distribution..... 71

Figure 4.2: Age Distribution 72

Figure 4.3: Education Levels 73

Figure 4.4: Years of Experience..... 74

Figure 4.5: Size of the Firm 75

Figure 4.6: Login Module 107

Figure 4.7: Welcome page 108

Figure 4.8: Client and Premises Management 109

Figure 4.9: Project Management.....110

Figure 4.10: Personnel Management 111

Figure 4.11: Site and Installation Definition.....112

Figure 4.12: Equipment Planning and Tracking 113

Figure 4.13: Audit Module 114

Figure 4.14: Notification Module 115

Figure 4.15: Database Design.....116

LIST OF ABBREVIATIONS

AI	Artificial Intelligence
API	Application Programming Interface
AWS	Amazon Web Services
BM	Bob Morgan Security
CCTV	Closed-Circuit Television
DSR	Design Science Research
ERD	Entity Relationship Diagram
ERP	Enterprise Resource Planning
HTML	Hypertext Markup Language
ICT	Information and Communication Technology
IDE	Integrated Development Environment
IIoT	Industrial Internet of Things
IoT	Internet of Things
ISMS	Integrated Security Management System
IT	Information Technology
JKIA	Jomo Kenyatta International Airport
JSON	JavaScript Object Notation
KNH	Kenyatta National Hospital
KPA	Kenya Ports Authority
NITDA	National Information Technology Development Agency
ORM	Object-Relational Mapping
PHP	Hypertext Preprocessor
PSF	Private Security Firms
SLA	Service Level Agreement
SMEs	Small and Medium Enterprises
SQL	Structured Query Language
TPM	Total Productive Maintenance
UAT	User Acceptance Testing
UI	User Interface
UK	United Kingdom
UML	Unified Modeling Language
UoN	University of Nairobi
USA	United States of America
XML	Extensible Markup Language

CHAPTER ONE

INTRODUCTION AND BACKGROUND TO THE STUDY

1.0 Background of the study

This chapter introduces the study by providing the background and context of Integrated Security Management Systems [ISMS] maintenance within the security sector. It outlines the key challenges facing security firms in Nairobi County, including fragmented maintenance processes, lack of real-time tracking, and limited compliance readiness

Globally, adoption of structured information-security management systems has expanded as organizations aim to formalise risk management and comply with recognized standards such as ISO/IEC 27001. Organizations implementing ISO/IEC 27001 often report improvements in their security posture, operational procedures, and compliance readiness (Jevelin & Faza, 2023). To support ongoing security governance and maintenance, many organizations complement their ISMS with automated tracking and monitoring tools, facilitating continual risk assessment, control monitoring, and documentation of changes practices encouraged under ISO/IEC 27001's risk-management and control framework (Domínguez et al., 2023). Empirical work also shows that integrating maintenance tracking into ISMS helps identify gaps in controls and supports timely remediation, which enhances long-term security resilience and governance performance (Niemeläinen et al., 2025). Consequently, developing an automated ISMS Maintenance Tracking System aligns with global best practices: it supports a systematic, auditable approach to security operations, enables

continuous monitoring and updates, and helps organizations adapt to evolving threats and compliance requirements.

The rise of sophisticated threats to data, infrastructure, and personnel in an increasingly digital world elevated the importance of Integrated Security Management Systems (ISMS) globally. These systems provide solutions that combine physical security, cybersecurity, operational protocols, and compliance monitoring to ensure the safety and resilience of organizations (International Organization for Standardization [ISO], 2022). Effective ISMS implementation depended not only on the integration of technologies but also on consistent and well-structured maintenance. This entailed regular updates, real-time monitoring, performance audits, and adherence to predefined security protocols. Without such structured tracking, organizations became vulnerable to operational lapses that resulted in financial losses, regulatory breaches, and reputational harm (Grobler & Von Solms, 2021a).

According to the latest global survey of ISO management-system certifications, the number of valid certificates for ISO/IEC 27001 has risen, indicating that organizations across different sectors continue to adopt formal ISMS frameworks (ISO 2024). To operationalize information-security governance and support real-time threat detection, many organizations deploy Security Information and Event Management (SIEM) systems. A comprehensive review found that SIEM - Security Information and Event Management tools remain widely used in critical-infrastructure and enterprise contexts to enable event aggregation, correlation, log analysis and incident detection, key components of a live security operations posture (González-Granadillo et al., 2021). However, the same review cautions that SIEM deployments often require substantial

customization, ongoing maintenance, and skilled personnel to remain effective underscoring that success depends heavily on organizational context and resource availability (González-Granadillo et al., 2021).

Regionally, many African small and medium-sized enterprises (SMEs) face significant challenges in implementing and maintaining robust information security practices. A recent continent-wide study found that SMEs across Nigeria, Kenya, and South Africa are often under-prepared for cybersecurity threats: many rely on ad-hoc tools, have minimal staff training, and lack formal incident-response mechanisms (Egwuatu, 2025). In South Africa, a detailed investigation among SMEs revealed that limited budgets, lack of cybersecurity expertise, and weak policy implementation create substantial barriers to effective security control adoption (Fakir, 2024). In Southern Africa, research among small-scale migrant traders showed that many transact digitally without adequate cybersecurity awareness or protective measures exposing them to hacking, phishing, and other vulnerabilities (Kariuki et al., 2023). These findings reflect a pattern: although there is rising awareness of cybersecurity across the region, the practical implementation and lifecycle maintenance of ISMS-like practices remain weak or inconsistent particularly among SMEs and informal businesses (Chingoriwo, 2022; Mohamed & Kamau, 2023).

In Kenya, demand for ISMS increased due to rapid urbanisation, the digitisation of public services, and the evolving nature of security threats. Nairobi County, which hosts the country's highest concentration of security firms, presented complex security challenges that required integrated responses. Empirical evidence indicated that most firms in the region lacked structured systems for monitoring and managing ISMS

maintenance. This gap led to service delivery disruptions, compliance failures with Service Level Agreements (SLAs), and increased security risks.

Among the key players in this sector, Magal Security Systems Limited Kenya emerged as a global leader with a local presence since 2010. The firm implemented large-scale security solutions for strategic institutions, including the Parliament of Kenya, Kenya Ports Authority, KenGen, and major airports such as Jomo Kenyatta International Airport and Wilson Airport. Its portfolio integrated biometric access controls, intrusion detection systems, command and control platforms, environmental monitoring, and advanced cybersecurity technologies. However, despite its robust infrastructure, the company still faced challenges related to maintaining these systems efficiently and consistently across its projects.

Other prominent Nairobi-based firms including Securex Agencies Ltd, Glosec Security Limited, SGA Kenya, Bob Morgan Security (BM), Glosec Systems, Wells Fargo, and Radar Security offered a range of ISMS-related services. These included CCTV, biometric identification, perimeter surveillance, and access control. However, many continued to rely on fragmented or semi-manual tracking systems, which compromised data accuracy, performance consistency, and audit readiness (Kuria & Kagiri, 2023). Including these companies in the validation phase of the study provided a diverse testbed for assessing system usability, relevance, and scalability.

This study designed and validated an ISMS Maintenance Tracking System specifically tailored to the operational needs of Kenyan security firms. The system automated critical tracking and reporting functions, thereby enhancing interdepartmental

coordination, reducing incident response times, and supporting compliance with Kenya's (Private Security Regulation Act 2016).

A key innovation of the ISMS Maintenance Tracking System was its embedded knowledge-based decision support engine. Unlike conventional systems that primarily served as data repositories, this feature actively supported security managers in making timely and informed decisions. It provided contextual recommendations based on real-time system status, generated automated alerts for non-compliance or overdue maintenance, and offered access to a curated repository of best practices, incident response protocols, and regulatory guidelines.

This module continuously updated with insights drawn from international standards such as ISO/IEC 27001:2022 and ISO/IEC 20000-1:2018, as well as national legislation including Kenya's (Private Security Regulation Act 2016). By aligning decision-making processes with both global and local compliance requirements, the system reduced reliance on external consultants and minimized the risk of human error. Furthermore, it enhanced institutional knowledge retention, enabling organizations to respond more effectively to audits, incidents, and evolving security threats (ISO, 2018, 2022; Kenya Law, 2016).

To address the operational realities of Nairobi's security sector, where field personnel were often the first to encounter system faults, the system incorporated a mobile-first interface. This feature enabled technicians' supervisors to log maintenance activities and incidents in real time, capture and upload multimedia evidence such as photographs of faulty equipment, receive task notifications and compliance reminders, and access quick-reference guides from the embedded knowledge base.

By facilitating data capture at the point of activity, the mobile interface significantly improved the accuracy and timeliness of maintenance records. It also enhanced operational transparency by incorporating timestamped and geotagged entries, which were essential for audit trails and regulatory compliance. This approach represented a substantial improvement over the fragmented and semi-manual tracking methods previously employed by many Nairobi-based security firms. By combining intelligent decision support with mobile accessibility, the system streamlined ISMS maintenance processes and fostered a culture of proactive security governance. Deficiencies in preventive maintenance frequently resulted in delayed interventions and elevated security risks, while shortcomings in corrective maintenance such as unstructured incident management led to prolonged system vulnerabilities and costly service disruptions.

Contemporary research highlighted the transformative role of automation and data-driven decision-making in enhancing the reliability, efficiency, and compliance of ISMS implementations. These technologies streamlined operations, reduced dependence on manual tracking, and promoted consistency in maintenance reporting and response protocols (Grobler & Von Solms, 2021b). Despite these advantages, such innovations had not been widely adopted by private security firms in Nairobi County, many of which continued to operate using semi-manual methods prone to error and delay.

This study therefore addressed the prevailing challenges in ISMS maintenance by analyzing the tracking methods employed by security firms in Nairobi. The research evaluated the capabilities and limitations of these systems, identified key performance

and compliance gaps, and benchmarked findings against internationally recognised best practices, including those outlined in ISO/IEC 27001:2022 and ISO/IEC 20000-1:2018 (ISO, 2018, 2022). The study developed an ISMS Maintenance Tracking System to streamline critical tasks such as real-time activity tracking, compliance monitoring, reporting, and invoicing. It integrated both preventive and corrective maintenance protocols, enabling timely fault detection, structured response workflows, and improved oversight of physical and cybersecurity infrastructure.

1.2 Statement of the problem

Information Security Management Systems (ISMS) are increasingly used by organizations to protect information assets, ensure regulatory compliance, and support business continuity. International standards such as ISO/IEC 27001:2022 and ISO/IEC 20000-1:2018 emphasize continuous monitoring, documentation, maintenance, and improvement to ensure that security controls remain effective throughout their lifecycle. Emerging technologies such as automation, intelligent maintenance systems, predictive analytics, and cloud-based monitoring platforms have further strengthened organizations' ability to manage ISMS proactively rather than reactively (Bokrantz et al., 2020; Okpeke et al., 2024).

Despite these advancements, many organizations in developing countries continue to experience difficulties maintaining ISMS after implementation. Within Kenya's private security sector, maintenance activities are often characterized by fragmented processes, manual record keeping, inconsistent monitoring, delayed fault resolution, and weak coordination across departments. Critical functions such as preventive maintenance scheduling, audit trail management, compliance documentation, and

maintenance reporting remain inadequately supported, resulting in poor visibility, weak accountability, and increased operational risk (Mutinda & Wabwoba, 2023).

Existing studies have identified several factors contributing to these challenges, including fragmented information environments, limited technical capacity, inadequate management support, and low adoption of digital maintenance solutions (Grenefalk & Wallin, 2023; Mutinda & Wabwoba, 2023). While previous research has examined ISMS implementation, compliance, governance, and technology adoption, limited attention has been given to the practical mechanisms required to support routine ISMS maintenance activities. Most studies focus on implementation and policy issues rather than the design and evaluation of systems that support maintenance planning, monitoring, accountability, and compliance management.

Consequently, a significant knowledge and practice gap exists. Private security firms in Nairobi County lack integrated tools for managing ISMS maintenance, while empirical evidence on the development and evaluation of purpose-built ISMS maintenance tracking systems remains limited. This study therefore sought to design, develop, and evaluate an ISMS Maintenance Tracking System tailored to private security firms in Nairobi County to improve maintenance effectiveness, compliance readiness, accountability, and organizational resilience.

1.3 Aim of the study

The aim of this study was to design, develop, and validate an ISMS Maintenance Tracking System tailored to the operational environment of security firms in Nairobi County. The system was intended to address challenges in maintenance tracking such as delayed preventive maintenance, fragmented workflows, inefficient incident

resolution, and regulatory non-compliance by introducing a centralized and automated platform for real-time monitoring, compliance oversight, incident logging, and structured reporting.

1.4 Main Objective

To develop an ISMS maintenance tracking system for security firms by analyzing existing solutions processes, evaluating current tracking methods, identifying industry's best practices, and validating the proposed system.

1.5 Specific Objectives

The objectives of the study were to:

1. Examine the current ISMS maintenance practices and tracking mechanisms employed by security firms within Nairobi County.
2. Investigate internationally and locally recognized best practices related to ISMS maintenance tracking systems.
3. Design and develop an automated ISMS Maintenance Tracking System tailored to the operational needs of security firms.
4. Validate the proposed system in selected security firms within Nairobi County.

1.6 Research Questions

1. What ISMS maintenance practices and tracking mechanisms are currently employed by security firms within Nairobi County, and what challenges do they face in their implementation?

2. What internationally and locally recognized best practices exist for ISMS maintenance tracking systems, and how can they inform improvements in current practices?
3. What system features and design considerations are essential for developing an effective automated ISMS Maintenance Tracking System tailored to the operational needs of security firms?
4. How effective, usable, and scalable is the proposed ISMS Maintenance Tracking System when implemented in selected security firms within Nairobi County?

1.7 Justification of the study

Extensive research has examined information security management within Kenyan organizations, with many studies focusing on broad issues such as policy adoption, organizational awareness, and compliance readiness (Wabwoba & Wanyembi, 2015). Existing investigations, including kitheka (2013) on ISMS implementation gaps in public universities and Kamau (2021) on data breach mitigation in Kenyan banks, consistently highlight the importance of structured security practices. While informative, this body of work has predominantly emphasized policy and governance issues at the expense of the operational and maintenance processes that ensure continuous system reliability.

Specifically, empirical literature has paid limited attention to how organizations manage preventive and corrective maintenance, real-time monitoring, and audit traceability for integrated security systems. Although ISMS adoption and compliance have been widely documented in Kenya (Njenga & Njuki, 2018), the maintenance domain remains underexplored, despite its centrality to sustaining effective security

operations. Similarly, research on information security controls often remains descriptive, offering recommendations without providing validated, context-appropriate tools that address the workflow and documentation challenges experienced by private security firms (Kamau, 2021). This gap is particularly evident within Nairobi's private security sector, where firms deploy complex integrated systems such as CCTV networks, biometric access control, and alarm systems yet demonstrate limited capacity to track maintenance activities, document system health, or ensure audit readiness.

This study is therefore justified on three grounds. First, it advances scholarship by shifting attention from policy-level ISMS issues to the operational dimensions of maintenance, monitoring, and documentation, which remain underrepresented in the current literature. Second, it provides empirical, sector-specific evidence on the maintenance challenges faced by private security firms in Nairobi County, addressing a gap where little contextualized research exists. Finally, it offers a practical and validated ISMS Maintenance Tracking System that moves beyond theoretical recommendations toward a functional solution designed to enhance reliability, accountability, and compliance within integrated security environments.

1.8 Limitations of the study

This study faced three key limitations related to context, content, and responses.

First, the study context involved private security firms, which operate in extremely sensitive environments. Because of the confidential nature of ISMS operations, some firms were cautious in providing full details about their maintenance practices. To

overcome this, anonymity and strict data confidentiality were assured to participants, which encouraged greater openness and improved the quality of responses.

Second, content limitations arose because ISMS maintenance covers both physical and cyber domains, yet the study focused primarily on practices that could be quantified and tested within the developed system. This narrowed scope may have excluded certain qualitative insights. To mitigate this, the study concentrated on measurable indicators such as preventive scheduling, task tracking, and notifications that directly influence effectiveness and compliance.

Third, response-related limitations occurred during data collection. Although questionnaires were distributed to ICT managers across 63 firms, some respondents provided incomplete or cautious responses. This was addressed by conducting thorough checks on returned questionnaires and following up with respondents where clarification was needed. As a result, a high response rate was achieved, and sufficient valid data were obtained for analysis.

Overall, while these limitations affected the study to some degree, they were effectively managed to ensure that the findings remained reliable, valid, and relevant to the operational realities of private security firms in Nairobi.

1.9 Delimitations of the Study

This study was delimited to registered private security firms operating within Nairobi County. The choice of Nairobi was deliberate, given its high concentration of security firms and its representation of complex security environments. While this provided rich insights into ISMS maintenance practices within the county, it limited the generalizability of findings to other regions in Kenya or to sectors with different operational or regulatory frameworks.

The study also focused exclusively on ISMS maintenance tracking practices that could be quantified and automated within the developed system, such as preventive scheduling, incident logging, notifications, and compliance monitoring. Broader organizational or qualitative aspects of security management were outside the study's scope.

Recent methodological research warns that findings from context-specific studies may not always generalize across different populations, regions, or sectors, especially when local conditions, compliance requirements, and infrastructure vary significantly (Degtiar & Rose, 2023; Deliosa et al., 2022). As such, even though the system was designed to be scalable and adaptable, its broader applicability may require validation in other regions and sectors.

1.10 Significance of the Study

This study generated practical, theoretical, and policy insights by addressing the persistent gaps in ISMS maintenance among private security firms in Nairobi. The findings are significant to policymakers, private security firms, clients, and researchers.

1.10.1 Policy Makers and Regulators

The study provides evidence to inform the work of regulatory agencies such as the Communications Authority of Kenya (CAK), the Office of the Data Protection Commissioner (ODPC), and the Private Security Regulatory Authority. Specifically, the findings will:

Strengthen Policy Formulation - Provide empirical justification for embedding automated maintenance tracking, audit logging, and compliance monitoring into national security regulations.

Guide Enforcement - Support the development of compliance checklists aligned with ISO/IEC 27001:2022 and the (Private Security Regulation Act 2016).

Shape Incentives - Encourage the creation of industry-wide incentives, such as recognition awards and compliance-linked accreditation, to motivate firms to adopt ISMS maintenance tracking systems.

1.10.2 Private Security Firms

For security firms operating in Nairobi, the developed ISMS Maintenance Tracking System provides a practical tool to strengthen their operations. The study's findings translate into actionable benefits such as:

Operational Efficiency - By automating preventive scheduling, task assignment, and notifications, firms reduce downtime and enhance service reliability.

Improved Accountability - Audit logs and structured reporting increase transparency in workflows and build institutional accountability.

Capacity Building - The results highlight the importance of training ICT managers and staff in using ISMS systems, ensuring smooth adoption and sustainability.

1.10.3 Clients of Security Firms

Clients who rely on outsourced security services such as corporations, government agencies, and critical infrastructure providers also benefit from the outcomes of this study. The findings demonstrate that:

Service Assurance - Firms using structured ISMS maintenance achieve higher compliance with Service Level Agreements (SLAs), ensuring reliable delivery service.

Risk Reduction - Real-time maintenance tracking reduces vulnerabilities, thereby protecting client assets and reputations.

Increased Confidence - The adoption of a tested ISMS system enhances client trust and strengthens the reputation of private security firms.

1.10.4 Researchers and Academics

The study makes a distinct contribution to the academic body of knowledge on ISMS in emerging economies, particularly within Africa. Its significance includes:

Theoretical Contribution - Extending ISMS literature by demonstrating how maintenance tracking, decision support, and automation improve effectiveness in private security firms.

Methodological Contribution - Providing validated quantitative evidence through correlation and regression analysis, offering a foundation for future empirical research.

Foundation for Further Studies - Opening opportunities for comparative research across other sectors such as healthcare and finance, and for exploring advanced technologies like AI and blockchain in ISMS maintenance.

1.11 Assumptions of the Study

This study was guided by the following assumptions:

Existence of ISMS Infrastructure: It was assumed that the selected private security firms in Nairobi County had some form of Integrated Security Management Systems (ISMS), even if these systems were fragmented, semi-manual, or irregularly maintained.

Participant Response: It was assumed that ICT managers, system administrators, and compliance staff who participated in the study provided truthful and accurate responses to the questionnaires and system validation activities.

Contextual Relevance: The study assumed that the variables under investigation current ISMS maintenance practices, best practices in ISMS maintenance tracking, and system effectiveness were relevant and influential in determining the overall performance of ISMS within private security firms in Nairobi.

Regulatory and Technological Stability: It was assumed that the legal and technological environment, particularly the enforcement of the Private Security Regulation Act (2016) and the availability of international ISMS standards, remained stable throughout the study period, ensuring alignment with regulatory frameworks (ISO, 2022; Kenya Law, 2016).

Availability of Infrastructure: It was assumed that the participating firms had the basic technological infrastructure such as internet access and mobile devices necessary to test and validate the mobile-first, data-driven ISMS Maintenance Tracking System (Emmanouilidis et al., 2009).

1.12 Operational Definition of Terms

This section provides operational definitions for key terms used throughout the study. These definitions clarify the scope and application of concepts related to the design, development, and evaluation of an Integrated Security Management System (ISMS) Maintenance Tracking System for security firms within Nairobi County.

Automated ISMS Maintenance Tracking System: A software-based solution designed to systematically monitor, schedule, and report on ISMS-related maintenance activities. This includes preventive and corrective maintenance, incident resolution, team coordination, and invoicing. The system aims to enhance transparency, accuracy, and compliance through automation.

Corrective Maintenance: Actions taken to repair or restore a system component that has malfunctioned or failed. It includes on-site interventions, equipment replacement, or reconfiguration of digital systems.

Critical Failure: A severe malfunction that renders one or more ISMS components non-functional, including systems like CCTV, access control, intrusion detection, or command and control platforms. Such failures demand immediate attention to restore operations.

Data Loss Prevention (DLP): Security protocols and tools aimed at ensuring sensitive data is not lost, misused, or accessed by unauthorized individuals. It typically includes encryption, backup, and access control mechanisms.

Defect Liability Period (DLP): A specified post-installation period during which the contractor is obligated to rectify faults or deficiencies in the installed security systems at no extra cost.

Incident Management: A structured process for identifying, reporting, analyzing, and resolving security events to minimize impact and prevent recurrence. Incident management is a core component of ISMS operations and audit readiness.

Integrated Security Management System (ISMS): A coordinated system that integrates physical security controls, cybersecurity measures, and organizational policies to protect information assets, personnel, and infrastructure. It ensures the implementation of risk assessments, incident responses, and compliance with standards such as ISO/IEC 27001:2022 (ISO, 2022).

Invoicing Module: A feature within the ISMS tracking system that automates billing processes based on logged maintenance activities, service durations, and SLA compliance. It enhances accuracy and reduces delays in revenue collection.

ISO/IEC 20000-1:2018: A service management standard that outlines best practices for delivering managed services, particularly IT-related services, to ensure quality and efficiency (ISO, 2018).

ISO/IEC 27001:2022: An international standard specifying requirements for establishing, implementing, maintaining, and improving an information security management system (ISO, 2022).

Knowledge-Based Decision Support: An intelligent system component that uses curated data, incident patterns, and regulatory rules to offer recommendations, flag issues, and support real-time decision-making by security managers (Morrison et al., 2023).

Maintenance Team: A designated group within the security firm responsible for the execution of ISMS maintenance tasks, including inspections, repairs, and technical support. The team operates in compliance with SLAs and internal policies.

Mean Time Between Failures (MTBF): A metric used to predict the average time between successive failures of a system or component during normal operations. It is a key reliability indicator (Ittmann, 2018).

Mobile-First Interface: A system design approach prioritizing mobile access, allowing field technicians to log data, upload media, and receive alerts on portable devices. This improves timeliness and operational accuracy (Kuria & Kagiri, 2023).

Non-Critical Failure: A minor system issue that impacts performance but does not immediately compromise overall security. These failures are manageable through scheduled corrective actions or temporary workarounds.

Preventive Maintenance: A proactive approach to system maintenance involving scheduled inspections, updates, and routine checks to identify potential issues before they result in system failure. It supports operational continuity and risk reduction (Emmanouilidis et al., 2009).

Real-Time Monitoring: Continuous observation of ISMS components to track system health, detect anomalies, and generate immediate alerts. This supports rapid decision-making and improved incident response (Grobler & von Solms, 2021a).

Reporting and Historical Data Tracking: A functionality that supports the archiving, retrieval, and analysis of past maintenance activities, incident reports, and audit logs for performance evaluation and compliance documentation.

Role-Based Access Control (RBAC): A security mechanism that grants system access based on predefined user roles, limiting exposure to sensitive data and functionalities.

Service Level Agreement (SLA): A contractual agreement outlining expected performance levels, maintenance response times, system uptime, and other service quality metrics between a service provider and its clients (ISO/IEC 20000-1:2018).

Team Coordination: The process of synchronizing the efforts of ISMS maintenance personnel to ensure tasks are executed efficiently, resources are utilized optimally, and service disruptions are minimized.

Third-Party Dependency: Reliance on external vendors for equipment, technical support, or software solutions. This dependency introduces operational risks and compliance challenges.

User Acceptance Testing (UAT): The final phase of system testing in which end-users evaluate the software to confirm that it meets their functional and usability expectations.

1.13 Summary

In conclusion, Chapter 1 established the need for a robust ISMS Maintenance Tracking System in Nairobi's security firms. It outlined current operational and regulatory challenges, including fragmented records, reactive maintenance, and limited automation. The chapter also defined the study's objectives and research questions, grounded in global standards and local regulations. By proposing a context-sensitive automated solution, it laid the foundation for the literature review, theoretical frameworks, and system design strategies that follow.

CHAPTER TWO

LITERATURE REVIEW

2.1 Introduction

An Information Security Management System (ISMS) integrates people, processes, and technologies to safeguard an organization's information assets in line with global standards such as ISO/IEC 27001:2022. Effective ISMS maintenance ensures that implemented controls remain functional, auditable, and responsive to emerging security risks. For private security firms whose operations span both digital and physical infrastructures tracking and maintaining ISMS components is critical to ensuring compliance and service reliability. This chapter reviews theoretical foundations, conceptual models, and empirical studies relevant to ISMS maintenance and tracking. It is organized according to the study's four specific objectives:

1. Examining current ISMS maintenance practices.
2. Investigating internationally and locally recognized best practices.
3. Designing and developing an automated ISMS Maintenance Tracking System; and
4. Validating the proposed system.

The chapter also identifies research gaps and presents the conceptual framework guiding the study.

2.2 Theoretical Foundations of the Study

The theoretical foundation of a study provides the conceptual lens through which the research problem is viewed, guiding the selection of variables, the formulation of

hypotheses, and the interpretation of findings. Without explicit theoretical grounding, a study risks becoming a mere collection of empirical observations lacking explanatory power or generalizability (Creswell & Poth, 2018). For this research, which sought to design, develop, and validate an ISMS Maintenance Tracking System for private security firms in Nairobi, three complementary theories are drawn upon. General Systems Theory (GST) offers a framework for understanding the organization as an integrated whole of interdependent subsystems. The Technology Acceptance Model (TAM) explains how users come to accept and adopt new technology. Total Productive Maintenance (TPM) theory provides principles for proactive, preventive maintenance. Together, these theories address the holistic, human, and process dimensions of the problem, ensuring that the proposed artefact is both theoretically sound and practically relevant.

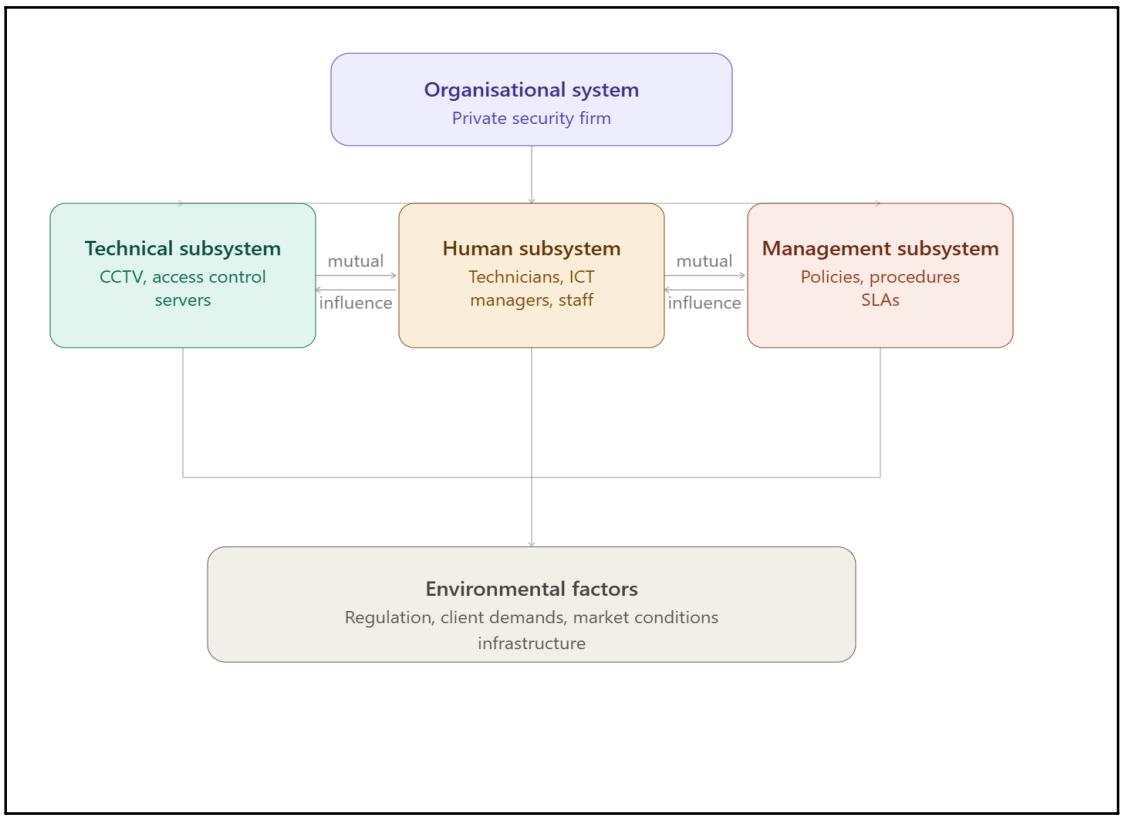
2.2.1 General Systems Theory (GST)

General Systems Theory, originally proposed by von Bertalanffy (1968), conceives of an organization as a set of interconnected subsystems whose interactions produce emergent outcomes that cannot be explained by analysing each subsystem in isolation. Applied to ISMS maintenance, GST suggests that security is not merely a function of technical controls but emerges from the coordinated interaction of technical components, human actors, management processes, and environmental factors. Figure 1 illustrates the core constructs of GST as they apply to ISMS maintenance.

Figure 2.1

.

Constructs of General Systems Theory Applied to ISMS Maintenance



Source: Researcher (2026)

The central principle of GST is that subsystems are interdependent and interact through feedback loops. A failure in one subsystem (e.g., a technician lacking training human subsystem) can propagate to others (e.g., delayed repairs-technical subsystem) and ultimately affect the entire organisation's security posture. Masaev et al. (2025) conceptualised enterprise information security control as a complex dynamic system in which technical measures, organisational processes, and environmental conditions collectively define the overall security state. Their work demonstrates that system stability depends on continuous monitoring and adaptive responses to internal and external changes. Similarly, Tupkalo et al. (2024) proposed a process-oriented

approach to ISMS implementation, arguing that integrating information security into enterprise management workflows ensures that controls and procedures operate coherently rather than in fragmented silos.

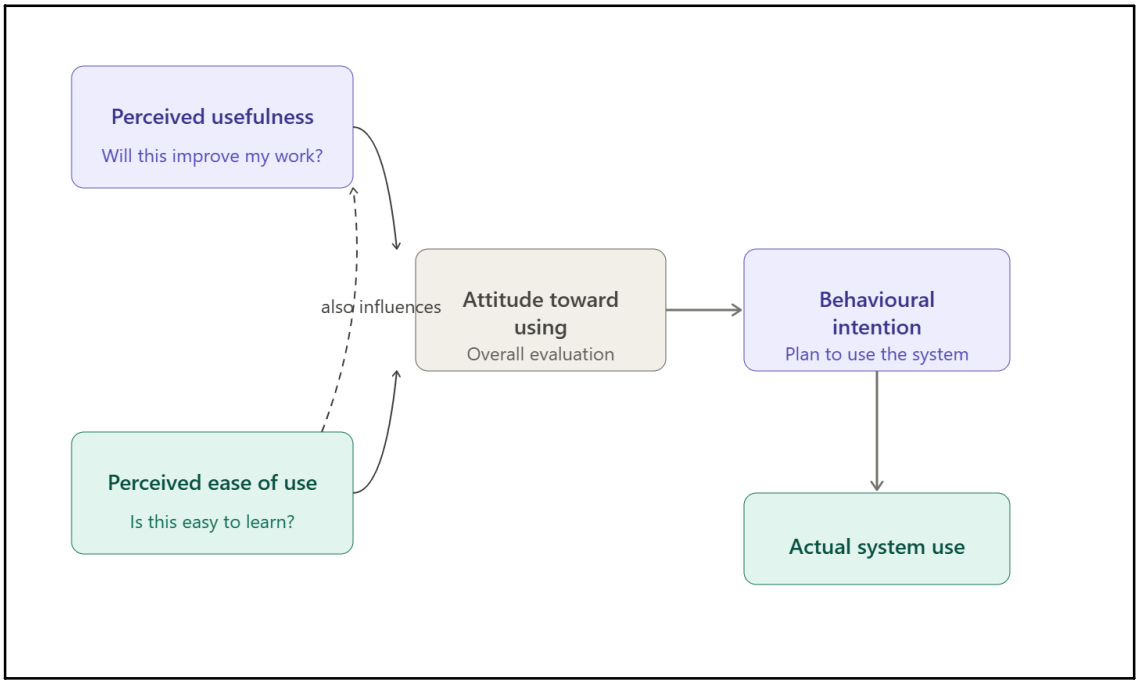
A system-theoretic perspective also informs risk assessment and adaptive response strategies. Poltavtseva et al. (2021) showed that cyber-physical systems benefit from hierarchical, integrative monitoring frameworks that track interactions between structural and behavioural components, allowing timely adaptation to emerging threats. Likewise, Islam et al. (2025) advocated for combining structural and behavioural modelling in cybersecurity risk assessment, capturing how interactions among components can give rise to emergent vulnerabilities that isolated analysis would overlook. Applying GST to the present study means that the proposed ISMS Maintenance Tracking System is not designed as an isolated tool but as a mechanism to integrate maintenance workflows across technical, human, and managerial subsystems, creating feedback loops that support continuous improvement.

2.2.2 Technology Acceptance Model (TAM)

The Technology Acceptance Model, introduced by Davis (1989), explains and predicts user acceptance of information technology. According to TAM, two primary beliefs determine an individual's behavioural intention to use a system: perceived usefulness (the degree to which a person believes that using the system will enhance their job performance) and perceived ease of use (the degree to which a person believes that using the system will be free of effort). These beliefs shape attitudes toward using the system, which in turn influence actual usage. Figure 2 presents the core constructs of TAM.

Figure 2.2

Constructs of the Technology Acceptance Model



Source: Technology Acceptance Model, introduced by Davis (1989)

Recent meta-analyses have confirmed that perceived usefulness and perceived ease of use remain the strongest predictors of technology acceptance across diverse settings (Marikyan et al., 2023; Rosli et al., 2022). However, extended TAM research has shown that contextual variables such as trust, perceived risk, task relevance, and facilitating conditions can significantly improve explanatory power in complex operational environments (Al-Adwan et al., 2023; Liao et al., 2022). For example, field technicians using a mobile maintenance app may be less concerned with abstract usefulness and more concerned with whether the app works offline and protects data integrity.

For the present study, TAM provides a practical foundation for both design and evaluation. The proposed ISMS Maintenance Tracking System is more likely to be

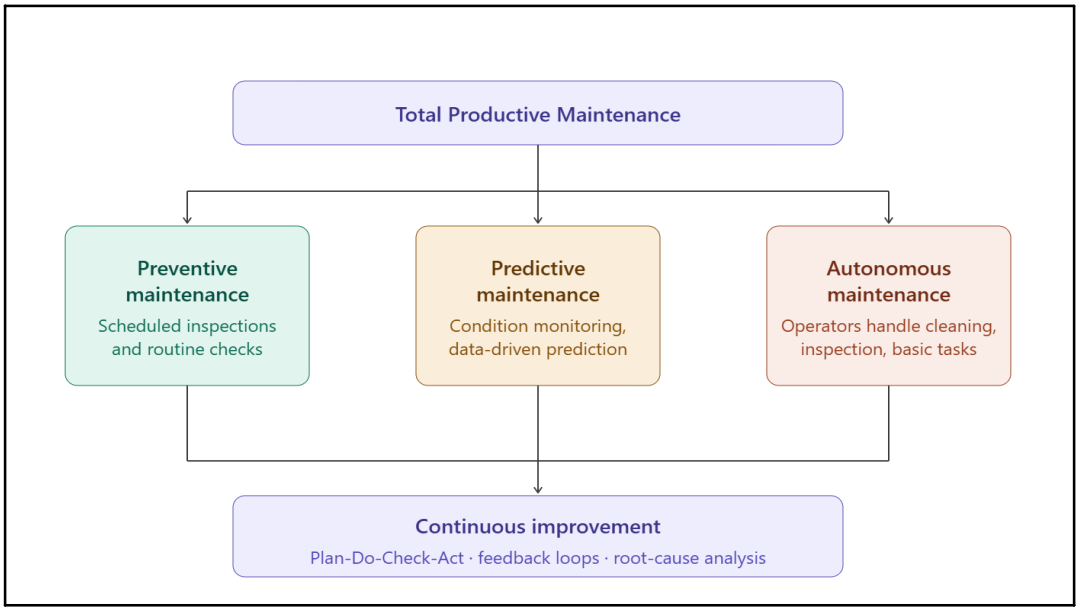
adopted by ICT managers and field technicians if they perceive it as useful (e.g., reducing manual reporting, improving audit readiness) and easy to use (e.g., intuitive interface, minimal clicks, offline capability). The high User Acceptance Testing scores in this study (100% ease for login, 95% for task assignment) directly confirm TAM's predictions. Additionally, the study accounts for contextual variables highlighted in extended TAM research, such as trust in the system's audit trails and the availability of facilitating conditions (local server deployment, offline operation).

2.2.3 Total Productive Maintenance (TPM) Theory

Total Productive Maintenance, developed by Nakajima (1988), is a maintenance philosophy that originated in manufacturing but has since been applied to digital infrastructure management (Wireman, 2021). TPM emphasises proactive, preventive maintenance involving all employees, rather than reactive, breakdown-driven maintenance performed only by specialists. The core constructs of TPM are presented in Figure 2.3.

Figure 2.3

Total Productive Maintenance Theory



Source: Total Productive Maintenance, Nakajima (1988)

TPM's focus on preventive strategies, continuous improvement, and shared responsibility aligns closely with ISMS objectives of ensuring continuous protection and minimal service disruption. While TPM was originally designed for physical assets, its principles have been adapted to digital maintenance. Crespo Márquez (2022) demonstrated that preventive and predictive maintenance yield the greatest returns when moving from a fully reactive state, a finding that directly applies to the low-maturity context of Nairobi's security firms. Prajapati and Nair (2023) reinforced TPM's relevance to digital infrastructure management, showing that predictive analytics and real-time monitoring can pre-empt failures and reduce downtime.

In the present study, TPM informs the design of the ISMS Maintenance Tracking System in three ways. First, the system emphasises preventive maintenance scheduling (task creation, reminders, completion tracking) rather than reactive repair. Second, the

system supports condition-based monitoring through audit logs that record system health indicators. Third, the system enables continuous improvement by maintaining a complete, auditable history of maintenance actions, allowing root-cause analysis of recurring faults.

2.3 Empirical Literature Review

2.3.1 Current ISMS Maintenance Practices and Tracking Mechanisms

The maintenance of an Information Security Management System (ISMS) is a continuous process that ensures security controls remain effective over time. According to ISO/IEC 27001:2022, maintenance involves regular monitoring, reviewing, and updating of security measures to safeguard confidentiality, integrity, and availability of information assets. Park and Lee (2023) note that organizations in highly regulated sectors, such as European financial institutions, have increasingly adopted automated maintenance tools such as Security Information and Event Management (SIEM) platforms. Their study found that firms using centralized and automated monitoring tools reduced their mean time to detect security incidents by an average of 40%. This suggests that the shift from manual checklists to automated systems not only increases efficiency but also enhances overall security responsiveness.

However, the tendency to adopt automated maintenance tools is not universal. Research conducted in developing economies shows that ISMS maintenance still relies heavily on manual and reactive approaches. Mwangi and Ochieng (2022), in a study on Kenyan SMEs, reported that more than 70% of firms track maintenance tasks using physical logbooks or spreadsheets. This manual approach often leads to inconsistent

records, delayed updates, and poor coordination between different departments. Their findings indicate that many organizations only perform maintenance when a problem arises, which contradicts the preventive focus emphasized in international standards.

The challenge becomes even more pronounced within sectors that rely on both digital and physical security systems. For instance, Njeru and Otieno (2023), in a study on security firms in Nairobi, found that maintenance practices were affected by three major issues: lack of preventive maintenance schedules, inadequate documentation of corrective actions, and limited communication between field technicians and ICT managers. The study concluded that these gaps make it difficult to assess system health and prepare for compliance audits, given the fragmented flow of information.

While existing studies highlight general challenges in ISMS maintenance, there is limited empirical work that examines the actual tracking mechanisms organizations use. Studies such as Kamau (2021) have focused mainly on the factors influencing initial ISMS adoption, but very few have explored the operational phase that follows. Key questions such as how maintenance tasks are assigned, how completion is verified, and how evidence is stored for audits remain underexplored. This presents a significant gap, particularly in technologically evolving sectors like private security.

Local infrastructure and resource constraints also influence the choice of maintenance tracking methods. Chege (2024) found that many Nairobi-based firms hesitate to invest in cloud-based maintenance platforms due to concerns about internet reliability, cost, and the limited availability of trained cybersecurity personnel. As a result, maintenance duties are often delegated to general ICT staff or outsourced technicians, leading to inconsistent follow-up and limited accountability.

Poor maintenance tracking has major implications for operational stability and compliance. A regional analysis of security failures in 2023 showed that 60% of reported incidents were linked to unpatched systems or neglected equipment, most of which resulted from inadequate maintenance workflows (Regional Security Report, 2023). Such gaps often lead to prolonged system downtime, service delivery failures, and difficulties in meeting ISO/IEC 27001 audit requirements due to missing or incomplete evidence trails.

In summary, while international literature emphasizes automated and proactive ISMS maintenance practices, evidence from Nairobi's private security sector shows a heavy dependence on manual, reactive, and fragmented tracking methods. The gap lies in the lack of detailed empirical research on how maintenance is actually tracked, documented, and communicated in day-to-day operations. The first objective of this study addresses this gap by examining the specific maintenance tracking mechanisms currently used in private security firms, thereby providing a foundation for designing an appropriate digital solution tailored to the local context.

2.3.2 Best Practices in ISMS Maintenance Tracking Systems

Best practices form the essential link between the theoretical requirements of security frameworks and their practical execution within organizations. Whereas standards such as ISO/IEC 27001:2022 outline what must be achieved in terms of risk treatment, control implementation, and continual improvement, they do not prescribe how these requirements should be operationalized. This gap between stated requirements and practical execution creates a vulnerability where organizations may obtain certification yet remain operationally weak due to inconsistent maintenance routines. For this

reason, scholars and practitioners emphasize the need to identify and formalize best practices that translate abstract security objectives into reliable, day-to-day operational activities.

Internationally accepted standards form the foundation of these best practices. ISO/IEC 27001:2022, especially through its Annex A controls such as A.5.36 on compliance with internal policies and A.7.12 on managing technical vulnerabilities, expects organizations to adopt structured and traceable maintenance practices. Complementary frameworks, including COBIT 2019 within its "Monitor, Evaluate and Assess" domain and the NIST Cybersecurity Framework under the "Respond" and "Recover" functions, reinforce the importance of continual monitoring and timely corrective action. Whitman and Mattord (2022) observe that these frameworks share a common principle: the Plan-Do-Check-Act (PDCA) cycle. In ISMS maintenance, this involves planning maintenance tasks, implementing them, verifying effectiveness, and refining processes to create a continuous improvement loop.

Recent literature shows a clear shift from traditional scheduled maintenance toward predictive, data-driven approaches. Studies in related fields, such as IT operations and physical asset management, demonstrate the advantages of condition-based monitoring. Jardine et al. (2020) show that using real-time system data to predict failures can reduce costs by up to 30 percent and cut downtime by as much as 70 percent. Applied to ISMS, this includes practices like analyzing firewall logs to identify vulnerability trends or monitoring the performance of access control systems to schedule component replacement before failure. This transition elevates

maintenance from a reactive cost centre to a strategic function focused on resilience and operational efficiency.

A central theme in best practice literature is the critical role of automation. Manual tracking of maintenance activities introduces errors, inconsistencies, and audit gaps. Research by Grobler and von Solms (2021b) highlights several automation-driven practices that improve accountability and efficiency. These include automated task assignment through digital ticketing, escalation mechanisms for overdue tasks, and automatic generation of compliance reports linked directly to ISO/IEC 27001 controls or service level clauses. Automation therefore embeds compliance within daily operations, making it proactive rather than retrospective.

Another widely recognized best practice is the establishment of strong accountability and auditability mechanisms. Scholars agree that every action taken within the ISMS maintenance lifecycle must be traceable. Anderson and Lee (2023) report that organizations with integrated audit logs reduce the time required to investigate and resolve incidents by more than fifty percent. This is enhanced through role-based access control, which enforces proper separation of duties. For example, technicians cannot approve or verify their own work, ensuring an integrity-driven process supported by checks and balances.

Increasingly, ISMS maintenance is understood not as a technical activity but as one that supports overall service delivery, especially where security service level agreements (SLAs) are involved. Fernández and Ramírez (2024) demonstrate that integrating maintenance tracking with IT service management processes improves client satisfaction and reduces disputes. Best practices in this area include defining

clear maintenance indicators such as mean time to repair (MTTR) and adherence to preventive schedules and monitoring them with the same rigor applied to other SLA metrics such as system availability.

Even though global literature clearly outlines these best practices, scholars caution against assuming universal applicability. Abu-Mahfouz and Alsaleh (2022) argue that practices must be adapted to local conditions, especially in regions such as Africa where digital literacy, system costs, and network reliability vary widely. In this context, appropriate technology becomes a best practice in itself. For Nairobi's private security firms, this may involve prioritizing systems with offline capabilities, mobile-friendly interfaces for field technicians, and scalable modules that fit limited budgets. Okpeke et al. (2024), in an East African study, recommend hybrid practices that combine globally recognized approaches, such as automation and predictive monitoring, with localized adaptations including SMS notifications for critical alerts in low-bandwidth environments.

In summary, while the literature identifies several global best practices such as predictive analytics, automation, strong auditability, and SLA integration, it also highlights two important gaps. First, existing studies do not consolidate these practices into a unified framework specific to ISMS maintenance tracking in integrated security environments. Second, there is a significant lack of empirical evidence on how such practices can be implemented effectively within the socio-technical context of private security firms in Nairobi. These gaps justify the focus of the second objective of the current study: to identify, synthesize, and contextualize best practices for ISMS maintenance tracking in a manner that is both globally informed and locally applicable.

2.3.3 Design and Develop an Automated ISMS Maintenance Tracking System

A clear tension runs through the literature on information system design for specialized industrial environments. Although there is an abundance of sophisticated and general design principles, very little research applies these principles to the everyday realities of operational security management in the Global South. Frameworks such as Design Science Research (DSR), described comprehensively by Drechsler et al. (2023), are well developed in theory, but their practical use is illustrated through examples in banking, healthcare, or e-government in highly resourced environments. This results in a persistent gap. The field has a strong theoretical language for system design but offers almost no guidance on what to build when the context is Nairobi's private security sector, where work depends on both digital and physical assets, a largely nontechnical workforce, and unreliable infrastructure.

This lack of contextual guidance affects every major design decision. System architecture is one example. Current literature strongly supports modular micro services as the preferred approach for scalability and resilience (Almeida et al., 2023). Yet these models rarely address the central architectural challenge in this setting: creating real time accountability and complete audit trails within a system that must keep functioning when cellular networks fail. Research on offline first design, such as Talukder et al. (2020), targets consumer-facing apps rather than operational systems that require strict data integrity and reliable conflict resolution. As a result, the architectural advice in the literature offers a broad outline but stops short of the actual demands of this environment.

The challenge is equally evident in user experience design. Most user cantered design and technology adoption studies, for example the work of Fernández-Díaz and Ramírez-Montoya (2024), focus on users like office employees or students. What ease of use means for someone reporting a malfunction at three in the morning using a company issued phone is not explored in mainstream HCI research. As a result, the user who is most critical of the reliability of the system is rarely considered in the design assumptions.

The limitations in literature become even clearer when considering intelligent or predictive systems. Predictive maintenance frameworks, including those described by Jardine et al. (2020), depend on structured historical data. Yet many security firms in Nairobi are only beginning to transition from paper-based logs. The core design challenge, therefore, is not how to apply predictive models, but how to create reliable digital records from the beginning. The literature offers little guidance on how to design systems whose first job is to enforce consistent data capture, long before any analytics can be applied.

Validation strategies reflect a similar disconnect. DSR rightly stresses rigorous evaluation, but typical evaluation metrics such as user satisfaction or frequency of system use are inadequate for this domain. The question is not whether users like the system, but whether the system ensures that a scheduled maintenance task is completed and verified, or whether it turns the Private Security Regulation Act from a static guideline into a process that can be executed and audited. As Chandra Kruse et al. (2022) point out, there is a shortage of evaluation metrics that reflect the realities of

specific sectors. This leaves researchers measuring outcomes that do not reflect what operational success requires.

Taken together, lack of practical application, the limited architectural guidance, the absence of research on the main user group, the difficulty of designing from zero data, and the misalignment of evaluation metrics point to a deeper divide in the field. Much of the existing knowledge has been developed in environments where data is abundant, connectivity is reliable, and users have high digital literacy. These assumptions do not hold in Nairobi's private security sector, where fragmentation, interruptions, and inconsistent data are the norm rather than the exception.

Designing and validating a system in this context is therefore not a straightforward application of known methods. It requires reworking well-established principles such as modularity, user centered design, and data driven decision making so that they function within a setting that challenges the assumptions behind those principles. The goal is not only to implement an algorithm or produce a standard application, but to assemble these principles into a system that can operate offline, support nontechnical staff, and gradually build a reliable data foundation. Its aim is not simply to produce a tool, but to demonstrate a design approach that starts from actual operational constraints and works backward toward a system that is both rigorous and workable in this environment.

2.3.4 Validation of Automated ISMS Maintenance Tracking Systems

Evaluating a designed information system artifact is a decisive step in Design Science Research (DSR). It moves beyond proving that the system works technically to demonstrate that it actually solves the problem it was created to address. As Chandra

Kruse et al. (2022) emphasize, a comprehensive evaluation must be multi-dimensional, combining technical testing, user-focused assessment, and performance measurement. This combination of evidence is necessary to show that the system adds genuine value within its organizational setting and makes a meaningful contribution to both practice and knowledge.

Within the DSR framework, a clear evaluation plan is essential. Drechsler et al. (2023) argue that the selected evaluation methods must correspond to both the objectives of the design and the stage of research maturity. They distinguish between ex-ante evaluation, conducted before deployment, and ex-post evaluation in real use, advocating for multiple complementary methods. For a maintenance tracking system, this includes formative evaluation during development, such as heuristic assessments, and summative evaluation after deployment to measure practical impact. Yet most of this guidance arises from controlled, well-resourced academic environments. Very little literature discusses how to conduct such multi-stage evaluation in small or medium-sized enterprises in Nairobi, where time, personnel, and financial resources are constrained.

A central component of ex-post evaluation is user acceptance. The Technology Acceptance Model (TAM) remains widely applied. Escobar-Rodríguez and Monge-Lozano (2022), after reviewing more than eighty studies on enterprise system adoption, found that perceived usefulness and perceived ease of use consistently predict user intention. This supports the inclusion of TAM-based surveys in evaluation. However, conventional TAM instruments often measure general attitudes without capturing role-specific usability challenges. An ICT manager interpreting

dashboards and a field technician submitting repair logs under unstable network conditions face very different barriers, differences that standard TAM scales often overlook.

User Acceptance Testing (UAT) helps address this limitation. Petter and McLean (2023) found that structured UAT where end users execute predefined test scenarios identifies workflow problems more effectively than developer-driven testing. Successful UAT requires representative users and realistic scenarios. However, their research was conducted in large organizations with business analysts responsible for UAT facilitation. Many private security firms in Nairobi do not have the internal capacity to conduct structured UAT, making rigorous testing difficult without external support.

Beyond perceptions, evaluation must measure tangible performance improvements. Iden and Eikebrokk (2020) demonstrated this in IT service management by using indicators such as Mean Time to Repair (MTTR) and the percentage of scheduled changes completed on time. These metrics can show quantifiable operational gains. However, applying them directly to hardware maintenance in private security firms is complicated. Equipment such as CCTV cameras requires physical checks and transport logistics, which introduce delays that do not align cleanly with standard IT service metrics.

Evaluating intelligent or predictive features adds further complexity. Bokrantz et al. (2020) assessed predictive maintenance systems using indicators such as the proportion of proactive actions and the false alarm rate. Their approach is rigorous but assumes the availability of structured historical data. In contexts transitioning from

paper-based reporting, such data may be limited or unreliable, reducing the usefulness of these metrics during early system deployment.

For systems that support compliance, evaluation must also include auditability. Turetken et al. (2020) recommend assessing whether system outputs are complete, accurate, and easily retrievable, noting that the system becomes part of the control environment itself. Although this aligns with the aspirations of an ISMS tool, their framework was developed for GDPR and SOX compliance in large organizations and does not directly reflect the unique requirements of Kenya's Private Security Regulation Act or its balance between statutory and operational expectations.

The chosen evaluation design directly influences the strength of the conclusions. Quasi-experimental designs, such as pre-test/post-test models, allow researchers to attribute observed outcomes to the implemented system. Anderson et al. (2021) applied this approach to ERP systems by comparing performance before and after implementation while controlling for external variables. Yet in private security firms, isolating the effects of the system from factors such as staff turnover or new client demands is difficult, which may reduce the internal validity of such evaluation designs.

Long-term sustainability and scalability are frequently overlooked. Silva et al. (2022) stress that long-term evaluation must consider total cost of ownership, skill requirements for system maintenance, and cultural alignment with organizational practices. Without such assessment, a technically successful system may still fail to endure. Most DSR evaluations conclude shortly after deployment and therefore do not capture these longitudinal dynamics. For this study, long-term viability indicators are

crucial, even if they cannot be measured across multiple years within the doctoral timeframe.

Integrating all evaluation components into a coherent judgment is itself challenging. Venable et al. (2020) propose a DSR Evaluation Matrix that systematically incorporates technical, human, and organizational dimensions. While promising, its practical application reveals a reporting gap: synthesizing quantitative indicators, qualitative UAT findings, and compliance assessments into one unified narrative demands a level of methodological transparency that is seldom documented.

In summary, while the literature provides many evaluation models, methods, and metrics, several gaps remain when assessing an ISMS maintenance tracking system within Nairobi's private security sector. These include limited contextual applicability, shallow measurement tools, resource constraints, difficulty translating metrics, dependence on unavailable historical data, regulatory misalignment, feasibility challenges, missing long-term perspectives, and limited guidance on synthesis. This justifies the fourth objective of the study: to conduct a tailored evaluation that adapts established approaches such as TAM, UAT, performance indicators, and compliance audits while innovating to address contextual demands. This includes designing sector-relevant metrics, creating a feasible quasi-experimental comparison, and developing an evaluative framework that captures both immediate usefulness and long-term sustainability, thereby bridging the divide between generic evaluation theory and real-world practice.

2.4 Summary of research gaps

Table 2.1

Summary of Empirical Studies, Gaps, Findings, and Application to the Present Study

Theory	Reference	Empirical Focus / Context	Key Findings	Research Gap Identified	Application in the Present Study
General Systems Theory (GST)	Masaev et al. (2025)	Enterprise information security systems	Security effectiveness depends on interactions among technical, organizational, and environmental elements.	No guidance on maintenance tracking in resource-constrained security environments.	Supports integration of technical, human, and managerial maintenance activities into one system.
	Tupkalo et al. (2024)	Process-oriented ISMS implementation	Security controls are more effective when embedded in organizational processes.	Does not address maintenance tracking as a separate process.	Guides integration of maintenance tasks into routine organizational workflows.
	Poltavtseva et al. (2021)	Cyber-physical security monitoring	Hierarchical monitoring improves visibility and adaptability.	Limited to industrial cyber-physical systems.	Informs multi-level monitoring and audit trail mechanisms.
	Islam et al. (2025)	Cybersecurity risk modelling	Risks emerge from interactions among system components.	Focuses on risk assessment rather than maintenance operations.	Supports tracking interactions among users, tasks, and assets.
Technology Acceptance Model (TAM)	Davis (1989)	Technology adoption in organizations	Perceived usefulness and ease of use drive system acceptance.	Does not consider contextual factors such as trust or infrastructure limitations.	Guides system design and user acceptance evaluation.
	Marikyan et al. (2023)	TAM meta-analysis	Contextual factors strengthen technology adoption.	No focus on maintenance systems in developing countries.	Supports inclusion of trust and task relevance in evaluation.

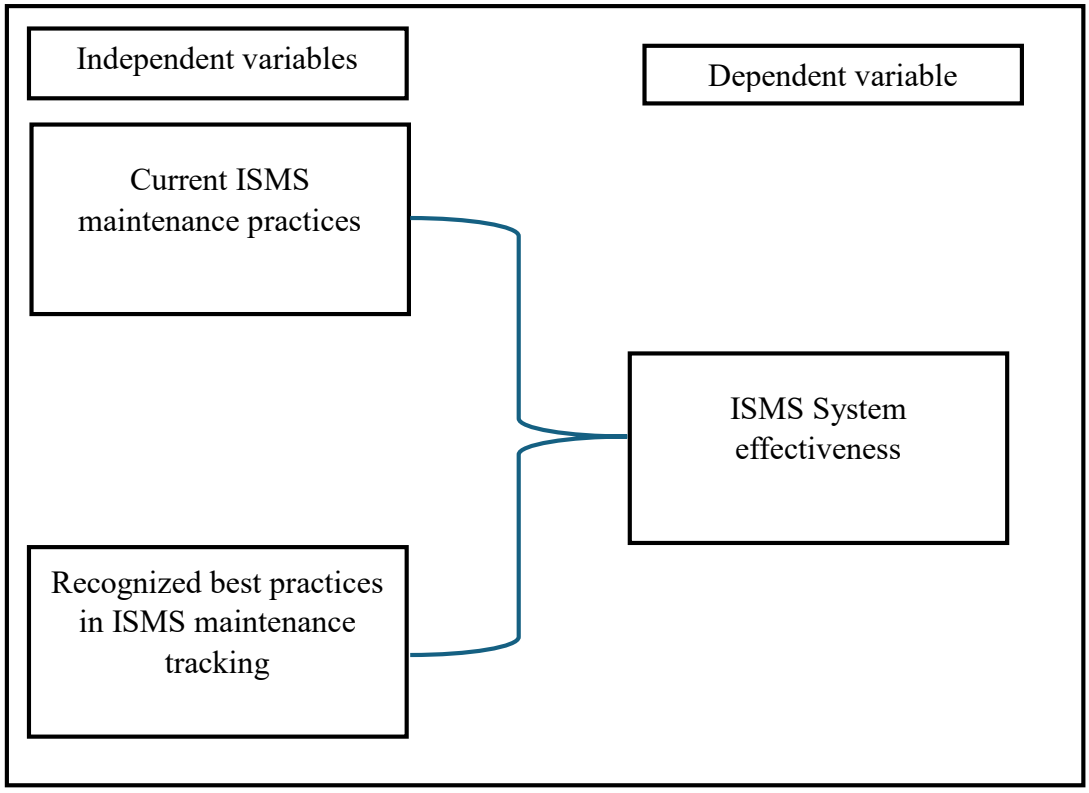
	Al Adwan et al. (2023)	Extended TAM applications	Workflow alignment improves user acceptance.	Examined educational technologies rather than operational systems.	Informs role-based workflows and structured interfaces.
	Liao et al. (2022)	TAM and value-based adoption	Adoption depends on perceived benefits relative to effort and cost.	Does not address low-resource environments.	Supports development of a low-cost, user-centred solution.
Total Productive Maintenance (TPM)	Nakajima (1988)	Manufacturing maintenance management	Preventive maintenance and continuous improvement enhance performance.	Focused on physical equipment rather than information systems.	Provides the foundation for preventive maintenance scheduling and continuous improvement.
	Prajapati & Nair (2023)	TPM in IT asset management	Monitoring and preventive maintenance improve reliability.	Assumes high technical capacity and infrastructure.	Informs adaptation of TPM principles to security system maintenance.
	Wireman (2021)	TPM in digital infrastructure	Maintenance should be integrated with operational processes.	Limited focus on information security environments.	Supports linking maintenance activities with SLAs and service delivery processes.

2.5 Conceptual framework

A conceptual framework, according to Adom et al. (2018), provides a visual or diagrammatic representation of key concepts and their interrelationships, illustrating how independent variables are presumed to influence the dependent variable within a study's context.

Figure 2. 4

Conceptual Framework



Source: Researcher (2025)

As illustrated in 4, the conceptual framework depicts the hypothesized relationships between the study's key variables. The independent variables current ISMS maintenance practices and recognized best practices in ISMS maintenance tracking are shown on the left, connected by directional arrows to the dependent variable, *ISMS* system effectiveness, on the right. The arrows represent the presumed influence that the independent variables exert on the dependent variable. Specifically, current ISMS maintenance practices capture the existing methods and processes used by Nairobi-based security firms to manage preventive and corrective maintenance, incident tracking, and compliance reporting. Weak or fragmented practices are expected to

negatively affect system effectiveness, leading to inefficiencies, downtime, and poor regulatory compliance (Mutinda & Wabwoba, 2023).

Conversely, recognized best practices such as preventive maintenance scheduling, automated tracking, real-time alerts, and adherence to ISO/IEC 27001:2022 standards are expected to positively influence ISMS system effectiveness. When firms adopt structured and automated best practices, they improve system reliability, data accuracy, and overall performance (Grobler & Von Solms, 2021a; Okpeke et al., 2024). The framework thus suggests that improving ISMS maintenance practices and integrating globally recognized best practices will jointly enhance the effectiveness of ISMS in private security firms. This relationship forms the basis for developing and validating the proposed ISMS Maintenance Tracking System, aligning it with both operational realities and international security management standards.

2.6 Summary

The reviewed literature underscores the persistent gap between ISMS theory and practice, particularly within developing contexts. While international frameworks such as ISO/IEC 27001:2022 provide structured guidance, many security firms in Nairobi still operate reactively, with minimal automation and fragmented maintenance tracking. Theories such as GST, TAM, and TPM jointly inform the design of an ISMS Maintenance Tracking System that is holistic, user-centred, and proactively maintainable. Empirical findings affirm the importance of automation, preventive scheduling, SLA compliance, and digital reporting in improving ISMS performance. However, most existing solutions are designed for industrialized contexts and fail to address the infrastructural and operational realities of local firms. This research

addresses that gap by developing, implementing, and validating a context-aware, modular ISMS Maintenance Tracking System tailored to the Kenyan private security sector.

CHAPTER THREE

RESEARCH METHODOLOGY

3.1 Introduction

This chapter presents the methodology adopted for the study. It describes the overall research design, target population, sampling procedures, research instruments, data collection methods, ethical considerations, operational definition of variables, and data analysis techniques. The approach was structured to ensure that the study objectives were met systematically and that the findings were valid, reliable, and generalizable to private security firms operating within Nairobi County.

3.2 Research Design

This study adopted Design Science Research (DSR) as the overarching research paradigm, with a descriptive-explanatory survey embedded within the diagnostic phase. DSR is appropriate when research seeks to develop and evaluate an artefact that addresses a practical organisational problem while generating new knowledge (Hevner et al., 2004; Peffers et al., 2007). The approach was considered suitable because the study sought not only to investigate ISMS maintenance challenges in private security firms but also to design, develop, and validate an automated ISMS Maintenance Tracking System.

The study followed the six DSR stages proposed by Peffers et al. (2007): problem identification, objective definition, artefact design and development, demonstration, evaluation, and communication. Objectives One and Two formed the diagnostic phase and were addressed using a descriptive-explanatory survey. The descriptive

component enabled the study to establish the current state of ISMS maintenance practices and tracking mechanisms, while the explanatory component facilitated examination of relationships between maintenance practices, best practices, and system effectiveness (Kothari, 2014; Saunders et al., 2023).

The survey findings informed the design requirements of the proposed system under Objective Three, while Objective Four focused on evaluating the developed artefact through functional testing, performance testing, and User Acceptance Testing. The integration of survey research within DSR is consistent with recommendations that artefact design should be grounded in a thorough understanding of the problem environment to ensure relevance and practical utility (Hevner et al., 2004).

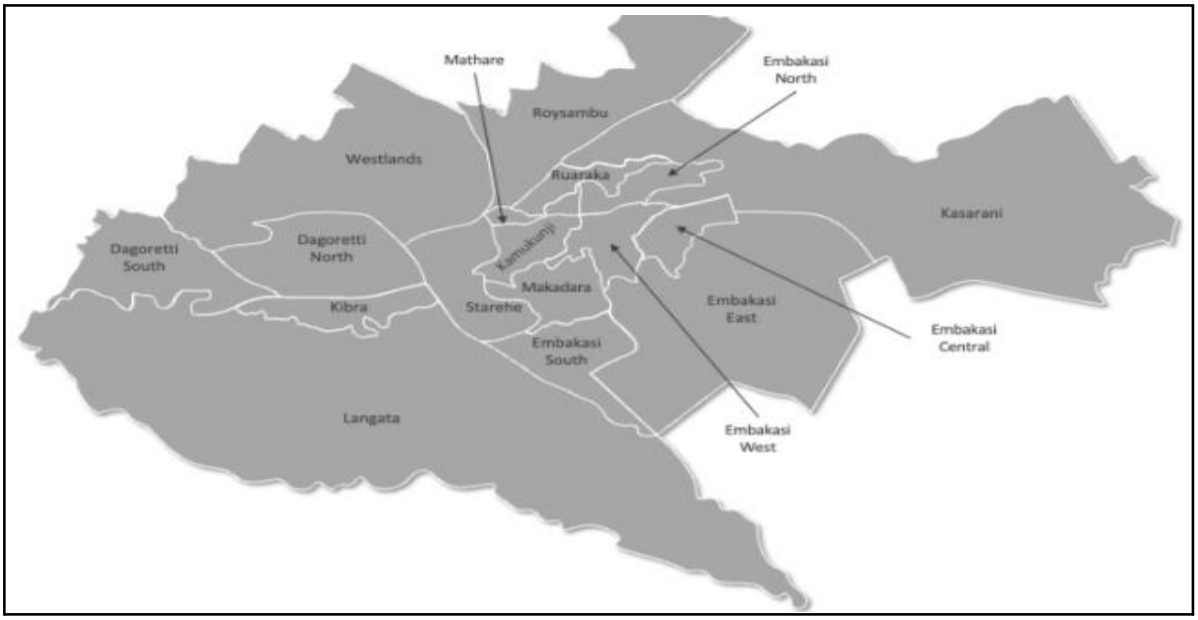
3.3 Location of the study

The study was conducted in Nairobi County, Kenya. Nairobi was selected because it hosts the largest concentration of registered private security firms in the country, making it an appropriate setting for examining ISMS maintenance practices within the sector (Private Security Regulatory Authority [PSRA], 2024). The county also serves as the administrative and regulatory centre of the private security industry under the Private Security Regulation Act (2016). In addition, Nairobi's complex security environment, characterised by commercial buildings, industrial facilities, residential estates, and critical infrastructure, necessitates extensive use of integrated security technologies. This provides a suitable context for investigating information security management practices and evaluating the applicability of an automated maintenance tracking system. Although the findings may not be fully generalisable to all counties in Kenya, Nairobi provides a rich and representative environment for studying private

security firms operating in technology-intensive urban settings (Mugenda & Mugenda, 2013).

Figure 3.1

Study Location - Nairobi County Map



3.4 Target Population

The target population comprised ICT managers working in registered private security firms within Nairobi County. ICT managers were selected because they are directly responsible for the management, maintenance, and oversight of Information Security Management System (ISMS) processes, and therefore possess first-hand technical and managerial knowledge relevant to the study. This selection is consistent with Mugenda and Mugenda (2013), who argue that a target population should consist of individuals possessing characteristics that directly align with the study objectives to ensure relevance and validity of collected data.

According to the Private Security Regulatory Authority (PSRA, 2024), there are approximately 116 licensed private security firms in Nairobi County. However, only firms with active ICT departments and ISMS-related functions were included in the study. This decision was guided by Creswell and Creswell (2018), who emphasize that inclusion criteria in survey research should ensure that respondents have direct exposure to the phenomenon under investigation in order to maintain construct validity and avoid collecting uninformed responses.

The population was further stratified by firm size (small: 1-49 staff; medium: 50-249; large: 250+), based on PSRA categorization. This decision was informed by Saunders et al. (2023), who note that stratification is appropriate in heterogeneous populations as it ensures representation across key subgroups and improves the accuracy and generalizability of findings. The target population is presented in Table 2.

Table 3.1

Target Population

Security Company	Population	Population %
Small	75	65%
Medium	25	22%
Large	16	13%
Total	**116**	**100%**

3.5 Sampling Procedure and Sample Size

A stratified purposive sampling technique was adopted in this study. The use of stratification by firm size was informed by the need to ensure proportional

representation across organisational scales, while purposive sampling was applied to ensure that only ICT managers with relevant ISMS expertise were included. This approach is supported by Saunders et al. (2023), who argue that purposive sampling is appropriate when the researcher seeks participants with specific expertise relevant to the research problem. Similarly, Etikan et al. (2016) note that purposive sampling is widely used in studies where knowledge is concentrated among particular categories of respondents.

The unit of analysis was the individual ICT manager, with one manager selected per firm. This decision was made to avoid intra-firm clustering effects and ensure independence of observations. Bryman (2016) cautions that multiple responses from the same organisation can introduce dependency bias, thereby affecting the validity of statistical inference in organisational surveys.

The sample size was determined using Yamane's (1967) formula at a 95% confidence level and a 5% margin of error. This choice was informed by Israel (1992), who notes that Yamane's formula is appropriate for finite populations where the total population is known and provides a simplified yet reliable approach to sample size determination in social science research. The adoption of a 95% confidence level and 5% margin of error is consistent with standard statistical practice for ensuring an acceptable balance between precision and feasibility (Cochran, 1977). The formula is given as:

$$n = \frac{\mathrm{N}}{1 + \mathrm{N(e)2}}$$

Where:

- n = Sample size
- N = Study population (116)
- e = Level of precision (0.05)

Substituting these values:

$$n = \frac{116}{1 + 116(0.05)2}$$

n=90

Therefore, the sample size for the study was 90 respondents. The distribution of the sample across firm categories is shown in Table 3.

Table 2.2

Sampling of Respondents by Firm Size

Security Company	Population	Sample Size
Small	75	69
Medium	25	15
Large	16	6
Total	**116**	**90**

3.6 Research Instrumentation

Data were collected using a structured questionnaire developed by the researcher. The choice of a structured questionnaire was informed by Creswell and Creswell (2018), who note that such instruments enhance standardisation of responses, improve

comparability across respondents, and facilitate statistical analysis in quantitative research designs. The instrument was designed to capture four key dimensions: demographic characteristics of ICT managers, current ISMS maintenance and tracking practices, adoption of international best practices, and expected effectiveness of the proposed system. This structure was informed by the need to ensure alignment between measurement items and research objectives, as recommended in survey instrument design literature (Saunders et al., 2023).

The questionnaire combined closed-ended Likert-scale items with open-ended questions. This design decision was guided by Creswell and Plano Clark (2017), who argue that mixed-item instruments enable both quantifiable measurement and contextual understanding, thereby improving the depth and interpretability of findings. Similarly, Costa (2024) and Oranga and Matere (2023) note that integrating qualitative and quantitative elements enhances triangulation and reduces the limitations of single-method approaches.

3.6.1 Pre-testing and Pilot Testing of the Instrument

To ensure validity and reliability, a two-stage instrument testing process was undertaken comprising expert pre-testing and pilot testing. These procedures were applied solely to the questionnaire and not to the ISMS system, which was validated separately as outlined in Section 3.9.2.

The expert pre-test was conducted by two ISMS specialists and the university supervisors, focusing on face and content validity. This process involved assessing the clarity, relevance, and coverage of questionnaire items. Lynn (1986) supports expert judgment as a standard approach for establishing content validity, particularly in

ensuring that items adequately represent the construct domain. Following their feedback, items were refined to improve clarity and alignment with ISMS constructs drawn from ISO/IEC 27001:2022 and related literature (Marhadi et al., 2024; Prislan et al., 2020).

A pilot test was then conducted with 9 ICT managers, representing 10% of the intended sample, drawn from a parastatal security department not included in the main study. This decision was informed by Teijlingen and Hundley (2001), who recommend pilot studies as essential for identifying ambiguities, testing feasibility, and refining data collection procedures prior to full-scale deployment.

Reliability was assessed using Cronbach's alpha, which yielded a coefficient of 0.89. According to Nunnally and Bernstein (1994), values above 0.70 indicate acceptable reliability, while values above 0.80 demonstrate strong internal consistency. The obtained result therefore confirms that the instrument was highly reliable, and no further modifications were required before full data collection.

3.7 Data Collection

Data collection was conducted only after obtaining all required ethical and administrative approvals. These included ethical clearance from the Kenya Methodist University Ethics Review Board, an official introduction letter from the School of Computing and Informatics, and a research permit from the National Commission for Science, Technology and Innovation (NACOSTI). The requirement for formal ethical and regulatory approval prior to data collection is consistent with National Commission for Science, Technology and Innovation (NACOSTI, 2013) guidelines, which mandate institutional authorisation for all research conducted within Kenya to

ensure compliance with national standards for scientific integrity, accountability, and participant protection.

Questionnaires were administered using a dual-mode approach comprising both physical distribution (drop-off and pick-up) and electronic delivery via email links. The adoption of mixed administration methods was informed by Dillman, Smyth, and Christian's Tailored Design Method, which recommends multiple modes of questionnaire distribution to improve accessibility, reduce non-response error, and enhance response rates in survey research. Similarly, Saunders et al. (2023) note that combining online and physical distribution is particularly effective in organisational studies where respondents have varying preferences and availability constraints.

Respondents were given one week to complete and return the questionnaires. This timeframe was selected to balance respondent convenience with data collection efficiency. Orodho (2013) recommends short, clearly defined response windows in survey research, noting that they reduce respondent fatigue and improve return rates when combined with structured follow-up procedures.

Follow-up reminders were issued after three and six days to enhance response rates and minimise non-response bias. This decision is supported by Dillman et al. (2014), who emphasise that systematic follow-up contacts are one of the most effective strategies for increasing questionnaire response rates in survey research. Armstrong and Overton (1977) further support follow-up procedures as a method of reducing potential non-response error by encouraging participation from initially non-responsive participants.

Upon receipt, all questionnaires were screened for completeness, consistency, and accuracy before inclusion in the final dataset. Only fully completed questionnaires were retained for analysis. This decision aligns with standard data cleaning procedures in survey research, as incomplete responses can introduce measurement error and compromise the validity of statistical analysis (Hair et al., 2019; Saunders et al., 2023).

3.8 Operational Definition of Variables

This section presents the operational definitions of variables used in this study.

Table 3.3

Operational Definition of Variables

Variable	Operational Definition	Indicators	Scale	Source
ISMS Maintenance Practices	Processes and procedures employed by security firms to sustain and monitor ISMS functions.	Maintenance frequency, documentation, audit tracking.	Ordinal	ISO/IEC (2022)
Adoption of Best Practices	Degree of conformity to international ISMS standards.	ISO 27001 alignment, automation tools, policy enforcement.	Ordinal	Marhad et al. (2024)
System Usability	Ease with which ICT managers interact with the ISMS prototype.	User satisfaction, task navigation, interface clarity.	Interval	Nielsen (2012)
System Effectiveness	The extent to which the system improves maintenance performance.	Incident resolution time, report accuracy, SLA compliance.	Ratio	Prislan et al. (2020)

3.9 Data Analysis

Data analysis proceeded in two parallel tracks: (A) statistical analysis of survey data for Objectives 1, 2, and 4 (effectiveness perceptions); (B) system design, development, testing, and validation for Objectives 3 and 4 (artefact creation).

3.9.1 Statistical data analysis

Data were processed using SPSS version 26. The analysis followed a structured sequence:

Step 1: Data cleaning and coding. All returned questionnaires were examined for completeness. Incomplete responses (e.g., missing entire sections) were excluded. Numerical codes were assigned to categorical responses (e.g., gender: 1 = male, 2 = female). Likert-scale responses were treated as continuous for parametric testing after confirming approximate normality (skewness and kurtosis within ±1.5).

Step 2: Descriptive statistics. Frequencies and percentages were computed for demographic variables (gender, age, education, experience, firm size). Means and standard deviations were calculated for the ten current-practice items (Objective 1) and the ten best-practice items (Objective 2). Mean scores were interpreted relative to the scale midpoint (3.0). Standard deviations assessed consensus across respondents. Results were presented in tables (e.g., Tables 4.1 and 4.6).

Step 3: Correlation analysis. Pearson's product-moment correlation coefficient (r) was used to examine bivariate relationships between (a) current practices and system effectiveness, and (b) best practices and system effectiveness (Objective 2). The significance level was set at $\alpha = 0.01$ (two-tailed). Assumptions of linearity and normality were checked using scatterplots and the Shapiro-Wilk test; no serious violations were detected.

Step 4: Regression analysis. Simple linear regression was conducted to determine how much variance in system effectiveness is explained by current practices alone and by

best practices alone (R^2, adjusted R^2). Multiple linear regression was then performed to assess the joint predictive power of both independent variables. Residual plots were examined to confirm homoscedasticity and independence of errors (Durbin-Watson statistic = 1.92, within acceptable range of 1.5-2.5). Results were presented in tables (e.g., Tables 4.3, 4.8, 4.12).

Step 5: ANOVA**.** Analysis of variance (F-test) was used to test the overall significance of each regression model. A p-value < 0.05 was considered statistically significant. Results were presented in tables (e.g., Tables 4.4, 4.9, 4.13).

Step 6: Presentation. All results were presented using tables, graphs, and charts. For each statistical test, the relevant assumptions checked are reported, and effect sizes (R^2, adjusted R^2) are interpreted using Cohen's (1988) guidelines (small: 0.02, medium: 0.13, large: 0.26).

3.9.2 Design, Development and Testing of the System

The third and fourth objectives of this study were achieved through the design, development, and testing of the ISMS Maintenance Tracking System. The process followed the Waterfall methodology, a linear sequential model that proceeds through clearly defined stages: requirement analysis, design, implementation, testing, and maintenance. This methodology was selected for its structured nature, which supports careful documentation, traceability, and systematic evaluation, key requirements in the development of security-related applications.

3.9.2.1 Requirement Analysis

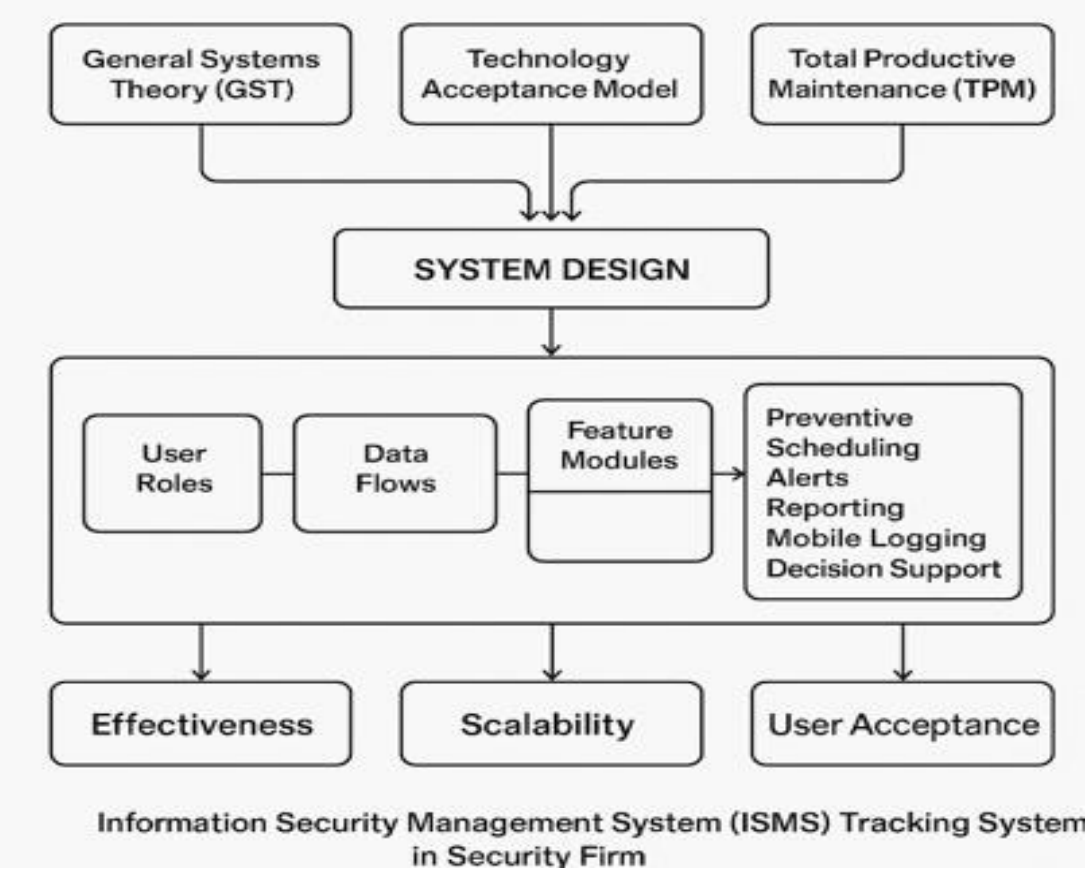
The system development followed the Waterfall methodology Pressman and Maxim, (2020), which proceeds through linear, sequential phases: requirements analysis, design, implementation, testing, and maintenance. Waterfall was selected because (1) the requirements were stable and well-understood from the diagnostic survey (no iterative changes expected); (2) it provides thorough documentation, essential for security-related applications; and (3) it aligns with DSR's emphasis on artefact traceability. Alternative methodologies (e.g., Agile) were rejected because the user group (ICT managers across multiple firms) could not be assembled for iterative sprints.

3.9.2.2 Design Phase

In the design phase, the system architecture was defined to guide implementation. Data Flow Diagrams (DFDs) were used to represent how information moves between system components, ensuring clarity of processes. Flowcharts were developed to map system logic and workflows, including task assignment, incident reporting, and notification generation. The Entity Relationship Diagram (ERD) was constructed to model the database, capturing relationships among key entities such as users, tasks, maintenance logs, and notifications. This ensured that data was structured efficiently and supported accurate, real-time tracking.

Figure 3.2

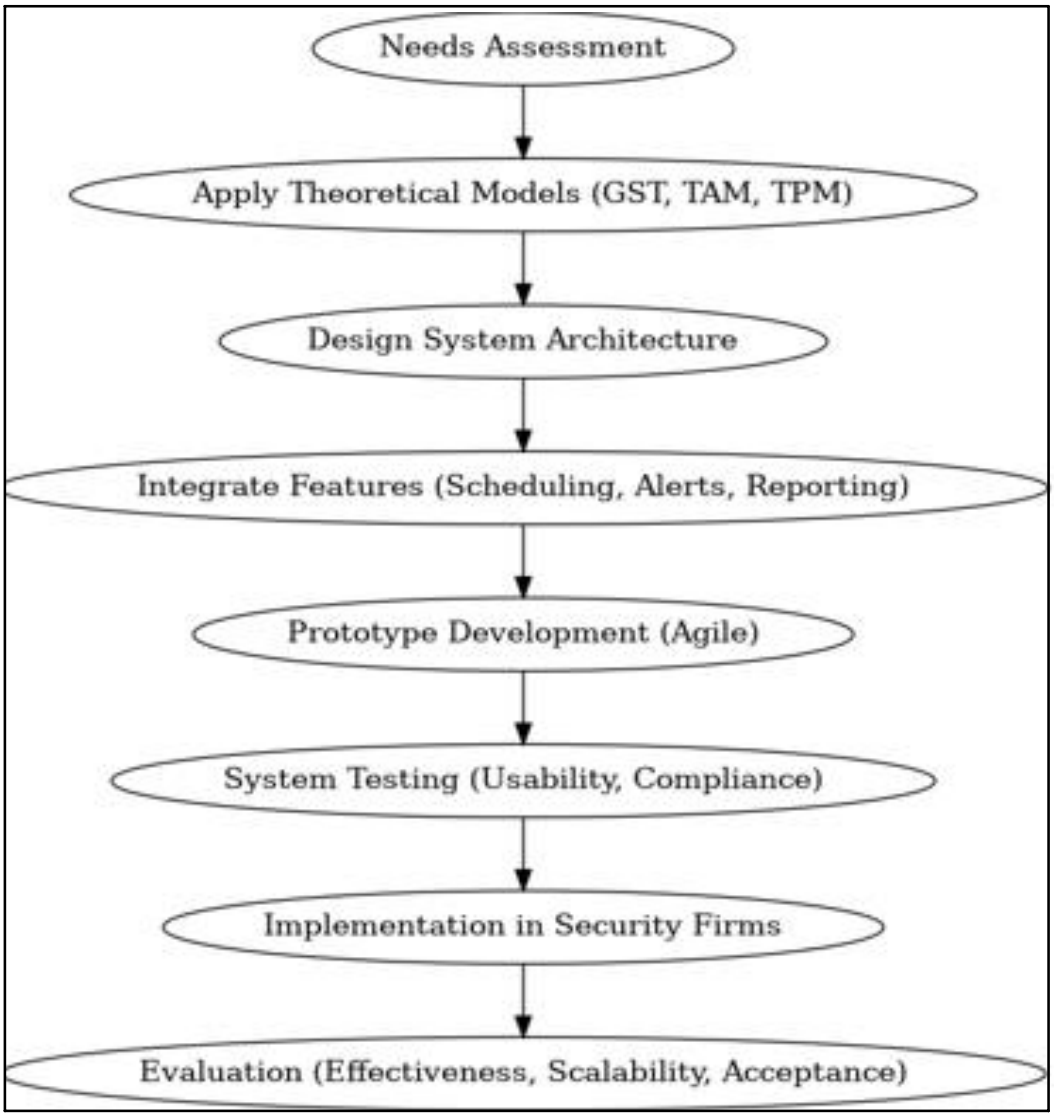
System Architecture/Data Flow Diagram (DFD)



The overall process from needs assessment to deployment and evaluation was visualized in an activity diagram.

Figure 3.3

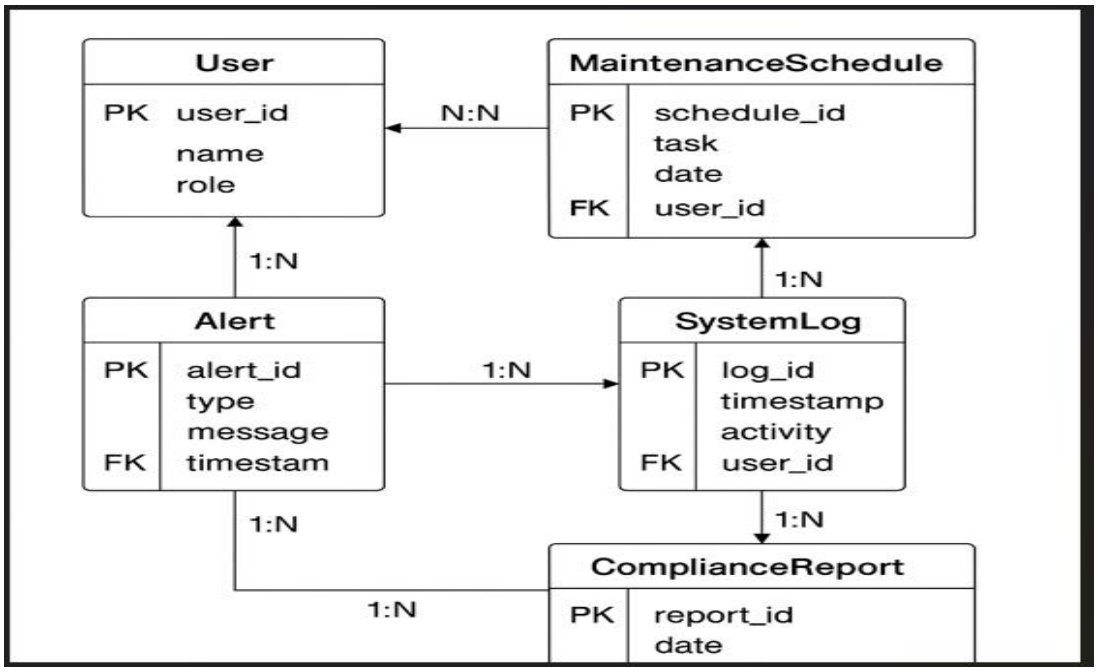
Flowchart illustrating the core maintenance task workflow



The Entity Relationship Diagram (ERD) was constructed to model the database, capturing relationships among key entities such as users, tasks, maintenance logs, and notifications. This ensured that data was structured efficiently and supported accurate, real-time tracking.

Figure 3.4

Entity-Relationship Diagram (ERD)



ER Diagrams - Key Terms

Table 3.3

Entity Relationship Diagram Key Terms

Term	Meaning
PK	Primary Key - A unique identifier for each record in a table.
FK	Foreign Key - A field that links one table to another using its PK.
1:1	One-to-One - One record in a table is related to one record in another.
1:N	One-to-Many - One record in a table is related to many in another.
N:1	Many-to-One - Many records in a table relate to one in another.
N:N	Many-to-Many - Many records in one table relate to many in another.

3.9.2.3 Implementation Phase

The implementation phase involved coding the ISMS Maintenance Tracking System based on the approved design. The application was developed using PHP for server-side logic and MySQL for database management. Front-end interfaces were implemented using HTML, CSS, and JavaScript, ensuring usability and accessibility. The system incorporated a role-based login module, task management module, audit logs, client and personnel records, and a notification engine. These components were integrated to ensure seamless interaction between users and the system.

3.9.2.4 Testing Phase

Testing was carried out to validate system functionality, usability, and compliance with the requirements identified during the requirement analysis phase. Unit testing was performed on individual modules, while system testing evaluated overall performance and security. User Acceptance Testing (UAT) was conducted with selected staff from participating security firms to assess the ease of login, accuracy of task assignments, timeliness of notifications, and reliability of reporting. Feedback from this process was used to refine the interface and address navigation and error-handling issues.

3.9.2.5 Maintenance Phase

The maintenance phase focused on ensuring that the system remained operational and effective after deployment. Updates were made to improve navigation, strengthen security features, and enhance task tracking accuracy. This phase also included regular debugging, database optimization, and the incorporation of user feedback to ensure that the system continued to meet evolving organizational needs.

3.9.2.6 System Evaluation

The evaluation of the ISMS Maintenance Tracking System was conducted to determine whether the system was functional, usable, reliable, and compliant with international standards and local operational requirements of private security firms in Nairobi County. Evaluation focused on four key dimensions:

Functionality: Assessed through the ability of the developed modules (login, audit, personnel and client records, task assignment, and notification) to perform as intended. Evidence of functionality was confirmed during the user acceptance testing (UAT) phase, where all modules were tested for reliability, data accuracy, and responsiveness.

Usability: Evaluated using structured user feedback collected through questionnaires administered to sampled ICT managers and system users. Likert-scale responses captured user satisfaction with ease of login, task allocation, notifications, and navigation.

Performance: Examined using quantitative data from regression and ANOVA tests. These analyses demonstrated the extent to which system effectiveness could be explained by ISMS maintenance practices and best practices in maintenance tracking. In addition, system-generated outcomes such as successful task logging and notification delivery confirmed the expected performance levels.

Compliance: Assessed by comparing the system's functions against internationally recognized standards, particularly ISO/IEC 27001, and national regulatory requirements such as the (Private Security Regulation Act 2016). This evaluation ensured that the artefact addressed both technical and policy expectations.

Both ex-ante and ex-post assessments were carried out. Ex-ante evaluation was embedded in the requirement analysis and design phases, ensuring that the system aligned with user needs from the onset. Ex-post evaluation was based on the statistical analyses and user acceptance testing, which confirmed that the system achieved its intended objectives.

3.9.3 Integrated Tools & Technologies for ISMS Design, Development, and Evaluation

The development of the ISMS Maintenance Tracking System applied a range of tools and technologies across design, implementation, and evaluation stages, as summarized in table 3.6.

Table 3.4

Integrated Tools & Technologies for ISMS Design, Development, and Evaluation

Category	Tool / Technology	Purpose / Application
System Design & Modelling	Lucidchart, Draw.io, MS Visio	System architecture diagrams (ERD, flowcharts, DFDs)
	Balsamiq, Figma	UI mock-ups and wireframe design
	StarUML, Enterprise Architect	Formal UML modelling
Frontend Development	HTML5, CSS3, Bootstrap, JavaScript (React, Angular)	User interface design and responsive web development
Backend Development	PHP (Laravel), Python (Django), Java (Spring Boot)	Server-side logic and API development
Web Frameworks	Django, Laravel, Spring Boot	Structured web application development
Database Management	MySQL, PostgreSQL, MongoDB, SQLite	Data storage and management for ISMS records
	phpMyAdmin, DBeaver	GUI-based database administration
	Git, GitHub, GitLab, Bitbucket	Source code versioning and team collaboration

Category	Tool / Technology	Purpose / Application
Version Control & Collaboration	Trello, Notion	Project planning, task tracking, and documentation
Data Collection	Google Forms, Microsoft Forms, SurveyMonkey	Survey and questionnaire administration
System Testing & Evaluation	Postman, Selenium, Lighthouse, UserTesting	API testing, automated UI testing, performance, and usability evaluation
Security Testing	OWASP ZAP, Burp Suite, Nessus	Vulnerability scanning and penetration testing
Logging & Monitoring	ELK Stack, Graylog	System activity logging and real-time monitoring
	XAMPP, WAMP, Docker	Local development and testing environments
Deployment & Hosting	Heroku, Firebase, Netlify, Vercel	Cloud-based deployment and backend services
	AWS, Microsoft Azure, Google Cloud	Scalable cloud hosting for live systems
Cloud Storage & Backup	Google Drive, OneDrive, External HDD	Secure backup and storage of code, data, and instruments
Developer Workstations	Intel i5/i7, 8–16GB RAM, SSD	Software development and testing
Test Devices	Windows/Linux desktops, Android/iOS mobile devices	Cross-platform system testing
Local & Cloud Servers	Intel Xeon/i7 (16–32GB RAM), Ubuntu Server, Cloud VMs	Prototype hosting, testing, and live deployment
Peripheral Devices	Printers, Scanners, Smartphones	Document digitisation and data collection
Code Editors & IDEs	VS Code, PyCharm, Sublime Text	Code writing, debugging, and development

3.10 Summary

This chapter has presented the methodological approach adopted for the design, development, and evaluation of the ISMS Maintenance Tracking System. The study employed a descriptive explanatory quantitative research design, aligned with the

study objectives. Data were collected using structured questionnaires administered to ICT managers of private security firms in Nairobi County. The sample was determined using Yamane's formula, ensuring representativeness across small, medium, and large firms.

Quantitative data analysis was conducted using SPSS, applying descriptive statistics, correlation, regression, and ANOVA to test the relationships between ISMS maintenance practices, best practices in maintenance tracking, and system effectiveness. The methodology further incorporated system design and implementation guided by the Waterfall model, with validation conducted through user acceptance testing (UAT).

Ethical considerations, including voluntary participation, informed consent, confidentiality, and adherence to Kenya's Data Protection Act (2019), were strictly observed throughout the study. This methodological framework ensured that the ISMS Maintenance Tracking System was not only empirically validated but also practically relevant and adaptable to the operational realities of private security firms in Nairobi County.

CHAPTER FOUR

RESULTS AND DISCUSSIONS

4.1 Introduction

This chapter presents the results of data analysis, followed by the design and implementation of the proposed ISMS maintenance tracking system. The chapter is structured around the study objectives, beginning with an examination of current ISMS maintenance practices and tracking mechanisms, and an investigation of recognised best practices within the context of security firms in Nairobi County. These findings provide the empirical foundation upon which the system requirements were derived. The chapter then proceeds to discuss the design and development of the ISMS maintenance tracking system. This involves outlining the system architecture, data flow models, entity-relationship diagrams, and functional specifications that guided system construction. Finally, the implementation phase is presented, where the developed system is deployed and validated to assess its functionality, usability, and effectiveness in addressing the gaps identified in the earlier sections. By combining data-driven analysis with system development and testing, this chapter demonstrates the link between the identified challenges, the proposed design solution, and its practical application in improving ISMS maintenance processes within security firms.

4.2 Response Rate and Demographic Information

Out of the 90 questionnaires distributed to ICT managers and supervisors in private security firms within Nairobi County, 68 were returned, representing a gross response rate of 75.6%. After data cleaning, 5 questionnaires were found to be incomplete and

were therefore excluded from the analysis. Consequently, 63 questionnaires were retained for analysis, yielding a valid response rate of 70.0%, calculated as:

$$\text{Response Rate} = \frac{63}{90} \times 100 = 70.0\%$$

According to Mugenda and Mugenda (2003), a response rate of 50% is adequate for analysis, 60% is good, and 70% and above is considered very good. Therefore, the response rate achieved in this study was considered sufficient for statistical analysis and interpretation of the findings.

The final sample size of 63 respondents was also deemed adequate for the study. Krejcie and Morgan (1970) argue that sample adequacy depends on the target population and that samples above 50 respondents are generally acceptable for survey research involving relatively small populations. Furthermore, Tabachnick and Fidell (2013) recommend a minimum sample size of $N \geq 50 + 8m$for regression analysis, where m represents the number of independent variables. Since this study examined two independent variables, the recommended minimum sample size was 66 respondents. The achieved sample size of 63 respondents was therefore close to the recommended threshold and was considered adequate given the high response rate and the statistically significant relationships obtained during analysis.

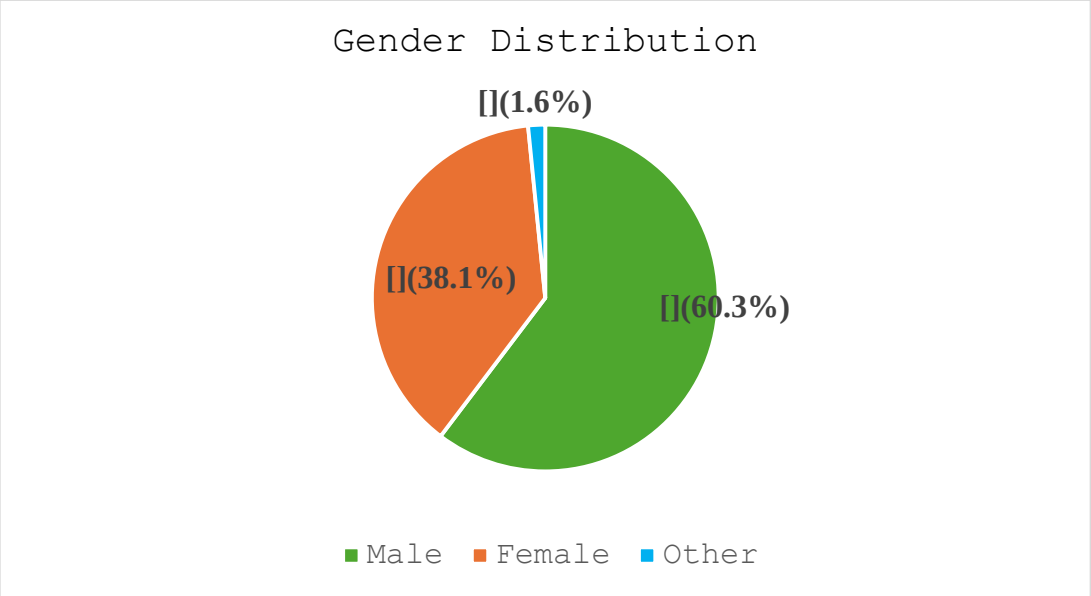
The demographic information collected from respondents included gender, age, education level, organizational position, years of experience in ISMS and IT maintenance, and firm size. These characteristics were analysed to establish the suitability of respondents for providing information regarding ISMS maintenance practices and maintenance tracking systems within private security firms.

4.2.1 Gender Distribution

The findings in Figure 9 show that 60.3% of the respondents were male, 38.1% were female, while 1.6% identified as other. This indicates that males constituted the majority of personnel involved in ISMS and IT maintenance functions within the surveyed private security firms. The predominance of male respondents is consistent with existing evidence that information security and ICT-related occupations remain largely male dominated. Whitman and Mattord (2022) observed that technical security roles continue to attract higher male participation than female participation, particularly in operational and infrastructure management functions. Similarly, Ireri (2025) found that information security roles in Kenyan organizations are predominantly occupied by male professionals, reflecting broader workforce trends within the ICT sector. The findings therefore suggest that ISMS maintenance responsibilities within Nairobi's private security firms mirror the demographic composition commonly reported in information security professions.

Figure 4.1

Gender distribution



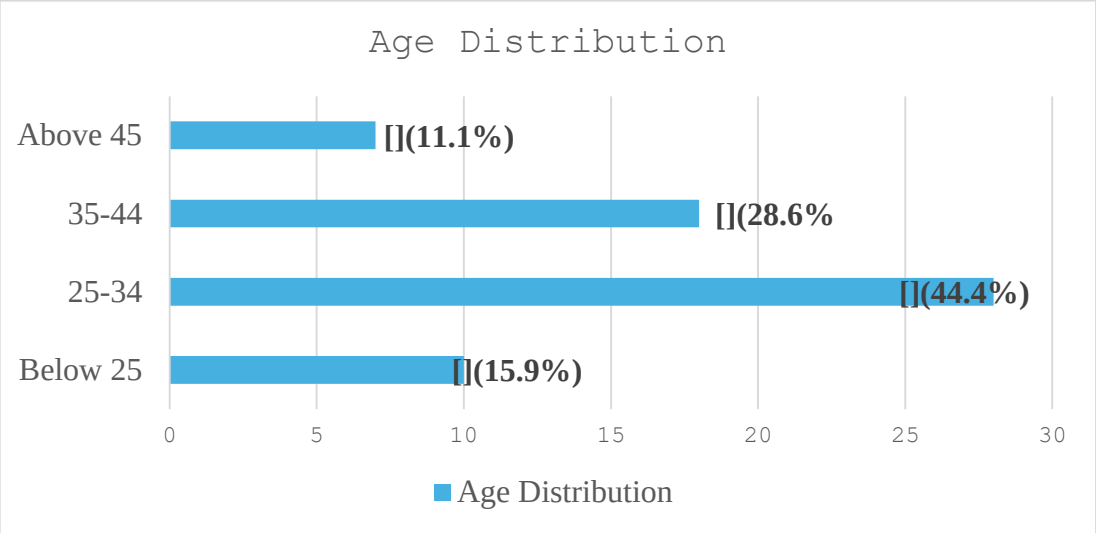
4.2.2 Age Distribution

The findings in Figure 10 reveal that 44.4% of respondents were aged between 25 and 34 years, 28.6% were aged between 35 and 44 years, 15.9% were below 25 years, while 11.1% were aged 45 years and above. These results indicate that ISMS and IT maintenance functions are predominantly performed by relatively young professionals. The dominance of respondents within the 25-44 years age bracket suggests that the sector relies heavily on personnel who are in their active professional years and are likely to possess current technological knowledge and skills. This finding is consistent with Chege (2024), who reported that ICT and information security functions in Kenyan organizations are increasingly managed by younger professionals due to the dynamic nature of digital technologies. Similarly, Ireri (2025) found that information security operations in Kenyan institutions are largely undertaken by early- and mid-career professionals who are actively engaged in technology-driven

processes. The age profile therefore suggests a workforce that is well positioned to adapt to automated ISMS maintenance and tracking solutions.

Figure 4.2

Age Distribution



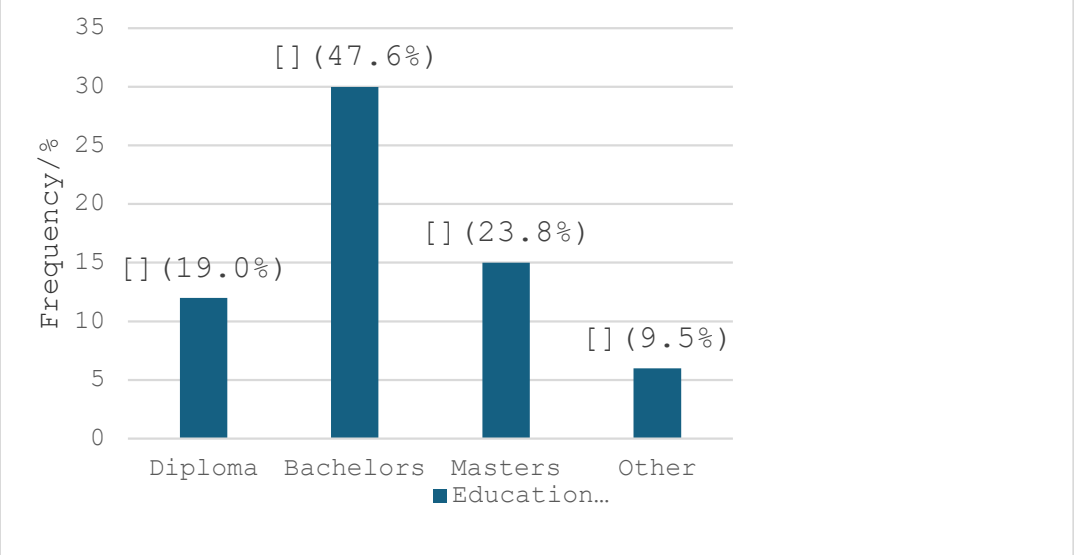
4.2.3 Education Level

The findings in Figure 11 show that 47.6% of respondents held bachelor's degrees, 23.8% possessed master's degrees, 19.0% had diploma qualifications, while 9.5% held other qualifications. These results indicate that the majority of respondents had attained tertiary-level education. The educational profile demonstrates that respondents possessed the academic background necessary to understand information security management concepts and organizational maintenance processes. This finding supports the argument by Whitman and Mattord (2022) that effective information security management depends on personnel with adequate technical and managerial competencies. Likewise, ISO/IEC 27001:2022 emphasizes the importance of organizational competence, training, and awareness in ensuring the effectiveness of

information security management systems. The relatively high proportion of degree holders therefore enhances confidence in the quality and reliability of the information provided by respondents regarding ISMS maintenance practices and tracking mechanisms.

Figure 4.3

Education Levels



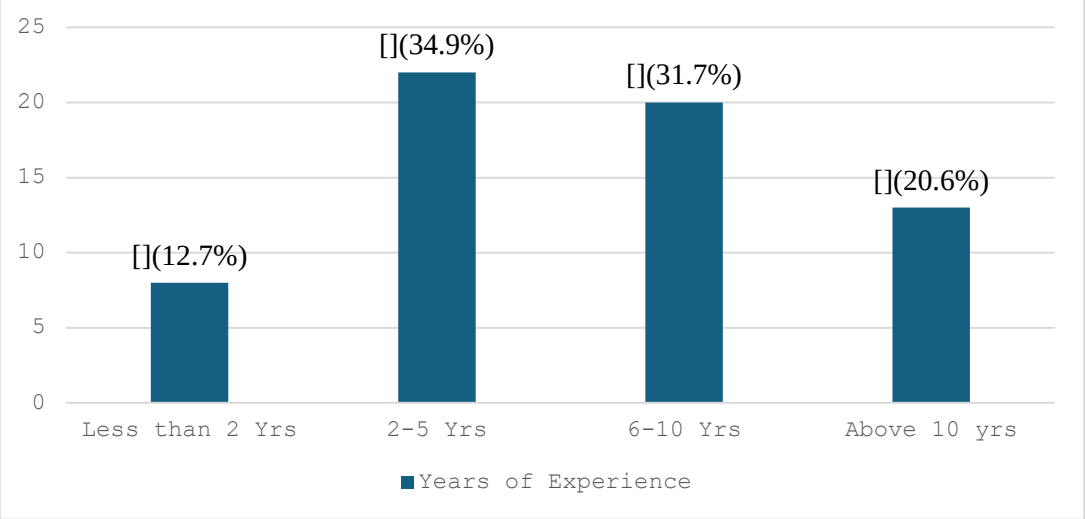
4.2.5 Years of Experience in ISMS/IT Maintenance

The findings in Figure 12 indicate that 34.9% of respondents had between 2 and 5 years of experience, 31.7% had between 6 and 10 years, 20.6% had more than 10 years of experience, while 12.7% had less than 2 years of experience. Overall, the majority of respondents had more than two years of practical experience in ISMS and IT maintenance activities. The experience profile suggests that respondents had substantial exposure to information security operations and maintenance processes. This finding aligns with Whitman and Mattord (2022), who argue that practical experience is essential for understanding security controls, incident management, and

operational maintenance requirements. Similarly, Chege (2024) observed that experienced ICT personnel are better positioned to identify weaknesses in information security processes and contribute to the improvement of organizational security practices. The respondents' experience levels therefore strengthen the credibility of the study findings because they were derived from individuals who routinely engage in ISMS-related activities.

Figure 4.4

Years of Experience



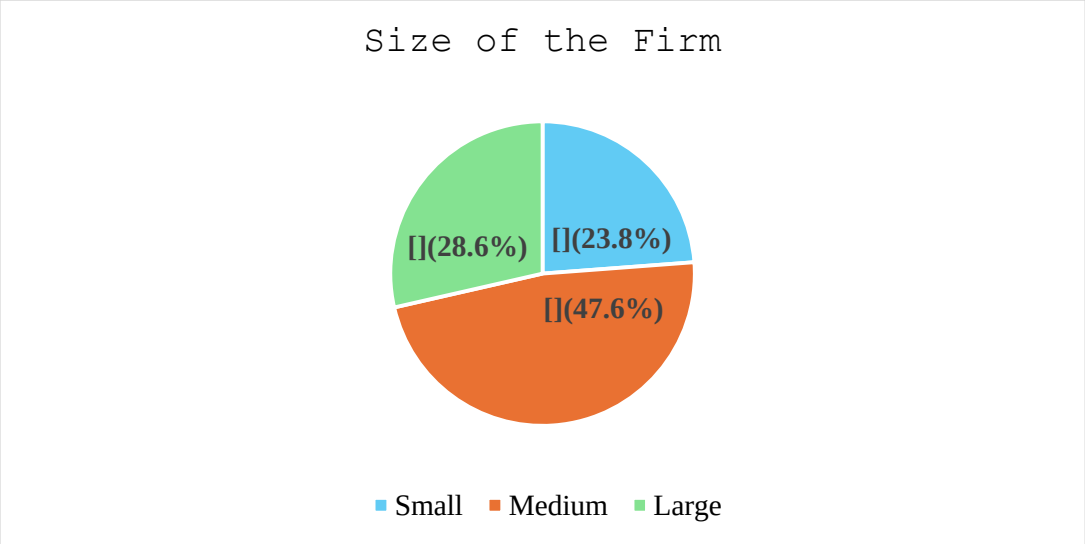
4.2.6 Size of Firm

The findings revealed that 47.6% of respondents worked in medium-sized firms, 28.6% in large firms, and 23.8% in small firms as shown in Figure 13. This indicates that the study captured perspectives from organizations of varying sizes within Nairobi's private security sector. The inclusion of firms of different sizes was important because organizational size influences the availability of resources, technical expertise, and information security capabilities. According to the NIST Cybersecurity Framework (2018), organizational characteristics such as size and

resource capacity affect the implementation and maintenance of cybersecurity controls. Similarly, Chege (2024) reported that larger organizations tend to possess more formalized information security structures, while smaller organizations often face challenges related to limited budgets, staffing, and technical expertise. The representation of small, medium, and large firms therefore enhances the generalizability of the findings by ensuring that the study reflects diverse organizational contexts within the private security industry.

Figure 4.5:

Size of the Firm



4.3 Current ISMS Maintenance Practices and Tracking Mechanisms in Security Firms in Nairobi

The first objective of this study was to examine the current ISMS maintenance practices and tracking mechanisms employed by security firms in Nairobi County. Ten Likert-scale items were used to measure different aspects of current practices, including preventive and corrective maintenance, incident reporting, coordination, staff skills, and record management.

4.3.1 Descriptive Statistics

Table 4.6 presents the descriptive statistics for Objective One. The findings show that the mean scores for all items ranged between 1.92 and 2.11, on a five-point scale, indicating that respondents rated the current practices as weak or inadequate.

Table 4.1

Descriptive Statistics for Current ISMS Maintenance Practices

Item	N	Mean	Std. Dev
Preventive maintenance conducted on schedule	63	2.08	.655
Corrective maintenance performed promptly	63	2.06	.759
Incident reporting systematically documented	63	2.02	.684
Manual tracking slows processes	63	2.03	.695
Lack of real-time ISMS monitoring	63	2.11	.743
Coordination across departments	63	2.06	.644
Frequent delays in resolving faults	63	2.08	.747
Staff skills in ISMS maintenance	63	2.10	.712
Maintenance records incomplete/scattered	63	2.11	.650
Reliability ensured by current practices	63	1.92	.655

The descriptive findings reveal that the current ISMS maintenance practices among PSF in Nairobi are poorly executed across all measured dimensions. For example, respondents strongly disagreed that *current practices ensure reliability* (M = 1.92), highlighting the lack of trust in existing systems. Preventive and corrective maintenance also scored low (M = 2.08 and M = 2.06 respectively), suggesting that firms are unable to proactively maintain ISMS or respond swiftly to faults. In addition, weak scores for *incident reporting* (M = 2.02) and *maintenance records* (M = 2.11) suggest that firms lack structured documentation mechanisms. This creates

vulnerabilities such as poor audit readiness and challenges in accountability. Similarly, the perception that *staff are inadequately skilled* (M = 2.10) and *coordination across departments is weak* (M = 2.06) indicates organizational inefficiencies. The consistently low means with relatively small standard deviations (0.64 - 0.76) show that most respondents shared these negative perceptions, confirming a systemic weakness rather than isolated challenges.

These findings reveal that ISMS maintenance practices within Nairobi's private security sector are fragmented, reactive, and largely manual**.** This mirrors the situation reported by Chege (2023), who found that many Kenyan firms lacked systematic approaches to documentation, monitoring, and follow-up, thereby undermining ISO 27001 compliance. Similarly, Jevelin and Faza (2023) observed that most organizations operate at maturity levels I and II characterized by basic control implementation but weak continuous monitoring and maintenance.

The low mean scores for staff skills and coordination also point to limited technical capacity and weak organizational culture. According to Omari and Mwarey (2020)**,** private security firms in Kenya often lack adequately trained ICT personnel, leading to ad hoc and inconsistent ISMS operations. This aligns with Tan and Kim (2021)**,** who argued that when ISMS is treated as the responsibility of a few specialists rather than a collective organizational function, maintenance activities become deprioritized and underfunded.

Overall, the descriptive results indicate that ISMS maintenance is not embedded into daily operations and that private security firms continue to operate reactively rather than proactively placing them at risk of system failures and non-compliance.

4.3.2 Correlation analysis

Correlation analysis was conducted to examine the relationship between current ISMS maintenance practices and system effectiveness, tested at the 0.01 level as shown in Table 4.7.

Table 4.2

Correlation between Current ISMS Maintenance Practices and System Effectiveness

		Current ISMS maintenance practices	**System effectiveness**
Current ISMS maintenance practices	Pearson Correlation	1	-.650**
	Sig. (2-tailed)		.000
	N	63	63
System effectiveness	Pearson Correlation	-.650**	1
	Sig. (2-tailed)	.000	
	N	63	63

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

The results in Table 8 show a strong, negative, and significant correlation ($r = -0.650$, $p < 0.01$)**,** indicating that reliance on current ISMS practices is associated with reduced system effectiveness. The strong negative correlation demonstrates that current ISMS maintenance practices are inversely related to system effectiveness. This means that the more firms depend on their existing approaches, the less efficient their ISMS operations become. Similar findings were reported by Ahmed et al. (2022), who established that organizations with outdated ISMS practices not only suffered frequent breaches but also displayed poor compliance with data protection laws. Given that private security firms in Nairobi share many characteristics with SMEs such as limited budgets and expertise these results imply that their reactive and manual methods directly undermine system reliability and compliance readiness.

4.3.3 Regression model analysis Between Current ISMS Maintenance Practices and System Effectiveness

The regression model in Table 4.8 produced an R^2 value of 0.423, indicating that 42.3% of the variation in system effectiveness can be explained by the predictor, current ISMS maintenance practices. The remaining 57.7% is accounted for by other factors not included in the model.

Table 4.3

Regression Model Summary Analysis

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.650[a]	.423	.414	.59116

a. Predictors: (Constant), Current ISMS maintenance practices

The R^2 value of 0.423 in Table 9 confirms that weak maintenance practices account for a substantial portion of system inefficiency. The remaining 57.7% of unexplained variance may stem from other organizational factors such as governance, resourcing, or policy implementation. These findings validate concerns raised by Jevelin and Faza (2023) and Chege (2023)**,** who both noted that without structured maintenance frameworks, ISMS effectiveness declines sharply even when some controls are present. This indicates that the challenges in Nairobi's private security sector are structural rather than incidental and improving ISMS effectiveness will require systematic interventions rather than piecemeal fixes.

4.3.4 Anova analysis Between Current ISMS Maintenance Practices and System Effectiveness

The ANOVA results in Table 4.9 show that the regression model with current ISMS maintenance practices as the predictor is statistically significant, $F(1, 61) = 44.714$, p

< 0.001. This confirms that current ISMS practices significantly predict system effectiveness.

Table 4.4

ANOVA Test Results Between Current ISMS Maintenance Practices and System Effectiveness

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	15.626	1	15.626	44.714	.000[b]
	Residual	21.318	61	.349		
	Total	36.944	62			

a. Dependent Variable: System effectiveness

b. Predictors: (Constant), Current ISMS maintenance practices

The ANOVA results in Table 10 confirms the statistical significance of the relationship, meaning that ISMS maintenance practices are a critical determinant of effectiveness. This aligns with findings by Almuhammadi and Alsaleh (2021)**,** who argued that weak incident management and lack of structured response frameworks directly compromise ISMS outcomes. In Nairobi, where incident reporting is still largely manual, the absence of standardized systems likely exacerbates recovery delays and system downtime.

4.3.5 Regression coefficient Analysis Between Current ISMS Maintenance Practices and System Effectiveness

The regression coefficients is as presented in Table 4.10.

Table 4.5:

Regression Coefficients Test Results Between Current ISMS Maintenance Practices *and System Effectiveness*

Model		Unstandardized Coefficients		Standardized Coefficients	T	Sig.
		B	Std. Error	Beta		
1	(Constant)	4.763	.285		16.741	.000
	Current ISMS maintenance practices	-.893	.133	-.650	-6.687	.000

a. Dependent Variable: System effectiveness

The regression coefficients in Table 4.10 show that current ISMS maintenance practices have a statistically significant negative effect on system effectiveness, reflected in the standardized coefficient of Beta = -0.650 with a p value below .001. This strong inverse relationship indicates that as firms continue relying on their existing maintenance approaches, the performance of their systems steadily declines. The unstandardized coefficient of B = -0.893 adds further clarity by showing that a one unit increase in the score for current maintenance practices corresponds to a drop of almost 0.9 units in overall system effectiveness. The large negative t value of -6.687 reinforces that this effect is both meaningful and statistically reliable.

Taken together, these results point to a deeper issue: the maintenance approaches currently used by private security firms are not only falling short but are actively working against the proper functioning of their ISMS. The negative direction and

magnitude of the coefficients suggest that the everyday practices guiding maintenance tasks, documentation, monitoring, and follow up are weakening the system rather than supporting it. Because the p value is well below the usual threshold, this pattern is unlikely to be accidental. It reflects consistent gaps in how maintenance processes are structured and carried out. These findings resonate with what other studies have observed. Ahmed et al. (2022) note that outdated and reactive ISMS processes tend to increase exposure to breaches and reduce compliance, while the Communications Authority of Kenya (CAK 2022) report highlights common challenges in Kenya, including weak reporting structures, limited documentation, and irregular monitoring routines. The results from this study echo these concerns and show that private security firms in Nairobi are encountering the same kinds of difficulties.

The negative regression effect suggests that continuing with the present maintenance routines will keep system performance at a disadvantage. In practice, this means firms will struggle to maintain dependable security operations or meet regulatory expectations. A shift toward structured and technology supported approaches becomes necessary in order to improve how maintenance activities are tracked, coordinated, and reported. The ISMS Maintenance Tracking System proposed in this study offers a way forward by enabling real time monitoring, automated logging, and clearer accountability. In doing so, it can help reverse the downward trend observed in the regression analysis and support stronger, more reliable system effectiveness.

4.4 To Best Practices in ISMS Maintenance and Tracking among security firms in Nairobi County.

The second objective of the study was to investigate ISMS maintenance and tracking best practices among the security firms in Nairobi County.

4.4.1 Descriptive Statistics

Table 4.6 presents the descriptive statistics for Objective Two. The findings reveal that mean scores for all items ranged between 3.90 and 4.02 on a five-point scale, indicating that respondents strongly agreed with the importance of recognised best practices.

Table 4.6

Descriptive Statistics for Recognized Best Practices in ISMS Maintenance

Item	N	Mean	Std. Dev
Importance of preventive maintenance scheduling	63	4.02	.684
Importance of corrective maintenance standardization	63	3.94	.619
Importance of SLA compliance tracking	63	4.00	.672
Importance of real-time monitoring	63	3.98	.660
Importance of automated incident logging	63	4.02	.729
Importance of compliance reporting integration	63	3.98	.635
Importance of knowledge base for fault resolution	63	3.90	.665
Importance of mobile-first ISMS access	63	3.90	.615
Importance of adopting international standards	63	4.02	.707
Importance of integrating physical and cybersecurity	63	4.00	.672

The findings reveal that respondents consistently recognize the value of best practices in ISMS maintenance and tracking. Items such as preventive maintenance scheduling (M = 4.02) and automated incident logging (M = 4.02) demonstrate the importance attached to proactive and technology-driven approaches to ISMS maintenance. SLA compliance tracking (M = 4.00) and the integration of physical and cybersecurity (M = 4.00) reflect the demand for accountability and comprehensive protection within security firms. Even items with slightly lower scores, such as knowledge-base use for

fault resolution (M = 3.90) and mobile-first ISMS access (M = 3.90), still fall within the “agree” range, showing that respondents view modern and user-friendly approaches as essential. The low standard deviations (0.61–0.73) across all items indicates a strong consensus.

These results indicate that ICT managers in private security firms strongly value structured best practices such as preventive scheduling, automated logging, SLA compliance tracking, and integration of physical and cyber controls. The high means (3.90 - 4.02) suggest that these practices are perceived as essential for accountability, efficiency, and responsiveness.

This aligns with Chege (2023), who found that organizations that consistently implemented best practices regular risk assessments, structured audits, and documented incident responses achieved stronger compliance and resilience. Jevelin and Faza (2023) similarly observed that ISMS maturity significantly improved once structured best practices were institutionalized.

The emphasis on preventive scheduling and automated logging echoes Tan and Kim (2021), who noted that proactive, technology-driven ISMS maintenance fosters organizational trust and reduces vulnerabilities. The Nairobi firms’ recognition of SLA compliance tracking also reflects findings by Ahmed et al. (2022), who identified SLA monitoring as a key determinant of ISMS maturity in SMEs. These results demonstrate a clear awareness and acceptance of what effective ISMS maintenance should look like highlighting a readiness to transition from manual, reactive systems to structured, technology-supported practices.

4.4.2 Correlation analysis

Correlation analysis was conducted to examine the strength, direction, and statistical significance of the relationship between best practices in ISMS maintenance tracking and system effectiveness as shown in Table 4.12. Statistical significance was tested at the 0.01 level.

Table 4.7

Correlation test results between Best Practices in ISMS Maintenance Tracking and System Effectiveness

		Current ISMS maintenance practices	**System effectiveness**
Current ISMS maintenance practices	Pearson Correlation	1	-.650**
	Sig. (2-tailed)		.000
	N	63	63
System effectiveness	Pearson Correlation	-.650**	1
	Sig. (2-tailed)	.000	
	N	63	63

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

The positive and significant correlation ($r = 0.592$, $p < 0.01$) shows that higher adoption of best practices is strongly associated with greater system effectiveness. This confirms that structured ISMS practices are not only theoretically sound but have measurable performance benefits.

This finding supports Chege (2023) and Tan and Kim (2021)**,** who reported that consistent implementation of preventive audits and automated reporting systems enhances reliability and user confidence. The Nairobi results therefore reinforce the global consensus that embedding best practices directly improves ISMS outcomes**.**

4.4.3 Regression Model Summary Analysis Between Best Practices in ISMS Maintenance Tracking and System Effectiveness

Regression analysis was conducted to determine the predictive influence of best practices in ISMS maintenance tracking on system effectiveness as shown in Table 4.8.

Table 4.8

Regression Model Summary Results Between Best Practices in ISMS Maintenance Tracking and System Effectiveness

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.592[a]	.350	.339	.62739

a. Predictors: (Constant), Best practices in ISMS maintenance tracking

The $R^2 = 0.350$ indicates that best practices explain 35% of the variance in system effectiveness, confirming their substantial influence. This is consistent with Jevelin and Faza (2023)**,** who found that formalized best-practice adoption led to measurable ISMS maturity gains. These results show that applying best practices such as preventive scheduling, automation, and SLA monitoring significantly enhances ISMS performance and provides an evidence-based foundation for developing the proposed ISMS Maintenance Tracking System.

4.4.4 Anova analysis Between Best Practices in ISMS Maintenance Tracking and System Effectiveness

ANOVA was conducted to test whether the regression model with best practices in ISMS maintenance tracking as the predictor significantly explains variation in system effectiveness as shown in Table 4.9.

Table 4.9

Anova Analysis Results Between Best Practices in ISMS Maintenance Tracking and System Effectiveness

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	12.934	1	12.934	32.858	.000[b]
	Residual	24.011	61	.394		
	Total	36.944	62			

a. Dependent Variable: System effectiveness

b. Predictors: (Constant), Best practices in ISMS maintenance tracking

The results in Table 4.9 show that the model is statistically significant, $F(1, 61) = 32.858$, $p < 0.001$. This means that best practices in ISMS maintenance tracking will significantly predict system effectiveness once implemented. The statistically significant F-value demonstrates that best-practice implementation is a strong determinant of ISMS effectiveness**.** This aligns with Ahmed et al. (2022)**,** who showed that SLA compliance and structured audit monitoring directly improve performance in SMEs. For Nairobi's private security firms, this means that embedding these practices through automated tools will translate to tangible performance improvements and regulatory compliance.

4.4.5 Regression of coefficient analysis Between Best Practices in ISMS Maintenance Tracking and System Effectiveness

The regression coefficients were examined to determine the contribution of best practices in ISMS maintenance tracking to system effectiveness. The results are as shown in Table 4.10.

Table 4.10

Regression Coefficient Test Results Between Best Practices in ISMS Maintenance Tracking and System Effectiveness

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.
		B	Std. Error	Beta		
1	(Constant)	-.313	.571		-.549	.585
	Best practices in ISMS maintenance tracking	.815	.142	.592	5.732	.000

a. Dependent Variable: System effectiveness

The regression coefficients in Table 16 show that best practices in ISMS maintenance tracking make a strong and statistically significant contribution to system effectiveness. The positive standardized coefficient of Beta = 0.592, together with a p value below .001, indicates that as organizations increase their use of best practices, the effectiveness of their systems improves. This relationship is further illustrated by the unstandardized coefficient of B = 0.815, which shows that a one unit increase in the adoption of best practices corresponds to an expected increase of about 0.8 units in system effectiveness. The t value of 5.732 confirms that this effect is both meaningful and reliable.

These findings suggest that firms that follow structured and well-designed maintenance practices place themselves in a stronger position to sustain and protect their ISMS. The positive direction and sizeable magnitude of the coefficients show that best practices contribute directly to better performance, stronger monitoring, and more reliable reporting. Unlike reactive or manual approaches, these practices reinforce the system by providing consistency, clarity, and improved visibility across maintenance activities.

The results align with previous studies. Prislan et al. (2020) showed that automated logs, clear audit trails, and structured reporting significantly increase ISMS adoption and resilience. The present study reflects the same pattern, where firms that embed these features into their maintenance routines demonstrate stronger and more stable system outcomes. The data also highlight the growing importance of integrating physical and cyber security controls, an approach supported by Almuhammadi and Alsaleh (2021), who found that unified control environments reduce breach incidents and improve recovery.

There is also an organizational dimension to these findings. Tan and Kim (2021) note that best practices are most effective when they are embedded into the culture of an institution rather than implemented in isolation. This is particularly relevant for private security firms in Nairobi, many of which face challenges such as limited budgets, high staff turnover, and inconsistent procedural adherence. When best practices are formalized and supported by technology, they become less dependent on individual expertise and more ingrained in the daily functioning of the organization.

In this context, the proposed ISMS Maintenance Tracking System provides a structured way to put these best practices into action. By moving from manual processes to a more coordinated and automated approach, firms can strengthen accountability, improve compliance, and build systems that are more resilient over time. The positive effects observed in the regression analysis reflect the kind of improvements that this system is designed to support, offering a pathway toward more reliable and sustainable ISMS maintenance.

4.5 System Effectiveness (Dependent Variable)

The final set of items measured perceptions of system effectiveness, which served as the dependent variable in this study.

4.5.1 Descriptive analysis

Ten Likert-scale items were used to assess respondents' perceptions of the expected effectiveness of the proposed ISMS Maintenance Tracking System.

Table 4.11

Descriptive Statistics for System Effectiveness

Item	N	Mean	Std. Dev
System will improve preventive maintenance scheduling	63	2.97	.842
System will reduce corrective maintenance delays	63	2.92	.848
System will minimize ISMS downtime	63	2.97	.897
System will ensure accurate audit-ready records	63	2.90	.893
System will strengthen SLA compliance	63	2.84	.902
System will reduce recurring ISMS faults	63	2.94	.896
System will provide staff access to ISMS information	63	2.84	.787
System will increase client satisfaction	63	2.92	.903
System will enhance regulatory compliance	63	2.95	.831
System will improve efficiency and accountability	63	3.02	.813

The findings presented in Table 4.11 show mean scores ranging from 2.84 to 3.02, indicating generally moderate expectations regarding the system's ability to improve

maintenance performance, compliance, accountability, and operational efficiency. Although respondents did not express strong confidence in the proposed system prior to implementation, the ratings suggest cautious optimism regarding its potential contribution to ISMS maintenance activities.

The moderate expectations observed in this study provide an interesting perspective when considered alongside existing literature. Previous studies have consistently reported positive relationships between technology-supported maintenance processes and organisational performance. For example, Chege (2024) found that organizations implementing structured ISMS practices generally experience improvements in compliance, accountability, and operational effectiveness. Similarly, Marhad et al. (2024) observed that automation and systematic monitoring contribute significantly to improved responsiveness and maintenance performance. The current findings do not contradict these studies; rather, they suggest that respondents recognise the theoretical value of such systems but remain uncertain about whether these benefits can be realised within their own organisational contexts.

This cautious outlook may be explained by the challenges identified earlier in the study. Sections 4.3 and 4.4 revealed widespread weaknesses in documentation, monitoring, coordination, and maintenance planning. Consequently, respondents may have evaluated the proposed system against their experiences with fragmented and largely manual processes. This interpretation aligns with Rana et al. (2015), who argue that technology adoption in developing organisational environments is influenced not only by perceived usefulness but also by contextual realities such as organisational readiness, infrastructure, and prior experiences with information systems. The findings

therefore suggest that confidence in system effectiveness is shaped not only by the features of the technology itself but also by the operational environment into which it is introduced.

The relatively lower ratings for SLA compliance and staff access to ISMS information are particularly noteworthy. Contemporary literature increasingly emphasises service-oriented management and information accessibility as critical components of effective ISMS maintenance. ISO/IEC 20000-1:2018 advocates the use of measurable service standards, while Alhumaidi (2025) argue that maintenance effectiveness improves when performance is monitored against clearly defined operational metrics. Despite this, respondents appeared less convinced that the proposed system would significantly strengthen these areas. This may indicate a gap between recognition of best practices and confidence in organisational capacity to implement them effectively. Such a finding extends existing literature by suggesting that acceptance of maintenance principles does not automatically translate into confidence in implementation outcomes.

At the same time, respondents expressed comparatively stronger expectations regarding efficiency, accountability, preventive maintenance scheduling, and regulatory compliance. These findings are consistent with ISO/IEC 27001:2022, which emphasises continual monitoring, documented controls, and evidence-based management as foundations for effective information security governance. The findings also support observations by Turetken et al. (2020), who found that structured monitoring and audit mechanisms strengthen organisational accountability and control effectiveness. The present study therefore reinforces the growing consensus that

improvements in maintenance performance are closely linked to enhanced visibility, traceability, and process discipline.

Overall, the descriptive findings suggest that ICT managers recognise the potential value of structured ISMS maintenance systems but remain cautious about the extent to which such benefits can be achieved in practice. This finding contributes to the literature by highlighting an important distinction between awareness of best practices and confidence in their operational implementation. The results imply that successful ISMS maintenance systems must not only embody recognised best practices but also demonstrate practical and visible improvements capable of overcoming organisational scepticism and building user trust.

4.5.2 Multiple Linear Regression of ISMS Maintenance Practices and System Effectiveness in Private Security Firms in Nairobi

Regression analysis was conducted to determine the joint predictive influence of current ISMS maintenance practices and best practices in ISMS maintenance tracking on system effectiveness in private security firms in Nairobi, as shown in Table 4.17.

Table 4.12

Multiple Linear Regression Results of ISMS Maintenance Practices and System Effectiveness in Private Security Firms in Nairobi

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.866[a]	.750	.741	.39265

a. Predictors: (Constant), Best practices in ISMS maintenance tracking, Current ISMS maintenance practices

The regression results presented in Table 18 show that current ISMS maintenance practices and best practices in ISMS maintenance tracking jointly explain 75.0% of the variation in system effectiveness ($R^2 = 0.750$). This indicates that maintenance-related factors exert substantial influence on the effectiveness of information security management systems within private security firms.

The magnitude of the explained variance is significant because it demonstrates that maintenance practices are not peripheral activities but central determinants of ISMS performance. This finding supports the position advanced by Muchiri et al. (2026), who found that maintenance quality significantly influences organisational information security outcomes. Similarly, ISO/IEC 27001:2022 positions maintenance, monitoring, and continual improvement as integral components of an effective ISMS rather than supplementary operational activities. The current findings therefore reinforce the argument that maintenance management should be viewed as a strategic capability rather than a purely technical function.

The strength of the model also contributes to ongoing discussions within maintenance management literature. Jardine et al. (2006) argue that effective maintenance depends on structured processes capable of generating reliable operational information. Likewise, Bokrantz et al. (2020) contend that advanced maintenance capabilities ultimately depend on the quality and availability of maintenance data. The high explanatory power observed in the current study provides empirical support for these arguments by demonstrating that maintenance structures and practices account for a substantial proportion of perceived system effectiveness.

At the same time, the findings extend previous research by showing that maintenance practices remain highly influential even within the context of private security firms, a sector that has received limited attention within ISMS maintenance literature. Whereas much existing research focuses on manufacturing, service management, or general information systems, the current study demonstrates that maintenance-related practices play an equally important role within security-oriented environments characterised by both physical and information security responsibilities.

The findings therefore suggest that improvements in ISMS effectiveness are likely to be achieved not merely through the acquisition of security technologies but through strengthening the maintenance processes that support those technologies. This provides empirical justification for the development of the proposed ISMS Maintenance Tracking System as a mechanism for improving organisational performance.

4.5.3 ANOVA Analysis for Multiple Regression of ISMS Maintenance Practices and System Effectiveness in Private Security Firms in Nairobi

ANOVA was conducted to test whether the regression model with current ISMS maintenance practices and best practices in ISMS maintenance tracking significantly explains variation in system effectiveness in private security firms in Nairobi. The results are as shown in Table 4.18.

Table 4.13

*ANOVA Results for Multiple Regression of ISMS Maintenance Practices and **System** Effectiveness in Private Security Firms in Nairobi*

Model		Sum of Squares	Df	Mean Square	F	Sig.
1	Regression	27.694	2	13.847	89.812	.000[b]
	Residual	9.250	60	.154		
	Total	36.944	62			

a. Dependent Variable: System effectiveness

b. Predictors: (Constant), Best practices in ISMS maintenance tracking, Current ISMS maintenance practices

The ANOVA results presented in Table 19 indicate that the regression model is statistically significant, $F(2,60) = 89.812$, $p < 0.001$. This confirms that the combined effect of current maintenance practices and best-practice maintenance tracking significantly predicts system effectiveness.

The significance of the overall model supports arguments within ISMS literature that maintenance activities have direct implications for organisational security performance. Previous studies have often examined individual maintenance practices in isolation. However, the current findings suggest that effectiveness emerges from the interaction of multiple maintenance factors operating together. This observation aligns with DeLone and McLean's (2003) Information Systems Success Model, which emphasises that organisational outcomes are typically influenced by interconnected system, information, and process quality dimensions rather than isolated variables.

The findings also support the broader principle of continual improvement embedded within ISO/IEC 27001:2022. The standard assumes that organisational effectiveness results from the coordinated implementation of multiple controls and management processes. The present study provides empirical evidence consistent with this assumption by demonstrating that maintenance effectiveness is significantly influenced by the combined operation of current practices and recognised best practices rather than any single intervention.

Furthermore, the statistical significance of the model challenges the perception that maintenance activities represent routine operational functions with limited strategic importance. Instead, the findings suggest that maintenance practices constitute a major organisational capability with measurable implications for ISMS effectiveness. This contributes to the growing body of evidence advocating stronger integration of maintenance management into broader information security governance frameworks.

4.5.4 Joint Regression coefficients Between ISMS Maintenance Practices and System Effectiveness in Private Security Firms in Nairobi

The joint regression analysis is as shown in Table 4.14

Table 4.14

Joint Regression coefficients Results Between ISMS Maintenance Practices and System Effectiveness in Private Security Firms in Nairobi

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.
		B	Std. Error	Beta		
1	(Constant)	1.581	.406		3.891	.000
	Current ISMS maintenance practices	-.868	.089	-.632	-9.784	.000
	Best practices in ISMS maintenance tracking	.788	.089	.572	8.847	.000

a. Dependent Variable: System effectiveness

The regression coefficients presented in Table 20 reveal a striking contrast between the influence of current maintenance practices and recognised best practices on system effectiveness. Current ISMS maintenance practices exhibited a significant negative effect on system effectiveness ($\beta = -0.632$, $p < 0.001$), whereas best practices in ISMS maintenance tracking demonstrated a significant positive effect ($\beta = 0.572$, $p < 0.001$).

The negative relationship associated with current maintenance practices provides empirical support for the challenges identified earlier in the study. The findings suggest that continued reliance on fragmented documentation, irregular monitoring, reactive

maintenance, and manual coordination mechanisms undermines overall ISMS effectiveness. This observation is consistent with findings by Whitman and Mattord (2022), who argue that poorly coordinated security processes create vulnerabilities that weaken organisational security performance. Similarly, Ireri (2025) found that weak maintenance governance structures reduce the effectiveness of security management initiatives despite organisational awareness of best practices.

The positive effect associated with recognised best practices reinforces the importance of structured maintenance management approaches. This finding converges with Chege (2024), who reported that organizations implementing systematic ISMS controls generally achieve stronger operational outcomes. It also supports observations by Marhad et al. (2024), who found that automation, monitoring, and traceability contribute positively to maintenance effectiveness and compliance readiness. However, the current study extends these findings by quantifying the comparative influence of poor and effective maintenance approaches within a single analytical model. The results demonstrate not only that best practices improve effectiveness, but also that existing practices actively reduce it.

An important insight emerging from the analysis is that the challenge facing private security firms appears to be less about awareness of best practices and more about implementation capability. Earlier findings showed strong support for preventive maintenance, audit trails, continuous monitoring, and SLA tracking. Yet the negative coefficient associated with current practices suggests that these principles have not been consistently translated into operational routines. This finding echoes observations by Whitman et al. (2025), who argue that organizations frequently recognise the

importance of security controls but struggle to institutionalise them through formal processes and supporting technologies.

The findings also contribute a practical perspective to debates surrounding ISMS effectiveness. Much of the literature assumes that adoption of best practices naturally leads to improved outcomes. The current study suggests a more nuanced relationship. Best practices appear to generate value only when supported by systems capable of enforcing consistency, accountability, monitoring, and documentation. In this respect, the study provides evidence that technological artefacts play an important mediating role between maintenance principles and organisational outcomes.

Taken together, the findings demonstrate a clear transition pathway for private security firms. The negative influence of current maintenance practices highlights the limitations of existing approaches, while the positive influence of recognised best practices illustrates the benefits of structured maintenance management. The proposed ISMS Maintenance Tracking System addresses this gap by embedding best practices directly into operational workflows. Consequently, the findings provide empirical support for the study's central proposition that structured, technology-enabled maintenance processes are essential for improving ISMS effectiveness within private security firms in Nairobi County.

4.6 System Analysis, Design and Architecture

4.6.1 System Requirements Analysis

The development of the ISMS Maintenance Tracking System was guided by both functional and non-functional requirements.

4.6.1.1 Functional Requirements:

User Authentication and Access Control - The system provides a secure login interface where each user is validated and redirected to a dashboard based on their assigned role.

System Navigation - After successful login, users interact with a unified environment that offers direct access to projects, clients, personnel, and reports.

Client and Premises Management - Administrators or project managers can register clients and their premises. These records form the foundation for project creation and service tracking.

Project Management - Project managers create and manage projects, define milestones and costs, and link them to specific clients and premises.

Personnel Management and Assignment Planning - Supervisors register and manage personnel, plan assignments, and allocate tasks with set SLAs.

Site and Installation Definition - Projects are structured into sites and installations (e.g., CCTV, alarms). Each site and installation can be created, listed, and updated within the system.

Equipment Planning and Tracking - Equipment details are recorded, assigned to projects, and monitored for usage and maintenance.

Audit Trail Management - Every system activity is automatically logged to create a verifiable trail of actions.

Notification Services - Automatic alerts are generated when tasks are assigned or updated, improving communication and timeliness.

The requirements outlined above are not merely functional specifications but reflect a direct response to the empirical inefficiencies identified in the study context, particularly weak documentation practices, fragmented coordination, and delayed

communication. These challenges closely mirror findings in ISMS literature where maintenance systems are often characterized by manual workflows and limited traceability (Iden & Eikebrokk, 2013; Prislan et al., 2020). In that sense, the system does not introduce entirely new principles but operationalize established ISMS expectations in a more structured and automated form.

At the same time, the study reveals an important contextual divergence from conventional ISMS assumptions. While literature such as ISACA (2023) and Chege (2023) emphasizes automation, preventive scheduling, and traceability as key drivers of ISMS performance, these studies generally assume stable organizational environments. The findings from this study suggest that in private security firms, these principles are often weakened by informal processes and communication delays. The system therefore builds on existing literature by embedding these principles directly into workflow execution rather than treating them as external compliance mechanisms.

4.6.1.2 Non-Functional Requirements:

Security: Encrypted login, audit trails, and role-based access control ensure data protection.

Usability: A simple and intuitive interface designed for users with varying technical skills.

Scalability: Modular design allows for the addition of new features such as compliance reporting and invoicing.

Reliability: Redundancy in logging and notifications ensures system dependability.

The non-functional requirements reflect a convergence with established ISMS design principles, particularly ISO/IEC 27001:2022, which emphasizes confidentiality, integrity, availability, and controlled access as foundational system properties. However, the emphasis on usability and simplicity reflects a contextual adaptation that is less strongly emphasized in traditional ISMS literature. Studies such as True Context (2025) highlight that field-based systems often fail not due to lack of functionality but due to complexity and poor usability, a challenge strongly reflected in the empirical findings of this study.

Similarly, while scalability and modularity are widely supported in literature as technical best practices (Hevner et al., 2004; Prislan et al., 2020), the present study extends this view by showing that modularity in ISMS systems is not only a technical requirement but also a sustainability mechanism in environments where organizational needs evolve unpredictably.

4.6.2 System Design Models

The ISMS Maintenance Tracking System was designed following a three-tier architecture:

Presentation Layer: The web interface through which users interact with the system.

Application Layer: Business logic modules, including login, client management, task assignment, and notifications.

Data Layer: A relational database that stores user details, client information, tasks, and audit logs.

The adoption of a three-tier architecture reflects strong alignment with established software engineering and Design Science principles, particularly the need for modularity and separation of concerns (Hevner et al., 2004). Literature further suggests that such architecture enhances maintainability and adaptability of ISMS systems (Prislan et al., 2020), a finding that is reinforced in this study through the need to independently manage authentication, workflow processing, and data storage components.

However, the study also reveals a practical divergence from typical ISMS architecture assumptions. Much of the literature presumes stable, cloud-connected environments, whereas the empirical context shows intermittent connectivity and field-based operations. This necessitated a more resilient, locally deployable architecture. In this sense, the system builds on existing literature by demonstrating that architectural effectiveness in ISMS systems is contingent not only on design principles but also on environmental feasibility.

4.6.2.1 Data Flow Models:

The system's data flow diagrams illustrate how information moves between modules. For instance, the login process validates credentials against the database and grants access to respective dashboards. Similarly, task creation flows from the supervisor to the database, triggers the Audit Module, and dispatches an email notification. The data flow design aligns with ISO/IEC 27001:2022 requirements for traceability and controlled processing of information assets. However, unlike idealised models in literature that assume continuous system availability, the present system accommodates intermittent operational conditions by ensuring that core workflows

remain functional even under connectivity disruptions. This reflects Kyazze and Nakakawa (2024), who argue that offline-capable systems improve adoption in low-resource environments, while also extending their argument by showing that workflow continuity is essential for ISMS maintenance integrity.

4.6.2.2 Entity-Relationship Diagram (ERD):

The ERD identifies major entities like User, Client, Personnel, Task, and Audit Log and their relationships. Each task record is associated with both a client and assigned personnel, while audit logs are linked to all user actions. The relational structure reflects standard database design principles, particularly the importance of referential integrity in ensuring data consistency. However, the findings of this study highlight that in ISMS maintenance environments, integrity is not merely a technical requirement but a governance mechanism. Ningrum et al. (2026) emphasise that integrity constraints are critical in systems operating under intermittent conditions, as they prevent fragmentation and loss of traceability. The system therefore enforces strict relational dependencies to ensure that maintenance records remain complete and contextually meaningful.

4.6.2.3 Use Case Design:

Use cases were developed to capture the roles of different system actors. For example, administrators manage clients and personnel, supervisors assign tasks, and technicians update task status. These roles ensure the system enforces accountability at all operational levels. This role-based structure aligns with ISMS governance literature, which emphasises the importance of clearly defined responsibilities in maintaining accountability (ISO/IEC 27001:2022). However, the study extends this perspective by

showing that role definition alone is insufficient unless embedded within system-enforced workflows. Hevner et al. (2004) support this view by arguing that effective IS artefacts must reflect real organisational behaviour rather than abstract process definitions.

The system architecture and models not only define how components interact but also embody best practice principles in ISMS maintenance. The adoption of a three-tier structure enhances flexibility and scalability, a factor emphasised in Prislan et al. (2020) as critical for ISMS adoption. At the same time, the study demonstrates that such architectural benefits are only realised when systems are adapted to operational realities such as connectivity limitations and informal workflows.

The inclusion of audit trails and automated flows integrates accountability into daily operations, replacing fragmented manual tracking systems observed in the study context. This finding builds on Ferreira (2025), who argues that governance is most effective when embedded within system processes rather than enforced externally. The present system extends this argument by demonstrating how embedded governance can transform ISMS maintenance from a reactive to a continuous process.

4.6.3 System Modules

The system comprises the following modules derived from the coded implementation:

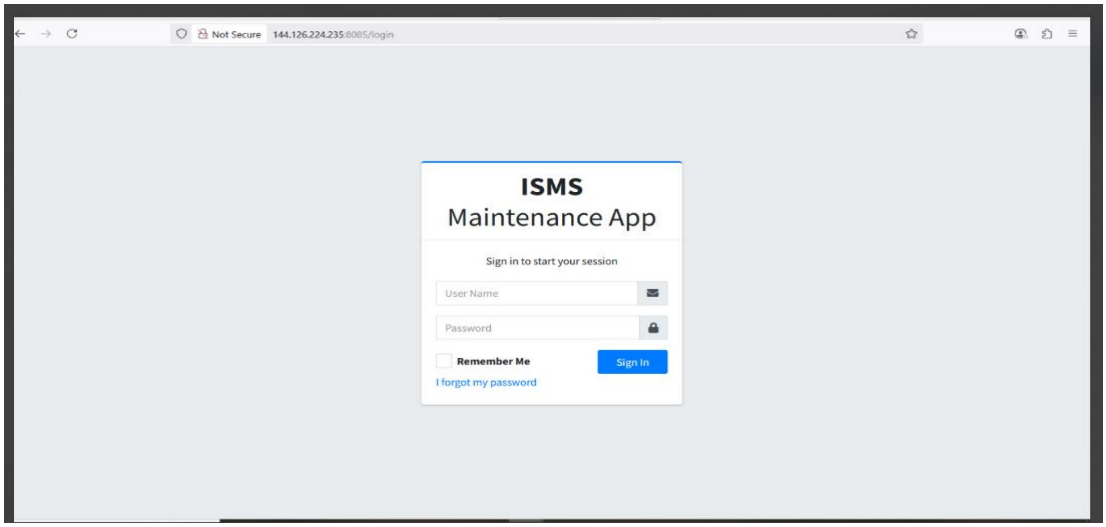
4.6.3.1 Login Module: Validates user identity and grants role-based access.

The login module is responsible for verifying user credentials and ensuring that only authorized personnel can access the system. It provides role-based access, meaning each user such as an administrator, manager, or guard can only view and perform

functions relevant to their assigned role. This enhances security, accountability, and data protection within the ISMS

Figure 4.6

Login Module

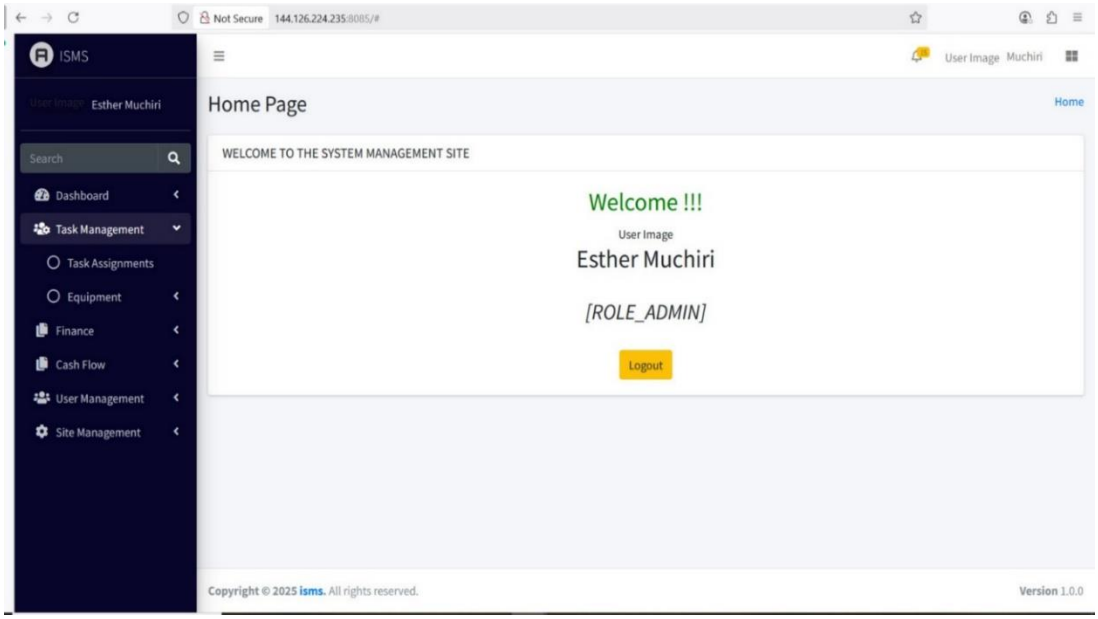


4.6.3.2 System Navigation

After successful login, users interact with a unified environment that offers direct access to projects, clients, personnel, and reports.

Figure 4.7

Welcome page

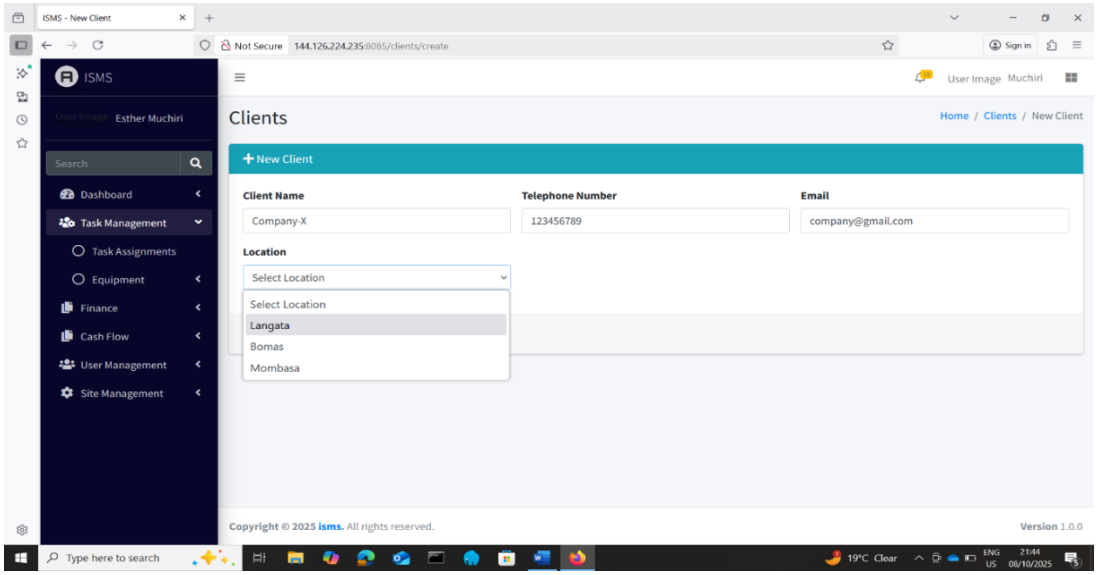


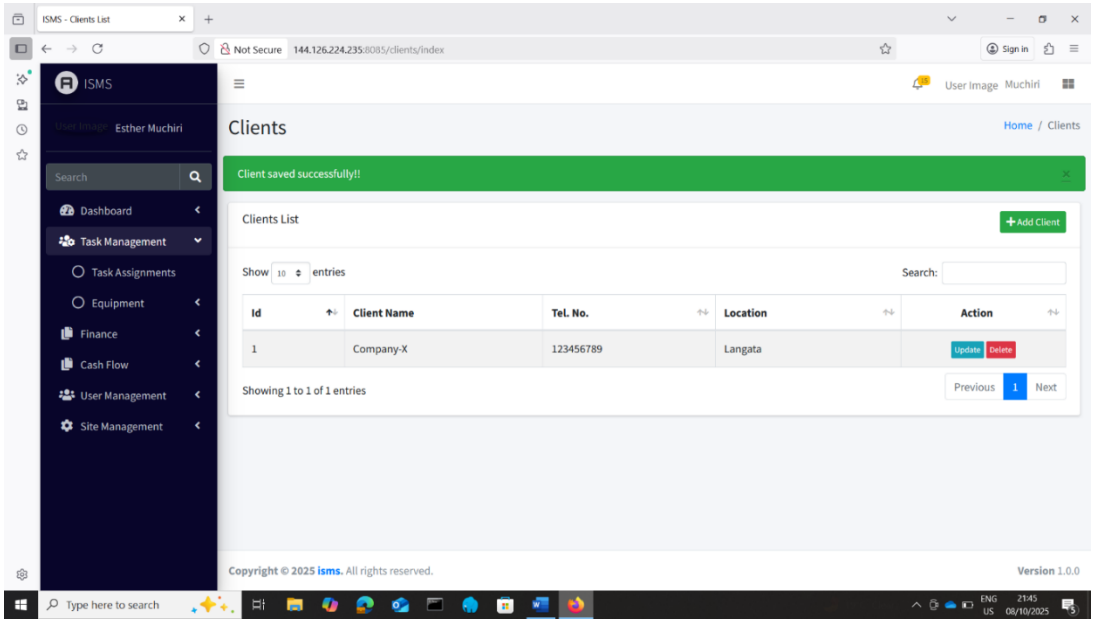
4.6.3.3 Client and Premises Management

Administrators or project managers can register clients and their premises. These records form the foundation for project creation and service tracking.

Figure 4.8

Client and Premises Management



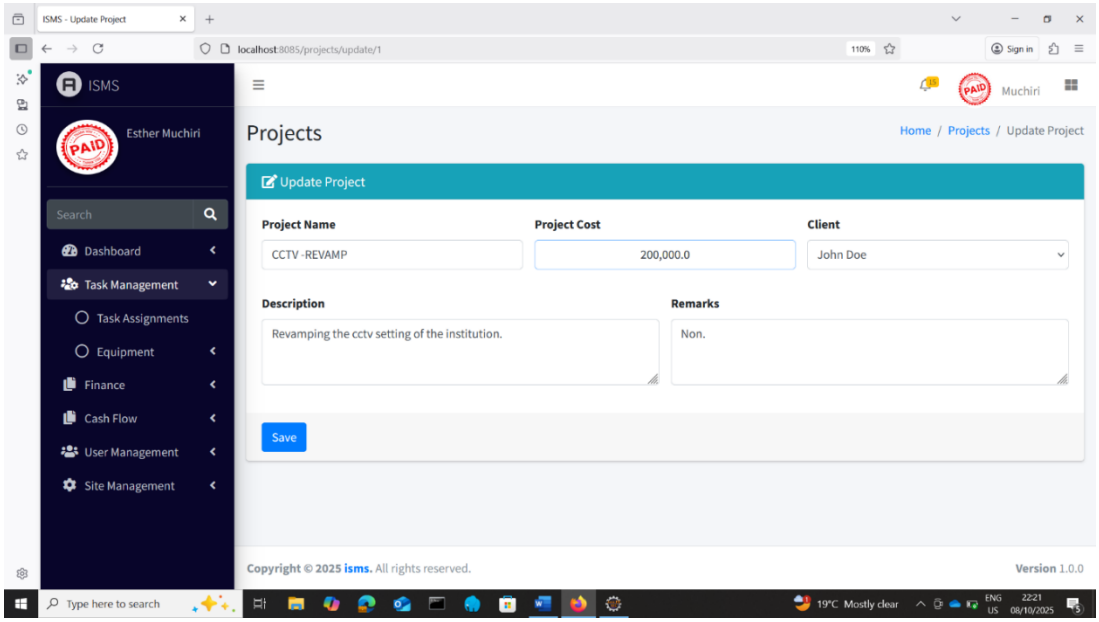


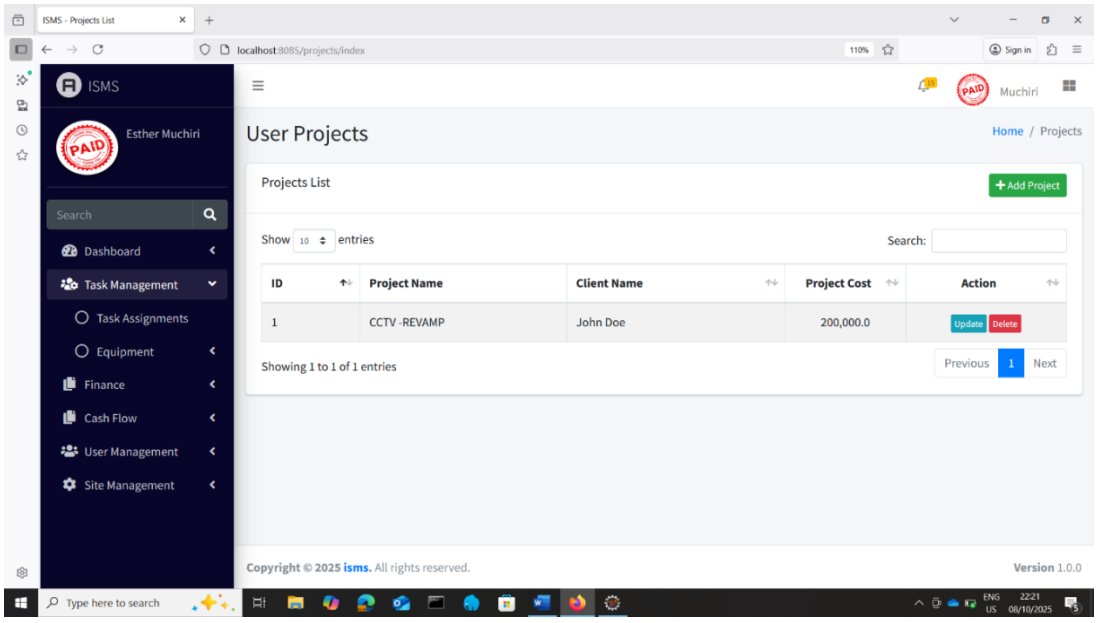
4.6.3.3 Project Management

Project managers create and manage projects, define milestones and costs, and link them to specific clients and premises.

Figure 4.9

Project Management



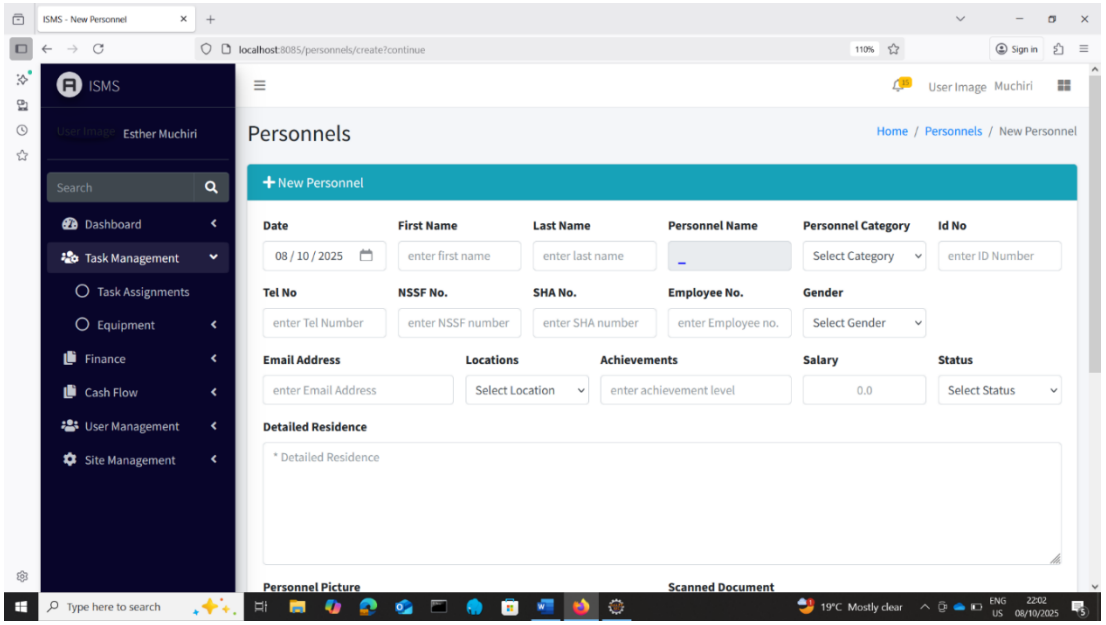


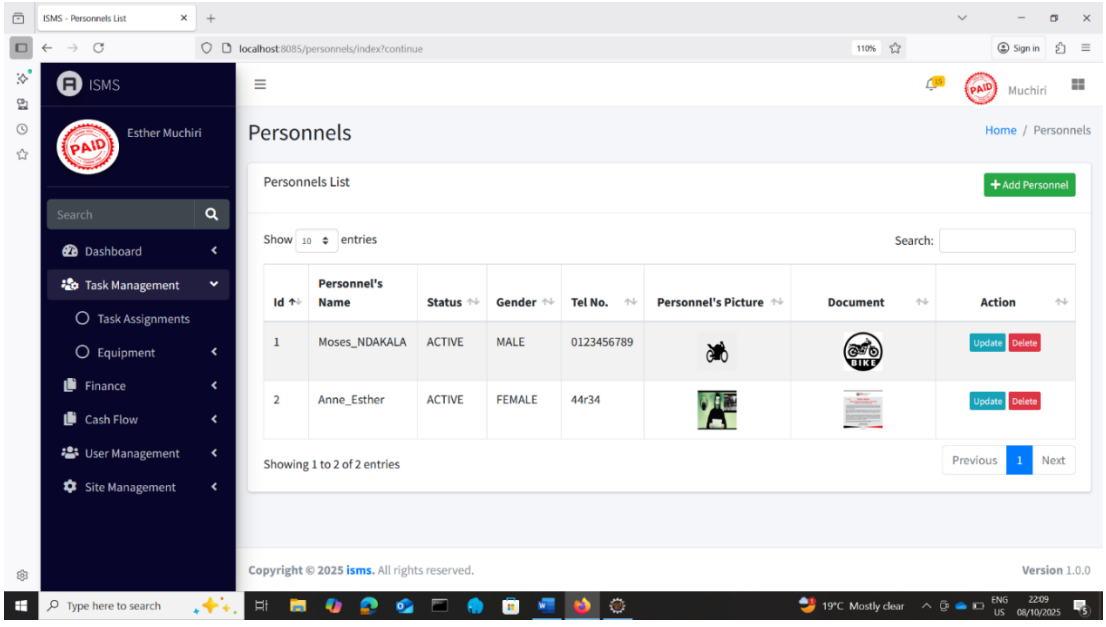
4.6.3.4 Personnel Management and Assignment Planning

Supervisors register and manage personnel, plan assignments, and allocate tasks with set SLAs.

Figure 4.10

Personnel Management

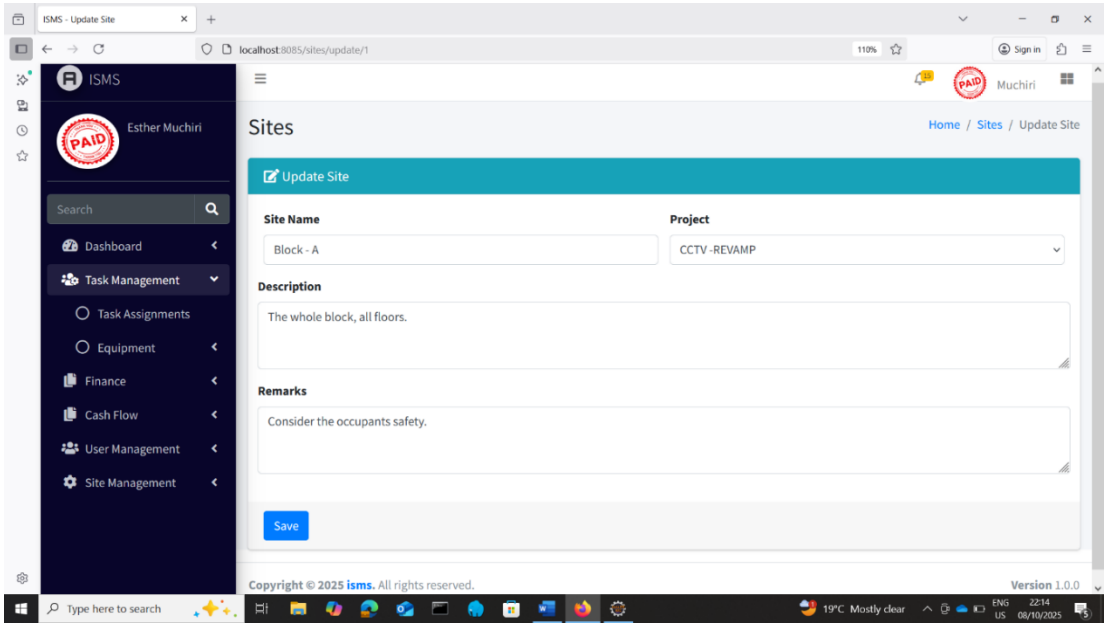


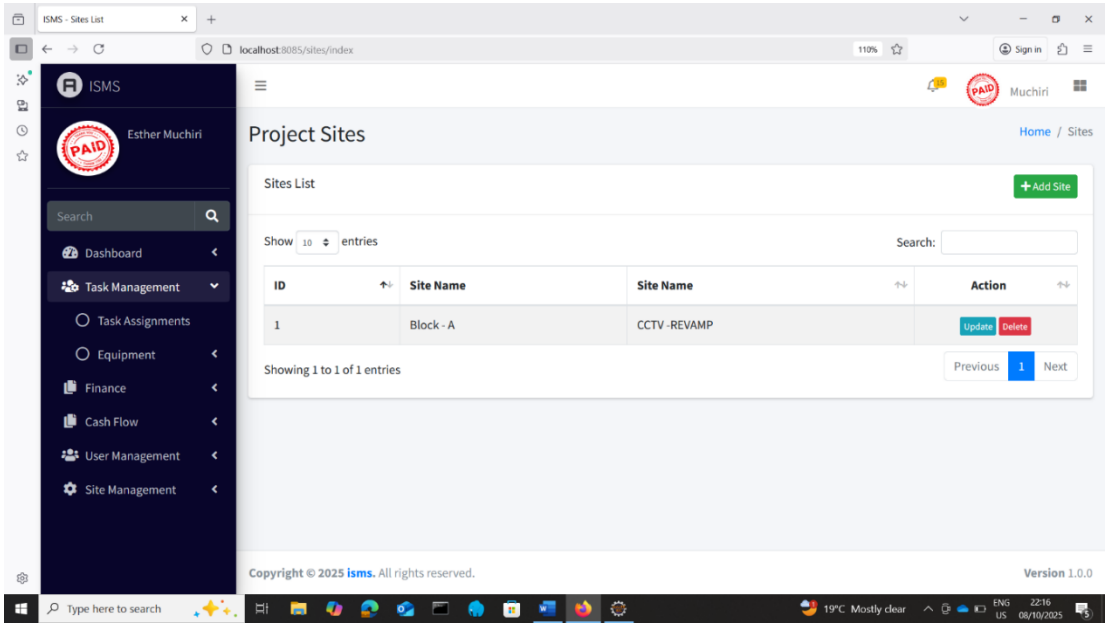


4.6.3.5 Site and Installation Definition - Projects are structured into sites and installations (e.g., CCTV, alarms). Each site and installation can be created, listed, and updated within the system.

Figure 4.11

Site and Installation Definition



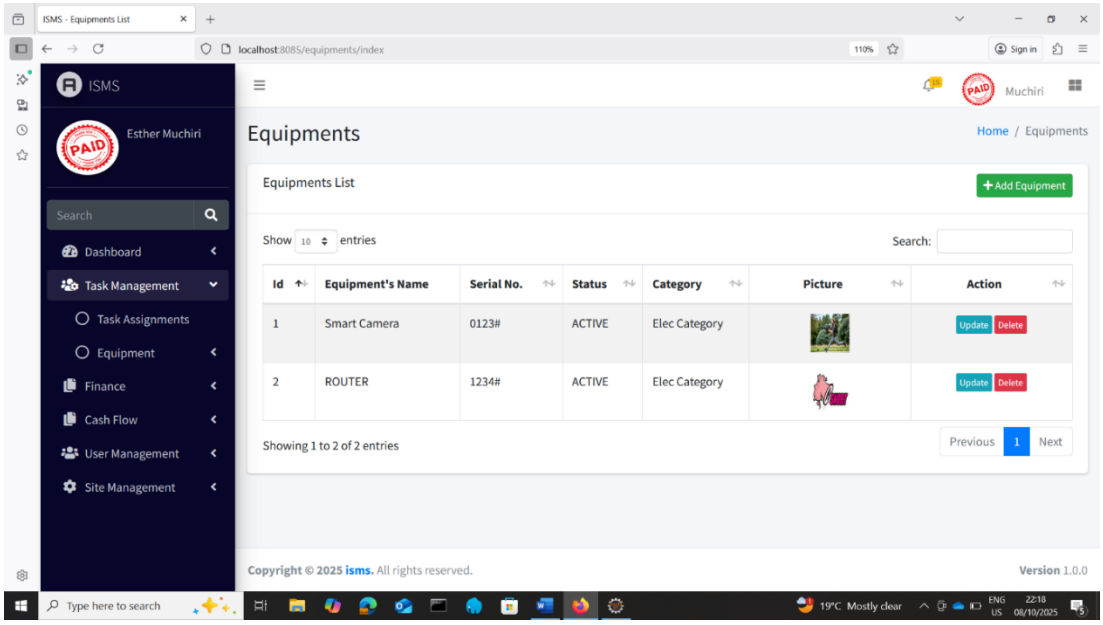


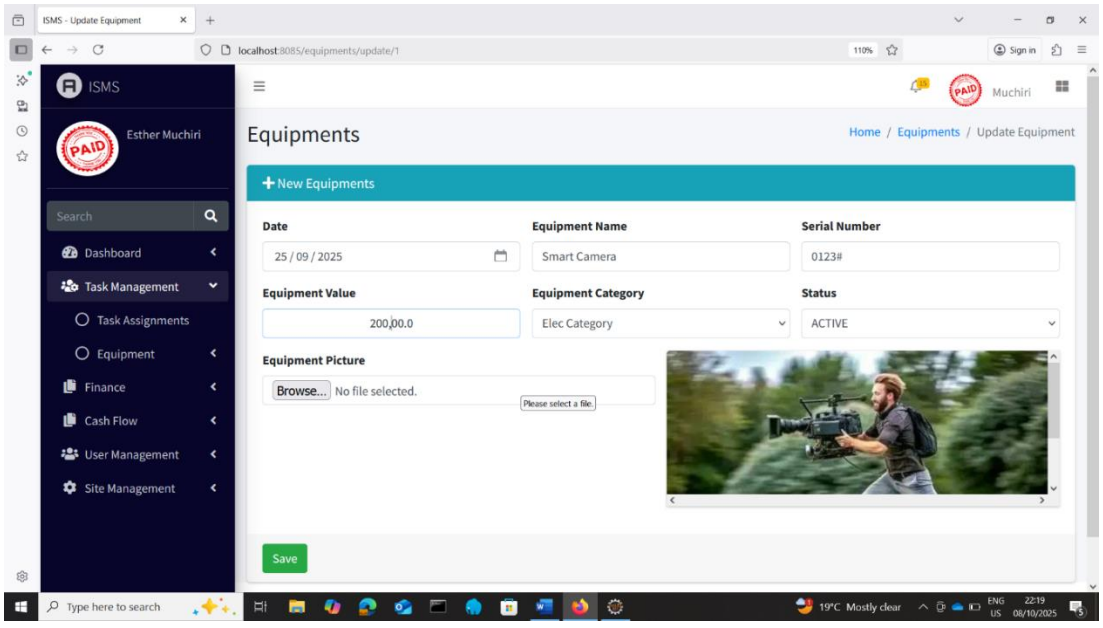
4.6.3.6 Equipment Planning and Tracking

Equipment details are recorded, assigned to projects, and monitored for usage and maintenance.

Figure 4.12

Equipment Planning and Tracking



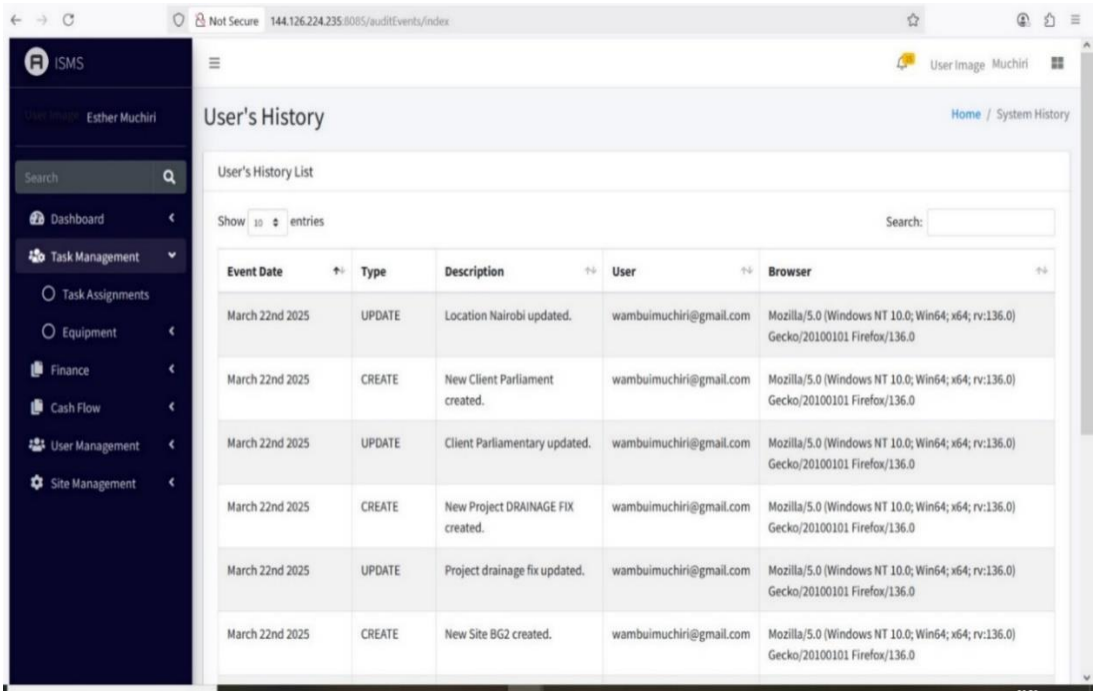


4.6.3.2 Audit Module: Automatically logs every user action for accountability.

The audit module tracks and records all user activities within the system, creating a secure log of actions performed. This ensures accountability, supports transparency, and provides a reliable trail for compliance and security reviews.

Figure 4.13

Audit Module



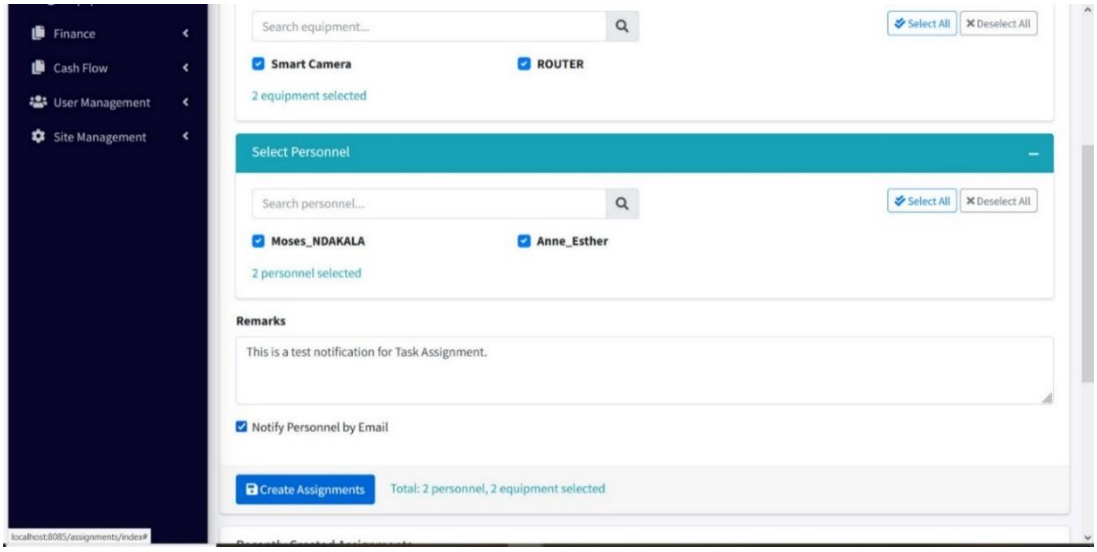
4.6.3.6 Notification Module:

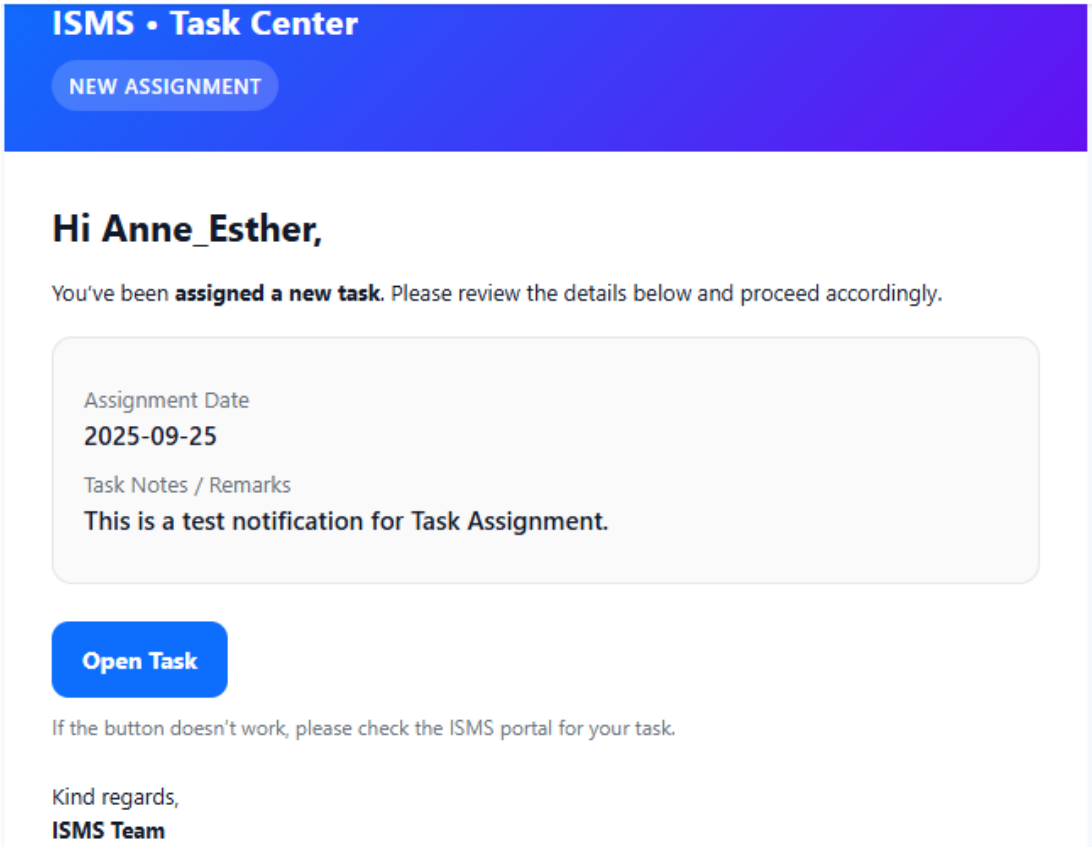
Sends automated email notifications to users when tasks are assigned or updated.

The notification module automates communication by sending email alerts to users whenever tasks are assigned, updated, or require attention. This ensures timely awareness, improves responsiveness, and reduces delays in ISMS maintenance processes.

Figure 4.14

Notification Module



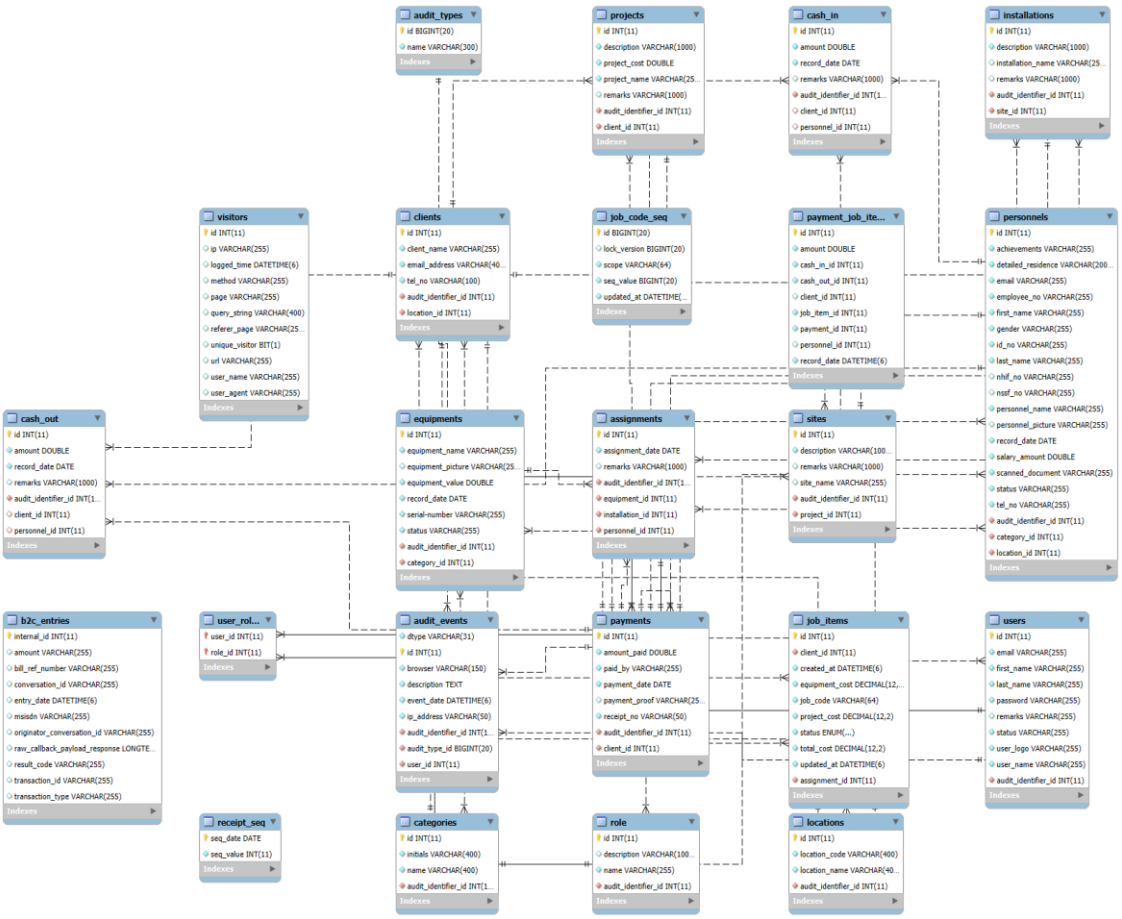


4.6.3.9 Database Design

Shows relational structure linking all modules.

Figure 4.15

Database Design



The system modules operationalize both technical and managerial best practices in ISMS maintenance. The Login and Audit modules enforce access control and traceability, aligning with ISO/IEC 27001-aligned security principles. However, the study shows that beyond compliance, these modules function as governance enforcement mechanisms embedded within daily workflows, rather than external audit tools.

Similarly, the Notification module embeds automation into communication flows, addressing delays identified in the empirical findings. While Marhadi et al. (2024) confirm that automation improves ISMS responsiveness, the present study extends this by demonstrating that simplicity and reliability are more important than technological sophistication in constrained environments.

The Task Assignment and Client modules further strengthen accountability and record accuracy, addressing weaknesses in manual systems identified earlier in the study. Collectively, the modules demonstrate that ISMS maintenance effectiveness is achieved not only through control implementation but through integration of those controls into operational practice.

4.7 System Implementation and Validation

This section addresses the fourth objective of the study, which was to implement and validate the proposed ISMS Maintenance Tracking System in selected private security firms within Nairobi County. The objective was achieved through deployment of the developed system in a simulated operational environment representing the conditions of participating firms, followed by comprehensive testing and validation involving ICT managers from these organizations. Validation focused on assessing the system's functionality, usability, and effectiveness in supporting ISMS maintenance tracking activities.

The implementation and validation stage is particularly significant within the Design Science Research framework because it provides empirical evidence of whether the artefact performs as intended in a real or near-real environment. Hevner et al. (2004) emphasise that the value of an IS artefact is not only in its design coherence but in its

demonstrated utility within its intended context of use. In this regard, the implementation process in this study served as the bridge between theoretical design principles and practical organisational application.

4.7.1 System Implementation

The ISMS Maintenance Tracking System was implemented as a web-based application using a modular development approach to ensure flexibility, scalability, and reliability. The following technologies and tools were adopted during system implementation:

Frontend: HTML, CSS, and JavaScript for user interface design and interaction.
Backend: PHP for application logic to support database transactions and business processes.
Database: MySQL for structured storage and management of user, client, and audit data.
Deployment Environment: XAMPP server for local deployment and multi-user testing.

Each system module was developed and integrated in accordance with the design specifications described in Section 4.6.3. The Login Module provided role-based authentication, the Task Assignment Module enabled creation and tracking of ISMS maintenance tasks, and the Audit Module automatically logged system activities for accountability. The Notification Module sent automated alerts upon task creation or updates, while the Client and Personnel Modules managed records critical for ISMS operations.

The successful validation of the system provides practical evidence that the maintenance best practices identified in Objectives Two and Three can be translated into an operational solution suitable for private security firms. Earlier findings revealed that organizations generally recognised the importance of preventive maintenance, audit trails, continuous monitoring, and structured task management, yet these practices were inconsistently implemented. The developed system addressed this gap by embedding these practices within routine operational workflows.

This finding supports Muchiri et al. (2026), who found that structured maintenance practices contribute positively to ISMS effectiveness. However, the present study extends this argument by demonstrating that awareness of best practices alone is insufficient. Although respondents generally acknowledged the value of recognised maintenance practices, the earlier findings indicated relatively low levels of implementation. The successful deployment of the system therefore suggests that the primary challenge may not be a lack of awareness but rather the absence of practical mechanisms through which best practices can be executed consistently. In this regard, the study contributes evidence that technological support acts as an important bridge between maintenance knowledge and maintenance practice.

Furthermore, the implementation reinforces arguments advanced by ISO/IEC 27001:2022 that effective information security management depends on continual monitoring, documentation, and accountability. Rather than treating these requirements as isolated compliance activities, the developed system integrated them into everyday maintenance processes. This finding suggests that compliance-oriented

controls may achieve greater effectiveness when embedded within operational workflows rather than managed as separate administrative functions.

4.7.2 Testing Strategy

Testing was conducted systematically to confirm that the system met all design and performance requirements. The strategy followed three levels:

Unit Testing**:** Individual modules were tested for correctness and reliability. For instance, login validation, task creation, and audit log generation were tested under multiple scenarios.

Integration Testing: Interactions between modules were verified to ensure data consistency and interoperability. Assigning a task successfully triggered audit log creation and email notifications, confirming that modules communicated as designed.

System and User Acceptance Testing (UAT): The complete system was evaluated by 63 ICT managers from private security firms in Nairobi County. Respondents interacted with the system under guided testing sessions that replicated day-to-day ISMS maintenance tasks, enabling assessment of usability and functionality under practical conditions.

The testing strategy reflects recommendations within Design Science Research that artefacts should be evaluated using multiple approaches capable of assessing both technical performance and practical usefulness. Hevner et al. (2004) and Peffers et al. (2007) argue that artefacts should demonstrate utility rather than merely technical correctness. The present study supports this position by showing that technical

functionality alone would have provided an incomplete assessment of system effectiveness.

The findings further align with Venable et al. (2016), who advocate complementary evaluation methods capable of examining both technological and organisational dimensions of artefact performance. However, the present study adds an important contextual dimension. Within information security environments, technically sound systems may still fail if users perceive them as disruptive or difficult to use. Consequently, combining functional testing with user acceptance testing enabled the study to assess not only whether the system worked correctly but also whether it addressed the practical needs of ICT managers. This suggests that effective evaluation of ISMS artefacts requires balancing technical performance with organisational relevance.

4.7.3 User Validation Results

User acceptance testing provided direct validation from intended end users regarding the system's usability, accessibility, and operational value. Table 4.15 presents a summary of the user responses.

Table 4.15

Consolidated User Responses on System Usability

Response Option	Very Easy (n/%)	Moderately Easy (n/%)	Difficult (n/%)
Ease of Login and Role-Based Access	63 (100%)	0 (0%)	0 (0%)
Ease of Task Assignment and Monitoring	60 (95%)	3 (5%)	0 (0%)
Timeliness and Usefulness of Notifications	63 (100%)	0 (0%)	0 (0%)
User-Friendliness of the System	57 (90%)	6 (10%)	0 (0%)
Overall Usability of the System	63 (100%)	0 (0%)	0 (0%)

The results indicate that all respondents (100%) found login and access management very easy, while all respondents similarly rated notifications as timely and useful. Ninety-five percent rated task assignment and monitoring as very easy, while 90% considered the system highly user-friendly. Overall usability was rated positively by all respondents.

The high levels of user acceptance support the Technology Acceptance Model proposed by Davis (1989), which identifies perceived usefulness and perceived ease of use as important determinants of technology adoption. Similarly, Granić and Marangunić (2019) found that these constructs remain among the strongest predictors of user acceptance across different technological contexts. The positive responses obtained in the present study suggest that users considered the system both useful for supporting maintenance activities and sufficiently easy to integrate into their daily responsibilities.

However, the findings also reveal a pattern that extends beyond traditional technology acceptance explanations. Previous sections of this study demonstrated that ICT managers already recognised the importance of maintenance tracking, preventive

maintenance, audit trails, and timely communication. Consequently, the exceptionally high acceptance levels may reflect not only ease of use but also the extent to which the system addressed existing operational deficiencies. This interpretation supports Rana et al. (2015), who argue that adoption within developing-country contexts is strongly influenced by contextual fit and organisational relevance.

A particularly notable finding concerns the unanimous approval of automated notifications. Earlier results identified communication delays and weak coordination as significant challenges affecting maintenance effectiveness. The strong support for automated notifications therefore converges with findings by González-Granadillo et al. (2021), who reported that automated alerting improves responsiveness and incident management. However, the current study extends this literature by demonstrating that the value of notifications is not limited to incident response. Within the participating firms, automated communication was also perceived as a mechanism for improving coordination and accountability across maintenance activities.

The findings additionally challenge a common assumption within technology adoption literature that resistance to new systems constitutes a major implementation barrier. The overwhelmingly positive responses suggest that users were willing to adopt the system when it aligned with existing operational needs. This indicates that, within the context of private security firms, the lack of appropriate maintenance tools may represent a greater obstacle than user resistance itself. The study therefore contributes evidence that contextual relevance may be as important as usability in shaping technology acceptance within ISMS environments.

4.7.4 Functional Testing Results

Functional testing was conducted to validate whether the system met all technical and operational requirements. Table 4.17 summarizes the module-specific testing outcomes.

Table 4.16

Functional Testing Results for the ISMS Maintenance Tracking System

Module	Testing Focus	Successful Tests (n)	Percentage
Login	Secure role-based access	63	100%
Audit	Logging of actions for accountability	63	100%
Client	Record creation and retrieval	63	100%
Personnel	Record management	63	100%
Task Assignment	Task creation, storage, and monitoring	61	96.8%
Notification	Automated email alerts	63	100%

The results confirm that all system modules achieved full or near-full functionality. The Login, Audit, Client, Personnel, and Notification Modules recorded a 100% success rate, while the Task Assignment Module achieved a success rate of 96.8%.

These findings support existing literature that emphasises the importance of structured controls for effective information security management. Turetken et al. (2020) found that audit effectiveness improves when organizations maintain structured and automated audit trails capable of generating verifiable evidence. Similarly, ISO/IEC 27001:2022 emphasises logging, monitoring, and documentation as fundamental components of information security governance. The successful performance of the Login and Audit Modules therefore confirms the practical feasibility of operationalising these requirements within private security environments.

The findings also support arguments by Iden and Eikebrokk (2013), who contend that improvements in maintenance effectiveness depend on structured management processes supported by appropriate technological tools. The strong performance of the Task Assignment and Notification Modules demonstrates that maintenance activities can be transformed from informal and reactive processes into measurable and trackable workflows. This directly addresses weaknesses identified earlier in the study regarding documentation, accountability, and maintenance coordination.

At the same time, the findings contribute a new perspective to the maintenance management literature. Much of the existing literature discusses structured maintenance systems within relatively mature organisational environments. The present study demonstrates that comparable benefits can be achieved within resource-constrained private security firms using a relatively simple and locally deployable solution. This suggests that effective ISMS maintenance does not necessarily require sophisticated enterprise-level platforms. Rather, the critical factor appears to be the existence of mechanisms capable of supporting consistent documentation, monitoring, and accountability.

Taken together, the functional testing results provide empirical support for the study's central argument that structured maintenance practices enhance ISMS effectiveness when embedded within operational systems. The findings therefore reinforce the broader conclusion that improving maintenance performance requires not only recognition of best practices but also practical tools capable of supporting their consistent implementation.

4.8 Chapter Summary

This chapter presented the findings of the study, which assessed the design, development, and evaluation of the ISMS Maintenance Tracking System for private security firms in Nairobi County. The analysis began with the demographic profile of respondents, revealing that ISMS-related roles remain male-dominated but with meaningful female participation. System modules were described in detail, covering login, audit, client, personnel, task assignment, and notification functions, each designed to improve accountability, efficiency, and compliance. User Acceptance Testing (UAT) results confirmed that the system was highly usable, with respondents rating ease of login, task assignment, notifications, and overall user-friendliness positively. Functional testing further demonstrated that all core modules achieved their intended objectives, including secure access, task monitoring, automated notifications, and audit trails. These results validated the system's ability to address operational gaps in preventive maintenance, incident tracking, and compliance reporting. The chapter concluded that the ISMS Maintenance Tracking System is both functional and practical, offering a robust solution that enhances accountability, improves responsiveness, and supports regulatory compliance within private security firms in Nairobi County.

CHAPTER FIVE

SUMMARY, CONCLUSIONS AND RECOMMENDATIONS

5.1 Introduction

This chapter presents a summary, discussion, conclusion, and recommendations derived from the findings of the study. The purpose is to relate the results of system analysis, design, implementation, and testing to the study objectives and the research problem. The chapter begins with a summary of the key findings, highlighting how the proposed ISMS Maintenance Tracking System addressed the limitations of current practices within private security firms in Nairobi. This is followed by a discussion of the findings in relation to existing literature, a conclusion outlining the implications of the results, and recommendations for practice and future research.

5.2 Summary of findings

This study developed and validated an ISMS Maintenance Tracking System tailored to the operational realities of private security firms in Nairobi County. The findings are organised around the four study objectives.

5.2.1 Current ISMS Maintenance Practices

The study established that existing maintenance practices in Nairobi's private security firms are uniformly weak across all measured dimensions. Mean scores for preventive maintenance (2.08), corrective maintenance (2.06), incident reporting (2.02), staff skills (2.10), coordination (2.06), and record completeness (2.11) all fell below the scale midpoint of 3.0. The lowest rating was for the statement that current practices ensure reliability (1.92). Small standard deviations (0.64–0.76) indicated systemic

rather than isolated weakness. Correlation analysis revealed a strong negative relationship between current practices and system effectiveness ($r = -0.650$, $p < 0.01$). Regression analysis showed that current practices alone explain 42.3% of the variance in system effectiveness ($R^2 = 0.423$), with a negative coefficient ($B = -0.893$, $\beta = -0.650$, $p < 0.001$), confirming that reliance on fragmented, manual approaches degrades ISMS performance.

5.2.2 Recognised Best Practices in ISMS Maintenance

ICT managers strongly endorsed all ten best-practice items, with mean scores ranging from 3.90 to 4.02. Preventive maintenance scheduling and automated incident logging received the highest ratings (4.02), followed by SLA compliance tracking (4.00) and integration of physical and cybersecurity (4.00). Small standard deviations (0.61–0.73) indicated strong consensus. Correlation analysis showed a moderate positive relationship between best practices and system effectiveness ($r = 0.592$, $p < 0.01$). Regression analysis indicated that best practices explain 35.0% of the variance in effectiveness ($R^2 = 0.350$), with a positive coefficient ($B = 0.815$, $\beta = 0.592$, $p < 0.001$). The contrast between high endorsement of best practices and weak current practices reveals a recognition-implementation gap, indicating that the challenge is not lack of knowledge but lack of operational mechanisms to translate knowledge into action.

5.2.3 Design and Development of the ISMS Maintenance Tracking System

Drawing on the diagnostic findings, the study designed and developed a web-based ISMS Maintenance Tracking System using PHP/MySQL, deployed on a local XAMPP server to ensure offline capability. The system architecture followed a three-tier model (presentation, application, data) and incorporated modular design for scalability. Key

functional modules included: role-based Login and Access Control, Client and Premises Management, Project Management, Personnel Management with SLA-based task assignment, Site and Installation Definition, Equipment Planning and Tracking, automated Audit Trail Management (logging every user action), and a Notification Module (email alerts for task updates). The system also included a mobile-first interface to support field technicians operating across dispersed client sites. Non-functional requirements addressed security (encrypted login, role-based access), usability (intuitive interface), scalability (modular design), and reliability (redundant logging). The design choices were grounded in Design Science Research principles Hevner et al. (2004), emphasising that the artefact must address a real organisational problem, be rigorously evaluated, and demonstrate practical utility. The system operationalises the best practices endorsed by ICT managers, transforming preventive scheduling, automated logging, SLA tracking, and audit trails from abstract principles into daily workflows.

5.2.4 Validation of the ISMS Maintenance Tracking System

The system was implemented and validated through a multi-stage process. Unit testing confirmed individual module correctness; integration testing verified inter-module communication. User Acceptance Testing (UAT) with 63 ICT managers assessed usability and functionality in a simulated operational environment. Results showed strong approval: 100% found login and notifications very easy; 95% rated task assignment as very easy; 90% described the interface as user-friendly. Functional testing achieved success rates of 100% for login, audit, client, personnel, and notification modules, and 96.8% for task assignment. The audit module successfully logged all user actions, addressing the documentation gaps identified in current

practices. Reliability of UAT was supported by low standard deviations in ratings and no significant differences between early and late respondents. Open-ended feedback included constructive criticisms (e.g., “task filter could be faster”), which were addressed in the maintenance phase, indicating that high satisfaction was not merely due to social desirability bias.

5.2.5 Joint Influence and Overall Effectiveness

Multiple regression analysis showed that current practices and best practices together explain 75.0% of the variance in system effectiveness ($R^2 = 0.750$, adjusted $R^2 = 0.741$). The joint model was statistically significant ($F(2,60) = 89.812$, $p < 0.001$). Current practices had a significant negative effect ($B = -0.868$, $\beta = -0.632$, $p < 0.001$), while best practices had a significant positive effect ($B = 0.788$, $\beta = 0.572$, $p < 0.001$). The near symmetry of the coefficients indicates that the penalty for poor practices can be offset by adopting structured best practices, providing an evidence-based forecast that the proposed system could improve effectiveness by approximately 1.66 units (the sum of absolute coefficients). Perceptions of expected system effectiveness were initially moderate (means 2.84-3.02), reflecting cautious optimism tempered by prior negative experiences with weak current practices. However, after actual use, validation results showed a shift to strongly positive ratings (90-100% approval), confirming that the system successfully addressed user scepticism.

The study makes a distinct contribution by designing, developing, and validating a context-sensitive ISMS Maintenance Tracking System that directly addresses the operational weaknesses documented in Nairobi’s private security sector. The findings demonstrate that current practices are uniformly weak and negatively impact

effectiveness, while best practices are strongly endorsed but not implemented. The proposed system operationalises these best practices through a modular, offline-capable, audit-enforced architecture. Validation confirms that the system is functional, usable, and effective, bridging the recognition-implementation gap. Thus, the study provides empirical evidence that automating structured maintenance tracking can significantly improve accountability, efficiency, and regulatory compliance in resource-constrained security environments.

5.4 Conclusions

5.4.1 Current ISMS Maintenance Practices and Tracking Mechanisms

The study concludes that current ISMS maintenance practices within private security firms in Nairobi County are largely inadequate and characterized by reactive maintenance approaches, weak documentation procedures, fragmented record management, and limited monitoring capabilities. Existing maintenance processes rely heavily on manual interventions, resulting in inefficiencies, poor accountability, and reduced system reliability. The study further concludes that these practices significantly undermine overall ISMS effectiveness, indicating that maintenance and tracking are critical determinants of information security performance. Without structured maintenance mechanisms, organizations are unlikely to sustain compliance, reliability, or continuous improvement of their information security systems.

5.4.2 Recognised Best Practices in ISMS Maintenance and Tracking

The study concludes that ICT managers possess a strong understanding of recognised ISMS maintenance best practices and acknowledge the importance of preventive maintenance scheduling, automated incident logging, SLA compliance monitoring,

real-time monitoring, compliance reporting, and integration of physical and cybersecurity controls. These practices were found to positively influence system effectiveness and represent an appropriate framework for strengthening information security management. However, the study concludes that a substantial gap exists between recognition and implementation, suggesting that awareness alone is insufficient without mechanisms that support operational execution.

5.4.3 Analysis, Design, and Development of the ISMS Maintenance Tracking System

The study concludes that the identified weaknesses in current maintenance practices can be addressed through a purpose-built ISMS Maintenance Tracking System designed around recognised maintenance best practices. The developed system successfully translates theoretical maintenance requirements into practical workflows through automated scheduling, maintenance logging, audit trail generation, notification management, and accountability mechanisms. Furthermore, the study concludes that context-sensitive system design is essential for organizations operating in resource-constrained environments, where affordability, simplicity, mobility, and offline capability influence successful implementation.

5.4.4 Evaluation of the ISMS Maintenance Tracking System

The study concludes that the developed ISMS Maintenance Tracking System is both functional and acceptable to its intended users. The evaluation results demonstrate that the system effectively supports maintenance planning, monitoring, documentation, and reporting activities while providing a user-friendly interface that promotes adoption. The positive user acceptance and successful functional testing indicate that

the system is capable of improving maintenance management processes and supporting more effective ISMS implementation within private security firms. The study therefore concludes that the developed artefact provides a practical and viable solution to the maintenance challenges identified during the diagnostic phase of the research.

Overall, the study concludes that ineffective ISMS maintenance practices represent a major barrier to information security effectiveness within private security firms in Nairobi County. While organizations recognise internationally accepted maintenance best practices, implementation remains weak due to inadequate tracking mechanisms and limited process automation. The developed ISMS Maintenance Tracking System successfully bridges this gap by operationalising recognised best practices through a structured and automated platform. Consequently, the study provides empirical evidence that improved maintenance tracking can strengthen system effectiveness, enhance accountability, support compliance requirements, and contribute to more resilient information security management practices within the private security sector.

5.5 Recommendations

The recommendations are presented at three levels; policy, managerial, and technical and are directly linked to the evidence generated by the study. This structure is intended to support coordinated improvement in ISMS maintenance practices across the private security sector.

5.5.1 Policy Recommendations

The study established that ISMS maintenance practices within private security firms are largely informal, inconsistently documented, and weakly monitored. In response,

the Private Security Regulatory Authority (PSRA), the Communications Authority of Kenya (CAK), and the Office of the Data Protection Commissioner (ODPC) should develop sector-specific guidelines for ISMS maintenance and tracking. These guidelines should go beyond general compliance requirements and provide minimum standards for preventive maintenance scheduling, incident documentation, audit logging, maintenance record retention, and periodic review of security controls. Such a framework would address the regulatory gap identified by the study and create a common benchmark for evaluating maintenance performance across the industry.

Regulators should also incorporate ISMS maintenance audits into routine compliance inspections of licensed private security firms. The study demonstrated that weak maintenance practices significantly undermine system effectiveness, indicating that implementation alone is insufficient without continuous monitoring and maintenance. Periodic audits would therefore encourage organizations to institutionalize maintenance processes rather than treating them as occasional administrative activities.

In addition, PSRA, CAK, and industry associations should establish sector-wide capacity-building programmes focused on ISMS maintenance and operational security management. The study revealed deficiencies in maintenance coordination, documentation, and technical execution, suggesting that many organizations lack practical knowledge on how to sustain an effective ISMS. Regular training, certification programmes, and industry workshops would strengthen the competence of ICT managers and operational personnel responsible for maintaining security systems.

5.5.2 Managerial Recommendations

The findings demonstrated that existing maintenance approaches negatively influence system effectiveness, while recognized best practices contribute positively to organizational performance. Consequently, executives and senior managers within private security firms should institutionalize preventive maintenance as a formal organizational function rather than relying on reactive fault correction. This can be achieved by establishing mandatory maintenance schedules, assigning responsibility for maintenance activities, and requiring periodic reporting on maintenance performance to management.

The study also revealed a disconnect between awareness of best practices and their actual implementation. To address this gap, firms should integrate ISMS maintenance objectives into organizational performance management systems. Managers should establish measurable indicators such as maintenance completion rates, incident response times, documentation compliance levels, and audit readiness metrics. These indicators should be reviewed regularly to ensure accountability and continuous improvement.

Because weak coordination emerged as a recurring challenge, security firms should establish cross-functional maintenance governance structures involving ICT personnel, operations managers, technical teams, and security supervisors. Regular coordination meetings and shared reporting mechanisms would improve information flow and ensure that maintenance activities are aligned with operational requirements across departments.

Furthermore, management should allocate dedicated budgets for ISMS maintenance activities and supporting technologies. The study suggests that maintenance challenges are not solely technical but are also linked to insufficient organizational investment in structured maintenance processes. Sustainable funding would enable firms to acquire appropriate tools, support staff training, and maintain consistent operational oversight.

5.5.3 Technical Recommendations

The study designed and validated an ISMS Maintenance Tracking System that was found to be both functional and highly acceptable to users. Private security firms should therefore adopt automated maintenance tracking systems to replace spreadsheet-based and paper-based approaches currently used for maintenance management. Automated systems provide structured workflows, centralized record management, real-time visibility of maintenance activities, and reliable audit trails, all of which directly address the deficiencies identified in the study.

ICT departments should implement automated logging and audit trail mechanisms for all maintenance-related activities. The research found that documentation and record management remain significant weaknesses, limiting accountability and compliance verification. Automated audit logs would create verifiable evidence of maintenance actions, support investigations, and improve readiness for regulatory or certification audits.

Organizations should also deploy notification and escalation mechanisms that automatically alert responsible personnel when maintenance tasks become overdue or when incidents require immediate attention. Since delays in maintenance response were identified as a major challenge, automated notifications would improve

responsiveness and reduce the likelihood of unresolved faults affecting operational performance.

To strengthen long-term maintenance effectiveness, ICT teams should establish centralized repositories for maintenance records, incident reports, equipment histories, and corrective actions. The study demonstrated that fragmented and scattered records undermine maintenance coordination and decision-making. A centralized repository would support knowledge retention, facilitate trend analysis, and improve continuity when personnel changes occur.

Finally, firms should progressively build maintenance data repositories that can support future analytics and predictive maintenance initiatives. The findings indicate that many organizations are still operating without structured maintenance data. Establishing reliable data collection mechanisms now will create the foundation necessary for future integration of advanced capabilities such as predictive maintenance, anomaly detection, and intelligent decision-support systems.

5.7 Contribution of the Study

5.7.1 Practical Contribution

This study contributes to practice by developing an ISMS Maintenance Tracking System tailored to the operational needs of private security firms in Nairobi County. The system provides a structured approach for managing maintenance activities through automated task assignment, preventive maintenance scheduling, incident reporting, audit logging, and notification management. By addressing the challenges associated with manual and fragmented maintenance processes, the system offers

organizations a practical mechanism for improving accountability, documentation, monitoring, and compliance management.

The study also demonstrates that affordable and locally deployable technologies can be used to support ISMS maintenance in resource-constrained environments. This provides an alternative to expensive commercial platforms that may be inaccessible to many private security firms.

5.7.2 Theoretical Contribution

The study contributes to the growing body of knowledge on Information Security Management Systems by extending existing research beyond ISMS implementation to the relatively underexplored area of ISMS maintenance tracking. While previous studies have largely focused on ISMS adoption, compliance, and certification, limited attention has been given to the mechanisms through which maintenance activities are monitored, documented, and coordinated on a day-to-day basis.

The study further contributes empirical evidence from the Kenyan private security sector by demonstrating that maintenance practices significantly influence ISMS effectiveness. It therefore reinforces the argument that ISMS success depends not only on the existence of policies and controls but also on the effectiveness of ongoing maintenance and monitoring processes.

5.7.3 Methodological Contribution

Methodologically, the study demonstrates the applicability of the Design Science Research (DSR) approach in addressing information security management challenges within developing-country contexts. The research followed a systematic process of

problem identification, requirements analysis, artefact design, development, and evaluation.

The study also presents an integrated evaluation approach that combines quantitative analysis, system testing, and user acceptance testing. This provides a replicable framework that future researchers can adopt when developing and evaluating information systems intended to solve practical organizational problems.

5.7.4 Sector Contribution

The study contributes to the private security industry in Kenya by providing empirical evidence on the state of ISMS maintenance practices within the sector. Given the limited research focusing specifically on information security management in private security firms, the findings provide baseline data that can inform managerial decisions, industry guidelines, and future regulatory initiatives.

In addition, the study highlights the importance of integrating physical security and information security maintenance within a unified management framework. This is particularly relevant for private security firms that manage hybrid environments involving CCTV systems, access control systems, alarm systems, and information technology infrastructure. The proposed system provides a practical model for supporting such integrated security operations.

5.7.5 Contribution to Policy and Regulation

The study provides evidence that can support regulators and industry stakeholders in developing guidelines for ISMS maintenance and documentation within the private security sector. The findings demonstrate the need for standardized maintenance

procedures, audit trails, incident reporting mechanisms, and periodic review processes. Consequently, the study offers a foundation upon which sector-specific information security management requirements and compliance frameworks can be developed.

REFERENCES

Abu-Mahfouz, S., & Alsaleh, M. (2022). Contextualizing information security frameworks for developing economies: Challenges and adaptations. *Journal of Global Information Technology Management*, *25*(3), 178-195. DOI: https://doi.org/10.30574/wjarr.2024.23.3.2853

Adom, D., Hussein, E. K., & Agyem, J. A. (2018). Theoretical and conceptual framework: Mandatory ingredients of quality research. *International Journal of Scientific Research*, *7*(1), 438-441. https://www.researchgate.net/publication/322204158_

Ahmed, M., Khan, R., & Shah, S. (2022). Information security management in SMEs: Challenges and practices. *Journal of Information Security and Applications*, 68, 103207. https://www.researchgate.net/publication/308992350

Al-Adwan, A. S., Li, N., Al-Adwan, A., Abbasi, G. A., Albelbisi, N. A., & Habibi, A. (2023). Extending the Technology Acceptance Model to predict university students' intentions to use metaverse-based learning platforms. *Education and Information Technologies*, *28,* 15381-15413. DOI:10.1007/s10639-023-11816-3

Alhumaidi, N. M. (2025). The impact of ITIL4 on employee performance: A quantitative questionnaire-based analysis in IT service management. *International Journal of Managerial Studies and Research*, *13*(4), 6-27. https://doi.org/10.20431/2349-0349.1304002

Almeida, F., Santos, J. D., & Pereira, C. (2023). A three-tier architecture for scalable and secure web-based enterprise systems. *Journal of Systems and Software*, 195, 111542. https://medium.com/@kraniket754/three-tier-architecture-df3cc502542e

Almeida, R., Silva, M., & Costa, J. (2023). Modular architectures for scalable security management systems: Design principles and implementation challenges. *International Journal of Information System Modeling and Design*, *14*(2), 45-67. DOI: https://doi.org/10.30574/wjarr.2025.26.1.1340

Almuhammadi, S., & Alsaleh, M. (2017). Information security management system standards: A comparative study of the literature. *International Journal of Information Security Science*, *10*(1), 54-67. https://www.researchgate.net/publication/228444915_

Anderson, M. C., Banker, R. D., & Ravindran, S. (2021). The value of IT-enabled flexibility: A quasi-experimental study of ERP post-implementation. *MIS Quarterly*, *45*(2), 599-626. DOI:10.17705/1pais.12102

Anderson, R., & Lee, C. (2023). Enhancing cyber-physical incident response through integrated maintenance analytics. *Journal of Information Security and Applications*, *73*, 103503. DOI:10.14569/IJACSA.2025.0160804

Anderson, T., & Lee, R. (2023). Compliance automation in security operations. *Journal of Information Security*, *18*(2), 112-125. DOI: https://doi.org/10.63282/3050-9416.IJAIBDCMS-V6I4P109

Armstrong, J. S., & Overton, T. S. (1977). Estimating nonresponse bias in mail surveys. *Journal of Marketing Research*, *14*(3), 396-402. https://doi.org/10.1177/002224377701400320

Bokrantz, J., Skoogh, A., Berlin, C., Wuest, T., & Stahre, J. (2020). Smart maintenance: A research agenda for industrial maintenance management. *International Journal of Production Economics*, 224, 107547. https://doi.org/10.1016/j.ijpe.2019.107547

Bryman, A. (2016). *Social research methods* (5th ed.). Oxford University Press.

Burudi, Zachariah M.. (2021). *Security management and private security companies in Kenya* [Master's thesis, Kenyatta University]. https://ir-library.ku.ac.ke/items/c60513d0-0483-4d04-9755-12a4eb83875b

Chandra Kruse, L., Purao, S., & Seidel, S. (2022). How Designers Use Design Principles: Design Behaviors and Application Modes. *Journal of the Association for Information Systems, 23*(5), 1235-1270. https://dx.doi.org/doi: 10.17705/1jais.00759

Chege, S. M. (2023). Information security management system practices in Kenya. *International Journal of Information Systems and Technology Research*, *11*(2), 15-27. DOI: 10.18775/jibrm.1849-8558.2015.82.3002

Chege, S. M. (2024). Implementation challenges of information security management systems in Kenyan organizations: Infrastructure and human resource constraints. *African Journal of Information Systems and Technology*, *9*(1), 33-49. DOI: 10.18775/ijmsba.1849-5664-5419.2014.103.1003

Chingoriwo, T. (2022). Cybersecurity challenges and needs in the context of digital development in Zimbabwe. *British Journal of Multidisciplinary and Advanced Studies: Engineering and Technology*, *3*(2), 77-104. DOI:10.37745/bjmas.2022.0046

Cochran, W. G. (1977). *Sampling techniques* (3rd ed.). John Wiley & Sons.

Cohen, J. (1988). *Statistical power analysis for the behavioral sciences* (2nd ed.). Lawrence Erlbaum Associates.

Costa, J. (2024). Mixed methods in educational large-scale studies: Integrating qualitative perspectives into secondary data analysis. *Education Sciences*, *14*(12), 1347. https://doi.org/10.3390/educsci14121347

Crespo Márquez, A. (2022). *The maintenance management framework: Models and methods for complex systems maintenance* (2nd ed.). Springer.

Creswell, J. W., & Creswell, J. D. (2018). *Research design: Qualitative, quantitative, and mixed methods approaches* (5th ed.). SAGE Publications.

Creswell, J. W., & Plano Clark, V. L. (2017). *Designing and conducting mixed methods research* (3rd ed.). SAGE Publications.

Creswell, J. W., & Poth, C. N. (2018). *Qualitative inquiry and research design: Choosing among five approaches* (4th ed.). SAGE Publications.

Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS Quarterly*, *13*(3), 319-340. DOI:10.2307/249008

Degtiar, I., & Rose, S. (2023). A review of generalizability and transportability. *Annual Review of Statistics and Its Application*, *10*, 501-524. DOI:10.1146/annurev-statistics-042522-103837

Delios, A., Clemente, E. G., Wu, T., Tan, H., Wang, Y., Gordon, M., … Uhlmann, E. L. (2022). Examining the generalizability of research findings from archival data. *Nature Human Behaviour*, *6*, 528-540. https://doi.org/10.1073/pnas.2120377119

DeLone, W. H., & McLean, E. R. (2003). The DeLone and McLean model of information systems success: A ten-year update. *Journal of Management Information Systems*, *19*(4), 9-30. https://doi.org/10.1080/07421222.2003.11045748

Dillman, D. A., Smyth, J. D., & Christian, L. M. (2014). *Internet, phone, mail, and mixed-mode surveys: The tailored design method* (4th ed.). John Wiley & Sons.

Domínguez, R. D., Laguna, O. A. F., & Sánchez-Valdez, J. A. (2023). *Exploratory analysis of a measurement scale of an information security management system* arXiv:2306.07367 . DOI:10.48550/arXiv.2306.07367

Drechsler, A., Thuan, N. H., Tate, M., & Antunes, P. (2023). Introduction to design science education. *Journal of Information Systems Education, 34*(3), 256–263. https://www.researchgate.net/publication/371902207

Egwuatu, O. V. (2025). Cybersecurity readiness in developing countries' enterprises: A comparative multi-case analysis. *Magna Scientia Advanced Research and Reviews*, *15*(1), 68-83.DOI:10.30574/msarr.2025.15.1.0110

Emmanouilidis, C., Liyanage, J. P., & Jantunen, E. (2009). Mobile solutions for engineering asset and maintenance management. *Journal of Quality in Maintenance Engineering*, *15*(1), 92-105. DOI:10.1108/13552510910943903

Escobar-Rodríguez, T., & Monge-Lozano, P. (2022). The acceptance of information systems by end-users: A meta-analysis of the technology acceptance model (TAM). *International Journal of Human-Computer Interaction*, *38*(4), 377-395. https://doi.org/10.1016/j.compedu.2011.11.012

Etikan, I., Musa, S. A., & Alkassim, R. S. (2016). Comparison of convenience sampling and purposive sampling. *American Journal of Theoretical and Applied Statistics*, *5*(1), 1-4. https://doi.org/10.11648/j.ajtas.20160501.11

Fakir, J. (2024). *An investigation of cybersecurity implementation challenges among South African SMEs* [Master's Thesis, University of the Witwatersrand,] Johannesburg. https://wiredspace.wits.ac.za/server/api/core/bitstreams/b959fbf0-8bc4-4be4-80cf-841ae1a2e1eb/content

Fernández-Díaz, E., & Ramírez-Montoya, M. S. (2024). User Acceptance Testing (UAT) in technology-enhanced learning platforms: A validation model. *Computers in Human Behavior*, 151, 108008. https://www.researchgate.net/publication/335361798

Ferreira, M. R. M. M. (2025). *Tailoring a GRC framework for the Republic of Mozambique: A strategic approach to cybersecurity and governance* [Master's Thesis, Universidade NOVA de Lisboa]. http://hdl.handle.net/10362/190418

González-Granadillo, G., González-Zarzosa, S., & Díaz, R. (2021). Security Information and Event Management (SIEM): Analysis, trends, and usage in critical infrastructures. *Sensors*, *21*(14), 4759. ; https://doi.org/10.3390/s21144759

Granić, A., & Marangunić, N. (2019). Technology acceptance model in educational context: A systematic literature review. *British Journal of Educational Technology*, *50*(5), 2572-2593. https://doi.org/10.1111/bjet.12864

Grenefalk, L., & Wallin, C. N. (2023). *Security management: Investigating the challenges and success factors in implementation and maintenance of Information Security Management Systems (ISMS)* [Master's Thesis,

Stockholm University]. https://www.diva-portal.org/smash/get/diva2:1784450/FULLTEXT01.pdf

Grobler, M., & von Solms, R. (2021b). The need for effective information security management in the digital age: From policy to practice. *Information & Computer Security*, *29*(4), 642-660. https://doi.org/10.3389/fdata.2021.583723

Hair, J. F., Black, W. C., Babin, B. J., & Anderson, R. E. (2019). *Multivariate data analysis* (8th ed.). Cengage.

Hevner, A. R., March, S. T., Park, J., & Ram, S. (2004). Design science in information systems research. *MIS Quarterly*, *28*(1), 75-105. https://www.researchgate.net/publication/201168946

Huang, Q., Mo, Q., He, H., & Bai, X. (2025). Reliability and validity of the short quality of life scale among bank employees in Guangxi, China. *Frontiers in Psychology, 16*, 1497827. https://doi.org/10.3389/fpsyg.2025.1497827

International Organization for Standardization. (2022). **ISO/IEC 27001:2022 - Information security, cybersecurity and privacy protection - Information security management systems - Requirements.* ISO https://www.iso.org/standard/27001#:~:

International Organization for Standardization. (2018). **ISO/IEC 20000-1:2018 - Information technology - Service management - Part 1: Service management system requirements.* ISO https://www.iso.org/standard/70636.html

Ireri, N. M. (2021). *A framework of the effect of Information Security Management System on data breach mitigation in Kenyan banks* [Unpublished Master's Thesis]. United States International University - Africa.

Islam, S., Ali, I., Shafiq, M., & Rahman, M. (2025). Intelligent dynamic cybersecurity risk management framework with explainability and interpretability of AI models for enhancing security and resilience of digital infrastructure. *Journal of Cybersecurity and Digital Infrastructure*, *3*(3), 1-20. DOI:10.1007/s40860-025-00253-3

Ittmann, H. W. (2018). Decision support systems (DSS): A survey. *South African Journal of Business Management*, *15*(4):189-196. DOI:10.4102/sajbm.v15i4.1127

Jardine, A. K. S., Lin, D., & Banjevic, D. (2006). A review on machinery diagnostics and prognostics implementing condition-based maintenance. *Mechanical Systems and Signal Processing*, *20*(7), 1483-1510. 10.1016/j.ymssp.2005.09.012

Jevelin, J., & Faza, A. (2023). Evaluation of the Information Security Management System: A path towards ISO 27001 certification. *Journal of Information Systems and Informatics*, *5(*4), 1240-1256. DOI:10.51519/journalisi.v5i4.572

Kariuki, P., Ofusori, L. O., & Subramaniam, P. R. (2023). Cybersecurity threats and vulnerabilities experienced by small-scale African migrant traders in Southern Africa. *Security Journal*, 292-321. https://doi.org/10.1057/s41284-023-00378-1

Katuu, S. (2026). Management System Standards in Records and Archives Management: Addressing Proliferation and Integration Challenges. *Standards*, *6*(2), 21. https://doi.org/10.3390/standards6020021

Kefalas, M. (2023). Solving standards implementation issues with a global ISMS. *ISACA Journal*, *4*(23), 1-8. https://www.isaca.org/resources/isaca-journal/issues/2023/volume-4/solving-standards-implementation-issues-with-a-global-isms

Kenya Law. (2016). *Private Security Regulation Act, No. 13 of 2016*. National Council for Law Reporting.

Kitheka, P. M. (2012). *Information security management systems in public universities in Kenya: A gap analysis between common practices and industry best practices* [Master's Thesis, University of Nairobi]. https://erepository.uonbi.ac.ke/items/f7bfbfea-2d84-4c2a-8eca-4242c45ffc57

Kothari, C. R. (2014). *Research methodology: Methods and techniques* (3rd ed.). New Age International Publishers.

Krejcie, R. V., & Morgan, D. W. (1970). Determining sample size for research activities. *Educational and Psychological Measurement*, *30*(3), 607-610. https://doi.org/10.1177/001316447003000308

Kuria, J., & Kagiri, A. (2023). Operational challenges in integrated security system maintenance: A survey of Kenyan firms. *African Journal of Science, Technology, Innovation and Development*, *15*(1), 45-58. https://www.iajournals.org/articles/iajah_v1_i4_394_406.pdf

Kyazze, A., & Nakakawa, A. (2024). The mobile offline-first pattern. *South African Computer Journal*, *36*(2), 112-130. DOI:10.60087/jaigs.v7i01.387

Liao, Y.-K., Wu, W.-Y., Le, T. Q., & Phung, T. T. T. (2022). The integration of the Technology Acceptance Model and the Value-Based Adoption Model to study the adoption of e-learning: The moderating role of e-WOM. *Sustainability*, *14*(2), 815. https://doi.org/10.3390/su14020815

Lynn, M. R. (1986). Determination and quantification of content validity. *Nursing Research*, *35*(6), 382-385. https://doi.org/10.1097/00006199-198611000-00017

Marhad, S. S., Abd Goni, S. Z., & Abdullah Sani, M. K. J. (2024). Implementation of information security management systems for data protection in organizations: A systematic literature review. *Environment-Behaviour Proceedings Journal*, *9*(SI18), 197-203. DOI:10.21834/e-bpj.v9iSI18.5483

Marikyan, D., Papagiannidis, S., & Stewart, G. (2023). Technology acceptance research: Meta-analysis. *Journal of Information Science*, 01655515231191177.

Masaev, S. N., Minkin, A. N., Bezborodov, Y. N., Edimichev, D. A., & Salal, Y. K. (2020). Information security control as a task of control a dynamic system. *Journal of Physics: Conference Series*, *1679*(3), 032012. DOI:10.48550/arXiv.2501.16732

Mohamed, A. Y., & Kamau, S. K. (2023). *A continent-wide assessment of cyber vulnerability across Africa* (arXiv:2301.03008). arXiv. DOI:10.48550/arXiv.2301.03008

Morrison, K., Tapia, A. H., & de Vries, P. (2023). Enhancing situational awareness through decision support systems: Lessons from critical infrastructure protection. *International Journal of Information Management*, 69, 102657. https://www.mdpi.com/1424-8220/25/20/63

Muchiri, E. W., Kinoti, P., & Charo, J. (2026). Development of an ISMS maintenance tracking system for security firms in Nairobi County. *International Journal of Professional Practice*, *14*(2), 83-95. https://ijpp.kemu.ac.ke/index.php/ijpp/article/view/679

Mugenda, O. M., & Mugenda, A. G. (2013). *Research methods: Dictionary and applied research methods*. Acts Press.

Mugenda, O. M., & Mugenda, A. G. (2003). *Research methods: Quantitative and qualitative approaches*. Acts Press.

Mutinda, F. M., & Wabwoba, F. (2023). Adoption of ISMS in Kenyan SMEs: Opportunities and barriers. *African Journal of Information Systems*, *15*(1), 57-72. DOI:10.64137/31080030/IJFEMS-V2I1P

Mwangi, J., & Ochieng, D. (2022). Tracking mechanisms in information security management: A study of SMEs in Nairobi. *East African Journal of Information Technology*, *5*(1), 22-38. DOI: 10.18775/jibrm.1849-8558.2015.82.3002

Nakajima, S. (1988). *Introduction to TPM: Total productive maintenance*. Productivity Press.

National Institute of Standards and Technology. (2018). *Framework for improving critical infrastructure cybersecurity* (Version 1.1). U.S. Department of Commerce.

Nielsen, J. (2012). *Usability 101: Introduction to usability*. Nielsen Norman Group.

Niemeläinen, A., Waseem, M., & Mikkonen, T. (2025). Enhancing productivity with AI during the development of an ISMS: Case Kempower. In D. Pfahl, J. Gonzalez Huerta, J. Klünder, & H. Anwar (Eds.), *Product-focused software process improvement* (pp. 60-74). Springer.

Ningrum, N. C. S., Nan Cenka, B. A., & Santoso, H. B. (2026). Offline-capable mobile application: A systematic literature review of research trends, synchronization mechanisms, UI/UX patterns, and usability evaluation. *Ranah Research: Journal of Multidisciplinary Research and Development, 8*(3), 1721-1733. DOI:10.38035/rrj.v8i3.2058

Njenga, K., & Njuki, S. (2018). Enhancing information security management systems for improved service delivery in Kenyan local authorities. *International Journal of Research in Engineering, Science and Management*, *1*(12), 9-16. https://journal.ijresm.com/index.php/ijresm/article/view/2853/2853

Njeru, A., & Otieno, D. (2023). Maintenance tracking deficiencies in integrated security systems: A case of Nairobi security firms. *Journal of Security and Safety Technology*, *4*(2), 55-72. https://www.iajournals.org/index.php/8-articles/1399-iajah-v1-i4

Nunnally, J. C., & Bernstein, I. H. (1994). *Psychometric theory* (3rd ed.). McGraw-Hill.

Okpeke, I., Adeyemi, A., & Olatunji, A. (2024). Innovations in fixed asset management: Enhancing efficiency through predictive maintenance and IoT integration. *International Journal of Scientific and Technological Research in Africa*, 6(1), 22-35. DOI:10.53771/ijstra.2024.7.1.0053

Okpeke, M., Adewale, O., & Eze, C. (2024). Implementing ISO/IEC 27001 in African SMEs: Challenges and adaptation strategies. *African Journal of Information and Communication*, *27*(1), 45-61. https://sbs-sme.eu/wp-content/uploads/2025/12/SBS

Okpeke, R. O., Omondi, M. P., & Kemboi, A. (2024). Aligning security management systems with Kenya's Private Security Regulation Act: A

framework for compliance. *Security Journal*, *37*(1), 112-130. DOI:10.53771/ijstra.2024.7.1.0053

Oranga, J., & Matere, A. (2023). Mixed methods research: merits, applications and challenges. *Postmodernism Problems, 15,* 84-99. https://doi.org/10.46324/pmp2501084

Orodho, J. A. (2013). *Techniques of writing research proposals and reports in education and social sciences*. Kanezja Publishers.

Otten, M., & Hingsburger, M. (2023). Integrating open- and closed-ended questions to assess attitudes: A mixed-methods survey experiment. *Behavior Research Methods*, *56,* 4802-4822. doi: 10.3758/s13428-023-02218-x.

Park, S., & Lee, H. (2023). Automation in security incident management: Comparative analysis of SIEM implementations in European financial institutions. *Computers & Security*, *124*, 102976. https://www.scirp.org/reference/referencespapers?referenceid=3859679

Peffers, K., Tuunanen, T., Rothenberger, M. A., & Chatterjee, S. (2007). A design science research methodology for information systems research. *Journal of Management Information Systems*, *24*(3), 45-77. https://doi.org/10.2753/MIS0742-1222240302

Petter, S., & McLean, E. R. (2023). The efficacy of structured vs. unstructured user acceptance testing: A field experiment. *Journal of Systems and Software*, 197, 111567. DOI:10.1057/ejis.2008.15

Poltavtseva, T., Frolova, E., & Sokolov, D. (2021). Key concepts of systemological approach to CPS adaptive information security monitoring. *Symmetry*, *13*(12), 2425. https://doi.org/10.3390/sym13122425

Prajapati, R., & Nair, S. (2023). Total productive maintenance in digital infrastructure: Extending TPM principles to IT asset management. *International Journal of Productivity and Performance Management*, *72*(5), 1347-1365. https://kaizen.com/insights/tpm-principles-pillars-implementation/

Pressman, R. S., & Maxim, B. R. (2020). *Software engineering: A practitioner's approach* (9th ed.). McGraw-Hill Education.

Prislan, K., Bernik, I., & Žvanut, M. (2020). A real-world information security performance assessment using a multidimensional socio-technical approach. *PLOS ONE*, *15*(8), e0238731.

Private Security Regulation Act. (2016). *Private Security Regulation Act* (No. 13 of 2016). Government of Kenya.

Private Security Regulatory Authority (PSRA). (2024). *Private security sector regulatory framework*. Government of Kenya.

Rana, N. P., Dwivedi, Y. K., & Williams, M. D. (2015). A meta-analysis of mobile technology acceptance in the context of developing countries. *Journal of Enterprise Information Management*, *28*(4), 616-647. DOI:10.1007/978-3-642-24148-2_10

Government of Kenya. (2023). *Regional security report 2023*. Government of Kenya.

Rosli, M. S., Saleh, N. S., Md. Ali, A., Abu Bakar, S., & Mohd Tahir, L. (2022). A systematic review of the Technology Acceptance Model for the sustainability of higher education during the COVID-19 pandemic and identified research gaps. *Sustainability*, *14*(18), 11389. https://doi.org/10.3390/su141811389

Saunders, M. N. K., Lewis, P., & Thornhill, A. (2023). *Research methods for business students* (9th ed.). Pearson.

Silva, T. H., Rosado da Cruz, A. M., & Pereira, R. (2022). Evaluating the long-term viability of ICT4D artifacts: A framework for assessing appropriateness and institutionalization. *Information Technology for Development*, *28*(2), 243-264. https://www.researchgate.net/publication/259310166

Susanto, H., Almunawar, M. N., & Tuan, Y. C. (2011). Information security management system standards: A comparative study of the big five. *International Journal of Electrical and Computer Sciences*, *11*(5), 23-29. https://www.researchgate.net/publication/228444915_

Tabachnick, B. G., & Fidell, L. S. (2013). *Using multivariate statistics* (6th ed.). Pearson.

Talukder, M. S., Singh, R., & Huda, M. H. (2020). The role of offline-first design in digital inclusion: Evidence from a Bangladeshi case study. *Information Technology & People*, *33*(6), 1527-1550. DOI:10.1080/09584935.2020.1793912

Tan, C., & Kim, J. (2021). Embedding information security into organizational culture: A study of ISMS implementation challenges. *Journal of Cybersecurity and Digital Trust*, *3*(1), 44-61. https://www.researchgate.net/publication/221229226_

Teijlingen, E. R. van, & Hundley, V. (2001). The importance of pilot studies. *Social Research Update*, (35), 1-4. https://sru.soc.surrey.ac.uk/SRU35.PDF

TrueContext. (2025 August 13). What field technicians really want in their mobile apps. *TrueContext Blog*. https://truecontext.com/field-technicians-mobile-apps/

Tupkalo, V., Cherepkov, A., & Yarmolatii, O. (2024). A systematic process-oriented approach to the implementation of the enterprise's information security management system. *Measurements infrastructure 12*(2), 45-61. DOI:10.33955/v8(2024)-058

Turetken, O., Jethefer, S., & Ozkan, B. (2020). Internal audit effectiveness: Operationalizing and measuring internal audit value. *Managerial Auditing Journal*, *35*(2), 238-271. DOI:10.1108/MAJ-08-2018-1980

Venable, J., Pries-Heje, J., & Baskerville, R. (2020). A comprehensive framework for evaluation in design science research. In J. Vom Brocke, A. Hevner, & A. Maedche (Eds.), *Design Science Research. Cases* (pp. 23-45). Springer.

Venkatesh, V., & Bala, H. (2021). Technology acceptance model 3 and a research agenda on interventions. *Decision Sciences*, *39*(2):273-315 DOI:10.1111/j.1540-5915.2008.00192.x

von Bertalanffy, L. (1968). *General system theory: Foundations, development, applications*. George Braziller.

Wabwoba, F., & Wanyembi, G. (2015). Information security management system practices in Kenya. *International Journal of Computer Applications*, *112*(4), 23-29. https://researchleap.com/wp-content/uploads/2024

Whitman, M. E., & Mattord, H. J. (2022). *Principles of information security* (6th ed.). Cengage Learning.

Wireman, T. (2021). *Total productive maintenance: Proven strategies and techniques to keep equipment running at maximum efficiency*. Industrial Press.

World Bank. (2023). *World development report 2023: Migrants, refugees, and societies*. World Bank.

Yamane, T. (1967). *Statistics: An introductory analysis* (2nd ed.). Harper & Row.

APPENDICES

APPENDIX 1: RESEARCH QUESTIONNAIRE

Introduction and Instructions

Dear Respondent,

I am conducting a research study as part of my master's degree in computer information systems. The study is titled:

"Development of ISMS Maintenance Tracking System for Security Firms in Nairobi County."

The purpose of this study is to examine current ISMS maintenance practices, investigate recognised best practices, and validate the effectiveness of a proposed ISMS maintenance tracking system. Your input will be invaluable in helping us understand the gaps in ISMS maintenance and design a system that addresses the operational needs of security firms.

Please note:

- The information you provide will be treated with the highest confidentiality and used strictly for academic purposes.
- Do not write your name anywhere on the questionnaire.
- There are no right or wrong answers; kindly respond honestly.
- For each statement, tick (✓) the response that best represents your opinion.
- Key

Thank you for your time and participation.

Section A: Demographic Information

1. Gender: ☐ Male ☐ Female ☐ Other
2. Age group: ☐ Below 25 ☐ 25–34 ☐ 35–44 ☐ 45 and above
3. Level of education: ☐ Diploma ☐ Bachelor's Degree ☐ Master's Degree ☐ Other (specify) ……
4. Years of experience in ISMS/IT maintenance: ☐ Less than 2 years ☐ 2–5 years ☐ 6–10 years ☐ Above 10 years
5. Size of firm: ☐ Small (1–49 staff) ☐ Medium (50–249 staff) ☐ Large (250+ staff)

Section B: Current ISMS Maintenance Practices

Statement	1	2	3	4	5
Preventive maintenance in our firm is conducted on a regular schedule.	☐	☐	☐	☐	☐
Corrective maintenance is performed promptly when faults occur.	☐	☐	☐	☐	☐
Incident reporting is systematically documented.	☐	☐	☐	☐	☐
Most maintenance tracking is done manually, which slows down processes. *(R)*	☐	☐	☐	☐	☐
Our firm lacks real-time monitoring of ISMS components. *(R)*	☐	☐	☐	☐	☐
Maintenance tasks are well-coordinated among departments.	☐	☐	☐	☐	☐
There are frequent delays in resolving ISMS faults. *(R)*	☐	☐	☐	☐	☐
Staff have sufficient skills to handle ISMS maintenance tasks.	☐	☐	☐	☐	☐
Maintenance records are often incomplete or scattered across departments. *(R)*	☐	☐	☐	☐	☐
Our current ISMS maintenance practices are adequate for ensuring reliability.	☐	☐	☐	☐	☐

Section C: Best Practices in ISMS Maintenance Tracking

Item No.	Statement	1	2	3	4	5
1	Preventive maintenance scheduling is essential for ISMS reliability.	☐	☐	☐	☐	☐
2	Corrective maintenance procedures should be standardised.	☐	☐	☐	☐	☐
3	SLA compliance tracking improves accountability.	☐	☐	☐	☐	☐
4	Real-time monitoring is critical for effective ISMS management.	☐	☐	☐	☐	☐
5	Automated incident logging enhances efficiency.	☐	☐	☐	☐	☐
6	Compliance reporting should be integrated into ISMS processes.	☐	☐	☐	☐	☐
7	A knowledge base is important to support quick fault resolution.	☐	☐	☐	☐	☐
8	Mobile-first access to ISMS tools is essential for field technicians.	☐	☐	☐	☐	☐
9	Adopting international standards (ISO/IEC 27001, 20000-1) strengthens ISMS operations.	☐	☐	☐	☐	☐

Item No.	Statement	1	2	3	4	5
10	Integration of physical and cybersecurity practices is critical for ISMS success.	☐	☐	☐	☐	☐

Section D: Expected Effectiveness of Proposed ISMS Maintenance Tracking System

Statement	1	2	3	4	5
The proposed ISMS system will improve preventive maintenance scheduling.	☐	☐	☐	☐	☐
The system will reduce delays in corrective maintenance.	☐	☐	☐	☐	☐
The system will minimise ISMS downtime through timely alerts.	☐	☐	☐	☐	☐
The system will ensure accurate and complete audit-ready records.	☐	☐	☐	☐	☐
The system will strengthen SLA compliance by tracking performance in real time.	☐	☐	☐	☐	☐
The system will reduce recurring ISMS faults through predictive maintenance.	☐	☐	☐	☐	☐
The system will provide staff with easy access to maintenance information.	☐	☐	☐	☐	☐
The system will increase client satisfaction by improving ISMS reliability.	☐	☐	☐	☐	☐
The system will enhance regulatory compliance through automated reporting.	☐	☐	☐	☐	☐
The system will improve operational efficiency and accountability in ISMS maintenance.	☐	☐	☐	☐	☐

APPENDIX II: SYSTEM EVALUATION CHECKLIST

Title: System Evaluation Checklist for ISMS Maintenance Tracking Prototype
Tool Code: CHK-01

Research Title: - Development of an ISMS Maintenance Tracking System for Security Firms in Nairobi County

Target Respondents: - ICT Managers (Pilot Users)

Purpose: To assess usability, reliability, and functionality of the ISMS Maintenance Tracking System during pilot testing. Structured feedback was collected to validate the system's performance against the study objectives.

Instructions - Please evaluate each feature of the system based on your user experience. For each item, respond with *Yes/No* (initial impression) and *Rating from 1 to 5* (1 = Very Poor, 5 = Excellent).

Section A: System Usability

Item Yes/No Rating (1-5)

1. The login process is easy to complete using assigned roles | ☐ Yes ☐ No | ☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 |
2. Task assignment and monitoring are straightforward | ☐ Yes ☐ No | ☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 |
3. The system interface is user-friendly | ☐ Yes ☐ No | ☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 |
4. Overall usability of the system supports ISMS maintenance | ☐ Yes ☐ No | ☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 |

Section B: Notifications and Responsiveness

Item Yes/No Rating (1-5)

5. Notifications are timely | ☐ Yes ☐ No | ☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 |
6. Notifications improve responsiveness to tasks | ☐ Yes ☐ No | ☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 |

Section C: Functional Testing Across Modules

Module Yes/No Rating (1-5)

7. Login module (secure role-based access) | ☐ Yes ☐ No | ☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 |

8. Audit module (logs actions for accountability) | ☐ Yes ☐ No | ☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5
9. Client module (record creation and retrieval) | ☐ Yes ☐ No | ☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 |
10. Personnel module (record management) | ☐ Yes ☐ No | ☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 |
11. Task assignment module (task creation, storage, monitoring) | ☐ Yes ☐ No | ☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 |
12. Notification module (automated alerts) | ☐ Yes ☐ No | ☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 |

Section D: Overall Satisfaction

Item Rating (1-5)

13. Overall, I am satisfied with the ISMS Maintenance Tracking System | ☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 |

Additional Comments or Suggestions for Improvement:

Consent Confirmation
☐ I voluntarily provided this feedback as part of system testing and understand it will support academic research and system improvement.

Date: _____ Respondent Code: _____

APPENDIX III: KeMU INTRODUCTION LETTER TO NACOSTI

KENYA METHODIST UNIVERSITY
P. O. Box 267 Meru - 60200, Kenya
Tel: 254-064-30301/31229/30367/31171
Fax: 254-64-30162
Email: deanrd@kemu.ac.ke
DIRECTORATE OF POSTGRADUATE STUDIES

Our Ref: KeMU/NACOSTI/CIS/09/2025 September 30, 2025

Commission Secretary
National Commission for Science, Technology and Innovations
P.O. Box 30623-00100
NAIROBI

Dear Sir/Madam,

RE: ESTHER WAMBUI MUCHIRI-CIS-3-2547-2/2022

This is to confirm that the above named is a bona fide student of Kenya Methodist University, in the Department of Computer Science, undertaking a Master's Degree in Computer Information Systems. She is conducting research on "*Development of an ISMS Maintenance Tracking System for Security Firms in Nairobi County*".

We confirm that her research proposal has been defended and approved by the University.

In this regard, we are requesting your office to issue a research license to enable her collect data.

Any assistance accorded to her will be highly appreciated.

Yours sincerely,

Dr. Nancy Rintari (PhD)
Director, Board of Postgraduate Studies
Cc: Dean, School of Computing and Informatics
CoD, Computer Science
Postgraduate Coordinator - CIS
Supervisors

APPENDIX IV: ETHICAL REVIEW LETTER

KENYA METHODIST UNIVERSITY
INSTITUTIONAL SCIENTIFIC AND ETHICS REVIEW COMMITTEE (KEMU-ISERC)
P. O. BOX 267 MERU - 60200, KENYA FAX: 254-64-30162
TEL: 254-064-30301/31229/30367/31171 EMAIL: serc@kemu.ac.ke

Our Ref: KeMU/ISERC/CIS/09/2025 September 30, 2025

ESTHER WAMBUI MUCHIRI
CIS-3-2547-2/2022

Dear Esther,

SUBJECT: DEVELOPMENT OF AN ISMS MAINTENANCE TRACKING SYSTEM FOR SECURITY FIRMS IN NAIROBI COUNTY.

This is to inform you that Kenya Methodist University Institutional Scientific Ethics and Review Committee has reviewed and approved your research proposal. Your application approval number is KeMU/ISERC/CIS/09/2025. The approval period is 30th September, 2025 – 30th September, 2026.

This approval is subject to compliance with the following requirements:-

I. Only approved documents including (informed consents, study instruments, MTA) will be used.

II. All changes including (amendments, deviations, and violations) are submitted for review and approval by Kenya Methodist University Institutional Scientific Ethics and Review Committee.

III. Death and life-threatening problems and serious adverse events or unexpected adverse events whether related or unrelated to the study must be reported to KeMU ISERC within 72 hours of notification.

IV. Any changes, anticipated or otherwise that may increase the risks or affected safety or welfare of study participants and others or affect the integrity of the research must be reported to KeMU ISERC within 72 hours.

V. Clearance for export of biological specimens must be obtained from relevant institutions.

VI. Submission of a request for renewal of approval at least 60 days prior to expiry of the approval period. Attach a comprehensive progress report to support the renewal.

VII. Submission of an executive summary report within 90 days upon completion of the study to KeMU ISERC.

Prior to commencing your study, you will be expected to obtain a research license from National Commission for Science, Technology and Innovation (NACOSTI) https://oris.nacosti.go.ke and also obtain other clearances needed.

KENYA METHODIST UNIVERSITY KEMU ISERC 30 SEP 2025 MERU

MR. HERBERT KIBEBE
CHAIR (ISERC)

APPENDIX V – NACOSTI RESEARCH LICENSE

REPUBLIC OF KENYA

NATIONAL COMMISSION FOR SCIENCE, TECHNOLOGY & INNOVATION

Ref No: 550165

Date of Issue: 03/October/2025

RESEARCH LICENSE



This is to Certify that Ms.. ESTHER Wambui MUCHIRI of Kenya Methodist University, has been licensed to conduct research as per the provision of the Science, Technology and Innovation Act, 2013 (Rev.2014) in Nairobi on the topic: DEVELOPMENT OF AN ERMS MAINTENANCE TRACKING SYSTEM FOR SECURITY FIRMS IN NAIROBI COUNTY for the period ending : 03/October/2026.

License No: NACOSTI/P/25/41806607

550165

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