

Effect of Technology-Oriented Factors on ISO/IEC 27001:2022 Implementation in Public Sector Organizations in Kenya

 Lubembe Khatievi Carolyne,  Abeka Silvanice and  Ogara Solomon

School of Informatics and Innovative Systems, Jaramogi Oginga Odinga University
of Science and Technology, P.O. Box 210 - 40601 Bondo – Kenya

Abstract

The effective implementation of ISO/IEC 27001:2022 in public sector organizations depends not only on the existence of an Information Security Management System (ISMS) but also on the technological conditions under which security requirements are operationalized. Drawing on the Task-Technology Fit theory, this study examined the effect of system quality, information quality and technology fit on ISO/IEC 27001:2022 implementation in public-sector organizations in Kenya. An explanatory cross-sectional design was employed among employees and management in 13 Kenyan public-sector organizations. From a target sample of 384 respondents, 343 usable responses were obtained, representing an 89.37% response rate. Reliability was established through Cronbach's alpha, while validity was assessed through face and content validity by subject matter experts. Data were collected using a structured questionnaire and analyzed using descriptive statistics and multiple linear regression. Information accuracy recorded the highest mean ($M = 4.31$, $SD = 0.840$), whereas information being logical recorded the lowest ($M = 2.66$, $SD = 1.180$). Among technology-fit indicators, task effectiveness and efficiency had the highest mean ($M = 3.90$, $SD = 0.953$), while increased output quantity had the lowest ($M = 2.84$, $SD = 1.190$). Multiple regression showed that system quality ($\beta = .231$, $p = .001$), information quality ($\beta = .222$, $p = .045$), and technology fit ($\beta = .222$, $p = .038$) were positively and significantly associated with ISO/IEC 27001:2022 implementation when people- and process-oriented factors were controlled. The overall nine-factor model explained 58.4% of the variance in implementation ($R^2 = .584$; adjusted $R^2 = .583$; $F(9, 333) = 29.840$, $p < .001$). The findings demonstrate that technological conditions are key to translating ISO/IEC 27001:2022 requirements into operational information-security practices. The study contributes contextual empirical evidence from Kenya and highlights the need to evaluate information-security implementation not merely in terms of the existence of technical controls but also in terms of system reliability, information quality, and alignment between technology capabilities and organizational tasks.

Keywords: ISO/IEC 27001:2022, information security management system, system quality, information quality, technology fit, public sector, Kenya

Correspondence: carolubembe@gmail.com

Copyright © 2026 Lubembe et al. This is an open-access article distributed under the terms of the Creative Commons Attribution License (CC BY).

Funding: The author received no financial support for the research, authorship and/or publication of this article

Data Availability Statement: The authors confirm that the data supporting the findings of this study are available within the article [and/or] its supplementary materials or upon reasonable request.

Competing interests: The authors declare no potential conflicts of interest with respect to the research, authorship and/or publication of this article.

Introduction

Information has become one of the most consequential assets held by public sector organizations, underpinning decision-making, service delivery, communication, and the execution of administrative processes (Rohan et al., 2023). Its value, however, is contingent on its accuracy, completeness, and availability, which obliges organizations to protect information against unauthorized access, disclosure, modification, destruction, and disruption while preserving its confidentiality, integrity, and availability (Yee & Zolkipli, (2021); Rahimli, (2025; Kaporo, 2024) As public institutions increasingly digitize their operations, the locus of information security concern has shifted from the mere installation of technical safeguards to the effective implementation and internalization of security controls within everyday organizational practice (Almuqrin, 2024; Araujo et al., 2024).

Information security standards provide a structured mechanism for identifying, managing, and mitigating information security risks (Taherdoost, 2022; Sekti, 2026). Among these, ISO/IEC 27001 is the most widely recognized international standard for establishing, implementing, maintaining, and

continually improving an Information Security Management System (ISMS) (Alrehili & Alhazmi, 2023; Taherdoost, 2022). The 2022 revision responded to a transformed cyber threat landscape by introducing updated controls, greater emphasis on organizational context, leadership, cloud and third-party security, and alignment with the high-level structure common to other management system standards (Leme et al., 2026; Vakhula et al., 2024). Yet the existence of a standard, even a comprehensively revised one, does not automatically translate into effective information security. Formal adoption and certification do not necessarily demonstrate that controls operate effectively in practice (Chavez et al., 2024; Efunwoye et al., 2025).

The implementation gap is particularly acute in public sector organizations. Evidence from Kenya shows a marked rise in cyberattack incidents targeting public institutions reported increases of 65% between 2020 and 2022 and 75% in 2022 alone with direct consequences for the availability of government platforms (Gichubi et al., 2024; Keefa et al., 2024). Kiarie (2024) attributed much of this exposure to unpatched software, weak

authentication, and chronic resource constraints. Kenya's aggressive e-government expansion has widened the attack surface further, making the protection of information stored, processed, and transmitted across government systems a strategic imperative (Karoki et al., 2025; Ohndyl et al., 2023). Ironically, Kenyan public institutions lag behind their private sector counterparts in ISO/IEC 27001 certification, suggesting that the difficulties lie less in the standard itself than in the conditions under which its requirements are operationalized.

A growing body of research emphasizes that implementation outcomes are shaped by interconnected socio-technical factors, including people, processes, and technology, which should be considered as an integrated system rather than as separate elements (Chen & Hai, 2024; Djebbar & Nordström, 2023). Within this framework, technology-related conditions provide a critical foundation for effective implementation. The security controls outlined in ISO/IEC 27001:2022, including access control, logging and monitoring, incident management, asset handling, and business continuity measures, are implemented through organizational information systems. Where systems are unreliable, where the information they produce is inaccurate or insufficient, or where the available technology does not fit the tasks it is meant to support, even well-designed security requirements degrade into formal compliance without substantive protection (Islam et al., 2026; Mirtsch, 2023). System quality, information quality, and technology fit therefore constitute a theoretically coherent and practically actionable set of predictors of implementation effectiveness.

Despite their importance, technology-related factors have often

been investigated separately or treated as background security controls in information security research, rather than being examined collectively as a predictive set grounded in the revised 2022 standard and applied within a developing-country public sector. Much of the available evidence predates ISO/IEC 27001:2022 or is drawn from private sector organizations in industrialized economies (Batte, 2025; Mirtsch, 2023; Suorsa & Helo, 2023). This study addresses that gap by isolating and empirically testing the effect of system quality, information quality, and technology fit on ISO/IEC 27001:2022 implementation in Kenyan public sector organizations.

Theoretical Framework

The study is anchored on Task–Technology Fit (TTF) theory, developed by Goodhue and Thompson (1995). The theory proposes that information technology contributes to individual and organizational performance when the capabilities of a technology are aligned with the tasks it is intended to support. Goodhue and Thompson (1995) conceptualized TTF as the degree to which technology characteristics match task requirements, arguing that such alignment enhances the effective use and performance impacts of information systems.

In the present study, the theory provides a basis for explaining how system quality, information quality, and technology fit may support the implementation of ISO/IEC 27001:2022 in public-sector organizations. High system quality can provide reliable and accessible technological infrastructure for implementing information-security requirements, while high information quality can provide accurate and sufficient information for security-related decisions and monitoring. Technology fit

reflects the extent to which information systems support the tasks required for operationalizing the standard.

The relevance of TTF to information-systems research is further supported by Jeyaraj (2022) meta-regression, which examined evidence from 100 studies and found that TTF is associated with technology-related perceptions, behaviours, and performance outcomes, while also emphasizing the importance of contextualizing TTF to specific technologies and users. Thus, TTF provides an appropriate theoretical foundation for examining whether the technological characteristics of information systems are associated with effective ISO/IEC 27001:2022 implementation in Kenyan public-sector organizations.

Empirical Review and Hypothesis Development

ISO/IEC 27001:2022 Implementation

Information security is an important organizational concern because information is a critical asset whose loss, unauthorized access, or compromise can affect organizational operations and continuity. ISO/IEC 27001 provides a structured approach for establishing, implementing, maintaining, and continually improving an Information Security Management System (ISMS). The standard emphasizes systematic identification and treatment of information-security risks and the integration of appropriate controls within organizational processes (Spruill et al., 2024).

Implementation of ISO/IEC 27001 extends beyond adopting individual security technologies or developing information-security policies. It requires organizations to assess information-security risks, establish appropriate

controls, define responsibilities, document processes, monitor performance, and continually improve the ISMS. Alrehili and Alhazmi (2023) explain that ISO/IEC 27001 provides requirements for establishing an ISMS, while supporting standards such as ISO/IEC 27002 provide guidance on security controls. Thus, implementation requires the integration of security requirements into routine organizational activities.

Risk assessment and treatment constitute important elements of implementation. Organizations need to identify information assets, threats, vulnerabilities, and associated risks before determining appropriate controls (Shaikh & Siponen, 2023). Implementation therefore involves an ongoing process through which organizations identify changing security risks, apply appropriate measures, and evaluate their effectiveness. Continuous monitoring, review, and improvement are consequently essential to maintaining an effective ISMS (Rohan et al., 2023).

Implementation also requires appropriate organizational structures and resources. Clearly defined responsibilities, management support, adequate resources, training, documentation, and regular evaluation facilitate the operationalization of information-security requirements. However, studies indicate that organizations may face barriers related to certification costs, implementation time, inadequate resources, and limited organizational capabilities (Hassan et al., 2022; Kamil et al., 2023; Plate, 2025). The presence of the standard therefore does not necessarily ensure that its requirements are effectively implemented.

Technology is particularly important to implementation because many ISMS activities depend on

information systems for storing, processing, retrieving, monitoring, and securing organizational information. The effectiveness of these activities may depend on whether systems are reliable and accessible, whether the information they generate is accurate and sufficient, and whether the technology adequately supports users' tasks. Consequently, technological conditions can influence how effectively organizations operationalize information-security requirements.

The relationship between technology and information-security implementation is consistent with information-systems success and task-technology fit perspectives. System quality concerns characteristics such as reliability, accessibility, responsiveness, and usability, while information quality concerns the accuracy, sufficiency, relevance, and usefulness of system outputs (DeLone & McLean, 2003). Task-technology fit further suggests that technology contributes to performance when its capabilities are aligned with users' task requirements (Goodhue & Thompson, 1995). These perspectives provide a basis for examining whether the quality and suitability of organizational information systems support ISO/IEC 27001:2022 implementation.

Although existing literature provides substantial evidence on ISMS requirements, risk management, governance, and implementation challenges, several gaps remain. First, much of the empirical literature has examined earlier versions of ISO/IEC 27001 rather than the 2022 edition (Culot et al., 2021). Second, studies have commonly examined individual implementation requirements or organizational challenges rather than the contribution of specific technology-oriented factors. Third, limited empirical evidence addresses ISO/IEC 27001:2022

implementation in Kenyan public-sector organizations.

The present study addresses this gap by examining the relationship between system quality, information quality, and technology fit and ISO/IEC 27001:2022 implementation in Kenyan public-sector organizations. This focus provides empirical evidence on how technological characteristics of organizational information systems are associated with the operationalization of the standard within the public-sector context.

System quality and ISO/IEC 27001:2022 implementation

System quality refers to the technical and operational characteristics of an information system, including reliability, availability, responsiveness, accessibility, usability, and flexibility (DeLone & McLean, 2003). In ISO/IEC 27001:2022 implementation, these characteristics provide an important technological foundation because security controls depend on information systems that can reliably support activities such as access management, monitoring, logging, backup, and incident management. Poor system performance or availability may therefore constrain the consistent operationalization of security requirements.

The DeLone and McLean (2003) Information Systems Success Model identifies system quality as a core determinant of information-system success and links it to system use, user satisfaction, and organizational benefits. Empirical evidence supports this relationship in public-sector environments. Apridiyanti et al. (2020), examining the Regional Financial Management Information System in the Sumedang District Government, found that system quality significantly influenced user satisfaction and net

benefits. Similarly, Nadir et al. (2024), studying the Regional Government Information System in Indonesia, demonstrated the relevance of system quality within the assessment of public-sector information-system success.

In Africa, Sausi et al. (2021), using a concurrent mixed-methods design involving 296 users across five regions in Tanzania, found that system quality had a significant positive effect on the success of the local government revenue-collection information system. This suggests that reliable technical characteristics are important for the effective operation of public-sector information systems.

In Kenya, Indeje and Qin (2011), in a qualitative case study of information-system development in the Kenyan public service, identified system quality as a principal dimension of information-system success. Research on Machakos County Government also incorporated system quality, information quality, and task-technology fit when examining information-system implementation and employee performance among 215 respondents. In addition, Mutong'wa et al. (2017), examining IFMIS use in Kenya's Government Treasury reported significant relationships involving information-system quality dimensions.

Evidence from Kenya's health-information systems further illustrates the practical importance of system quality. A post-implementation evaluation of DHIS2 assessed system quality through characteristics such as ease of use, accessibility, integration, functionality, availability, responsiveness, and consistency, demonstrating the relevance of these characteristics when evaluating public-sector information systems.

Despite this evidence, majority of the existing studies examine general information-system success, financial-

management systems, e-government, or health-information systems, rather than ISO/IEC 27001:2022 implementation. Consequently, limited empirical evidence directly establishes whether system quality influences ISO/IEC 27001:2022 implementation in Kenyan public-sector organizations. The present study addresses this gap by examining system quality as a technology-oriented determinant of implementation. Accordingly, the study tests the following null hypothesis:

H₀₁: System quality has no significant positive effect on ISO/IEC 27001:2022 implementation in public-sector organizations in Kenya.

Information quality and ISO/IEC 27001:2022 implementation

Information quality refers to the accuracy, completeness, relevance, timeliness, and consistency of information generated and used by an information system (DeLone & McLean, 2003). In ISO/IEC 27001:2022 implementation, reliable information is important because security decisions depend on accurate records of assets, risks, vulnerabilities, incidents, and control performance. Poor-quality information can therefore weaken risk assessment, monitoring, reporting, and corrective action.

Empirical evidence generally supports a positive relationship between information quality and effective information-system outcomes. Tewamba et al. (2019), in a study of information security management systems, found that information-system quality dimensions were associated with information-security risk-management maturity and organizational performance. Similarly, Sausi et al. (2021), using data from 296 users of a local government revenue-collection information system in Tanzania, found that information quality

significantly contributed to system success. In Ghana, Owusu and Akpe-Doe (2022) reported that information quality influenced users' perceptions of e-government effectiveness, while Owusu (2023) found that information quality did not significantly influence system use. These contrasting findings suggest that the contribution of information quality may depend on the organizational and technological context.

Evidence from Kenya also indicates the importance of information quality in public-sector information systems. Ayim (2019) found a significant relationship between the use of Integrated Financial Management Information Systems and the performance of government ministries, with information quality forming an important aspect of system effectiveness. However, these studies largely examine financial management, e-government, or general information-system performance rather than the implementation of an information security management system based on ISO/IEC 27001:2022.

The literature therefore establishes the relevance of information quality to effective information-system and security-management outcomes, but an empirical gap remains concerning its specific effect on ISO/IEC 27001:2022 implementation in Kenyan public-sector organizations. Accordingly, the study tests the following null hypothesis:

H₀₂: Information quality has no significant positive effect on ISO/IEC 27001:2022 implementation in public-sector organizations in Kenya.

Technology fit and ISO/IEC 27001:2022 implementation

Technology fit refers to the extent to which the capabilities of a technology correspond with the requirements of the tasks it is intended to support (Goodhue & Thompson, 1995). In

ISO/IEC 27001:2022 implementation, fit is important because security controls need to integrate with existing workflows, systems, and operational requirements. Poor alignment may increase the effort required to comply and encourage employees to circumvent security procedures. Soliman and Mohammadnazar (2022), for example, found that employees may justify information-security policy noncompliance in organizational contexts, highlighting the importance of how security requirements are experienced in practice.

Empirical research generally supports the importance of task–technology alignment for effective technology use. A meta-analysis by Cane and McCarthy (2009) found that task–technology fit influences information-system use and performance, although the strength of the relationship varies across contexts. More recently, Jeyaraj (2022), based on 104 findings from 100 studies, reported that task–technology fit generally predicts technology-related outcomes, while noting that effects differ according to the type of users, technologies, and dependent variables.

Evidence from information security further strengthens this relationship. Chen and Hai (2024), using mixed methods to investigate critical success factors for information security management, examined factors associated with information-security management performance. Alassaf and Alkhalifah (2026), using PLS-SEM with 288 employees from public and private organizations in Saudi Arabia, found that task–technology fit positively predicted information-security policy compliance intentions and subsequent compliance behaviour. Vakhula et al. (2024) also demonstrated the relevance of technology-process alignment through a security-as-code approach to fulfilling

ISO/IEC 27001:2022 requirements, particularly configuration-management requirements.

In Kenya, Oyugi (2012) found a positive relationship between task characteristics, technology characteristics, and adoption of project-management information systems among NGOs in Nakuru. Although this provides contextual evidence that technology–task alignment influences technology adoption, it does not address information-security management or ISO/IEC 27001 implementation. The broader literature therefore indicates that technology fit can facilitate effective technology use and security compliance, but there is limited empirical evidence on whether it directly influences ISO/IEC 27001:2022 implementation in Kenyan public-sector organizations. Accordingly, the study tests the following null hypothesis:

H₀₃: Technology fit has no significant positive effect on ISO/IEC 27001:2022 implementation in public-sector organizations in Kenya.

Methodology

Research design and setting

The study adopted an explanatory cross-sectional survey design, appropriate for quantifying associations and testing hypothesized cause-effect relationships between technology-oriented predictors and implementation effectiveness (Skinner & Dancis, 2026). The setting comprised thirteen Kenyan public service parastatals purposively selected because they had established ISMS environments and had pursued satisfaction of ISMS requirements: the Communication Authority of Kenya, Kenya National Highway Authority, Kenya Plant Health Inspectorate Service, Kenya Revenue Authority, Kenyatta University Teaching

Referral and Research Hospital, Moi Teaching and Referral Hospital, National Construction Authority, National Hospital Insurance Fund, National Housing Corporation, National Social Security Fund, Office of the Attorney General, Unclaimed Financial Assets Authority, and the Kenya Bureau of Standards.

Population and sampling

The target population consisted of management and employees directly involved in information security management, including heads of IT, human resources, compliance and risk management, legal and policy, and audit and internal control departments, as well as senior management, management representatives, operational/technical staff (e.g., data protection officers, IT security officers, network engineers, system administrators), and support staff. Using the Fisher et al. (1992) formula cited in Kennedy (2022) with $z = 1.96$, $p = 0.5$, and $d = 0.05$, the minimum sample was determined as 384 respondents. Within each organization, respondents were drawn through stratified sampling across the functional strata described above, followed by simple random sampling of individuals within each stratum. This combined purposive (organization-level) and stratified random (individual-level) approach ensured that respondents possessed sufficient exposure to the technology and processes under study.

Research instrument

Primary data were collected using a structured, self-administered questionnaire developed from the literature and aligned with the study constructs. Technology-oriented constructs were measured with twelve items on a five-point Likert scale (Strongly Disagree = 1 to Strongly Agree = 5). System quality was measured with four

items (system accessibility for information storage, efficiency of information search, capacity to add useful information, dependability and response speed); information quality with four items (logical, accurate, sufficient, and suitable information); and technology fit with four items (increased output quantity, increased task effectiveness and efficiency, increased output quality, and reduced time spent on jobs). The dependent variable implementation of ISO/IEC 27001:2022 was measured with ten items capturing communication of the standard, planning, training, integration with existing policies, leadership commitment, fit to public sector security needs, measurable objectives, resource sufficiency, monitoring, and continual review and improvement.

Reliability and validity

Content and face validity were established through expert review by university supervisors and specialists in ISO standards, whose feedback was incorporated to refine item wording, clarity, and relevance (Asher, 2024). A pilot study involving 38 respondents (approximately 10% of the sample, consistent with Bujang et al., 2024) was conducted outside the main sample. Internal consistency was assessed using

Cronbach's alpha, with coefficients of 0.70 or higher considered acceptable (Forero, 2024).

Data analysis

Data were screened, coded, and analyzed using SPSS version 29. Descriptive statistics (frequencies, percentages, means, and standard deviations) characterized respondents and construct distributions. Hypotheses were tested using multiple linear regression, which estimates the effect of each predictor on implementation while holding the other predictors constant. The technology-oriented assessment model was specified as:

$$Y = \beta_0 + \beta_1(SYQ) + \beta_2(INQ) + \beta_3(TEF) + \epsilon$$

where Y is implementation of ISO/IEC 27001:2022, SYQ is system quality, INQ is information quality, TEF is technology fit, β_0 is the constant, β_1 – β_3 are regression coefficients, and ϵ is the error term.

Results and Discussion

Response rate and respondent characteristics

Of the 384 questionnaires administered, 343 were returned complete and usable, a response rate of 89.37% (Table 1).

Table 1. Demographic characteristics of respondents (N = 343)

Characteristic	Category	Frequency	Percentage
Gender	Male	202	58.9
	Female	141	41.1
Age	20–30 years	33	9.5
	31–40 years	142	41.3
	41–50 years	146	42.7
	Above 50 years	22	6.5
Education	College	66	19.1
	Undergraduate	185	53.8
	Postgraduate	93	27.1
Work experience	Below 5 years	33	9.6
	5–10 years	90	26.1

11–15 years	153	44.5
16–20 years	22	6.3
21–30 years	25	7.4
Above 30 years	21	6.1

Source: Field data (2024).

Respondents were predominantly male (58.9%) and female (41.1%), with the majority aged 31–50 years (84.0%). Most held undergraduate (53.8%) or postgraduate (27.1%) qualifications, and 44.5% had 11–15 years of organizational experience. This profile indicates that respondents were mature, well-educated, and sufficiently tenured to credibly assess their organizations' ISMS technology environment.

Reliability of the technology-oriented constructs

Cronbach's alpha coefficients for all technology-oriented items fell within the acceptable 0.70–0.90 band (Forero, 2024), confirming internal consistency (Table 2). Item-total correlations were predominantly above 0.30, and no item's deletion would have materially improved scale reliability, supporting retention of all twelve items.

Table 2: Reliability statistics for technology-oriented constructs (pilot, n = 38)

Construct	Items	Cronbach's alpha if item deleted (range)	Decision
System quality	4	0.679 – 0.715	Reliable ($\alpha \geq .70$ scale level)
Information quality	4	0.671 – 0.701	Reliable ($\alpha \geq .70$ scale level)
Technology fit	4	0.683 – 0.749	Reliable ($\alpha \geq .70$ scale level)

Source: Field data (2024). All item-total correlations and alpha-if-deleted statistics fell within the acceptable 0.70–0.90 band, and overall construct alphas exceeded .70.

Descriptive statistics

System Quality

System quality was assessed using four items measuring the accessibility, efficiency, usefulness, dependability, and responsiveness of organizational information systems. Respondents rated each item on a five-point Likert scale ranging from strongly disagree (SD) to strongly agree (SA). As presented in Table 4.12, all items recorded mean scores above the midpoint of 3.00, indicating generally positive perceptions of system quality. Efficient information search received the highest rating (M = 3.86, SD = .917),

followed by system accessibility for storing information (M = 3.80, SD = .874). The ability to add useful information recorded a mean of 3.66 (SD = 1.170), while system dependability and response speed had the lowest rating (M = 3.57, SD = 1.096). These findings suggest that the systems generally provide adequate access to information and support information retrieval, although dependability and responsiveness remain comparatively weaker aspects. The variation in responses, particularly for information input and system responsiveness, indicates differences in

users' experiences with system performance. Overall, the findings indicate that system quality provides a

supportive technological environment for organizational information security activities.

Table 3: Descriptive Statistics for System Quality

System Quality Item	SD (%)	D (%)	U (%)	A (%)	SA (%)	Mean	SD
The organization's system is accessible for storing information	2.3	3.4	25.3	49.4	19.5	3.80	.874
The organization's system allows for efficient search of information	2.3	2.3	28.7	40.2	26.4	3.86	.917
The organization's system allows for useful information to be added	5.7	9.2	28.7	26.4	29.9	3.66	1.170
The system is dependable and fast responding	1.1	20.7	20.7	34.5	23.0	3.57	1.096

Source: Field Data (2024)

Information Quality

Information quality was assessed using four items measuring the logicality, accuracy, sufficiency, and suitability of

information provided by the organization's system. The findings are presented in Table 4.

Table 4: Descriptive Statistics for Information Quality

Information Quality Item	SD (%)	D (%)	U (%)	A (%)	SA (%)	Mean	SD
Information provided by the organization's system is logical	19.5	29.9	19.5	27.6	3.4	2.66	1.180
Information provided by the organization's system is accurate	1.1	2.3	10.3	36.8	49.4	4.31	.840
Information provided by the organization's system is sufficient	4.6	10.3	5.7	43.7	35.6	3.95	1.120
Information provided by the organization's system is suitable	2.3	4.6	13.8	40.2	39.1	4.09	.960

Source: Field Data (2024)

As shown in Table 4, information accuracy recorded the highest mean (M = 4.31, SD = .840), followed by suitability (M = 4.09, SD = .960) and sufficiency (M = 3.95, SD = 1.120). In contrast, logicality recorded the lowest mean (M = 2.66, SD = 1.180). Overall, the findings indicate that respondents generally perceived the information as accurate, suitable, and sufficient, although concerns were evident regarding its logicality. This suggests that while the systems provide

useful and accurate information, consistency and logical organization of information may require improvement.

Technology Fit

Technology fit was assessed using four items measuring the extent to which the organization's system supports task effectiveness, output quality, time efficiency, and output quantity. The findings are presented in Table 5.

Table 5: Descriptive Statistics for Technology Fit

Technology Fit Item	SD (%)	D (%)	U (%)	A (%)	SA (%)	Mean	SD
The organization’s system increases output quantity	19.5	17.2	26.4	33.3	3.4	2.84	1.190
The organization’s system increases job task effectiveness and efficiency	4.6	3.4	12.6	56.3	23.0	3.90	.953
The organization’s system increases output quality	2.3	9.2	17.2	42.5	28.7	3.86	1.014
The organization’s system reduced time spent on jobs	4.6	9.2	19.5	42.5	24.1	3.72	1.075

Source: Field Data (2024)

As shown in Table 5, increasing job task effectiveness and efficiency recorded the highest mean ($M = 3.90$, $SD = .953$), followed by increasing output quality ($M = 3.86$, $SD = 1.014$) and reducing time spent on jobs ($M = 3.72$, $SD = 1.075$). Increasing output quantity recorded the lowest mean ($M = 2.84$, $SD = 1.190$). Overall, the findings indicate that the systems generally fit users’ tasks by improving effectiveness, efficiency, and

output quality, although their contribution to increasing output quantity was less evident.

Implementation of ISO/IEC 27001:2022 Standard for IS

Implementation of the ISO/IEC 27001:2022 standard was assessed using 10 items and the findings are presented in Table 6.

Table 6: Implementation of ISO/IEC 27001:2022 Standard for IS

	SD	D	U	SA	A	Mean	SD
The organization effectively communicates the importance of standards to all relevant stakeholders	3.4	13.8	16.1	41.4	25.3	3.71	1.099
The implementation process is well-planned and structured	8.0	5.7	26.4	27.6	32.2	3.70	1.045
There is adequate training provided to staff regarding the requirements of standards	4.6	2.3	24.1	36.8	32.2	3.90	1.035
Standards are integrated into existing information security policies and procedures	2.3	3.4	13.8	48.3	32.2	4.05	.901
Leaders demonstrate commitment to ensuring successful implementation	2.3	6.9	11.5	44.8	34.5	4.02	.976
Implementation meets the information security needs of the public sector	2.3	6.9	21.8	49.4	19.5	3.77	.924
	5.7	5.7	9.2	58.6	20.7	3.83	1.014
There are clear and measurable objectives set for the implementation	2.3	3.4	25.3	41.4	27.6	3.89	.933
	2.3	3.4	25.3	49.4	19.5	3.80	.874

Resources allocated for implementation are sufficient								
There is a systematic approach to monitoring and assessing the progress of implementation	2.3	2.3	28.7	40.2	26.4	3.86	.917	
Implementation is regularly reviewed and improved based on feedback and evaluation								

Source: Field Data (2024)

As shown in Table 6, all items recorded mean scores above the midpoint of 3.00, indicating generally positive perceptions of ISO/IEC 27001:2022 implementation. The highest rating was for integration of standards into existing information security policies and procedures (M = 4.05, SD = .901), followed by leadership commitment (M = 4.02, SD = .976). Training (M = 3.90, SD = 1.035) and adequacy of resources (M = 3.89, SD = .933) were also positively rated. The lowest mean was recorded for the implementation process being well-planned and structured (M = 3.70, SD = 1.045), followed closely by communication of the importance of standards (M = 3.71, SD = 1.099). Overall, the findings suggest that implementation was relatively well supported through policy integration, leadership commitment, training, and resource allocation, although planning and stakeholder communication showed comparatively greater scope for improvement.

Inferential Statistics

Model summary

The model produced R = .764, R² = .584, adjusted R² = .583, and a standard error of the estimate of .33310.

Table 7: Model summary

Model	R	R ²	Adjusted R ²	Std. Error
1	.764	.584	.583	.33310

Predictors: technology fit.

The R² of .584 indicates that 58.4% of the observed variation in ISO/IEC 27001:2022 implementation was explained jointly by the predictors. The remaining 41.6% represents variation associated with factors not included in the model, measurement error, and unexplained variation.

Table 8: ANOVA for the predictive model

Source	SS	df	MS	F	p
Regression	2.481	9	0.276	29.840	<.001
Residual	3.077	333	0.009		
Total	3.597	342			

Dependent variable: ISO/IEC 27001:2022 implementation.

The overall regression model was statistically significant, F(9, 333) = 29.840, p < .001.

Hypothesis Testing

The first hypothesis examined whether system quality had a significant positive effect on ISO/IEC 27001:2022 implementation. The results presented in Table 9 show that system quality had a positive and statistically significant effect on implementation (B = 0.274, β = .231, t = 3.519, p = .001). Since the p-value was below .05, H01 was rejected. This means that, holding the other variables constant, higher system-quality levels were associated with higher levels of ISO/IEC 27001:2022 implementation.

The finding is consistent with DeLone and McLean (2003), whose Information Systems Success Model identifies system quality as a fundamental determinant of system use, user satisfaction, and organizational benefits. It is also consistent with Sausi et al. (2021), who found that system quality significantly and positively influenced the success of a local-government revenue-collection information system in Tanzania. Similarly, Kenyan public-sector research has identified system quality as an important dimension of information-system success (Indeje & Qin, 2011). These studies provide support for the present finding by demonstrating that reliable, accessible, usable, and responsive systems contribute to effective operation of organizational technologies.

The present finding, however, extends this evidence to ISO/IEC 27001:2022 implementation. Whereas earlier studies largely focused on information-system success or system use, the present study demonstrates that system quality is also associated with implementation of an information-security management standard. This relationship is plausible because the implementation of security requirements depends partly on the availability and dependable operation of organizational technological infrastructure. Therefore, the rejection of H01 indicates that system quality represents a significant technology-oriented factor in ISO/IEC 27001:2022 implementation among Kenyan public-sector organizations.

The second hypothesis assessed the effect of information quality on ISO/IEC 27001:2022 implementation. The results presented in Table 9 indicate a positive and statistically significant relationship ($B = 0.183$, $\beta = .222$, $t = 2.033$, $p = .045$). Since $p < .05$, H02 was rejected. Thus, higher information-quality levels

were associated with higher implementation of ISO/IEC 27001:2022, controlling for the other factors in the model.

This finding agrees with DeLone and McLean (2003), who identify information quality as a core component of information-system success. It also corresponds with Sausi et al. (2021), who reported a significant positive effect of information quality on the success of a local-government information system in Tanzania. Evidence from Ghana likewise indicates that information quality can contribute to system usage and user satisfaction in public-sector information systems (Owusu & Akpe-Doe, 2022). However, Owusu (2023) reported that information quality did not significantly influence system use in another Ghanaian e-government context, suggesting that its effect may vary according to the institutional and technological setting.

The third hypothesis examined whether technology fit had a significant positive effect on ISO/IEC 27001:2022 implementation. The regression results presented in Table 9 show a positive and statistically significant effect ($B = 0.192$, $\beta = .222$, $t = 2.104$, $p = .038$). Since the p -value was below .05, H03 was rejected. The result indicates that greater alignment between organizational technologies and users' task requirements was associated with higher levels of ISO/IEC 27001:2022 implementation.

The finding is consistent with Goodhue and Thompson (1995), whose Task–Technology Fit theory proposes that performance improves when technology capabilities match the requirements of the tasks being performed. It is also consistent with more recent information-security evidence. Alassaf and Alkhalifah (2026) found that task–technology fit positively predicted information-security policy compliance intentions and

subsequent compliance behaviour. This supports the argument that technologies that fit users' work requirements can facilitate security-related behaviour.

The present finding extends these studies by shifting the outcome from individual technology use or security-policy compliance to organizational implementation of ISO/IEC 27001:2022. Where security technologies are compatible with organizational processes and users' tasks, security procedures may

be easier to incorporate into routine operations. Conversely, substantial mismatch between technology and work requirements may create additional operational difficulties. The rejection of H03 therefore indicates that technology fit is a significant technology-oriented factor associated with ISO/IEC 27001:2022 implementation in Kenyan public-sector organizations.

Table 9: Regression coefficients for technology-oriented factors

Predictor	B	SE	β	t	p	Decision
System quality	0.274	0.078	0.231	3.519	.001	Reject H01
Information quality	0.183	0.090	0.222	2.033	.045	Reject H02
Technology fit	0.192	0.091	0.222	2.104	.038	Reject H03

Source: Field data (2024). Dependent variable: Implementation of ISO/IEC 27001:2022; model $R^2 = 0.584$; $F(9, 333) = 29.840$, $p < .001$.

Substituting the estimated coefficients into the model specification yields the validated technology-oriented assessment model illustrated in Figure 1:

$$Y = 1.715 + 0.274(SYQ) + 0.183(INQ) + 0.192(TEF) + \epsilon$$

where the constant and coefficients are estimated within the integrated socio-technical model ($R^2 = 0.584$). The positive coefficients indicate that higher levels of each technology-oriented factor were associated with higher implementation scores, holding the other predictors constant. Specifically, a one-unit increase in system quality was associated with a 0.274-unit increase in implementation, while equivalent increases in information quality and technology fit were associated with 0.183-unit and 0.192-unit increases, respectively. These results correspond with the individual hypothesis tests, which established statistically significant positive relationships for all three factors.

The model also shows that system quality had the largest unstandardized coefficient ($B = 0.274$) among the three technology-oriented factors. However, comparisons of relative importance should preferably rely on the standardized coefficients because the variables may be measured on different scales. The standardized coefficients were $\beta = .231$ for system quality, $\beta = .222$ for information quality, and $\beta = .222$ for technology fit, indicating relatively similar contributions to ISO/IEC 27001:2022 implementation. Thus, the findings suggest that dependable systems, quality information, and appropriate technology alignment are complementary technological conditions for implementation rather than evidence that one factor overwhelmingly dominates the others.

The model therefore provides an empirical basis for assessing ISO/IEC 27001:2022 implementation from a technology-oriented perspective. Its principal contribution is to demonstrate that technological conditions explain a

meaningful proportion of variation in implementation after accounting for other factors in the integrated model.

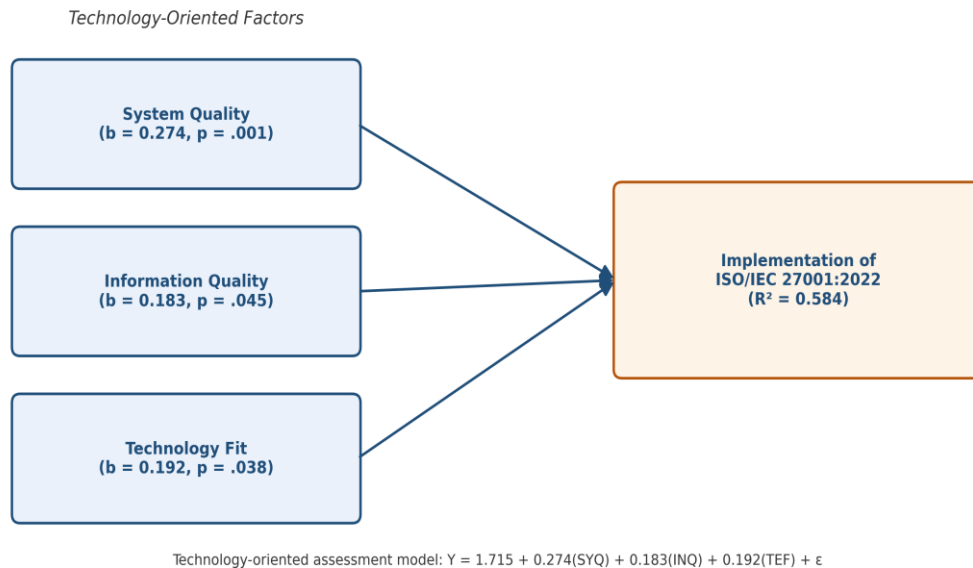


Figure 1. Validated technology-oriented assessment model for ISO/IEC 27001:2022 implementation

Conclusion

The study concludes that technology-oriented factors are significantly associated with the implementation of ISO/IEC 27001:2022 in Kenyan public-sector organizations. Specifically, system quality, information quality, and technology fit each demonstrated a positive and statistically significant relationship with implementation, with system quality, information quality, and technology fit.

The overall model explained 58.4% of the variance in ISO/IEC 27001:2022 implementation ($R^2 = .584$), indicating that technological conditions constitute an important component of effective implementation. The findings further suggest that organizations require reliable and accessible systems, accurate and sufficient information, and technologies that adequately support organizational tasks to operationalize information-security requirements.

Recommendations

For public sector managers and information security practitioners, the validated model offers a data-driven diagnostic: implementation assessments should weight system quality most heavily, then technology fit, then information quality, while recognizing that all three matter jointly. Practically, the findings argue for prioritizing infrastructure reliability and modernization (system quality), enterprise information integration to resolve the logical-coherence deficit (information quality), and user-centered security tooling selection aligned to workflows (technology fit). For policymakers and regulators, the results imply that ISO/IEC 27001:2022 compliance frameworks and capacity-building programs should embed technology-readiness criteria rather than assuming that standards adoption alone

produces security outcomes. The model can also serve as a monitoring framework within which government-wide implementation maturity can be tracked over time.

Theoretical implications

The study contributes to Task–Technology Fit (TTF) theory by providing empirical evidence that technology-related characteristics are relevant to the implementation of information-security management standards. The findings show that system quality, information quality, and technology fit each had a positive and statistically significant relationship with ISO/IEC 27001:2022 implementation. These findings extend the application of TTF beyond its traditional focus on technology use and individual performance (Goodhue & Thompson, 1995) to the implementation of an organizational information-security management standard.

Specifically, the results demonstrate that implementation is associated not only with the availability of technology but also with the quality of systems, quality of information generated by those systems, and alignment between technology capabilities and organizational tasks. The study therefore provides contextual empirical support for applying TTF to information-security standards implementation and extends its application to public-sector organizations in Kenya.

Limitation and Future Research

The study has limitations. First, its cross-sectional design precludes causal inference; longitudinal designs would strengthen claims about directionality. Second, although the technology estimates are net of people and process factors, the coefficients derive from a

model estimated on a single empirical context, and external validation across sectors and countries recommended in the source study remains outstanding.

Third, the remaining 41.6% of unexplained variance indicates omitted factors (e.g., regulatory pressure, resource endowments, threat exposure) that future models should incorporate. Fourth, a mixed-methods extension could unpack the mechanisms behind the low logical-coherence ratings observed for organizational information.

Finally, re-estimating a technology-only hierarchical regression on primary data, and testing mediation through security behavior, would sharpen the model's policy precision.

References

- Alassaf, M., & Alkhalifah, A. (2026). Determinants of information security policy compliance: Integrating task-technology fit and threat avoidance appraisals in the digital workplace. *Frontiers in Psychology*, 17, 1861737. <https://doi.org/10.3389/fpsyg.2026.1861737>
- Almuqrin, A. (2024). How about enhancing organizational security: Critical success factors in information security management performance. *Journal of Global Information Management*, 32(1), 1–18. <https://doi.org/10.4018/JGIM.358745>
- Alrehili, A. A., & Alhazmi, O. H. (2023). ISO/IEC 27001 standard: Analytical and comparative overview. In *International Conference on Advances in Data-driven Computing and Intelligent Systems* (pp. 143–156). Springer Nature Singapore. https://doi.org/10.1007/978-981-99-9524-0_12
- Apridiyanti, A., Suharman, H., & Adrianto, Z. (2020). Successful implementation of information systems in public sector organizations. *Journal of Accounting Auditing and Business*, 3(1).

- <https://doi.org/10.24198/jaab.v3i1.25351>
- Araujo, M. S. D., Machado, B. A. S., & Passos, F. U. (2024). Resilience in the context of cyber security: A review of the fundamental concepts and relevance. *Applied Sciences*, 14(5), 2116. <https://doi.org/10.3390/app14052116>
- Asher, A. D. (2024). Approaches for improving validity in quantitative research articles. *portal: Libraries and the Academy*, 24(2), 209–215. <https://doi.org/10.1353/pla.2024.a923703>
- Ayim, O. R. (2019). *The relationship between Integrated Financial Management Information System and performance of government ministries in Kenya*. Kenyatta University. <https://ir-library.ku.ac.ke/items/3a418aa9-47e9-4a6a-84bd-b159892cdd02>
- Batte, B. (2025). ISO 27001 and alternative frameworks for managing information security risks. *SSRN*. <https://doi.org/10.2139/ssrn.5546398>
- Bujang, M. A., Omar, E. D., Foo, D. H. P., & Hon, Y. K. (2024). Sample size determination for conducting a pilot study to assess reliability of a questionnaire. *Restorative Dentistry & Endodontics*, 49(1), e3. <https://doi.org/10.5395/rde.2024.49.e3>
- Cane, S., & McCarthy, R. (2009). Analyzing the factors that affect information systems use: A task-technology fit meta-analysis. *Journal of Computer Information Systems*, 50(1), 108–123. <https://doi.org/10.1080/08874417.2009.11645368>
- Chavez, S., Anahue, J., & Ticona, W. (2024). Implementation of an ISMS based on ISO/IEC 27001:2022 to improve information security in the internet services sector. In *2024 14th International Conference on Cloud Computing, Data Science & Engineering (Confluence)* (pp. 184–189). IEEE. <https://doi.org/10.1109/Confluence60223.2024.10463392>
- Chen, H., & Hai, Y. (2024). Exploring the critical success factors of information security management: A mixed-method approach. *Information & Computer Security*, 32(5), 545–572. <https://doi.org/10.1108/ICS-03-2023-0034>
- Culot, G., Nassimbeni, G., Podrecca, M., & Sartor, M. (2021). The ISO/IEC 27001 information security management standard: Literature review and theory-based research agenda. *The TQM Journal*, 33(7), 76–105. <https://doi.org/10.1108/TQM-09-2020-0202>
- 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>
- Djebbar, F., & Nordström, K. (2023). A comparative analysis of industrial cybersecurity standards. *IEEE Access*, 11, 85315–85332. <https://doi.org/10.1109/ACCESS.2023.3303205>
- Efunwoye, I. O., Gogate, M., Hussain, A., Asim, M., Ahmad, J., Hussain, A., & Dashtipour, K. (2025). Evaluating the efficacy and applicability of contemporary cybersecurity frameworks and standards. In *Cybersecurity, Cybercrimes, and Smart Emerging Technologies* (pp. 365–372). CRC Press. <https://doi.org/10.1201/9781003614197-33>
- Forero, C. G. (2024). Cronbach's alpha. In *Encyclopedia of Quality of Life and Well-being Research* (pp. 1505–1507). Springer. https://doi.org/10.1007/978-3-031-17299-1_622
- Gichubi, P. M., Maake, B., & Chweya, R. (2024). Cybersecurity framework for Kenyan universities in conformity with ISO/IEC 27001:2022 standard. *Open Access Library Journal*, 11(8),

- 1–16.
<https://doi.org/10.4236/oalib.1110810>
- Goodhue, D. L., & Thompson, R. L. (1995). Task-technology fit and individual performance. *MIS Quarterly*, 19(2), 213–236.
<https://doi.org/10.2307/249689>
- Hassan, M., Saeedi, K., Almagwashi, H., & Alarifi, S. (2022). Information security risk awareness survey of non-governmental organization in Saudi Arabia. In *The International Research & Innovation Forum* (pp. 39–71). Springer.
https://doi.org/10.1007/978-3-031-19560-0_4
- Indeje, W., & Qin, Z. (2011). Stakeholder perception of information systems development success in the public sector. *Management Science and Engineering*, 5(2).
<https://doi.org/10.3968/j.mse.1913035X20110502.004>
- Islam, M. M., Bhuiyan, M. R. I., Islam, S. H., Tabassum, M. N., & Billah, M. (2026). Unlocking the mediating and moderating role of information security in information systems: A combined TAM, ISM, and HBM model. *Human Behavior and Emerging Technologies*, 2026(1), 5593002.
<https://doi.org/10.1155/hbe2/5593002>
- Jeyaraj, A. (2022). A meta-regression of task-technology fit in information systems research. *International Journal of Information Management*, 65, 102493.
<https://doi.org/10.1016/j.ijinfomgt.2022.102493>
- Kamil, Y., Lund, S., & Islam, M. S. (2023). Information security objectives and the output legitimacy of ISO/IEC 27001: Stakeholders' perspective on expectations in private organizations in Sweden. *Information Systems and e-Business Management*, 21(3), 699–722.
<https://doi.org/10.1007/s10257-023-00646-y>
- Kaporo, S. K. (2024). *Electronic records management and security of public leaders' confidential information in Tanzania: A case of the President's Office, Ethics Secretariat* [Master's thesis, University of Dodoma].
- Karoki, G. K., Mwingirwa, I. M., & Kamau, S. (2025). Cyber espionage vulnerabilities in Kenya's e-government ecosystem: A case study of a public institution. *The Eastern Africa Journal of Policy and Strategy*, 89–105.
- Keefa, B., Mayoka, G. K., Nkamwesiga, L., & Nyamadi, M. (2024). Information security in higher education institutions: A systematic literature review. *ORSEA Journal*, 302–320.
<https://doi.org/10.56279/orseaj.C2024.18>
- Kennedy, I. (2022). Sample size determination in test-retest and Cronbach alpha reliability estimates. *British Journal of Contemporary Education*, 2(1), 17–29.
<https://doi.org/10.52589/BJCE-FY266HK9>
- Kiarie, N. (2024). Enhancing digital resilience: A cybersecurity readiness assessment of Kenyan TVET institutions. *Journal of the Kenya National Commission for UNESCO*, 5(1).
<https://doi.org/10.62049/jkncu.v5i1.191>
- Leme, R. D. S., de Souza Pinto, J., Zanon, L. G., Sigahi, T. F., Moraes, G. H. S. M. D., Moro, S. R., & Anholon, R. (2026). Information security management: A fuzzy DEMATEL analysis of the new ISO/IEC 27001:2022 controls. *Information & Computer Security*, 34(3), 413–434.
<https://doi.org/10.1108/ICS-10-2024-0269>
- Mirtsch, M. (2023). Adoption of the information security management system standard ISO/IEC 27001—A study among German organizations. *International Journal for Quality Research*, 17(3), 747–768.
<https://doi.org/10.24874/IJQR17.03-08>

- Nadir, R., Kartini, & Tawakkal. (2024). Model kesuksesan sistem informasi DeLone & McLean terhadap Sistem Informasi Pemerintah Daerah (SIPD) pada Pemda Kabupaten Wajo. *Prosiding Seminar Nasional Terapan Riset Inovatif*, 9(2), 175–184.
- Ohndyl, G. O., Kimuyu, J., & Sidha, Z. (2023). Information security threats to e-government services in Kenya. *Global Journal of Human-Social Science: H Interdisciplinary*, 23(7).
- Owusu, A. (2023). Assessing the impact of e-government systems from citizens' perspective: Evidence from Ghana. *Electronic Government, an International Journal*, 19(3), 376–400.
<https://doi.org/10.1504/EG.2023.130583>
- Owusu, A., & Akpe-Doe, C. (2022). Assessing the effectiveness of e-government services in Ghana: A case of the Registrar General's Department. *International Journal of Electronic Government Research*, 18(1), 1–23.
<https://doi.org/10.4018/IJEGR.289827>
- Oyugi, T. O. (2012). *Influence of task technology fit framework on adoption of project management information system in non-governmental organizations' projects in Nakuru town*. University of Nairobi.
<https://erepository.uonbi.ac.ke/ite ms/57bf3d8c-6e66-44a1-af1d-1d0f3811afc0>
- Plate, A. (2025). ISMS: A management framework for information security. In *Encyclopedia of Cryptography, Security and Privacy* (pp. 1305–1307). Springer Nature Switzerland.
https://doi.org/10.1007/978-3-030-71522-9_289
- Rahimli, R. S. (2025). *Security and privacy in information processing* [Doctoral dissertation].
- Rohan, R., Pal, D., Hautamäki, J., Funilkul, S., Chutimaskul, W., & Thapliyal, H. (2023). A systematic literature review of cybersecurity scales assessing information security awareness. *Heliyon*, 9(3), e14234.
<https://doi.org/10.1016/j.heliyon.2023.e14234>
- Sausi, J. M., Kitali, E. J., & Mtebe, J. S. (2021). Evaluation of local government revenue collection information system success in Tanzania. *Digital Policy, Regulation and Governance*, 23(5), 437–455.
<https://doi.org/10.1108/DPRG-04-2021-0055>
- Sekti, B. A. (2026). IT service information security management. In *Cases on Information Systems Service Management* (pp. 61–94). IGI Global Scientific Publishing.
<https://doi.org/10.4018/979-8-3373-2352-7.ch003>
- Shaikh, F. A., & Siponen, M. (2023). Information security risk assessments following cybersecurity breaches: The mediating role of top management attention to cybersecurity. *Computers & Security*, 124, 102974.
<https://doi.org/10.1016/j.cose.2022.102974>
- Skinner, E., & Dancis, J. (2026). Descriptive and explanatory designs. In *Human Development—Revision*.
- Soliman, W., & Mohammadnazar, H. (2022). New insights into the justifiability of organizational information security policy noncompliance: A case study. In *Proceedings of the 55th Hawaii International Conference on System Sciences* (pp. 6812–6821). University of Hawai'i.
<https://doi.org/10.24251/HICSS.2022.823>
- Spruill, C., Khalil, M., & Olatunbosun, S. (2024). Models for security management. In *World Congress in Computer Science, Computer Engineering & Applied Computing* (pp. 354–361). Springer Nature Switzerland.
https://doi.org/10.1007/978-3-031-85933-5_26
- Suorsa, M., & Helo, P. (2023). Information security failures measured and ISO/IEC 27001:2022 controls ranked by general data protection

- regulation penalty analysis. In *2023 11th International Conference on Cyber and IT Service Management (CITSM)* (pp. 1–5). IEEE. <https://doi.org/10.1109/CITSM60085.2023.10455413>
- Taherdoost, H. (2022). Understanding cybersecurity frameworks and information security standards—A review and comprehensive overview. *Electronics*, 11(14), 2181. <https://doi.org/10.3390/electronics11142181>
- Tewamba, H. N., Kamdjoug, J. R. K., Bitjoka, G. B., Wamba, S. F., & Mi Bahanag, N. N. (2019). Effects of information security management systems on firm performance. *American Journal of Operations Management and Information Systems*, 4(3), 99–108.
- Lubembe et al. <https://doi.org/10.11648/j.ajomis.20190403.15>
- Vakhula, O., Kurii, Y., Opirskyy, I. R., & Susukailo, V. (2024). Security as code concept for fulfilling ISO/IEC 27001:2022 requirements. In *Proceedings of the Workshop on Cybersecurity Providing in Information and Telecommunication Systems (CPITS 2024)* (pp. 59–72). <https://doi.org/10.55056/ceur-ws.org/Vol-3654/paper6.pdf>
- Yee, C. K., & Zolkipli, M. F. (2021). Review on confidentiality, integrity and availability in information security. *Journal of ICT in Education*, 8(2), 34–42. <https://doi.org/10.37134/jictie.vol8.2.4.2021>