Assessment of ERP System Security Vulnerabilities: Technical, Logical and Physical Security Measures in Selected TVET Institutions in the Nyanza Region, Kenya

Towett Limo Elia[1*], James Abila[1], Lamek Ronoh[1]

[1] *Rongo University, P.O. Box 103-40404, Rongo, Kenya*

[*]*Correspondence email:* towelia.limo@gmail.com

Abstract

Enterprise resource planning (ERP) systems promise streamlined processes, better data management and improved decision-making, yet they expose organizations to security vulnerabilities that can compromise sensitive records. Empirical evidence on ERP security in Kenya's technical and vocational education and training (TVET) institutions is limited. The study assessed the technical security measures, evaluated the logical security measures and examined the physical security measures that safeguard ERP systems in selected TVET institutions in the Nyanza region of Kenya, and determined the relationships among the three dimensions. A descriptive quantitative survey used a questionnaire whose validity was established through expert review and whose reliability was high (Cronbach's $\alpha = .886$). A census was conducted of 32 ICT heads of department and ICT technicians in 16 TVET institutions implementing ERP systems. Data were analyzed in SPSS version 27 using means, standard deviations, Spearman's correlation and Cramér's V with exact significance tests. Technical measures were rated secure ($M = 3.61$, $SD = 0.92$), whereas logical ($M = 3.29$, $SD = 0.99$) and physical ($M = 3.31$, $SD = 1.07$) measures were rated neutral. The lowest-rated items were fire detection ($M = 2.59$), staff training ($M = 2.84$), physical access logs ($M = 2.97$) and a dedicated IT security team ($M = 3.00$). Technical and logical measures were strongly correlated ($r_s = .690$, $p < .001$), and technical and physical ($r_s = .507$, $p = .003$) and physical and logical measures ($r_s = .483$, $p = .005$) were moderately correlated. ERP systems in the sampled institutions were secure only in their technical dimension; logical and physical weaknesses require attention. Because the three dimensions are interdependent, they should be strengthened together. The findings provide a baseline for ERP security research in TVET institutions.

Keywords: *ERP security, security vulnerabilities, technical security, logical security, physical security, TVET institutions, Kenya*

IJPP 14(9);12-25

1.0 Introduction

Information security is essential for protecting information systems and the data they process, and for safeguarding the confidentiality, integrity and availability of that data. When security is compromised, the costs are financial (Tunggal, 2025), reputational and legal (Susanto et al., 2011). Cybersecurity is the practice of protecting data and information transmitted and stored on electronic devices from hacking, malicious attacks, sabotage and data theft (Asaad & Saeed, 2022); it therefore depends on keeping the confidentiality, integrity and availability of systems and their data under continuous control.

Institutions across sectors have adopted digital technologies, and the enterprise resource planning (ERP) system is one of the most widely adopted platforms. An ERP system is an integrated software platform that an organization uses to manage and automate business practices across its operations (Investopedia, 2024). In Kenya's technical and vocational education and training (TVET) institutions, ERP systems support supply chain management, human resource management, finance and academic processes such as course registration and examination processing. They were introduced to cope with large trainee numbers and to deliver efficient services, replacing simple desktop applications.

Implementation of ERP systems has nonetheless brought challenges, chief among them cybersecurity vulnerabilities. A vulnerability is a weakness in a security procedure, control or information system that cybercriminals can exploit to gain unauthorized access. Check Point Software Technologies (2024) lists eight common categories: zero-day exploits, remote code execution, unpatched software, poor data sanitization, misconfiguration, credential theft, unauthorized access and vulnerable application programming interfaces (APIs).

Problem Statement

ERP systems promise streamlined processes, improved data management and better decision-making, but they also introduce a wide range of security vulnerabilities. These can compromise sensitive information such as student records, financial data and internal communications. Without robust technical, logical and physical security measures, institutions are exposed to cyber threats, unauthorized access and data breaches that can jeopardize the entire ERP system. Large-scale breaches show how weaknesses in information systems translate into losses. In 2014, attackers compromised JPMorgan Chase and obtained contact details linked to about 83 million accounts, and in 2017 the Equifax breach affected about 147 million customers (Kost, 2024). Neither case was specific to ERP systems, but both illustrate the scale of harm that follows when security controls fail. Unauthorized access to servers and workstations has exposed both organizational and client data, and compromised data integrity arising from unauthorized access has produced legal consequences, financial loss and reputational damage (Susanto et al., 2011).

Kenyan TVET institutions face particular difficulties in ensuring that ERP implementation adheres to strict security protocols. They may lack adequate resources, trained personnel and a mature framework for addressing technical, logical and physical security concerns, which heightens the risk of vulnerabilities during and after implementation and threatens the effectiveness of the system. Yet empirical evidence on the security of ERP systems in TVET institutions, as opposed to their general cybersecurity readiness, remains limited. This gap motivated the present study.

Objectives of the Study

The general objective was to assess ERP system security vulnerabilities in selected TVET institutions in the Nyanza region of Kenya.

Literature Review

ERP Systems and Security Vulnerabilities

ERP systems integrate core organizational functions into a single platform, so a weakness in one component can expose the whole. When cybercriminals exploit such weaknesses, they can disrupt operations by wiping, stealing or encrypting data and then demanding payment to restore access (Susanto et al., 2011). The risk is not hypothetical. A 2019 IDC survey of 430 IT decision-makers, sponsored by the security vendor Onapsis (2019) found that 64% of respondents whose organizations ran SAP or Oracle E-Business Suite reported an ERP-related breach in the preceding 24 months, and financial data was compromised in 34% of such breaches (Onapsis, 2019). Because the survey was vendor-sponsored and limited to two commercial platforms, these figures indicate the order of magnitude of the problem rather than its precise extent.



Research on ERP security has taken several directions. Chang et al. (2014) showed that authentication and network security are central to protecting cloud-based ERP environments from unauthorized access and service disruption. A systematic review of a decade of ERP research identified risk management among the five most frequently studied concerns, alongside implementation, integration approaches, user participation and decision-making (Martins, 2022). More recent work notes that the integration of emerging technologies into ERP systems creates new targets for malicious attacks and data breaches (Anica-Popa et al., 2024).

ERP systems may be deployed on-premises, in the cloud or in a hybrid arrangement (Cook, 2024). Preliminary investigation by the researchers indicated that most TVET institutions in the study area host their ERP systems on their own premises, together with the supporting infrastructure. This makes physical security, in addition to technical and logical security, directly relevant to the protection of these systems.

Technical Security Measures

Technical measures are the hardware and software tools used to protect information systems. In this study they comprise encryption, regular security updates and patches, MFA, strong password policies, regular vulnerability assessments and role-based access control. Unpatched software is a well-documented route to compromise. The Equifax breach, which exposed the records of about 147 million customers, has been attributed to a failure to patch a known vulnerability (Kost, 2024). Authentication is a second recurrent weakness. In a study of ERP systems in Kenyan universities, Kimani et al. (2023) reported that systems commonly relied on username and password authentication, which is easily compromised, and linked ERP security weaknesses to authentication mechanisms, vulnerabilities and user training; they proposed an MFA prototype to address them.

ERP systems are also frequently accessed through web interfaces and therefore share the threat profile of web applications. In January–March 2024, Kenya's National KE-CIRT/CC detected 199,435 web application attacks, an increase of 174.95% over the previous quarter, and issued 2,681,912 advisories on web application attacks (Communications Authority of Kenya, 2024).

Logical Security Measures

Logical measures, as operationalized here, are the policies, rules, procedures and organizational arrangements that govern human behavior and access to the system: documented policies, a dedicated security team, staff training, compliance audits, authorized access and incident response. The human dimension is well established as a source of vulnerability. Gupi and Kadena (2021) described humans as the weakest link in cybersecurity because their behavior varies with circumstances, and they identified workload, inadequate staffing, risky behavior, low motivation and inadequate use of technology as contributing factors. Asaad and Saeed (2022) found that growing dependence on digital systems amplifies exposure to threats compared with offline processes and stressed the need for strong security policies that are actually followed. Foya (2022), studying audit firms, found that employees' perceptions of cybersecurity left systems exposed and that many organizations were unprepared to respond to cyberattacks because awareness training was conducted infrequently.

Insider access is a particular concern. In the 2019 breach at Desjardins, a Canadian financial cooperative, a malicious employee was able to access and exfiltrate the personal information of nearly 9.7 million individuals over more than two years, and the Privacy Commissioner of Canada attributed the breach to gaps in administrative and technological safeguards. The case illustrates why access authorization, monitoring and audit controls matter.

Physical Security Measures

Physical measures protect ERP hardware and the rooms that house it. Unauthorized physical access through unlocked doors, missing surveillance or the absence of guards can enable theft of servers, direct tampering with hardware or the introduction of malware, rendering the system unavailable and unreliable. Other physical threats include equipment theft, insider threats, power outages and inadequately controlled fire and flood hazards that disrupt ERP operations (Khairallah, 2024).

ERP and Cybersecurity in the Kenyan and TVET Context

Evidence from Kenya and comparable settings points to security challenges that are organizational as well as technical. Ngozwana (2013) examined socio-organizational influences on information security during ERP implementation in South Africa. Rather than treating ERP security as a purely technical matter, the study explored how power, dependency and exchange relations shape the adoption of security measures, and found that some of these factors influence information security. Anomah and Mahama (2025), studying ERP implementation in nine Ghanaian universities, identified cross-functional challenges and concluded that ERP implementation is a socio-technical rather than a purely technical undertaking. This view supports attention to logical and physical, as well as technical, security measures.

In Kenya's TVET sector, Kiarie (2024) assessed cybersecurity readiness and identified insufficient funding, a shortage of skilled cybersecurity personnel, the lack of comprehensive cybersecurity policies, weak user awareness training, outdated software and hardware, limited infrastructure and inadequate security governance, together with weaknesses in MFA and the absence of vulnerability scanning. These are general cybersecurity vulnerabilities rather than findings about ERP systems specifically.

Theoretical Framework

The study draws on institutional theory (Meyer & Rowan, 1977; DiMaggio & Powell, 1983), which holds that organizations adopt structures and practices not only for efficiency but also to conform to the norms and expectations of their environment and so gain legitimacy. DiMaggio and Powell (1983) identified three mechanisms

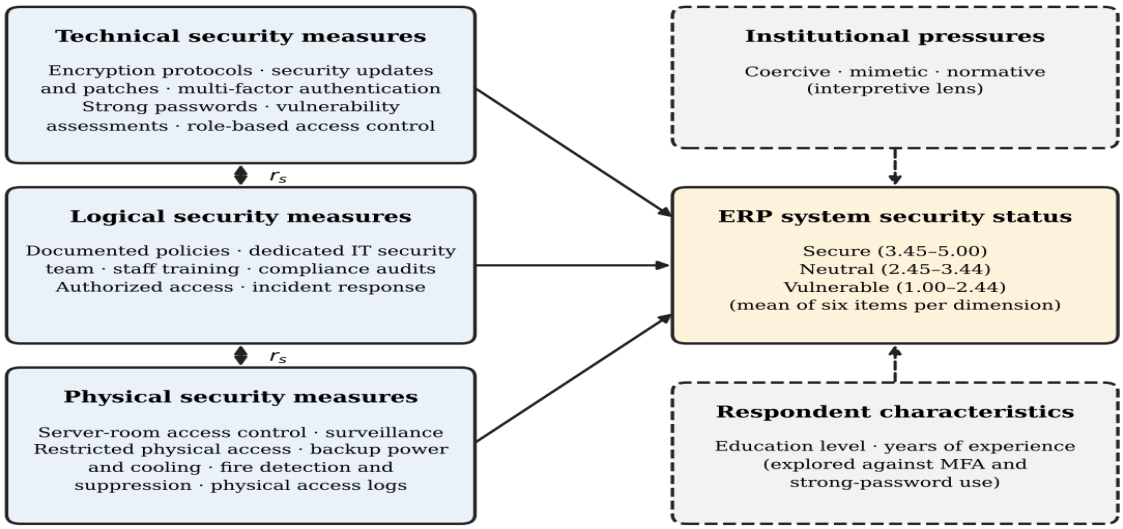
of institutional isomorphism: coercive pressures from law and regulation, mimetic pressures that lead organizations to imitate peers under uncertainty, and normative pressures from professional standards. Applied to cybersecurity, the theory suggests that institutions strengthen security measures not only for technical reasons but also in response to legal requirements such as Kenya's Data Protection Act of 2019, and the Computer Misuse and Cybercrimes Act of 2018. The theory is used here as an interpretive lens. If institutions respond to similar pressures, similar patterns of strength and weakness would be expected across TVETs, but the study did not measure institutional pressures directly.

Conceptual Framework

A conceptual framework contextualizes research, guides the formulation of research questions and aligns the analytical tools and methods with those questions (Ravitch & Riggan, 2016). Figure 1 presents the framework for this study. Technical, logical and physical security measures, each assessed through six items, jointly determine the security status of the ERP system, classified as secure, neutral or vulnerable. The three dimensions are expected to be interrelated. Respondents' education level and years of experience were explored in relation to MFA and strong-password use, and institutional pressures serve as the interpretive lens.

Figure 1

Conceptual Framework of the Study



Note. Solid arrows show the relationships examined; dashed arrows show contextual factors. r_s = Spearman's rank correlation.

Research Gap and Contribution

The reviewed literature offers evidence on general cybersecurity readiness in Kenyan TVET institutions (Kiarie, 2024), on ERP authentication in Kenyan universities (Kimani et al., 2023) and on the socio-technical challenges of ERP implementation in Ghana and South Africa (Anomah & Mahama, 2025; Ngozwana, 2013). To the authors' knowledge, however, these studies do not assess technical, logical and physical security together for ERP systems in TVET institutions, where ERP platforms are commonly hosted on-premises and physical safeguards therefore matter. This study differs

from earlier work in its focus on ERP systems, its joint treatment of the three security dimensions and its TVET setting. It contributes an empirical baseline for ERP security in TVET institutions, evidence on how the three dimensions relate to one another and a set of evidence-based priorities for institutional action.

2.0 Materials and Methods

Research Design

A descriptive survey design with a quantitative approach was used. A questionnaire collected data that described the current security measures aimed at securing ERP systems in the selected TVET institutions.

Study Area

The study was conducted in selected TVET institutions in the Nyanza region of Kenya. The region was chosen because its institutions reflect a range of levels of ICT infrastructural development. The focus was on the security measures currently in place, which would reveal vulnerabilities in the implementation of ERP systems.

Population and Sampling

The target population comprised the ICT heads of department and ICT technicians who were responsible for implementing and managing ERP systems in the 16 TVET institutions in the region that were using such systems. Because the population was small, a census was used. This yielded 32 respondents, an average of two per institution.

Research Instrument, Validity and Reliability

Data were collected with a structured questionnaire covering respondents' education level and years of relevant experience and three security dimensions: technical, logical and physical measures. Each dimension had six items rated on a 5-point Likert scale (1 = strongly disagree, 2 = disagree, 3 = uncertain, 4 = agree, 5 = strongly agree). Validity was established through review by subject experts. Reliability was assessed with Cronbach's alpha, which was .886 and above the .70 threshold conventionally regarded as acceptable (Nunnally, 1978).

Data Collection

The questionnaire was administered to the 32 respondents in the 16 TVET institutions after the approvals described in Section 3.7 had been obtained.

Data Analysis

Data were coded and analyzed with SPSS version 27. Descriptive statistics (means and standard deviations) summarized responses. Mean scores were interpreted using the study's criteria: 1.00–2.44 = vulnerable, 2.45–3.44 = neutral and 3.45–5.00 = secure. Dimension scores were computed as the mean of the six items in each dimension.

Inferential analysis used Spearman's rank correlation to examine relationships among the three-dimension scores, a choice appropriate for ordinal data and a small sample. Correlation strength was interpreted as moderate (.40–.59) or strong (.60–.79) (Evans, 1996). Associations between respondents' education level and years of experience (three categories each) and responses to the MFA and strong-password items (five response categories) were examined with Cramér's V and with approximate and exact (Fisher's exact test) significance values, the latter because of the small sample. Following Cohen (1988), for tables in which the smaller dimension has three categories, V values of approximately .07, .21 and .35 were taken to indicate small, medium and large associations. The significance level was $\alpha = .05$.

Ethical Considerations

Approval was obtained from Rongo University and from the National Commission for Science, Technology and Innovation (NACOSTI) before data collection. Participants gave informed consent by signing a consent form, and participation was voluntary, with participants informed that they could withdraw at any time. Anonymity was maintained, and paper records

were digitized and password-protected so that the identities of institutions and participants would not be exposed.

3. 0 Results and Discussion

Respondent Profile

The 32 respondents were the ICT officers directly managing ERP systems in the 16 TVET institutions. Most held a bachelor's degree (71.9%), followed by a diploma (15.6%) and a postgraduate qualification (12.5%). Most had 1–5 years of relevant experience (65.6%), while 31.3% had 6–10 years and 3.1% had more than 10 years (Table 1).

Table 1

Education Level and Relevant Experience of Respondents (N = 32)

Characteristic	*n*	%
Education level		
Diploma	5	15.6
Bachelor's degree	23	71.9
Postgraduate qualification	4	12.5
Years of relevant experience		
1–5 years	21	65.6
6–10 years	10	31.3
More than 10 years	1	3.1

Note. Frequencies were derived from the reported percentages and the sample size.

Technical Security Measures

Table 2 summarizes the technical security items. Respondents agreed that ERP implementations followed industry-standard encryption protocols (M = 3.75, SD = 1.22), that regular security updates and patches were applied (M = 3.69, SD = 1.15), that strong password policies were enforced (M = 3.88, SD = 1.16) and that role-based access control was employed (M = 3.84, SD = 1.19); all four fall in the secure range. Two items were rated neutral: MFA (M = 3.38, SD = 1.19), which approached the secure threshold, and regular vulnerability assessments (M = 3.16, SD = 1.17).

Table 2

Technical Security Items: Means, Standard Deviations and Interpretation

Item	*M*	*SD*	Interpretation
1. The ERP system implementation at our institution follows industry-standard encryption protocols.	3.75	1.22	Secure
2. Regular security updates and patches are applied to the ERP system to protect against vulnerabilities.	3.69	1.15	Secure
3. Our ERP system has multi-factor authentication (MFA) mechanisms in place to prevent unauthorized access.	3.38	1.19	Neutral

Item	*M*	*SD*	Interpretation
4. Strong password policies are enforced in the ERP system to enhance data security.	3.88	1.16	Secure
5. Vulnerability assessments are conducted regularly on the ERP system to identify and address potential threats.	3.16	1.17	Neutral
6. The ERP system employs role-based access controls (RBAC) to limit access to sensitive information.	3.84	1.19	Secure

Note. $N = 32$. Items were rated from 1 (strongly disagree) to 5 (strongly agree). Interpretation: 1.00–2.44 = vulnerable; 2.45–3.44 = neutral; 3.45–5.00 = secure.

Logical Security Measures

Table 3 shows the results for logical measures. Respondents agreed that access to the ERP system was granted only to authorized personnel ($M = 3.97$, $SD = 1.43$) and that incident response procedures were in place ($M = 3.47$, $SD = 1.08$). Four items were rated neutral. Documentation and communication of security policies and procedures ($M = 3.44$, $SD = 1.22$) fell at the upper boundary of the neutral band, just below the secure threshold. Respondents were uncertain whether a dedicated IT team was responsible for monitoring and managing ERP security ($M = 3.00$, $SD = 1.30$) and whether regular compliance audits were conducted ($M = 3.03$, $SD = 1.18$). Staff training on ERP security protocols received the lowest rating ($M = 2.84$, $SD = 1.17$), which, although within the neutral band, marks it as the weakest logical measure.

Table 3

Logical Security Items: Means, Standard Deviations and Interpretation

Item	*M*	*SD*	Interpretation
1. Security policies and procedures for ERP system implementation are clearly documented and communicated.	3.44	1.22	Neutral
2. Our institution has a dedicated IT security team responsible for monitoring and managing ERP system security.	3.00	1.30	Neutral
3. Staff members undergo regular training on ERP security protocols and best practices.	2.84	1.17	Neutral
4. Regular audits are conducted to ensure compliance with ERP security policies and procedures.	3.03	1.18	Neutral
5. Access to the ERP system is granted only to authorized personnel with the required credentials and approval.	3.97	1.43	Secure
6. Incident response procedures are in place to handle security breaches in the ERP system.	3.47	1.08	Secure

Note. $N = 32$. Items were rated from 1 (strongly disagree) to 5 (strongly agree). Interpretation: 1.00–2.44 = vulnerable; 2.45–3.44 = neutral; 3.45–5.00 = secure.

Physical Security Measures

Table 4 presents the physical measures. Respondents agreed that server rooms housing the ERP systems were physically secured with access control measures ($M = 3.66$, $SD = 1.26$), that the infrastructure was located in a secure environment with surveillance monitoring ($M = 3.78$, $SD = 1.29$) and that unauthorized personnel

were restricted from areas where ERP hardware was stored ($M = 3.63$, $SD = 1.29$). Backup power and cooling systems ($M = 3.22$, $SD = 1.36$) and the maintenance of physical access logs ($M = 2.97$, $SD = 1.40$) were rated neutral. Fire detection and suppression systems received the lowest rating on the entire instrument ($M = 2.59$, $SD = 1.24$); this is still within the neutral band but close to the vulnerable range (below 2.45).

Table 4

Physical Security Items: Means, Standard Deviations and Interpretation

Item	*M*	*SD*	Interpretation
1. The server rooms housing the ERP system are physically secured with access control measures.	3.66	1.26	Secure
2. The ERP system infrastructure is located in a secure environment with surveillance monitoring.	3.78	1.29	Secure
3. Unauthorized personnel are restricted from accessing physical locations where ERP hardware is stored.	3.63	1.29	Secure
4. Backup power and cooling systems are in place to ensure uninterrupted operation of the ERP infrastructure.	3.22	1.36	Neutral
5. Fire detection and suppression systems are installed to protect the ERP system's physical infrastructure.	2.59	1.24	Neutral
6. Physical access logs are maintained to track who enters and exits areas where ERP hardware is stored.	2.97	1.40	Neutral

Note. $N = 32$. Items were rated from 1 (strongly disagree) to 5 (strongly agree). Interpretation: 1.00–2.44 = vulnerable; 2.45–3.44 = neutral; 3.45–5.00 = secure.

Overall Ratings of the Three Dimensions

Table 5 gives the dimension scores. Technical measures ($M = 3.61$, $SD = 0.92$) fell in the secure band. Logical measures ($M = 3.29$, $SD = 0.99$) and physical measures ($M = 3.31$, $SD = 1.07$) fell in the neutral band, indicating that the ERP systems could not be classified as secure on these dimensions and that areas of weakness need to be addressed.

Table 5

Dimension Scores for Technical, Logical and Physical Security Measures

Dimension	*M*	*SD*	Interpretation
Technical	3.61	0.92	Secure
Logical	3.29	0.99	Neutral
Physical	3.31	1.07	Neutral

Note. $N = 32$. *Dimension scores are the mean of six items. Interpretation bands are as in Table 2.*

Relationships Among the Security Dimensions

Spearman's correlation coefficients are shown in Table 6. Technical and logical measures were strongly and positively correlated (r_s = .690, p < .001): institutions whose respondents rated technical measures higher also tended to rate logical measures higher. Technical and physical measures were moderately and positively correlated (r_s = .507, p = .003), as were physical and logical measures (r_s = .483, p = .005). All three relationships were statistically significant at the .01 level.

Table 6

Spearman's Rank Correlations Among Technical, Logical and Physical Security Measures

Relationship	r_s	p	Strength
Technical and logical	.690	< .001	Strong
Technical and physical	.507	.003	Moderate
Physical and logical	.483	.005	Moderate

Note. N = 32. Strength was interpreted following Evans (1996).

Respondent Characteristics, MFA and Strong Passwords

Table 7 reports the associations between respondents' education level and years of experience and their responses on MFA and strong passwords. None of the four associations was statistically significant at the .05 level. The effect sizes were nonetheless medium to large (V = .284 to .400). Education level and MFA (V = .284; approximate p = .740, exact p = .834), years of experience and MFA (V = .312; approximate p = .622, exact p = .644) and years of experience and strong passwords (V = .290; approximate p = .716, exact p = .581) showed medium associations, and education level and strong passwords showed a large association (V = .400; approximate p = .250, exact p = .305). With only 32 respondents, these tests had little power, so the results show no detectable association rather than demonstrating independence.

Table 7

Associations Between Respondent Characteristics and Responses on MFA and Strong Passwords

Variables	Cramér's V	Approximate p	Exact p
Education level × MFA	.284	.740	.834
Education level × strong passwords	.400	.250	.305
Years of experience × MFA	.312	.622	.644
Years of experience × strong passwords	.290	.716	.581

Note. N = 32. Exact p values are from Fisher's exact test.

Discussion

This study assessed ERP security in selected Kenyan TVET institutions across three dimensions. By the study's criteria, only technical measures were rated secure; logical and physical measures were rated neutral, so the ERP systems cannot be regarded as secure across all dimensions. The discussion considers each dimension in turn, the pattern across them and the interpretation offered by institutional theory.

Technical measures. Respondents rated encryption, patching, strong password policies and role-based access control as secure. The two weaker items, MFA and vulnerability assessments, match the weaknesses that Kiarie (2024) identified in Kenyan TVET institutions generally, namely weak MFA and the absence of vulnerability scanning. They also echo the authentication weaknesses that Kimani et al. (2023) reported for ERP systems in Kenyan universities. The finding matters because credential theft and unpatched or unassessed systems are among the common vulnerability categories described by Check Point Software Technologies (2024).

Logical measures. Restricting access to authorized personnel and having incident response procedures were the strongest logical items, whereas training, a dedicated security team and compliance audits were the weakest. This pattern is consistent with the shortage of skilled personnel, weak awareness training and inadequate security governance that Kiarie (2024) reported for TVET institutions, and with the emphasis that Gupi and Kadena (2021), Foya (2022) and Asaad and Saeed (2022) place on human factors, awareness and enforced policy. Weak monitoring and audit capacity is also a concern because insider misuse of access, as in the Desjardins case, is detected through such controls.

Physical measures. Perimeter controls (secured server rooms, surveillance and restricted access) were rated secure, but fire detection and suppression received the lowest rating on the instrument, and physical access logs and backup power and cooling were also weak. Because most of these institutions host their ERP systems on-premises, such gaps expose the infrastructure to the environmental and tampering risks described by Khairallah (2024) and could compromise availability, one of the three pillars of information security.

Pattern across dimensions. Across all three dimensions, the lowest-rated items were largely those concerned with monitoring, assurance and capacity (vulnerability assessments, audits, access logs, fire detection, training and dedicated security staffing) rather than basic access restriction. MFA and backup power were also among the weaker items. This pattern suggests that the sampled institutions had invested more in controls that restrict access than in controls that detect, verify or recover from incidents. Because the study was not designed to test this, it is offered as an observation for future research.

Interdependence of the dimensions. The positive correlations indicate that institutions that rated one dimension highly tended to rate the others highly. Possible explanations include shared drivers such as leadership commitment, budget and policy, which fits the emphasis in the recommendations on policy and dedicated funding. Other explanations are also possible. Respondents from the same institution may share a response tendency, and the two respondents per institution are not independent observations. The correlations therefore describe association, not causation.

Institutional theory. The similar profiles of strength and weakness across institutions are consistent with institutional theory, which would predict that institutions facing similar legal, professional and peer pressures adopt similar practices. For example, the widespread weakness in fire detection and access logging could reflect mimetic processes, in which institutions follow the practice of their peers, and the strength of access-restriction controls could reflect coercive

or normative pressures. The data cannot, however, confirm these mechanisms, because institutional pressures were not measured. The theory is best regarded as a plausible interpretive frame.

Respondent characteristics. Education level and years of experience were not significantly associated with MFA or strong-password responses. Given the small sample, this should not be read as evidence that these characteristics are unrelated to security practice.

4.0 Conclusion

The study assessed the technical, logical and physical security measures protecting ERP systems in selected TVET institutions in the Nyanza region and the relationships among them. The conclusions follow the objectives.

First, technical measures were rated secure overall (M = 3.61), but MFA and regular vulnerability assessments did not reach the secure threshold. Second, logical measures were neutral (M = 3.29): access authorization and incident response were adequate, whereas staff training, a dedicated security team and regular audits were weak. Third, physical measures were neutral (M = 3.31): perimeter controls were adequate, whereas fire detection, physical access logs and backup power were weak. Fourth, the three dimensions were positively and significantly correlated, indicating that they reinforce one another and that strengthening one is likely to go together with strengthening the others.

Overall, the ERP systems in the sampled institutions were secure in the technical dimension but only moderately secure in the logical and physical dimensions, and areas of weakness remain in all three. The three dimensions must be implemented together if ERP systems are to be secure.

5.0 Recommendations

TVET institutions that have not implemented MFA should do so for administrators and users of ERP systems so that access is verified through more than one factor.

Institutions should conduct vulnerability assessments of their ERP systems on a regular schedule and act on the findings.

Institutions should provide regular cybersecurity training for ICT staff and ERP users, with content that keeps pace with evolving threats, including those enabled by artificial intelligence (AI).

Institutions should establish a dedicated cybersecurity team to monitor and protect ERP systems and should conduct regular ERP security audits to establish vulnerability levels and track performance.

Institutions that lack power backup plans should provide backup power for the rooms and infrastructure that host ERP systems, install fire detection and suppression systems, and keep records of who accesses the ERP infrastructure.

Institutions should develop strong cybersecurity policies, provide a dedicated budget for implementing them and enforce them consistently, as these are the enabling conditions for addressing the weaknesses identified.

Limitations and Future Research

The findings should be interpreted in light of several limitations. The sample was a census of 32 respondents in 16 institutions in one region, which limits generalization and statistical power. The data are self-reported perceptions of ICT staff and were not verified through technical testing or physical inspection. Respondents were nested within institutions, so observations were not fully independent. The correlational design does not support causal inference. The interpretation bands for mean scores were specific to this study, and reliability was reported for the questionnaire as a whole rather than for each dimension. Finally, institutional theory was used interpretively and institutional pressures were not measured.

Future research should replicate the study with larger, multi-region samples and in universities and other learning institutions to allow comparison. Studies should combine perception data with technical vulnerability scanning and physical inspections, measure institutional pressures directly and account for the clustering of respondents within institutions. Periodic data collection on ERP vulnerabilities in TVET institutions could also be used to develop machine learning models that predict security vulnerabilities in ERP systems.

References

Anica-Popa, L.-E., Vrîncianu, M., Pugna, I.-B., & Boldeanu, D.-M. (2024). Addressing cybersecurity issues in ERP systems – Emerging trends. *Proceedings of the International Conference on Business Excellence, 18*(1), 1306–1323. https://doi.org/10.2478/picbe-2024-0108

Anomah, S., & Mahama, A. (2025*). Enterprise resource planning implementation complexity in higher education finance: A socio-technical examination of Ghanaian universities.* EDPACS. Advance online publication. https://doi.org/10.1080/07366981.2025.2586487

Asaad, R. R., & Saeed, V. A. (2022). A cyber security threats, vulnerability, challenges and proposed solution. *Applied Computing Journal, 2*(4), 227–244. https://doi.org/10.52098/acj.202260

Chang, B. R., Tsai, H.-F., Tsai, Y.-C., & Chang, Y.-S. (2014). Applying authentication and network security to in-cloud enterprise resource planning system. *Vietnam Journal of Computer Science, 1*(2), 129–140. https://doi.org/10.1007/s40595-014-0015-8

Check Point Software Technologies. (2004). *Top 8 cyber security vulnerabilities*. https://www.checkpoint.com/cyber-hub/cyber-security/top-8-cyber-security-vulnerabilities/

Cohen, J. (1988). *Statistical power analysis for the behavioral sciences* (2nd ed.). Lawrence Erlbaum Associates. https://doi.org/10.4324/9780203771587

Communications Authority of Kenya. (2024). *Cyber security report Q3 2023/2024 (January–March 2024).* https://repository.ca.go.ke/handle/123456789/1379

Computer Misuse and Cybercrimes Act, No. 5 of 2018 (Kenya). https://new.kenyalaw.org/akn/ke/act/2018/5/eng@2022-12-31

Cook, B. (2024). *ERP system types: Everything you need to know*. Tipalti. https://tipalti.com/accounts-payable-hub/types-of-erp-systems/

Data Protection Act, No. 24 of 2019 (Kenya). https://kdic.go.ke/sites/default/files/2021-07/TheDataProtectionAct__No24of2019.pdf

DiMaggio, P. J., & Powell, W. W. (1983). The iron cage revisited: Institutional isomorphism and collective rationality in organizational fields. *American Sociological Review, 48*(2), 147–160. https://doi.org/10.2307/2095101

Evans, J. D. (1996). *Straightforward statistics for the behavioral sciences*. Brooks/Cole Publishing Company. https://books.google.com/books?id=8Ca2AAAAIAAJ

Foya, D. (2022). Assessing cyber security awareness and organizational preparedness on cyber security in audit

firms: The case of the Big 4 audit firms, EY, Deloitte, KPMG and PwC, 2017–2020. *International Journal of Scientific & Engineering Research, 13*(3), 623–647. https://www.researchgate.net/publication/360240606_Assessing_Cyber_Security_Awareness_and_organisational_preparedness_on_cyber_security_in_audit_firms_The_case_of_the_big_4_audit_firms_EY_Deloitte_KPMG_PWC_2017_2020_1

Gupi, M., & Kadena, E. (2021). Human factors in cybersecurity: Risks and impacts. *Security Science Journal, 2*(2), 51–64. https://doi.org/10.37458/ssj.2.2.3

Investopedia. (2024). *Enterprise resource planning: Meaning, components and examples.* https://www.investopedia.com/term/e/erp.asp

Khairallah, M. (2024). *Physical security assessment handbook: An insider's guide to securing a business* (2nd ed.). CRC Press. https://www.routledge.com/Physical-Security-Assessment-Handbook-An-Insiders-Guide-to-Securing-a/Khairallah/p/book/9781032790800

Kiarie, N. (2024). Enhancing digital resilience: A cybersecurity readiness assessment of Kenyan TVET institutions. *Journal of the Kenya National Commission for UNESCO, 5*(1). 1-14. https://doi.org/10.62049/jkncu.v5i1.191

Kimani, C., Obuhuma, J. I., & Roche, E. (2023). Multi-factor authentication for improved enterprise resource planning systems security. *International Journal of Information Technology and Computer Science, 15*(3), 42–54. https://doi.org/10.5815/ijitcs.2023.03.04

Kost, E. (2024). Biggest data breaches in financial services. UpGuard. https://www.upguard.com/blog/biggest-data-breaches-financial-services

Martins, E. J. da S. (2022). *Major concerns and systematic literature review on enterprise resource planning [*Master's dissertation, Instituto Politécnico de Coimbra]. http://hdl.handle.net/10400.26/43128

Meyer, J. W., & Rowan, B. (1977). Institutionalized organizations: Formal structure as myth and ceremony. *American Journal of Sociology, 83*(2), 340–363. https://doi.org/10.1086/226550

Ngozwana, K. N. (2013). *Socio-organizational influences on information security during ERP implementation* [Master's thesis, University of Johannesburg]. https://hdl.handle.net/10210/8764

Nunnally, J. C. (1978). *Psychometric theory* (2nd ed.). McGraw-Hill.

Onapsis. (2019). *New IDC survey highlights that business-critical applications are at risk.* https://www.onapsis.com/blog/new-idc-survey-highlights-business-critical-applications-are-risk

Ravitch, S. M., & Riggan, M. (2016). *Reason and rigor: How conceptual frameworks guide research* (2nd ed.). SAGE Publications.

Susanto, H., Almunawar, M. N., & Tuan, Y. C. (2011). Information security management system standards: A comparative study of the big five. *International Journal of Electrical & Computer Sciences, 11*(5), 21–29. https://citeseerx.ist.psu.edu/document?doi=369403470302f205811fcb8ac84c5e51be3c030f&repid=rep1&type=pdf

Tunggal, A. T. (2025). *What is the cost of a data breach in 2023?* UpGuard. https://www.upguard.com/blog/cost-of-data-breach