International Journal of Professional Practice (IJPP) Vol.14 Issue No.2 2026

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

Muchiri Esther Wambui[1*], Patrick Kinoti[1], Joel Charo[1]

[1] *Kenya Methodist University P.O. Box 1017 – 60200, Meru, Kenya*

**Correspondence email: esthermuchiri001@gmail.com*

Abstract

The increasing reliance on integrated security technologies in Kenya's private security sector has intensified the need for effective maintenance of Integrated Security Management Systems (ISMS) to ensure operational continuity, compliance, and resilience. This study examined current ISMS maintenance practices, identified recognized best practices, and developed a digital ISMS Maintenance Tracking System tailored for private security firms in Nairobi County. Guided by the Design Science Research (DSR) paradigm and theoretically grounded in General Systems Theory (GST), the Technology Acceptance Model (TAM), and Total Productive Maintenance (TPM), the research followed a two-phase process, including a diagnostic quantitative survey to assess existing and best ISMS maintenance practices and the design, development, and validation of an ISMS Maintenance Tracking System via User Acceptance Testing (UAT). Using a descriptive and developmental research design, structured questionnaires were administered to 90 sample respondents, yielding a 70% response rate. Data were analyzed descriptively and inferentially. Results show that current maintenance practices are weak and negatively associated with system effectiveness ($B = -0.893$, $p < 0.001$; $R^2 = 0.423$), while best practices, including preventive scheduling, SLA monitoring, and real-time logging, positively predict effectiveness ($B = 0.815$, $p < 0.001$; $R^2 = 0.350$). The combined model ($F(2,60) = 89.812$, $p < 0.001$; $R^2 = 0.750$) explains 75% of the variance in effectiveness. UAT demonstrated high usability and functionality (over 90% satisfaction across modules). The study concludes that replacing fragmented, reactive procedures with an automated, standards-aligned tracking system substantially improves ISMS reliability, accountability, and compliance. The study recommends adopting ISO/IEC 27001-aligned maintenance frameworks and deploying the developed system in phases. In practice, the study provides a validated maintenance tool; for policy, it offers evidence to inform regulatory frameworks; and theoretically, it extends DSR applications to context-driven ISMS solutions that support Kenya's Private Security Regulation Act (2016) and SDG 9.

Keywords: *Design science research, ISMS, Kenya, Maintenance tracking, Private security firms*

IJPP 14(2); 83-95

1.0 Introduction

The growing complexity of data, infrastructure, and personnel threats has heightened the global importance of Integrated Security Management Systems (ISMS). These systems unify physical and cybersecurity measures, operational controls, and compliance monitoring to enhance organizational resilience (International Organization for Standardization, 2022). Their effectiveness depends on consistent maintenance, regular updates, real-time monitoring, and performance audits. Without these, organizations risk financial losses, regulatory breaches, and reputational damage (Grobler & Solms, 2021).

Globally, sectors such as finance, energy, and government invest in ISMS aligned with ISO/IEC 27001 and ISO/IEC 20000-1 standards (International Organization for Standardization, 2018, 2022). Tools such as IBM QRadar and ServiceNow ITSM automate threat detection but often require local customization. Across Africa, countries such as South Africa and Nigeria have adopted ISMS through national reforms, yet many organizations still face irregular maintenance, poor monitoring, and limited technical capacity (Mutinda & Wabwoba, 2023).

In Kenya, ISMS adoption has grown due to digitalization and evolving threats, particularly in Nairobi County, where many firms lack structured systems for ISMS maintenance, leading to service disruptions and compliance failures. Magal Security Systems Limited (Kenya), established in 2010, has deployed large-scale ISMS solutions for institutions such as Parliament, Kenya Ports Authority, Jomo Kenyatta International Airport, and KenGen. These institutions continue to face challenges in consistently maintaining the system. Other key firms, including Securex Agencies Ltd, SGA Kenya, and Wells Fargo, still rely on fragmented or semi-manual systems, which affect data accuracy and performance (Kuria & Kagiri, 2023).

This study analyzed ISMS maintenance tracking methods among Nairobi's security firms, assessing their strengths, weaknesses, and compliance gaps. It benchmarked these methods against international standards (ISO, 2018; ISO, 2022). It developed an ISMS Maintenance Tracking System to enhance real-time monitoring, compliance reporting, and preventive and corrective maintenance, ensuring structured responses and improved oversight of security operations.

Statement of the Problem

Kenya's security firms face persistent challenges in maintaining Integrated Security Management Systems (ISMS), particularly in tracking and managing maintenance tasks. Weak preventive maintenance, delayed incident response, poor coordination, and inconsistent invoicing lead to operational disruptions, SLA breaches, and financial losses (Mutinda & Wabwoba, 2023). Grenefalk and Wallin (2023) attribute these failures to fragmented systems, limited executive support, resistance to change, a weak security culture, and low system accessibility. Many security SMEs operate with unstructured maintenance routines and minimal ISMS visibility (Mutinda & Wabwoba, 2023). In Nairobi's high-risk environment, the absence of integrated tracking tools fosters reactive management and poor audit readiness. Despite global frameworks such as ISO/IEC 27001:2022 and ISO/IEC 20000-1:2018, most firms still depend on semi-manual systems. This underscores the need for a localized ISMS Maintenance Tracking System that enables real-time monitoring, integrates preventive and corrective maintenance, and aligns with global standards and the Private Security Regulation Act (2016).

Research Objectives

The primary objective of this study was to develop an ISMS maintenance tracking system for security firms by analyzing existing solution processes, evaluating current tracking methods, identifying industry best practices, and validating the proposed system. The specific objectives were to:

i. Examine the current ISMS maintenance practices and tracking mechanisms used by security firms in Nairobi County.
ii. Investigate internationally and locally recognized best practices for ISMS maintenance tracking systems.
iii. Design and develop an automated ISMS Maintenance Tracking System tailored to the operational needs of security firms.
iv. Implement and validate the proposed system in selected security firms in Nairobi County.

Theoretical Foundations

This study was grounded in three complementary theories: General Systems Theory (GST), the Technology Acceptance Model (TAM), and Total Productive Maintenance (TPM), which guided the conceptualization and design of the ISMS Maintenance Tracking System. GST, advanced by von Bertalanffy (1968) views organizations as integrated systems of interdependent subsystems working toward shared goals. In the context of ISMS maintenance, it offers a holistic lens through which technical controls, human roles, and management processes interact to sustain reliability and efficiency. This perspective informed the system's modular architecture, ensuring interoperability among maintenance, audit, and reporting modules and creating continuous feedback loops essential for system learning and improvement (Kast & Rosenzweig, 2022).

"The study concludes that current ISMS maintenance practices in Nairobi's private security firms are inadequate and reactive, negatively affecting system effectiveness"

TAM, developed by Davis (1989) and refined by Venkatesh and Bala (2021) posits that technology adoption depends on perceived usefulness and ease of use. It guided the user-centered design of the ISMS Maintenance Tracking System, emphasizing intuitive navigation, clear interfaces, and functional simplicity to promote user satisfaction and acceptance, an approach consistent with Agarwal and Prasad (2023) and Alghamdi and Bach (2024). TPM, introduced by Nakajima (1988), emphasizes proactive maintenance, continuous improvement, and shared responsibility to enhance system performance. Its principles shaped the system's automation and scheduling logic, embedding preventive maintenance alerts, accountability tracking, and predictive diagnostics (Wireman, 2010). Collectively, these theories ensured that the ISMS Maintenance Tracking System is holistic in structure, user-centric in design, and proactive in functionality, effectively translating theoretical insight into practical application within Kenya's private security sector.

Review of ISMS Maintenance Practices

Empirical literature shows that Information Security Management System (ISMS) maintenance in security firms, especially in developing economies, remains fragmented, reactive, and largely manual (Mutinda & Wabwoba, 2023; Kuria & Kagiri, 2023). Reliance on paper-based reporting, irregular updates, and limited automation hampers proactive fault detection and timely incident

response. Although global frameworks such as ISO/IEC 27001, COBIT 2019, and the NIST Cybersecurity Framework provide structured guidance, implementation in Kenya's private security sector has been inconsistent due to limited technical capacity, weak oversight, and organizational inertia (Chege, 2024).

Globally, ISMS maintenance has evolved toward predictive, integrated management. Studies in advanced economies indicate that digital dashboards, analytics, and AI-driven diagnostics enhance system uptime and compliance (Serrano et al., 2022; Anderson & Lee, 2023). Reports from Gartner (2024) and Capgemini (2023) confirm that automation and SLA tracking substantially reduce downtime. However, these advancements remain elusive in emerging economies, where infrastructure constraints, high deployment costs, and low digital literacy hinder adoption (Ndungu & Kimani, 2023). Most existing ISMS maintenance tools are designed for mature digital environments and lack adaptability to resource-constrained contexts such as Nairobi's private security sector. As Chege (2024) and Crespo Márquez (2022) note, off-the-shelf systems often overlook hybrid operations that manage both physical and digital assets, resulting in underutilization and frequent abandonment.

Best practice literature identifies preventive maintenance, SLA monitoring, and real-time incident logging as essential to effective ISMS operations (Whitman & Mattord, 2022; Khan et al., 2021). However, few Kenyan firms have automated these functions or adapted them to local conditions. The inability to acquire or customize costly imported systems underscores the need for affordable, modular, and context-aware solutions suited to limited infrastructure and varying user competence. Overall, the literature highlights a persistent gap: while global ISMS standards and tools are well developed, their adoption in Kenya remains shallow due to a lack of localization. This study addresses that gap by developing and validating an automated, user-centered ISMS Maintenance Tracking System tailored to Nairobi's private security sector.

2.0 Materials and Methods

Research Approach and Design

The study adopted a descriptive and developmental research design guided by the Design Science Research (DSR) paradigm. The descriptive component provided an in-depth understanding of current ISMS maintenance and tracking mechanisms, while the developmental aspect focused on designing and validating an automated ISMS Maintenance Tracking System. According to Kothari (2014), descriptive research is suitable for systematically describing the characteristics of a phenomenon without manipulating variables. The developmental approach aligns with Pressman and Maxim (2020) who, emphasize integrating design science principles into system-oriented research to transform empirical findings into functional technological solutions. This dual design was appropriate, as it enabled both diagnosing existing ISMS maintenance gaps and developing a prototype to address them.

Study Population and Sampling

The study targeted ICT managers in licensed private security firms in Nairobi County, identified from the Private Security Regulatory Authority (PSRA, 2024) database of 116 firms. ICT managers were selected for their technical and managerial expertise in ISMS maintenance and tracking. Purposive sampling was used to select firms with active ISMS operations, which were then stratified by size to ensure representativeness. Using Yamane's (1967) formula at a 95% confidence level and 5% margin of error, a sample of 90 ICT managers was derived.

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

where n = sample size, N = study population (116), and e = level of precision (0.05).

This resulted in a sample size of 90 respondents.

Instrumentation and data collection procedures

Primary data were collected using a structured

questionnaire designed to assess four dimensions: (1) existing ISMS maintenance and tracking practices, (2) adoption of best practices, (3) system effectiveness, and (4) user evaluation of the developed system. The instrument contained Likert-scale items (1 = Strongly Disagree to 5 = Strongly Agree).

Examples of questionnaire items included:

- *Current Practices: "Our firm maintains a documented ISMS maintenance schedule."*
- *Best Practices: "Preventive maintenance and SLA compliance tracking are consistently enforced."*
- *System Effectiveness: "The ISMS maintenance system has improved response time and reduced system downtime."*

To ensure validity, the questionnaire was reviewed by two ISMS practitioners and two academic experts from the Kenya Methodist University School of Computing and Informatics. Construct validity was established by aligning items with ISO/IEC 27001:2022 standards and related studies (Whitman & Mattord, 2022). A pilot test with nine ICT managers yielded a Cronbach's Alpha of 0.89, confirming strong reliability (Nunnally & Bernstein, 1994).

Following ethical clearance from the Kenya Methodist University Ethics Review Board and NACOSTI, the questionnaire was administered both in person and via Google Forms. Participation was voluntary, and informed consent was obtained from all respondents. Confidentiality and data protection were maintained in accordance with the Kenya Data Protection Act (2019).

Data Analysis

Data were analyzed using SPSS Version 26. Descriptive statistics (frequencies, percentages, means, and standard deviations) summarized respondents' characteristics and ISMS practices. Pearson correlation was used to assess relationships between variables, and multiple regression was used to assess the predictive power of best practices on ISMS effectiveness. ANOVA was used to test regression models, with $p < 0.05$ as the criterion for statistical significance.

System Development Process

The ISMS Maintenance Tracking System was designed, developed, and validated using the Waterfall model, which proceeds sequentially through requirement analysis, design, implementation, testing, and maintenance (Pressman & Maxim, 2020). Requirements were derived from survey findings and consultations with ICT managers, emphasizing preventive maintenance scheduling, SLA monitoring, audit trail logging, and automated notifications to enhance accountability and compliance. A three-tier architecture was adopted for modularity and scalability. The presentation layer, built with HTML5, CSS3, and JavaScript, provided an intuitive interface. The application layer, implemented in PHP (Laravel Framework), handled business logic, authentication, and integration with predictive analytics modules. The data layer, based on MySQL, ensured secure storage of maintenance logs and SLA records. Predictive maintenance analytics were embedded through Python scripts integrated with PHP APIs, using regression models to forecast system faults and prompt early interventions. Implementation was carried out in a local XAMPP environment and later mirrored on Heroku for cloud testing. The system's core modules (login, scheduling, audit, notification, and predictive dashboard) were validated through multi-stage testing. User Acceptance Testing (UAT) by fifteen ICT managers indicated over 90% satisfaction with usability, reliability, and performance.

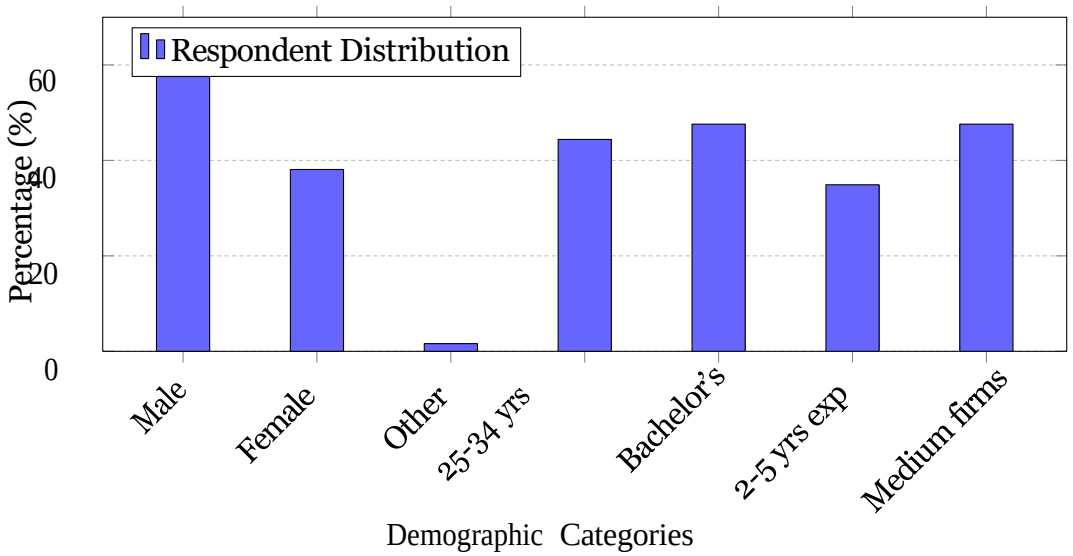
3.0 Results and Discussion

Response Rate and Demo- graphics

Of 90 targeted respondents, 68 returned questionnaires, 63 of which were deemed valid, yielding a 70% effective response rate. Most respondents were male (60.3%), aged 25–34 (44.4%), and held a bachelor's degree (47.6%). Additionally, 34.9% had 2–5 years of experience, and medium-sized security firms employed 47.6% of the workforce.

Figure 1

Demographic Distribution of Survey Respondents



Current ISMS Maintenance Practices

The first objective assessed current ISMS maintenance practices and tracking mechanisms among security firms in Nairobi County. Using ten Likert-scale items, the results showed consistently low mean scores (1.92-2.11 on a five-point scale), indicating that existing ISMS maintenance practices are generally weak and inadequately structured.

Table 1

Mean Scores for Current ISMS Maintenance Practices

Practice Item	Mean	Std. Dev.
Preventive maintenance scheduling	1.92	0.67
Corrective action effectiveness	1.98	0.71
Incident reporting mechanisms	2.05	0.69
Team coordination	2.03	0.73
Documentation practices	1.96	0.65
Real-time monitoring	1.94	0.68
Compliance tracking	2.11	0.74
Resource allocation	2.08	0.70
Performance auditing	1.99	0.66
Staff training adequacy	2.01	0.72
Overall Mean	2.01	0.69

Correlation analysis showed a strong, negative, and statistically significant correlation between current ISMS maintenance practices and system effectiveness ($r = -0.650$, $p<0.01$). Regression analysis yielded an R^2 of 0.423, indicating that current ISMS maintenance practices explain 42.3% of the variation in system effectiveness. ANOVA results confirmed that the regression model was statistically significant, $F(1, 61) = 44.714$, $p<0.001$. The regression coefficients indicated that current ISMS maintenance practices have a statistically significant negative

effect on system effectiveness (β = -0.650, p < 0.001). The unstandardized coefficient (B = −0.893) shows that for every one-unit increase in reliance on existing ISMS maintenance practices, system effectiveness decreases by approximately 0.9 units.

Best Practices in ISMS Maintenance

The second objective investigated recognized best practices for ISMS maintenance and tracking. Mean scores for all items ranged from 3.90 to 4.02 on a five-point scale, indicating that respondents strongly agreed with the importance of these practices.

Table 2

Mean Scores for ISMS Best Practices

Best Practice Item	Mean	Std. Dev.
Automated preventive scheduling	4.02	0.58
Real-time monitoring systems	3.98	0.61
SLA compliance tracking	3.95	0.59
Integrated audit trails	3.97	0.62
Automated notification systems	4.01	0.57
Role-based access control	3.93	0.63
Predictive maintenance analytics	3.90	0.65
Documentation automation	3.96	0.60
Performance dashboards	3.94	0.61
Integration of physical and cyber controls	3.99	0.59
Overall Mean	**3.97**	**0.61**

Correlation analysis showed a moderate, positive, and statistically significant correlation between best practices in ISMS maintenance tracking and system effectiveness (r = 0.592, p < 0.01). Regression analysis produced an R^2 value of 0.350, indicating that best practices in ISMS maintenance tracking explain 35.0% of the variation in system effectiveness. ANOVA confirmed that the model was statistically significant, F (1, 61) = 32.858, p < 0.001.

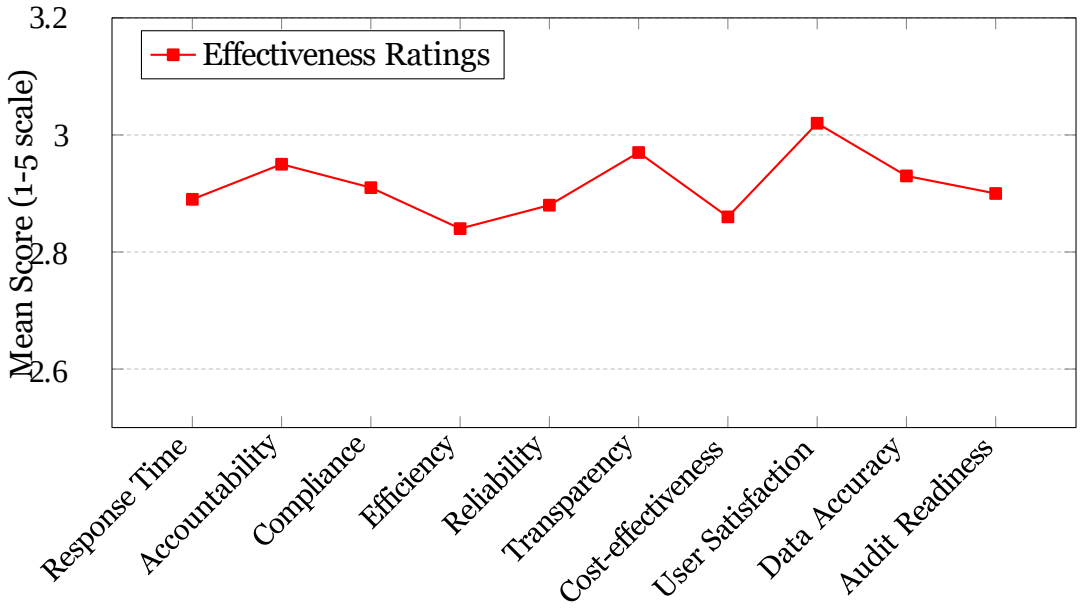
The regression coefficients indicate that best practices in ISMS maintenance tracking have a positive, statistically significant effect on system effectiveness (β = 0.592, t = 5.732, p < 0.001). The unstandardized coefficient (B = 0.815) indicates that for every one-unit increase in the adoption of best practices, system effectiveness increases by 0.815 units.

System Effectiveness

Ten Likert-scale items measured perceptions of system effectiveness. Mean scores ranged from 2.84 to 3.02 on a five-point scale, indicating that respondents were generally neutral about system effectiveness.

Figure 2

Expected System Effectiveness Across Multiple Dimensions



Multiple linear regression analysis showed that the combined effect of current ISMS maintenance practices and best practices in ISMS maintenance tracking explained 75.0% of the variation in system effectiveness (R^2 = 0.750). ANOVA confirmed that the regression model was statistically significant, with F (2, 60) = 89.812 and p<0.001.

Table 3

Multiple Regression Analysis Results

Variable	B	SE	*β*	p-value
Constant	3.245	0.412	-	<0.001
Current Practices	-0.868	0.095	-0.632	<0.001
Best Practices	0.788	0.089	0.572	<0.001

R = 0.866, R^2 = 0.750, Adjusted R^2 = 0.741 F (2,60) = 89.812, p<0.001

Regression coefficients indicated that current ISMS maintenance practices have a statistically significant negative effect on system effectiveness ($B = -0.868$, $\beta = -0.632$, $p < 0.001$). In contrast, best practices in ISMS maintenance tracking have a positive and statistically significant effect ($B = 0.788$, $\beta = 0.572$, $p < 0.001$).

User Acceptance Testing

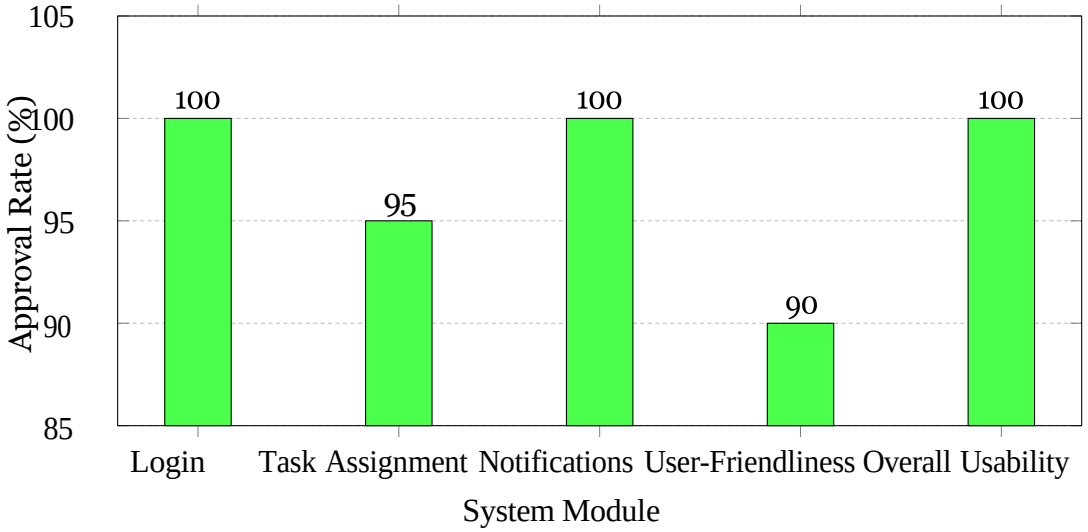
User Acceptance Testing (UAT) was conducted with 63 ICT managers from private security firms. The results showed strong approval across all modules:

- 100% found it easy to interact with the system during login and access using their assigned roles
- 95% rated task assignment and

monitoring as very easy
- 100% confirmed that notifications were timely and useful
- 90% described the system as very user-friendly
- 100% agreed that the system is usable in supporting ISMS maintenance

Figure 3

User Acceptance Testing Results by Module



Functional testing confirmed that all core modules met their intended objectives, with success rates above 96%. The login, audit, client, personnel, and notification modules achieved 100% success, while the task assignment module achieved 96.8%.

Discussion

The study reveals that ISMS maintenance practices, the adoption of recognized best practices, and system design collectively shape the effectiveness of information security management in Nairobi's private security sector. The results show that ISMS effectiveness depends less on capital investment and more on systematic process redesign, automation, and adherence to best practices. This supports Chege (2023) and Jevelin and Faza (2023) who, observed that structured monitoring, documentation, and follow-up are stronger predictors of ISMS maturity than the scale of investment. The findings, therefore, affirm that localized, modular, and technology-driven innovations can achieve reliability comparable to that of large enterprise systems when grounded in consistent maintenance routines and accountability mechanisms.

Current ISMS maintenance practices among Nairobi's private security firms were found to be fragmented, reactive, and largely manual, characterized by weak preventive maintenance, inconsistent reporting, and inadequate staff capacity. These weaknesses align with findings by Chege (2024), Jevelin and Faza (2023) and Omari and Mwarey (2020) who, documented similar gaps in ISMS management across Kenyan firms. The persistence of such deficiencies suggests structural challenges, including underfunded ICT functions, poor coordination, and a lack of a security-oriented culture, that inhibit proactive maintenance. As Tan and Kim (2021) argue, when ISMS is treated as the responsibility of a few specialists rather than an organization-wide function,

accountability diminishes, and compliance risks increase.

Conversely, respondents strongly endorsed recognized best practices, including preventive scheduling, automated incident logging, SLA monitoring, and the integration of physical and cybersecurity controls. These practices align with Ahmed et al. (2022) and Almuhammadi and Alsaleh (2021) who, found that automation, standardization, and unified control mechanisms enhance system reliability and regulatory compliance. The Nairobi findings further support Prislan et al. (2020) who emphasized that embedding audit trails and real-time reporting mechanisms strengthens trust, usability, and accountability in ISMS environments. Thus, institutionalizing these practices transforms ISMS maintenance from a reactive routine into a proactive governance function.

The development and validation of the ISMS Maintenance Tracking System provides practical evidence that integrating automation, auditability, and modular design can overcome the inefficiencies of manual systems. This aligns with Marhad et al. (2024) who reported that automation improves ISMS responsiveness and compliance outcomes. Validation outcomes from Nairobi confirm that user-centered, automated designs promote usability and institutional adoption, consistent with global trends toward intelligent security management systems. Beyond individual firms, the study contributes to the broader agenda of cybersecurity resilience and digital transformation in Kenya. By embedding audit trails, preventive maintenance, and accountability features, private security firms align their operations with national data protection objectives and Sustainable Development Goal 9 on industry, innovation, and infrastructure. The study, therefore, extends the ISMS literature by demonstrating that context-specific, low-cost, design-driven solutions can strengthen both organizational and regulatory capacities.

4.0 Conclusion

The study concludes that current ISMS maintenance practices in Nairobi's private security firms are inadequate and reactive, negatively affecting system effectiveness. It further concludes that adopting recognized best practices, such as preventive scheduling, automated incident logging, and SLA monitoring, significantly enhances accountability, compliance, and efficiency. The developed ISMS Maintenance Tracking System effectively integrates these practices through automation and modular design, improving usability and reliability. Overall, the study concludes that transitioning from manual, fragmented processes to structured, automated systems strengthen ISMS governance and operational resilience.

5.0 Recommendations

The study concludes that private security firms should replace manual ISMS maintenance with standardized, automated practices aligned with ISO/IEC 27001 to improve efficiency, accountability, and compliance. Adoption of the developed ISMS Maintenance Tracking System will institutionalize best practices such as preventive scheduling, SLA monitoring, and audit logging, strengthening organizational resilience and data protection. Regulators such as CAK and ODPC should enforce structured ISMS maintenance through mandatory compliance audits and targeted incentives, ensuring sector-wide consistency and accountability. These actions will enhance national cybersecurity resilience and support

Kenya's digital transformation goals. Future research should explore cross-sector applications and emerging technologies, including AI and blockchain, to expand ISMS innovation and ensure sustainable information security management.

References

Agarwal, R., & Prasad, J. (2023). Technology acceptance and adoption in emerging economies: Revisiting TAM for the digital era. *Journal of Information Systems Research, 34*(2), 145–160. https://www.mdpi.com/1996-1073/17/8/1982

Ahmed, M., Khan, R., & Shah, S. (2022). Information security management in SMEs: Challenges and practices. *Journal of Information Security and Applications, 68*(1), 103207. https://files01.core.ac.uk/download/pdf/162231466.pdf

Alghamdi, A., & Bach, C. (2024). User experience and technology adoption in cybersecurity systems: An empirical validation of TAM2. *Information Technology Journal, 19*(3), 200–214. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4786584

Almuhammadi, S., & Alsaleh, M. (2021). Information security governance framework for small and medium enterprises. *Computers & Security, 109*, 102393. https://www.mdpi.com/2079-9292/12/17/3629

Anderson, P., & Lee, K. (2023). Predictive analytics in information system maintenance: Trends and frameworks. *Computers in Industry, 151*, 103988. https://link.springer.com/chapter/10.1007/978-981-96-7134-2_40

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

Capgemini. (2023). *World quality report 2023–24.* Capgemini Research Institute. https://www.capgemini.com/research/world-quality-report

Chege, J. (2024). *Adoption of information security standards in Kenyan SMEs* (Tech. Rep.). Kenya Institute of ICT Research.

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

Creswell, J. W., & Creswell, J. D. (2018). *Research design: Qualitative, quantitative, and mixed methods approaches* (5th 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. https://misq.umn.edu/misq/article-abstract/13/3/319/191/Perceived-Usefulness-Perceived-Ease-of-Use-and

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. https://www.emerald.com/jqme/article/15/1/92/248120

Gartner. (2020). *Market guide for IT infrastructure monitoring tools* (Tech. Rep.). Gartner Inc.

Gartner. (2024). *Forecast analysis: IT operations and monitoring tools, worldwide, 2024.* Gartner Inc.

Government of Kenya. (2019). *Data Protection Act, No. 24 of 2019.* Kenya Gazette

Supplement No. 181 (Acts No. 24). http://kenyalaw.org/kl/fileadmin/pdfdownloads/Acts/2019/DataProtectionAct__No24of2019.pdf

Grenefalk, L., & Wallin, C. N. (2023). *Security management: Investigating the challenges and success factors in the implementation and maintenance of Information Security Management Systems (ISMS)* [Master's thesis, Stockholm University].Sweden. https://su.diva-portal.org/smash/get/diva2:1784450/FULLTEXT01.pdf

Grobler, M., & von Solms, R. (2021). The need for effective information security management in the digital age. *Information & Computer Security*, *29*(4), 642–660. https://ersj.eu/journal/3427

Hevner, A. R., March, S. T., Park, J., & Ram, S. (2004). Design science in information systems research. *MIS Quarterly, 28*(1), 75–105. https://misq.umn.edu/misq/article-abstract/28/1/75/261/Design-Science-in-Information-Systems-Research1?redirectedFrom=fulltext

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

International Organization for Standardization (2022). *ISO/IEC 27001:2022 information security, cybersecurity, and privacy protection - information security management systems requirements.* https://www.iso.org/standard/82875.html

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. https://pdfs.semanticscholar.org/ffd0/c571f1e24b8a354d65fe317c34ee07528117.pdf

Kast, F. E., & Rosenzweig, J. E. (2022). *Organization and management: A systems and contingency approach* (Rev. ed.). McGraw-Hill.

Khan, A., Ahmad, S., & Rahman, M. (2021). Proactive information security management practices in SMEs. *Journal of Cybersecurity Research*, *6*(2), 89–105. https://www.nature.com/articles/s41598-025-97204-y

Kothari, C. R. (2014). *Research methodology: Methods and techniques* (4th Ed.). New Age International Publishers.

Kuria, J. N., & Kagiri, D. (2023). Development of IT-based tools for service management in security firms: A case of Nairobi County. *East African Journal of Information Technology*, *3*(2), 90–105. I: https://doi.org/10.37284/eajit.7.1.1757

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. https://ebpj.e-iph.co.uk/index.php/EBProceedings/article/view/5483

Mutinda, F. M., & Wabwoba, F. (2023). Adoption of ISMS in Kenyan SMEs: Opportunities and barriers. *African Journal of Information Systems, 15*(1), 57–72. https://www.academia.edu/25799851/The_African_Journal_of_Information_Systems_Absorptive_Capacity_and_ICT_Adoption_Strategies_for_SMEs_a_Case_Study_in_Kenya_Recommended_Citation

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

Ndungu, J., & Kimani, P. (2023). Barriers to automation in Kenyan ICT enterprises. *African Journal of Technology and Innovation, 4*(1), 112–127. https://cedred.or.ke/jais/images/august2025/1PDF_Ndunga__Kithome_Arti%EF%AC%81cial_Intelligence_in_Communication_Scholarship.pdf

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

Omari, L., & Mwarey, D. (2020). Information security compliance practices in Kenyan financial institutions. *African Journal of Information Systems, 12*(4), 211 - 230. https://www.researchgate.net/publication/382181008_Information_Security_Management_System_Practices_in_Kenya

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

Private Security Regulatory Authority (PSRA). (2024). *List of licensed private security companies.* PSRA Kenya. https://psra.go.ke

Prislan, K., Mihelič, A., & Bernik, I. (2020). A real-world information security performance assessment using a multidimensional socio-technical approach. *PLOS ONE, 15*(9), e0238739. https://journals.plos.org/plosone/article?id=10.1371/journal.pone.0238739

Serrano, L., Ortega, F., & Liu, H. (2022). Predictive maintenance in cybersecurity systems using AI-driven analytics. *Computers & Industrial Engineering, 170,* 108373. https://www.mdpi.com/2223-7747/14/21/3390

Tan, Y., & Kim, J. (2021). Organizational accountability in information security management. *Information Management Journal, 58*(4), 303–319. https://www.sciencedirect.com/science/article/pii/S2444569X24001495

Venkatesh, V., & Bala, H. (2021). Technology acceptance model 3 and a research agenda on interventions. *Decision Sciences, 52*(3), 567–606. https://onlinelibrary.wiley.com/doi/full/10.1111/j.1540-5915.2008.00192.x

Whitman, M. E., & Mattord, H. J. (2022). *Principles of information security* (7th Ed.). Cengage Learning.

Wireman, T. (2010). *Total productive maintenance* (2nd Ed.). Industrial Press.

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