© OCT 2026 | IRE Journals | Volume 10 Issue 4 | ISSN: 2456-8880
DOI: https://doi.org/10.64388/IREV10I4-1723603

Influence of System Interoperability on Data Security in Digitised Government Services: Evidence from Public Officers Undertaking the Senior Management Course at the Kenya School of Government, Baringo Campus, Kenya

IMO IMUNYO ERIC[1], DONALD MWACHOFI MWAZIGHE[2], ROBINA OWINO[3], MARY CHEPKIRUI BOMETT[4], SHERINE JEPKOECH KANDIE[5], NAHUM JEPKEMOI KOTUT[6], PASSY TERESA ACHIENG AKUNO[7], JOHN NAPOO[8]

[1, 2, 3, 4, 5, 6, 7, 8] *Kenya School of Government, Baringo Campus, Kenya*

Abstract- ***Governments are increasingly linking their digital platforms so that information can move across ministries, agencies and counties without duplication. Such interoperability improves coordination, yet it also widens the surface through which personal, financial and administrative data may be exposed. This study assessed the influence of system interoperability on data security in digitised government services, drawing on the experience of public officers undertaking the Senior Management Course (Cohort 229/2026) at the Kenya School of Government, Baringo Campus. The study was anchored on the Technology Acceptance Model and Systems Theory and adopted a descriptive design within a convergent mixed methods approach. A census of the 94 eligible participants was conducted using a structured online questionnaire containing closed and open ended items; 84 responses were received (89.4 percent), of which 82 respondents who had interacted with integrated government systems such as eCitizen, IFMIS, iTax and HRMIS were retained for analysis. Quantitative data were analysed using descriptive statistics, Pearson correlation and multiple regression in SPSS version 28, while open ended responses were analysed thematically. System interoperability was rated highly (overall mean = 3.83, SD = 0.80), with coordination across departments (M = 4.02) and the contribution of connectivity to service delivery (M = 3.91) rated highest and smooth exchange of information across systems rated lowest (M = 3.68). Data security recorded an overall mean of 3.50 (SD = 0.97), with the weakest ratings on the minimal occurrence of breaches (M = 2.88) and the adequacy of existing safeguards (M = 3.31). System interoperability had a strong, positive and statistically significant relationship with data security ($r = 0.61$, $p < 0.001$) and remained a significant predictor when modelled alongside data sharing practices and access control mechanisms ($B = 0.29$, $\beta = 0.31$, $t = 3.22$, $p = 0.002$). The qualitative findings indicated that the security benefits of integration are realised only where connections between systems are supported by encryption, controlled exchange points, user awareness and continuous monitoring. The study concludes that system interoperability significantly influences data security in digitised government services and recommends that ICT units, in consultation with the Ministry responsible for ICT and the Communications Authority of Kenya, strengthen secure integration through encryption of data in transit, controlled and documented data exchange interfaces, periodic vulnerability assessment and interoperability standards that embed security by design.***

Index Terms- ***Data security, digitised government services, e-government, ICT system integration, Kenya, system interoperability***

I. INTRODUCTION

Digitised government services are public services delivered through electronic platforms, databases, portals and networked information systems. They enable public institutions to receive applications, keep records, share information and deliver services through digital channels rather than through fragmented manual processes. As the scope of digitised services has grown, the integration of the underlying ICT systems has become a central concern of digital governance, because integration is what allows separate platforms to communicate and operate in a coordinated manner [1], [2].

ICT system integration is achieved principally through system interoperability, that is, the ability of different systems and applications to communicate, exchange and

make use of information across institutional boundaries. Interoperability supports faster information flow, reduces duplication of records and improves coordination across institutions. At the same time, it increases the movement of personal, financial and administrative data across systems, and every additional connection is a potential point of unauthorised access, misuse, alteration or loss. Data security, understood as the protection of digital information from unauthorised access, disclosure, alteration, loss and breach, therefore becomes a central rather than a peripheral concern in integrated digital government [3], [4].

The United Nations E-Government Survey 2024 observes that governments are investing heavily in digital infrastructure and online services to improve efficiency, inclusion and responsiveness, and stresses that these investments must rest on secure and resilient systems if public trust is to be sustained [1]. The World Bank similarly links GovTech maturity to integrated platforms, shared services, core government systems and data governance, while emphasising safeguards for privacy and cybersecurity [2]. In Africa, the African Union Digital Transformation Strategy 2020 to 2030 identifies digital infrastructure, digital identity, cybersecurity and personal data protection as foundations of inclusive digital transformation, while acknowledging that uneven infrastructure, limited technical capacity and weak data governance continue to expose integrated systems to risk [5], [6].

Kenya has moved decisively in this direction. The Kenya National Digital Master Plan 2022 to 2032 identifies digital government services, data management, cybersecurity, digital infrastructure and data protection as pillars of national digital transformation [7]. Platforms such as eCitizen, the Integrated Financial Management Information System (IFMIS), the Integrated Tax Management System (iTax) and the Human Resource Management Information System (HRMIS) illustrate the shift from stand alone processes to connected services. These platforms have improved access and efficiency, but they have also multiplied the volume of sensitive data processed across public systems. The Data Protection Act, 2019 and the Office of the Data Protection Commissioner (ODPC) provide the legal and regulatory framework for the protection of personal data, and the Kenya Institute for Public Policy Research and Analysis has argued that the expanding digital economy requires stronger protection of personal data and lawful processing [8].

Despite these frameworks, the threat environment continues to intensify. The Communications Authority of Kenya recorded 860.1 million cyber threat events between October and December 2024, a 27.2 percent increase on the previous quarter [9], while the ODPC received 7,188 complaints and reports relating to violations of data privacy and protection rights between 2020 and 2024 [10]. These figures suggest that while integration improves coordination and accessibility, weaknesses in the way systems are connected may expose them to unauthorised access, breaches and misuse of sensitive information, thereby undermining public trust and institutional credibility.

Existing Kenyan and African studies have concentrated largely on e-government adoption, digital transformation and cybersecurity in general terms, with limited empirical attention to how the specific dimensions of ICT system integration influence data security. Studies that have examined interoperability tend to focus on technical infrastructure rather than on the experience of the public officers who use interconnected systems daily [3], [11]. This paper addresses that gap. It reports the first of three objectives of a wider study on ICT system integration and data security, namely to assess the influence of system interoperability on data security in digitised government services, using data collected from public officers drawn from ministries, state departments, state corporations and county governments who were undertaking the Senior Management Course (SMC) Cohort 229/2026 at the Kenya School of Government (KSG), Baringo Campus.

The paper is organised as follows. Section 2 reviews the theoretical and empirical literature and states the research gap. Section 3 describes the methodology. Section 4 presents and discusses the findings. Section 5 draws conclusions, makes recommendations and suggests areas for further study.

II. LITERATURE REVIEW

A. Theoretical Framework

The study was guided by the Technology Acceptance Model (TAM) and Systems Theory. TAM, developed by Davis [12], holds that individuals are more likely to adopt and use a technological system when they perceive

it to be useful and easy to use, and that these perceptions shape attitudes, intentions and actual use. The model has been widely applied to e-government and information systems research, although critics note that it concentrates on individual perceptions and gives limited attention to organisational, social and security related factors, particularly in institutional settings where system use is mandatory rather than voluntary [13]. TAM is nonetheless relevant here because the security of an interoperable system depends in part on how public officers interact with it. Officers who understand interoperability functions and accept the procedures that accompany them are more likely to use exchange channels as intended, whereas poor acceptance encourages informal workarounds that bypass safeguards.

Systems Theory, advanced by von Bertalanffy [14], views organisations as sets of interconnected and interdependent components in which a change in one component affects the operation of the others. Its key constructs are interdependence, interaction, integration and feedback. The theory provides the natural lens for interoperability: an integrated government platform is a system of systems, and a weakness at any point of connection can compromise the security of the whole environment. Taken together, TAM explains the human dimension of interoperability and data security, while Systems Theory explains the structural dimension.

B. Empirical Review

Interoperability in government has been associated with clear efficiency gains but also with elevated exposure to security risk. Almarabeh and AbuAli [3], in a descriptive study of digital government interoperability and information security, found that interoperable systems improved efficiency and coordination through seamless information exchange, but that weak security standards and inconsistent controls increased exposure to cyber threats and unauthorised access. Their focus was technical infrastructure, with little attention to the experience of users within integrated systems.

Bwalya and Mutula [6], using a comparative case study of selected African countries, observed that interoperability among government systems enhanced service delivery and institutional coordination, while weak cybersecurity frameworks, inadequate technical capacity and inconsistent enforcement of data governance policies left integrated systems vulnerable. The broad regional scope of that study limited its ability to speak to the situation of public officers in a single national context.

In Kenya, Mwangi and Kihara [11] conducted a cross-sectional study of ICT integration and data security in public institutions and found that interoperability improved efficiency and information accessibility but that increased interconnectivity heightened exposure to unauthorised access, breaches and system vulnerabilities where security mechanisms were weak. The study concentrated on institutional ICT infrastructure and gave limited attention to the behavioural and operational factors that shape security outcomes. Related Kenyan work by Wanjiru and Omwansa [15] on information sharing within integrated platforms and by Otieno and Mutua [16] on ICT security management practices reached similar conclusions: integration delivers efficiency, but its security dividend depends on the strength of controls at the points where systems meet.

Standards bodies reinforce this view. NIST [4] treats system and communications protection, boundary protection and the security of interconnections as distinct control families precisely because integration creates security obligations that stand alone systems do not carry. The OECD Digital Government Index likewise treats data driven, integrated government as a maturity dimension that must be balanced against trust and security [17].

C. Research Gap

Three gaps emerge from the literature. Conceptually, previous studies have examined digital government adoption, transformation and cybersecurity in broad terms, with limited attention to system interoperability as a specific determinant of data security. Contextually, most studies have been conducted in international or broad organisational settings, leaving little empirical evidence from Kenya's public sector. Methodologically, existing work has relied largely on descriptive or purely quantitative designs, limiting the understanding of both statistical relationships and the lived experience of officers who use interconnected systems. This study addressed these gaps by examining the influence of system interoperability on data security through a convergent mixed methods design among serving public officers.

D. Conceptual Framework and Hypothesis

System interoperability was conceptualised as the independent variable, measured through system compatibility, smooth information exchange, system connectivity, reduction of duplication, coordination across departments and timely access to information. Data security was the dependent variable, measured through protection of personal data, control of unauthorised access, minimal occurrence of breaches, confidentiality, integrity of information and adequacy of institutional safeguards. The study tested the null hypothesis that system interoperability has no statistically significant influence on data security in digitised government services (H01) against the alternative that a significant influence exists.

III. METHODOLOGY

A. Research Design

The study adopted a descriptive research design within a convergent mixed methods approach [18]. Quantitative and qualitative data were collected in the same phase through a single instrument and integrated at the interpretation stage. The quantitative strand measured the relationship between system interoperability and data security, while the qualitative strand captured respondents' own accounts of the security challenges and remedies associated with integrated systems. Triangulation of the two strands strengthened the validity of the conclusions.

B. Population and Sampling

The target population comprised public officers in Kenya's public service who interact with digitised government systems in the course of service delivery. The accessible population was the SMC Cohort 229/2026 at KSG Baringo Campus, an online cohort of 103 senior public officers drawn from ministries, state departments, state corporations and county governments. Nine members of the research team were excluded to preserve objectivity, leaving an accessible population of 94. Because this population was small and fully enumerable, a census approach was adopted, which eliminated sampling error and ensured that every eligible officer had the opportunity to participate. The unit of analysis was the individual public officer.

C. Instrument, Validity and Reliability

Data were collected using a structured questionnaire with five sections: respondent characteristics; system interoperability; data sharing practices; access control mechanisms; and data security, followed by open ended items on security challenges, suggested measures and additional views. Closed items were rated on a five point Likert scale from 1 (strongly disagree) to 5 (strongly agree). The instrument was piloted on respondents with characteristics similar to the study population and refined on the basis of their feedback. Content and construct validity were secured through supervisor review and alignment of every item with the study objectives. Internal consistency was assessed using Cronbach's alpha in SPSS, with a coefficient of 0.70 or above taken as acceptable [19].

D. Data Collection and Analysis

Following supervisor approval, the questionnaire was deployed as a Google Form and the link shared through the official class communication platform. Data were cleaned, coded and analysed in SPSS version 28. Descriptive statistics (frequencies, percentages, means and standard deviations) summarised the ratings, with mean scores of 3.50 to 5.00 interpreted as high, 2.50 to 3.49 as moderate and below 2.50 as low. Pearson's product moment correlation established the strength and direction of the relationship between system interoperability and data security. Multiple regression was then used to estimate the influence of system interoperability on data security while controlling for the other two dimensions of ICT system integration examined in the wider study, data sharing practices and access control mechanisms, using the model:

$$Y = \beta_0 + \beta_1 X_1 + \beta_2 X_2 + \beta_3 X_3 + \varepsilon$$

where Y is data security, X_1 is system interoperability, X_2 is data sharing practices, X_3 is access control mechanisms, β_0 is the constant, β_1 to β_3 are the regression coefficients and ε is the error term. The coefficient of interest for this paper is β_1. Significance was tested at the 5 percent level. Open ended responses were analysed thematically by organising, coding and grouping responses into recurring themes, which were then integrated with the quantitative results during discussion.

E. Ethical Considerations

Approval to conduct the study was obtained through the Kenya School of Government and the research supervisor. Participation was voluntary and informed

consent was obtained before data collection. No names or contact details were collected, responses were stored in password protected files accessible only to the researchers and supervisor, and data were used strictly for academic purposes. Given the subject matter, particular care was taken in the secure handling of research data.

IV. FINDINGS AND DISCUSSION

A. Response Rate and Respondent Characteristics

Of the 94 eligible officers, 84 submitted valid responses, a response rate of 89.4 percent, which exceeds the 70 percent threshold that Mugenda and Mugenda [20] regard as very good. Respondents were predominantly male, with a substantial proportion of female officers and a small number who preferred not to disclose gender. Most were aged between 41 and 50 years, followed by those aged 31 to 40 and those aged 51 and above, and most had served in the public sector for more than 10 years. Respondents were drawn from state departments, state corporations, ministries and county governments. Eighty two respondents (97.6 percent) reported having used integrated digital government systems such as eCitizen, IFMIS, iTax or HRMIS; the two respondents who had not were excluded from the substantive analysis, which is therefore based on n = 82. The profile confirms that the respondents were experienced officers with direct, practical exposure to interoperable government systems.

B. Descriptive Findings on System Interoperability

Table 1 presents the ratings on the six interoperability indicators.

Table 1
Respondents' Ratings of System Interoperability (n = 82)

Indicator	Mean	SD	Interpretation
Integrated systems in my institution are compatible with each other	3.74	0.81	High
Government systems allow smooth exchange of information	3.68	0.87	High
System connectivity has improved service delivery	3.91	0.76	High
Integrated systems have reduced duplication of records and processes	3.83	0.79	High
System interoperability enhances coordination across departments	4.02	0.72	High
Integrated systems support timely access to information	3.77	0.84	High
Overall mean score	3.83	0.80	High

Note. Research data (2026).

System interoperability recorded an overall mean of 3.83 (SD = 0.80), indicating that respondents agreed that integrated systems in their institutions were compatible, connected and capable of supporting timely information access. The highest rated indicator was the enhancement of coordination across departments (M = 4.02, SD = 0.72), followed by the contribution of connectivity to service delivery (M = 3.91, SD = 0.76) and the reduction of duplication (M = 3.83, SD = 0.79). These are the classic efficiency dividends of integration described by Almarabeh and AbuAli [3] and by the World Bank [2], and the relatively low standard deviations show that this view was widely shared.

The lowest rated indicator was smooth exchange of information across government systems (M = 3.68, SD = 0.87). Although still within the high range, the combination of the lowest mean and one of the higher standard deviations suggests that a meaningful minority of officers experienced friction in moving information between platforms. This is consistent with Mwangi and Kihara [11], who found that connectivity in Kenyan public institutions was uneven, and it matters for security because friction in the formal exchange channel is precisely what tempts users to move data through informal channels such as personal email, removable media or messaging applications, which sit outside institutional controls.

C. Descriptive Findings on Data Security

Table 2 *Respondents' Ratings of Data Security (n = 82)*

Indicator	Mean	SD	Interpretation
Personal data within integrated systems is protected	3.64	0.92	High
Unauthorised access to information is controlled	3.47	1.04	Moderate
Data breach incidents are minimal	2.88	1.26	Moderate
Confidentiality of digital information is maintained	3.72	0.81	High
Digital information is accurate and its integrity is maintained	3.95	0.69	High
Existing institutional data security measures are adequate	3.31	1.12	Moderate
Overall mean score	3.50	0.97	High

Note. Research data (2026).

Data security recorded an overall mean of 3.50 (SD = 0.97), at the boundary between the moderate and high ranges. Respondents were most confident about the accuracy and integrity of information (M = 3.95, SD = 0.69) and about confidentiality (M = 3.72, SD = 0.81). They were least confident that breach incidents were minimal (M = 2.88, SD = 1.26) and that existing safeguards were adequate (M = 3.31, SD = 1.12); the large standard deviations on these two items point to sharply divergent experiences across institutions. The pattern is instructive when read against Table 1: officers perceive interoperability as well established but perceive the protective measures that should accompany it as lagging. Integration, in other words, has run ahead of security, which is the condition that Bwalya and Mutula [6] identified as the principal vulnerability of digital government in Africa.

D. Correlation between System Interoperability and Data Security

Table 3 *Pearson Correlation between System Interoperability and Data Security (n = 82)*

Variable	r	Sig. (2-tailed)	Interpretation
System interoperability	0.61	0.000	Strong positive, significant

Note. Research data (2026).

System interoperability had a strong, positive and statistically significant relationship with data security ($r = 0.61$, $p < 0.001$). Officers who rated their institutions' systems as more compatible, better connected and better coordinated also rated data security more highly. The direction of the relationship is important: it does not support the view that integration is inherently corrosive of security. Rather, where interoperability is properly implemented, with defined interfaces, consistent standards and coordinated management, it tends to bring order to data flows that would otherwise occur through uncontrolled means, and this order shows up as better security outcomes.

E. Regression Results

Table 4 summarises the multiple regression model in which data security was regressed on system interoperability together with data sharing practices and access control mechanisms, and Table 5 reports the coefficients.

Table 4 *Model Summary and ANOVA*

Statistic	Value
R	0.74
R Square	0.55
Adjusted R Square	0.53
Std. Error of the Estimate	0.48
F (3, 78)	33.09
Sig.	0.000

Note. Research data (2026).

© OCT 2026 | IRE Journals | Volume 10 Issue 4 | ISSN: 2456-8880
DOI: https://doi.org/10.64388/IREV10I4-1723603

Table 5 *Regression Coefficients*

Variable	B	Std. Error	Beta	t	Sig.
(Constant)	0.82	0.36		2.28	0.025
System interoperability	0.29	0.09	0.31	3.22	0.002
Data sharing practices	0.21	0.08	0.24	2.63	0.010
Access control mechanisms	0.38	0.10	0.39	3.80	0.000

Note. Research data (2026).

The model was statistically significant, $F(3, 78) = 33.09$, $p < 0.001$, and the three dimensions of ICT system integration jointly explained 55 percent of the variation in data security ($R^2 = 0.55$, adjusted $R^2 = 0.53$). Within this model, system interoperability had a positive and statistically significant influence on data security ($B = 0.29$, $SE = 0.09$, $\beta = 0.31$, $t = 3.22$, $p = 0.002$). Holding the other two dimensions constant, a one unit improvement in the interoperability score was associated with a 0.29 unit improvement in the data security score. The null hypothesis H01 was therefore rejected. In standardised terms, interoperability was the second strongest of the three predictors ($\beta = 0.31$), behind access control mechanisms ($\beta = 0.39$) and ahead of data sharing practices ($\beta = 0.24$). This ordering is itself informative: the security value of connecting systems is substantial, but it is somewhat smaller than the value of controlling who can use those connections, which is consistent with the Systems Theory expectation that the integrity of a system of systems is governed by its weakest interface and its weakest user.

F. Qualitative Findings

The open ended responses corroborated and explained the quantitative pattern. On challenges, respondents observed that integrated systems can expose sensitive information to users in linked institutions who do not have proper authorisation for it, and that system downtime, unpatched software and technical vulnerabilities at the points where systems connect create openings for cyber threats, data loss and unauthorised manipulation. Several linked these problems to inadequate technical support and inconsistent monitoring of the integrated environment. Limited user awareness of data protection requirements was also raised, reinforcing the TAM proposition that acceptance and understanding of a system shape how securely it is used.

On remedies, respondents called for stronger governance of integration itself: data should move between systems only through approved channels with clear authorisation, institutions should conduct regular audits of integrated systems and review system logs for suspicious access patterns, and officers should receive continuous training on responsible data handling. Respondents acknowledged that integration reduces duplication and speeds up service delivery, but stressed that because many systems and users are connected, a weak control in one institution can affect the security of the wider digital environment. This is a direct expression of the interdependence construct in Systems Theory and it explains why interoperability, although positively associated with security on average, is experienced by some officers as a source of risk.

G. Discussion

Taken together, the findings show that system interoperability in Kenya's digitised government services is well developed in its efficiency dimension and that it exerts a significant positive influence on data security. This finding both agrees with and refines the existing literature. Almarabeh and AbuAli [3], Bwalya and Mutula [6] and Mwangi and Kihara [11] all reported that interoperability improves efficiency while raising security exposure. The present study confirms the efficiency effect and the presence of exposure, but demonstrates statistically that the net effect of interoperability on perceived data security is positive and significant. The reconciliation lies in the qualitative findings: interoperability strengthens security where connections are designed, standardised and governed, and weakens it where information is exchanged through ad hoc or poorly maintained links. The lowest rated interoperability indicator (smooth exchange) and the lowest rated security indicators (minimal breaches and adequacy of safeguards) together identify where the exposure sits.

The findings also speak to the theoretical framework. Systems Theory is supported by the strong correlation and by respondents' own accounts of risk propagating across institutional boundaries. TAM is supported by the

emphasis respondents placed on user awareness and on the temptation to bypass formal channels when exchange is not smooth. Practically, the results indicate that the Kenya National Digital Master Plan's twin priorities of system integration and cybersecurity [7] should be pursued as a single agenda rather than as sequential ones.

V. CONCLUSION AND RECOMMENDATIONS

A. Conclusion

The study concluded that system interoperability significantly influences data security in digitised government services. Compatibility, connectivity, coordination across departments, reduction of duplication and timely access to information were found to support the protection of digital information, and the relationship between interoperability and data security was strong, positive and statistically significant both in isolation and when the other dimensions of ICT system integration were controlled. At the same time, the comparatively weaker ratings on smooth exchange of information, breach prevention and adequacy of safeguards, together with the qualitative evidence, show that the security benefits of interoperability are conditional. They are realised only where the interfaces between systems are secured and governed, and they can be reversed where they are not.

B. Recommendations

Arising from the finding that system interoperability had a positive and significant influence on data security, the study recommends that:

- ICT units, in consultation with the Ministry responsible for ICT and the Digital Economy and the Communications Authority of Kenya, should strengthen secure system integration by encrypting data in transit between platforms, establishing controlled and documented data exchange points, and conducting periodic vulnerability assessments of interconnections and application programming interfaces.
- The Ministry responsible for ICT should adopt and enforce government wide interoperability standards that embed security by design, so that compatibility between systems is achieved through standard, secured interfaces rather than through bespoke or informal links.
- Accounting officers and heads of ICT should prioritise the smoothness and reliability of official exchange channels, since friction in those channels drives officers towards unofficial and uncontrolled means of moving data.
- ICT units and internal audit units should institute continuous monitoring of the integrated environment, including review of interface logs, patch status and uptime, and should treat a security weakness in any connected institution as a shared risk requiring coordinated response.
- Human resource departments, ICT units and data protection officers should provide continuous awareness training so that officers understand both the benefits and the obligations that accompany interoperable systems.

C. Limitations and Areas for Further Study

The study relied on self reported perceptions, which may be affected by social desirability, and it was confined to a single online SMC cohort, which limits generalisation. Reliability and validity measures were applied to mitigate these limitations. Future studies should replicate the analysis among other officer groups and within specific institutions that operate major platforms such as eCitizen and HRMIS, should adopt longitudinal designs to track how interoperability and security co-evolve, and should complement perception data with technical measures such as interface audits, encryption coverage and incident records.

REFERENCES

[1] United Nations Department of Economic and Social Affairs, *United Nations E-Government Survey 2024*. New York: United Nations, 2024. United Nations DESA

[2] World Bank, *GovTech Maturity Index 2022 Update: Trends in Public Sector Digital Transformation*. Washington, DC: World Bank, 2022.

[3] T. Almarabeh and A. AbuAli, "E-government interoperability and information security challenges in public administration," *J. Softw. Eng. Appl.*, vol. 12, no. 4, pp. 215–228, 2019.

[4] National Institute of Standards and Technology, *Security and Privacy Controls for Information Systems and Organizations, NIST SP 800-53 Rev.*

5. Gaithersburg, MD: U.S. Dept. of Commerce, 2020. NIST

[5] African Union, *Digital Transformation Strategy for Africa (2020–2030)*. Addis Ababa: African Union Commission, 2020. African Union

[6] K. J. Bwalya and S. Mutula, "Digital government transformation and cybersecurity challenges in Africa," *Afr. J. Inf. Syst.*, vol. 13, no. 2, pp. 88–104, 2021.

[7] Ministry of ICT, Innovation and Youth Affairs, *Kenya National Digital Master Plan 2022–2032*. Nairobi: Government Printer, 2022.

[8] Kenya Institute for Public Policy Research and Analysis, *Strengthening Data Protection in Kenya: Opportunities and the Way Forward*. Nairobi: KIPPRA, 2024.

[9] Communications Authority of Kenya, *Cyber Security Report: Quarter Two 2024/2025*. Nairobi: CA, 2025.

[10] Office of the Data Protection Commissioner, *Annual Report 2023/2024*. Nairobi: ODPC, 2024.

[11] P. Mwangi and A. Kihara, "ICT integration and data security in Kenyan public institutions," *Int. J. Inf. Technol. Comput. Sci.*, vol. 14, no. 2, pp. 34–48, 2022.

[12] F. D. Davis, "Perceived usefulness, perceived ease of use, and user acceptance of information technology," *MIS Quart.*, vol. 13, no. 3, pp. 319–340, 1989. Crossref

[13] V. Venkatesh and F. D. Davis, "A theoretical extension of the technology acceptance model: Four longitudinal field studies," *Manage. Sci.*, vol. 46, no. 2, pp. 186–204, 2000. Crossref

[14] L. von Bertalanffy, *General System Theory: Foundations, Development, Applications*. New York: George Braziller, 1968.

[15] L. Wanjiru and T. Omwansa, "ICT integration and information sharing practices in Kenya's public sector," *Afr. J. Inf. Syst.*, vol. 14, no. 3, pp. 102–118, 2022.

[16] J. Otieno and S. Mutua, "ICT security management practices in public institutions in Kenya," *J. Inf. Secur. Digit. Gov.*, vol. 5, no. 2, pp. 63–79, 2023.

[17] Organisation for Economic Co-operation and Development, *Digital Government Index: 2019 Results*. Paris: OECD Publishing, 2021.

[18] J. W. Creswell and V. L. Plano Clark, *Designing and Conducting Mixed Methods Research*, 3rd ed. Thousand Oaks, CA: SAGE, 2018.

[19] J. C. Nunnally and I. H. Bernstein, *Psychometric Theory*, 3rd ed. New York: McGraw-Hill, 1994.

[20] O. M. Mugenda and A. G. Mugenda, *Research Methods: Quantitative and Qualitative Approaches*. Nairobi: Acts Press, 2003.