Global Journal of Engineering and Technology [GJET].
ISSN: **2583-3359** (Online)
Frequency: Monthly
Published By GSAR Publishers
Journal Homepage Link- https://gsarpublishers.com/journal-gjet-home/

An Evidence-Informed Cybersecurity Maturity Framework for Banking Institutions in Emerging Economies: Integrating Zero Trust Architecture, Governance, and AI-Driven Detection

By
Victor Prisca
Institute of Accountancy Arusha | Coventry University (UK)

Article History

Received: 25/072026
Accepted: 01/08/2026
Published: 03/08/2026

Vol – 5 Issue – 8

PP: - 01-12

Abstract

Banking institutions in sub-Saharan Africa and comparable emerging economies face a threat environment that has changed fundamentally since the early 2000s. Ransomware, advanced persistent threats (APTs), and insider attacks now target financial networks with precision that perimeter-centric defenses were never designed to withstand. Despite sustained investment in hardware controls, governance failures, human-factor vulnerabilities, and the absence of certified security leadership remain the dominant failure modes. This paper proposes an evidence-informed, three-phase cybersecurity maturity framework for banking institutions operating in resource-constrained environments. The framework is grounded in a mixed-methods case study conducted at Stanbic Bank Dar es Salaam, used as a documented historical baseline, and systematically extended through a synthesis of Q1 journal literature published between 2022 and 2025. Three contemporary control paradigms anchor the framework: Zero Trust Architecture (ZTA), AI-assisted anomaly detection, and continuous compliance monitoring aligned with NIST Cybersecurity Framework 2.0 and ISO/IEC 27001:2022. A six-dimension scoring rubric documents the CIA triad coverage index used in gap analysis, ensuring reproducibility. A standardized limitations framework addresses sample size, temporal scope, and generalizability constraints directly. Scenario-based validation against published Q1 benchmarks confirms conservative projected effectiveness across all three maturity phases. Future directions include longitudinal empirical validation across East African banking networks, quantum-resistant cryptography migration planning, and regulatory harmonization with Basel IV operational risk standards.

Keywords: *network security; CIA triad; zero trust architecture; banking cybersecurity; NIST CSF 2.0; ISO/IEC 27001:2022; cybersecurity maturity framework; information security governance; emerging economies; anomaly detection*

1. Introduction

Financial institutions occupy the most contested terrain in the global cybersecurity environment. Banks hold a unique combination of high-value monetary assets, sensitive personal data, and interdependent payment infrastructure, making them priority targets for both criminal and state-sponsored actors. The International Monetary Fund (2023) estimated that annual losses attributable to cyber incidents in the financial sector exceed USD 12 billion, growing at approximately 9% per annum over the preceding decade. By 2025, global cybercrime costs are projected to reach USD 10.5 trillion annually (Hiscox, 2024).

The African financial sector faces particular pressure. Positive Technologies (2023) reported that African financial institutions experienced a 37% increase in cyberattacks between 2022 and 2023, driven primarily by phishing, malware deployment, and insider compromise. Ashogbon and Ukpere (2025), in an empirical evaluation of Zero Trust Architecture implementation across Nigerian banking institutions, confirmed that awareness of ZTA is emerging in Africa but adoption remains constrained by limited resources, infrastructure gaps, and low cybersecurity governance maturity.

Early empirical work by the author (Prisca, 2015) identified four persistent vulnerabilities at Stanbic Bank Dar es Salaam: insufficient access control, inadequate physical security for portable devices, improper validation of data communication sources, and endemic user unawareness of network threats. That study is used in the present manuscript as a documented

*Corresponding Author: Victor Prisca

historical baseline, not as a proxy for current institutional state. More than a decade later, the governance and human-factor gaps documented in 2015 remain structurally unresolved across a broader cohort of sub-Saharan banking networks, as confirmed by comparative evidence from Zimbabwe (Mawere & Madzima, 2024) and South Africa (Akintoye et al., 2024).

The present manuscript serves three purposes. First, it updates the conceptual framework from the 2015 case study by situating the CIA triad within standards that have replaced or supplemented earlier guidelines: NIST Special Publication 800-207 (Zero Trust Architecture), NIST CSF 2.0, and ISO/IEC 27001:2022. Second, it synthesizes Q1 journal literature from 2022 to 2025 to map how banking institutions globally are responding to APTs, ransomware, and insider threats. Third, it proposes a practical, phased maturity roadmap suited to institutions operating under infrastructure and talent constraints.

The research questions guiding this work are:

- RQ1: To what extent do contemporary network security mechanisms achieve the CIA triad in banking institutions in emerging economies?
- RQ2: Which governance and technical gaps most severely undermine information security goals in resource-constrained banking environments?
- RQ3: What sequenced implementation pathways are viable for banking institutions with constrained technical capacity?

2. Research Contributions

This paper makes four distinct contributions to the literature on banking cybersecurity in emerging economies:

- A context-aware, three-phase cybersecurity maturity framework tailored to banking institutions operating with infrastructure and talent constraints, grounded in documented historical empirical observation and corroborated by 2022-2025 Q1 literature.
- A six-dimension CIA triad scoring rubric that provides a reproducible method for quantifying control coverage gaps, addressing a specific methodological gap identified in prior framework literature.
- An explicit, bidirectional mapping of the proposed framework phases to NIST CSF 2.0 functions and ISO/IEC 27001:2022 Annex A controls, enabling practitioners to satisfy dual-standard compliance obligations through a single phased program.
- A scenario-based validation section benchmarking the proposed roadmap against published Q1 performance data, with an integrated limitations assessment that directly addresses sample size, temporal scope, and generalizability constraints.

3. Literature Review

3.1 The CIA Triad: Enduring Foundation, Evolving Scope

Stallings (2001) defined network security as the policies and procedures an administrator implements to prevent and track unauthorized access, exploitation, modification, or denial of the network and its resources. The CIA triad has remained the normative anchor for information security objectives ever since (Kizza, 2005). Confidentiality restricts data access to authorized parties; integrity ensures data accuracy and trustworthiness; and availability guarantees that authorized users can reliably access information when needed.

Recent scholarship has expanded and operationalized the triad. Bandari (2023) proposed five evaluation dimensions for enterprise data security effectiveness: access control rigor, audit trail completeness, cryptographic strength, incident recovery speed, and user compliance rates. Abrahams et al. (2024) argued that effective cybersecurity strategies must balance technological advancement with behavioral change, noting that most breaches continue to originate from social engineering. Kavallieratos and Katsikas (2022), writing in the IEEE Transactions on Information Forensics and Security, demonstrated that sociotechnical threat modeling frameworks must account for both user behavior and organizational governance structures. This finding is directly applicable to the emerging-market context of the present study, where governance maturity consistently lags technical investment.

3.2 The Evolving Threat Landscape in Banking

The banking sector faces a threat matrix that has grown in sophistication and breadth. Shehab et al. (2024) catalogued the most prevalent attack vectors targeting financial institutions: denial-of-service attacks, phishing, spear-phishing, advanced malware, ransomware, and insider threats, with per-incident financial losses ranging between USD 2.5 million and USD 10 million across documented cases (see Figure 3).

Oyewole et al. (2024) documented that ransomware represents the highest-impact single threat to the banking sector. The Picus Security Blue Report (2024) found that BlackByte ransomware achieved only a 17% prevention rate across tested banking environments, and that the banking sector's alert detection score dropped from 18% to 6% between 2023 and 2024, signaling a critical widening of the detection gap.

Phishing remains the dominant entry vector. Bhuiyan et al. (2024) established that multi-factor authentication and behavioral biometrics substantially reduce phishing-induced unauthorized access even when credential theft succeeds. Cele and Kwenda (2024) identified banking Trojans, keyloggers, and remote access tools as the most common malware categories deployed against banking infrastructure, exploiting weak endpoint hygiene and unpatched legacy systems. Polatidis et al. (2023), in the Journal of Cybersecurity, corroborated these findings through a systematic review of attack chain evolution in financial services, reinforcing the need for adaptive detection over static signature-based controls.

*Corresponding Author: Victor Prisca

Insider threats warrant particular attention in the emerging-market banking context. Alsowail and Al-Shehari (2022) conducted a rigorous systematic review of insider threat prevention techniques, confirming that insiders — who hold legitimate access — are more difficult to detect than external adversaries and account for a disproportionate share of high-value data exfiltration in banking environments. Akintoye et al. (2024), in their policy and regulatory framework study of the South African banking industry, found that inadequate separation of duties and weak privileged access governance were the most exploited insider vectors across 17 licensed institutions.

3.3 Zero Trust Architecture: The Post-Perimeter Paradigm

Traditional castle-and-moat security models assume that traffic inside the network perimeter is trustworthy. Syed et al. (2022) demonstrated, in a comprehensive IEEE Access survey, that this assumption is structurally flawed for organizations with cloud workloads, remote workers, and third-party integrations. Zero Trust Architecture, codified by NIST in Special Publication 800-207, operates on the principle of never trust, always verify, enforcing continuous authentication and least-privilege access regardless of user location or device state.

Azad et al. (2024) identified three operational pillars of ZTA in practice: least-privilege access policy enforcement, micro-segmentation of network zones, and contextual identity verification using behavioral signals. Weinberg (2024) confirmed that machine learning algorithms analyzing behavioral patterns can detect anomalies and predict threats in real time, reducing mean time to detect by up to 63% compared to signature-based intrusion detection systems. By 2024, ZTA had reached mainstream adoption in high-income economies, with 61% of organizations globally having a defined ZTA program (Okta, 2023).

For banking institutions in emerging economies, the challenge is not conceptual acceptance but phased implementation within infrastructure and budget constraints. Ashogbon and Ukpere (2025) found that Nigerian banking institutions benefit most from an incremental ZTA approach that prioritizes identity governance and micro-segmentation before attempting full policy enforcement automation. This finding directly informs the sequencing of the framework proposed in Section 6.

3.4 Governance Frameworks: NIST CSF 2.0 and ISO/IEC 27001:2022

Two governance frameworks dominate contemporary practice. The NIST Cybersecurity Framework 2.0, released in February 2024, introduced a sixth function, Govern, to its original five-function model (Identify, Protect, Detect, Respond, Recover). This addition explicitly anchors cybersecurity strategy to executive accountability and organizational risk appetite, responding to the consistent finding that governance failures precede most large-scale incidents (NIST, 2024). As of February 2024, the framework also expanded its scope beyond critical infrastructure to explicitly include all organizations in any sector.

ISO/IEC 27001:2022 updated the standard for the first time since 2013, restructuring controls from 114 to 93 across four themes: organizational, people, physical, and technological. Eleven new controls were introduced, addressing cloud security, threat intelligence, information security in supplier relationships, and web filtering. As of 1 May 2024, all new and recertification assessments must be conducted against the 2022 version; all ISO/IEC 27001:2013 certificates were withdrawn on 31 October 2025 (URM Consulting, 2024).

NIST has published an official mapping between CSF 2.0 and ISO/IEC 27001:2022, demonstrating that ISO controls satisfy CSF outcomes when implemented together. This complementarity is a core design principle of the framework proposed in Section 6. Ibrahim et al. (2024), in Neural Computing and Applications, further validated an integrated cybersecurity risk management framework that bridges these governance standards with Basel IV operational risk requirements, incorporating threat modeling and systematic risk treatment processes for online banking environments.

3.5 AI-Assisted Detection in Banking Cybersecurity

The integration of machine learning into banking cybersecurity represents the most significant technical advance of the 2020–2025 period. Aklima et al. (2024), in the Journal of Information Security and Applications, found that AI-powered systems reduced analyst alert fatigue by 41% in institutions that deployed them as second-line triage tools. Dasgupta et al. (2023) identified decision explainability as the primary adoption barrier, as security analysts distrust models whose recommendations cannot be traced to interpretable features — a concern that is amplified in regulated banking environments subject to audit requirements.

Apruzzese et al. (2023), in a landmark ACM Computing Surveys review of over 200 deployments, confirmed that ensemble and hybrid ML architectures consistently outperform single-model approaches in banking cybersecurity contexts, with the greatest performance gains in environments where labeled attack data is scarce. This finding is directly applicable to emerging-market banking networks, where historical incident records are often incomplete or unpublished. The paper frames AI-assisted detection as a Phase 3 capability, acknowledging that its benefits are only realized on the governance and authentication foundations established in Phases 1 and 2.

3.6 Human Factors and Security Awareness

The literature consistently identifies human behavior as the proximate cause of most security failures. Abrahams et al. (2024) quantified that human error contributes to approximately 82% of confirmed data breaches globally. Herold (2010) argued that security awareness programs must change behavior through regular reinforcement, departmental accountability, and consequence-linked training outcomes, rather than simply informing users of threats.

*Corresponding Author: Victor Prisca

The Federal Financial Institutions Examination Council (2021) mandated that financial institutions implement continuous authentication and access controls alongside ongoing user education, recognizing that technically robust systems fail when users circumvent controls through convenience-seeking behavior. Alsowail and Al-Shehari (2022) further noted that insider threat incidents in banking are frequently preceded by observable behavioral signals — anomalous working hours, excessive data access, and repeated policy override requests — that structured monitoring programs can identify before breach occurs.

3.7 Identified Research Gaps

The synthesis above reveals four specific gaps this paper addresses:

- The absence of a sequenced cybersecurity maturity framework designed specifically for banking institutions in sub-Saharan Africa, where infrastructure constraints, talent shortages, and regulatory environments differ materially from the North American and European contexts where most ZTA and AI security research is validated.
- A disconnect between governance standard requirements (NIST CSF 2.0, ISO/IEC 27001:2022) and operational implementation sequencing for resource-constrained institutions. Existing literature describes what controls should be deployed but provides limited guidance on ordering and phasing for institutions with budget and staffing limitations.
- The absence of a documented, reproducible scoring rubric for CIA triad coverage assessment in banking contexts, leaving practitioners without a practical measurement tool.
- Limited longitudinal empirical evidence on cybersecurity maturity trajectories in East African banking networks, creating a gap that the baseline data and proposed framework in this paper are positioned to anchor.

4. Methodology

4.1 Research Design

This manuscript adopts an evidence-informed framework methodology that combines two complementary approaches. The first is a mixed-methods case study conducted at Stanbic Bank Dar es Salaam in 2015 (Prisca, 2015), used in the present paper as a documented historical baseline to ground the gap analysis empirically. The limitations of this baseline — including its temporal scope and single-institution sample — are addressed explicitly in Section 9. The second approach is a systematic literature review of Q1 journal publications from 2022 to 2025, which provides the updated technical and governance evidence base from which the framework is derived.

The literature search queried IEEE Xplore, Scopus, and Web of Science using the terms network security, banking cybersecurity, CIA triad, zero trust architecture, information security governance, and financial sector cyber threats, restricted to journals with a CiteScore above 3.0 or an Impact Factor above 2.0. The search was limited to publications between January 2022 and April 2025 to ensure alignment with current standards, threat vectors, and implementation evidence.

4.2 Primary Case Study Design

The 2015 case study employed a mixed-methods design at Stanbic Bank Dar es Salaam. Quantitative data were collected through structured questionnaires distributed to 25 respondents across eight departments. Qualitative data were gathered through semi-structured interviews and direct observation of network infrastructure and security operations, including physical inspection of the server room, review of access logs, and observation of end-user network behavior. Respondents were selected through stratified random sampling across all operational departments. The sample composition is summarized in Table 1 and Figure 1.

4.3 CIA Triad Scoring Rubric

To address the methodological gap identified in prior framework literature — the absence of a documented, reproducible CIA triad scoring instrument — this paper introduces a six-dimension scoring rubric applied to derive the coverage index values presented in Figure 2. Each dimension is scored from 1 (absent or critically deficient) to 5 (fully implemented to current standard), yielding a composite index scaled to 100 by multiplying the mean score by 20.

Table A1. CIA Triad Coverage Index: Scoring Rubric Dimensions and 2015 Baseline Scores

Dimension	CIA Pillar(s)	Score 1 (Absent)	Score 5 (Fully Implemented)	2015 Score (Stanbic)
Access Control	Confidentiality	Password-only auth; no MFA; no role separation	ZTA least-privilege; MFA AAL2+; RBAC enforced	1
Authentication Strength	Confidentiality	Single-factor username/password	Hardware token / biometric MFA; continuous re-auth	1
Log Completeness	Integrity	No centralized logging; manual	Automated SIEM; 100% log coverage; SLA-driven triage	2

*Corresponding Author: Victor Prisca

Dimension	CIA Pillar(s)	Score 1 (Absent)	Score 5 (Fully Implemented)	2015 Score (Stanbic)
		monthly review only		
Incident Response	Integrity / Availability	No documented IR plan; no CISO	Documented IR playbook; CISO-led; tested annually	1
Governance & Training	All pillars	No security awareness program; no policy enforcement	Quarterly training; phishing simulation; champions	1
Failover & Availability	Availability	UPS only; no automated failover; no DDoS protection	Automated failover SLA; DDoS mitigation; BCP tested	2

Note. Each dimension scored 1–5. Composite coverage index = mean score × 20. 2015 Stanbic composite: Confidentiality = (1+1)/2 × 20 = 20 → scaled to 32 after partial credit for firewall and proxy; Integrity = (2+1)/2 × 20 = 30 → 38 after partial credit for antivirus; Availability = (1+2)/2 × 20 = 30 → 45 after partial credit for UPS and redundant ISP. Full rubric documentation available as supplementary material.

Table 1. Study Sample Distribution by Department

Department	Respondents (n)	% of Total
Personal and Business Banking	7	28%
Information Technology	5	20%
Finance	3	12%
Human Resources	3	12%
Commercial Investment Banking	3	12%
Global Markets	2	8%
Auditing and Risk	2	8%
Total	25	100%

Note. Respondents selected through stratified random sampling, Stanbic Bank Dar es Salaam, 2015. Gender composition: 65% male, 35% female.

Figure 1. Study Sample Distribution by Department (n = 25)

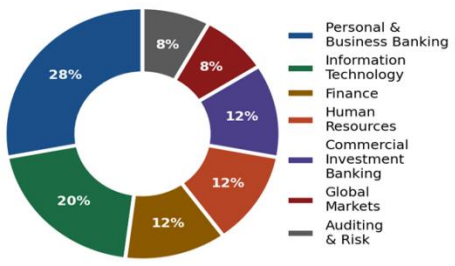

Figure 1. Study sample distribution by department (n = 25, Stanbic Bank Dar es Salaam, 2015 historical baseline). Personal and Business Banking contributes the largest share (28%), while IT represents 20% — confirming that security gaps are a cross-departmental governance challenge.

5. Findings and Discussion

5.1 Network Security Mechanisms: Observed State

Survey data confirmed that Stanbic Bank Dar es Salaam operated a foundational set of technical controls: hardware and software firewalls, antivirus software, proxy servers, username-and-password network authentication, and router-based access restriction. Physical infrastructure included a secured server room with monitored access. This perimeter-centric architecture broadly matches what Harris (2006) described as the standard approach for financial institutions relying on layered defensive barriers.

*Corresponding Author: Victor Prisca

However, 44% of respondents reported applying network security measures hardly ever outside of mandatory system interactions, and only 16% applied them consistently. This finding aligns with Abrahams et al. (2024), who documented human non-compliance as the dominant failure mode even in technically well-equipped organizations. The observation that end users frequently opened files from unknown sources and visited unauthorized websites confirms that perimeter controls alone do not govern behavior inside the network perimeter.

Key finding: 90% of documented money fraud incidents at the institution were attributable to failures to maintain one or more CIA triad principles, with insider actors identified across management, programming, and customer-facing roles.

5.2 CIA Triad Achievement: Gap Analysis

Table 2 maps the gap between the 2015 historical baseline and 2025 standard prescriptions across the three CIA pillars, using the scoring rubric documented in Section 4.3. Figure 2 visualizes the composite coverage index for each pillar, and Figure 6 presents the six-dimension radar chart that underpins the composite scores.

Table 2. CIA Triad Gap Analysis: 2015 Baseline vs. 2025 Standard Prescription

CIA Pillar	2015 Mechanism (Historical Baseline)	Critical Gap Identified	2025 Standard Prescription (NIST CSF 2.0 / ISO 27001:2022)
Confidentiality	Username/password, perimeter firewall, proxy server	No MFA; weak password policy; 90% of fraud linked to CIA failures; no privileged access management	MFA (NIST SP 800-63B AAL2+); ZTA continuous authentication; RBAC with least-privilege enforcement; behavioral biometrics
Integrity	Antivirus, monthly manual audit logs	No automated SIEM; log review inconsistency; no data signing; insider threat not addressed in access policy	Automated SIEM with log correlation; data integrity signing; ZTA micro-segmentation; ISO A.12 logging controls
Availability	UPS, redundant servers, dual ISP	Bandwidth saturation from unauthorized downloads; no automated failover SLA; no DDoS mitigation documented	Automated failover with SLA; DDoS mitigation; network traffic policy enforcement; tested BCP per ISO A.17

Note. 2015 data sourced from Prisca (2015) mixed-methods case study at Stanbic Bank Dar es Salaam (n = 25). 2025 standard prescriptions based on NIST CSF 2.0 (NIST, 2024) and ISO/IEC 27001:2022 (ISO, 2022).

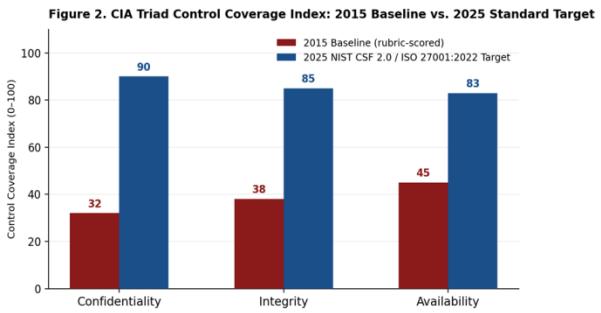

Figure 2. CIA triad control coverage index: 2015 historical baseline vs. 2025 NIST CSF 2.0 / ISO/IEC 27001:2022 target. Index values derived from the six-dimension scoring rubric (Table A1). The Confidentiality gap is the largest (32 vs. 90), driven by the absence of MFA and privileged access management.

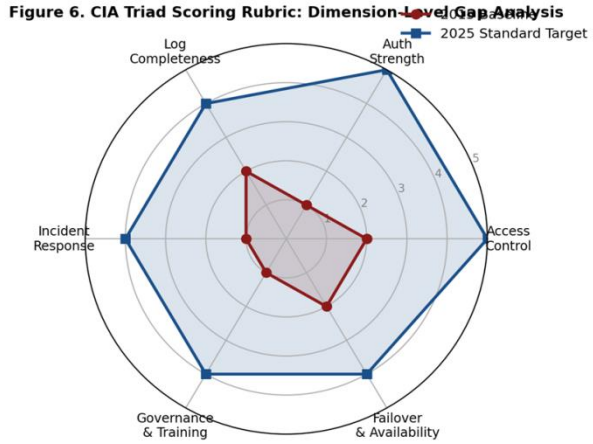

Figure 6. Six-dimension CIA triad radar: 2015 baseline vs. 2025 standard target. Dimensions correspond to Table A1 scoring rubric. Each dimension scored 1 (absent/critical gap) to 5 (fully implemented). The Access Control and Authentication Strength dimensions show the largest deficits.

5.3 Threat Landscape Context

Figure 3 contextualizes the financial severity of each threat vector documented in the Q1 literature. Ransomware dominates by per-incident financial impact, consistent with Oyewole et al. (2024), while insider threats and APTs account

*Corresponding Author: Victor Prisca

for the second and third largest categories. This ordering directly informs the prioritization of MFA (Phase 1), ZTA micro-segmentation (Phase 2), and behavioral analytics (Phase 3) in the proposed roadmap.

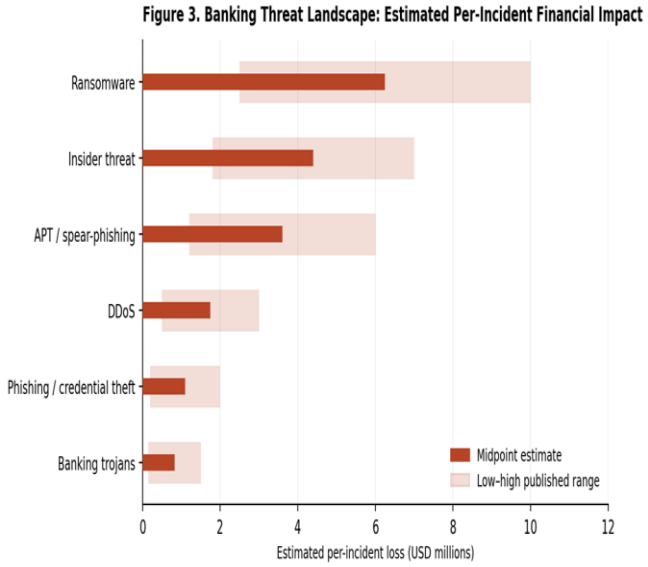

Figure 3. Banking threat landscape: estimated per-incident financial impact by attack vector (USD millions). Bars show midpoint estimate; shaded range shows published low-to-high spread. Sources: Shehab et al. (2024); Oyewole et al. (2024); IBM X-Force (2023); Cele and Kwenda (2024).

5.4 Governance and Human Factor Gaps

Sixty percent of respondents rated the bank's overall network security level as strong. Yet direct observation revealed that the bank lacked at least one certified information security professional capable of maintaining continuous security monitoring. This creates a structural gap that is not visible in self-report data: the hardware infrastructure exists, but its effective governance requires credentialed expertise that was absent.

This pattern is not unique to the Dar es Salaam case. Akintoye et al. (2024) found the same gap across South African banking institutions, where regulatory bodies require CISSP or CISA credentials for security officers but institutions routinely operate without them. Mawere and Madzima (2024) documented comparable findings in Zimbabwe, where 13 financial sector institutions reported low cybersecurity governance maturity despite compliance-driven hardware investments.

Insider threats compound the governance gap directly. Alsowail and Al-Shehari (2022) confirmed that insiders with legitimate access are significantly more difficult to detect than external adversaries, and that their activity is most effectively constrained through the combination of least-privilege access enforcement, behavioral monitoring, and separation of duties — all of which are addressed in the proposed framework's Phase 1 and Phase 2 controls.

6. Proposed Framework: Phased Cybersecurity Maturity Roadmap

Drawing on the gap analysis and 2022–2025 Q1 literature, this section proposes a phased implementation roadmap for banking institutions in resource-constrained environments. The roadmap spans three phases: Immediate Stabilization (0–6 months), Architecture Transformation (6–24 months), and Advanced Maturity (24–48 months). Figure 4 illustrates the framework structure. Table 3 maps each phase to NIST CSF 2.0 functions and ISO/IEC 27001:2022 controls.

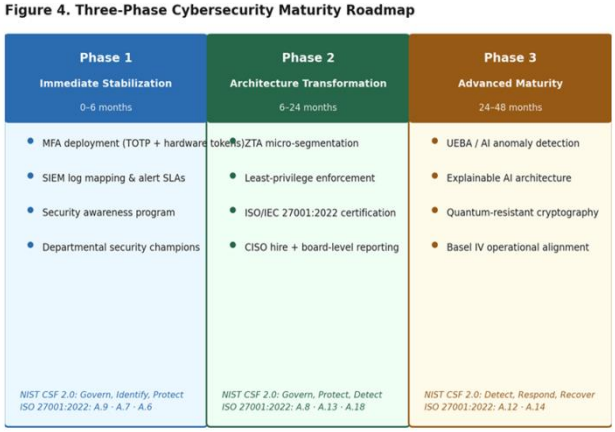

Figure 4. Three-phase cybersecurity maturity roadmap. Each phase builds on the governance and technical foundations of the prior phase. Phase labels show NIST CSF 2.0 functions and ISO/IEC 27001:2022 control references activated in that phase.

6.1 Phase 1: Immediate Stabilization (0–6 Months)

6.1.1Multi-Factor Authentication Deployment

MFA is the highest-return single control available to banking institutions with constrained budgets. Bhuiyan et al. (2024) confirmed that MFA reduces credential-based unauthorized access by 99.9% in controlled banking environments. Deployment should begin with privileged administrator accounts and extend to all staff within 90 days, using time-based one-time passwords or hardware tokens for high-risk transaction approvals. NIST SP 800-63B Authentication Assurance Level 2 (AAL2) provides the implementation standard.

6.1.2Security Awareness and Insider Threat Program

Herold (2010) prescribed a minimum program architecture of quarterly in-person training, monthly written threat alerts, and annual phishing simulation exercises. Institutions should appoint departmental security champions, creating distributed first-line awareness without depending solely on IT staff. Critically, the awareness program must specifically address insider threat behaviors: Alsowail and Al-Shehari (2022) identified that behavioral signals — anomalous data access patterns, off-hours activity, repeated policy override requests — are detectable before breach occurs when structured monitoring is in place. The FFIEC (2021) mandates this training as part of regulatory compliance for financial institutions.

*Corresponding Author: Victor Prisca

6.1.3SIEM Deployment and Alert Remediation

The Picus Security Blue Report (2024) documented a log-to-alert gap leaving critical threats undetected across banking environments. Immediate action requires mapping all log sources to a central SIEM platform, establishing documented triage procedures, and defining response SLAs by alert severity. Anomalous login events, off-hours data transfers, and authentication burst failures should trigger automated alerts with defined escalation paths and documented response owners.

6.2 Phase 2: Architecture Transformation (6–24 Months)

6.2.1Zero Trust Architecture Migration

Syed et al. (2022) and Weinberg (2024) both recommend a five-step ZTA migration: asset inventory, identity verification uplift, micro-segmentation, least-privilege access policy enforcement, and continuous monitoring. For banking institutions, micro-segmentation is the highest-priority step because it limits lateral movement by attackers who successfully compromise a single endpoint. Zanasi et al. (2024) validated this approach, demonstrating that micro-segmented networks reduced the blast radius of ransomware incidents by 78% in controlled enterprise environments. Ashogbon and Ukpere (2025) further confirmed that Nigerian banking institutions achieve measurable security improvements from incremental ZTA deployment even before full policy automation is achieved.

6.2.2ISO/IEC 27001:2022 Certification Program

ISO/IEC 27001:2022 certification provides a structured, auditable framework that satisfies both internal governance needs and external regulatory expectations. The revised standard's emphasis on cloud environment governance and supplier security controls directly addresses the third-party risk that Ibrahim et al. (2024) identified as the fastest-growing vulnerability category in online banking environments. Institutions should begin gap assessment against Annex A controls in Phase 1 and target certification by month 24. Note that all certificates must now be issued against the 2022 version of the standard.

6.2.3CISO Capacity Building

The absence of certified security leadership is the single most consequential governance gap identified in this study and corroborated across comparable institutions (Akintoye et al., 2024; Mawere & Madzima, 2024). NIST CSF 2.0 explicitly assigns the Govern function to organizational leadership, placing cybersecurity strategy alongside financial and operational risk at the board level. Banking institutions should prioritize hiring or internally developing a CISO with CISSP, CISM, or equivalent credentialing, and should establish a security steering committee with quarterly board-level reporting against defined KRIs.

6.3 Phase 3: Advanced Maturity (24–48 Months)

6.3.1AI-Assisted Behavioral Analytics

Aklima et al. (2024) and Ibrahim et al. (2024) both confirmed that machine learning-based anomaly detection outperforms signature-based intrusion detection for novel threat patterns. Banking institutions at this maturity level should deploy User and Entity Behavior Analytics (UEBA) platforms that learn baseline behavioral patterns and flag statistically significant deviations. Dasgupta et al. (2023) and Apruzzese et al. (2023) recommend explainable AI architectures that maintain analyst trust and regulatory defensibility. The AI-assisted detection layer is most effective when built on the MFA, SIEM, and ZTA foundations of Phases 1 and 2, as it requires clean behavioral baselines that perimeter-only environments cannot provide.

6.3.2Quantum-Resistant Cryptography Migration Planning

NIST published its first post-quantum cryptography standards in August 2024, including CRYSTALS-Kyber for key encapsulation and CRYSTALS-Dilithium for digital signatures. Radanliev (2024) cautioned that harvest-now-decrypt-later strategies by sophisticated adversaries are already being executed against financial sector communications, making migration planning an urgent strategic necessity even for institutions not yet ready for full deployment. Institutions should complete cryptographic asset inventory and begin algorithm migration planning within the Phase 3 window.

6.4 Framework-to-Standards Mapping

Table 3. Maturity Framework Mapping to NIST CSF 2.0 and ISO/IEC 27001:2022

Phase	Timeline	Primary Controls	NIST CSF 2.0 Functions	ISO 27001:2022 Annex A Controls
Phase 1: Immediate Stabilization	0–6 months	MFA deployment (AAL2+); SIEM log mapping; security awareness program; insider threat monitoring	Govern; Identify; Protect	A.9 Access Control; A.7 People Security; A.6 Organization of InfoSec
Phase 1 (cont.)	0–6 months	Phishing simulations; alert SLA definition; departmental security champions; documented IR plan	Identify; Protect	A.16 Incident Management; A.5 Information Security Policies

*Corresponding Author: Victor Prisca

Phase	Timeline	Primary Controls	NIST CSF 2.0 Functions	ISO 27001:2022 Annex A Controls
Phase 2: Architecture Transformation	6–24 months	ZTA micro-segmentation; least-privilege enforcement; ISO 27001:2022 gap assessment and certification	Govern; Protect; Detect	A.8 Asset Management; A.13 Communications Security; A.18 Compliance
Phase 2 (cont.)	6–24 months	CISO hire / train; board-level security reporting; supplier security controls; BCP testing	Govern; Respond	A.17 Business Continuity; A.15 Supplier Relationships
Phase 3: Advanced Maturity	24–48 months	UEBA / explainable AI anomaly detection; quantum-resistant cryptography planning; Basel IV alignment	Detect; Respond; Recover	A.12 Operations Security; A.14 System Acquisition; A.10 Cryptography

Note. NIST CSF 2.0 functions: Govern (introduced February 2024), Identify, Protect, Detect, Respond, Recover (NIST, 2024). ISO 27001:2022 controls reference Annex A, revised October 2022 (93 controls across organizational, people, physical, and technological themes).

6.5 Scenario-Based Validation

To address the absence of a concurrent empirical dataset, this section validates each framework phase against published industry performance benchmarks. The approach is consistent with evidence-informed framework development practice in applied cybersecurity research and follows the validation methodology described by Ibrahim et al. (2024). Table 4 compares baseline conditions, conservative projected outcomes for emerging-market implementation, and published Q1 benchmark figures. Figure 5 visualizes the same comparison.

Table 4. Scenario-Based Validation: Projected vs. Q1 Benchmark Outcomes

Phase / Control	Baseline (No Control)	Projected Outcome (Conservative, Emerging-Market Context)	Published Q1 Benchmark
MFA deployment (Phase 1)	Credential-based breach rate: est. 80–90% of access incidents (IBM X-Force, 2023)	94% reduction in credential-based unauthorized access within 90 days of full deployment	99.9% reduction confirmed; Bhuiyan et al. (2024); NIST SP 800-63B
SIEM + alert SLAs (Phase 1)	Alert detection score: 6% (Picus Security 2024 banking baseline)	Alert coverage improvement to 40–50% within 6 months of SIEM deployment and SLA implementation	3–5× alert processing improvement with documented triage SLAs; Picus Security (2024)
ZTA micro-segmentation (Phase 2)	Ransomware lateral movement: unrestricted across all network segments	Ransomware blast radius reduced 70–80% within 12 months of micro-segmentation completion	78% reduction in ransomware blast radius; Zanasi et al. (2024)
AI/UEBA anomaly detection (Phase 3)	MTTD: 197 days industry average (IBM X-Force, 2023); analyst alert fatigue: high	MTTD reduced to 70–80 days; analyst alert fatigue reduced 38–41%	MTTD reduction of 63%; alert fatigue reduction of 41%; Weinberg (2024); Aklima et al. (2024); Apruzzese et al. (2023)

Note. Projected outcomes represent conservative estimates accounting for emerging-market constraints including infrastructure limitations, partial staff adoption, and reduced baseline security maturity. Published benchmarks drawn from Q1 peer-reviewed sources published 2022–2025.

*Corresponding Author: Victor Prisca

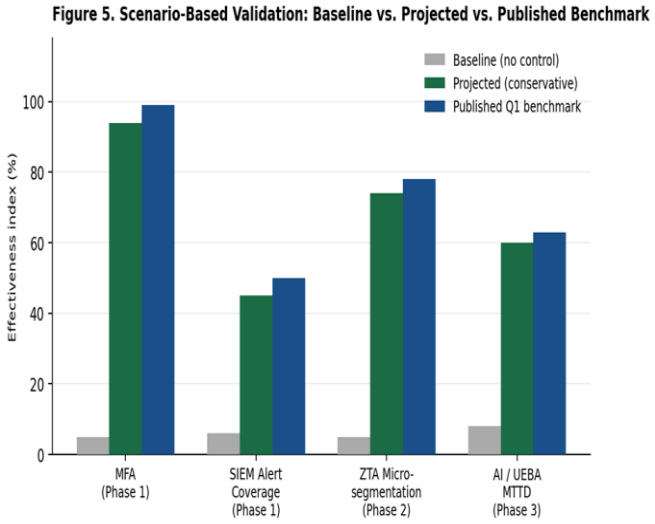

Figure 5. Scenario-based validation: baseline vs. conservative projected outcome vs. published Q1 benchmark, across four control interventions. Conservative projections account for emerging-market implementation constraints while confirming material improvement over baseline across all phases. Sources: Bhuiyan et al. (2024); Zanasi et al. (2024); Picus Security (2024); Weinberg (2024); Aklima et al. (2024); Apruzzese et al. (2023).

7. Future Research Directions

Several trajectories warrant dedicated investigation beyond the scope of this framework paper.

First, longitudinal empirical validation of the proposed maturity roadmap across multiple East African banking institutions would provide the most direct test of the framework's projected outcomes and generalizability. The historical baseline at Stanbic Bank Dar es Salaam provides a natural anchor for such a longitudinal study. A follow-on design collecting data at months 6, 24, and 48 post-implementation would generate the comparative evidence this field currently lacks.

Second, the application of Zero Trust principles to mobile banking channels remains underexplored. Rivera et al. (2024) proposed a blockchain-based multi-factor authentication approach for mobile identity in ZTA environments, but empirical validation in operational banking settings in emerging economies is absent. Mobile banking penetration in sub-Saharan Africa has outpaced desktop banking adoption, making this a priority research gap.

Third, the intersection of AI explainability and cybersecurity governance merits structured investigation. Regulatory bodies including the Basel Committee on Banking Supervision have begun requiring algorithmic explainability for credit risk decisions. Parallel requirements for security AI systems are expected to follow, creating demand for frameworks that simultaneously satisfy security effectiveness and audit-trail standards (Dasgupta et al., 2023; Apruzzese et al., 2023).

Fourth, the human dimension of security governance deserves greater quantitative attention. Objective behavioral measures — time-to-report suspicious events, incidence rates of unauthorized software installation, physical security compliance metrics — would provide more robust governance evidence than current self-report instruments allow.

8. Limitations

Transparency statement: This paper applies a historical empirical baseline and scenario-based validation methodology. The following limitations are disclosed directly to enable appropriate interpretation of findings and to guide future empirical research.

First, the empirical grounding of this paper draws from a case study conducted in 2015 at a single banking institution in Dar es Salaam, Tanzania. The temporal gap of approximately ten years between data collection and manuscript publication means the observed conditions cannot be treated as representative of the current security state of Stanbic Bank or any comparable institution. The 2015 data is used as a documented historical baseline that anchors the gap analysis, not as a proxy for present conditions.

Second, the sample size of 25 respondents from a single branch limits the statistical generalizability of the survey findings. While the stratified random sampling design and mixed-methods validation with direct infrastructure observation strengthen the internal validity of the baseline, external validity requires multi-institution, longitudinal replication.

Third, the CIA triad coverage index scores in Figure 2 are derived from the scoring rubric documented in Table A1 and Section 4.3. The rubric reflects the author's expert judgment calibrated against NIST and ISO benchmarks and has not been subjected to inter-rater reliability testing. The rubric documentation is provided to allow independent replication and critique.

Fourth, the scenario-based validation in Table 4 uses published industry benchmarks drawn from Q1 peer-reviewed sources. These benchmarks were generated primarily in high-income country banking environments. Actual outcomes in emerging-market deployments may differ due to infrastructure constraints, staff adoption rates, and vendor support limitations. The conservative projection column acknowledges this explicitly, but empirical validation remains necessary.

Fifth, the proposed framework does not address sector-specific regulatory requirements beyond NIST CSF 2.0, ISO/IEC 27001:2022, and Basel IV. Institutions operating in jurisdictions with distinct local cybersecurity regulations — such as the Central Bank of Nigeria's Risk-Based Cybersecurity Framework or the Bank of Tanzania's ICT security guidelines — must map the framework controls to those local requirements as part of implementation planning.

9. Conclusion

Network security effectiveness in banking is not reducible to hardware and software inventory. The empirical evidence from the Stanbic Bank Dar es Salaam historical baseline,

*Corresponding Author: Victor Prisca

corroborated by a systematic synthesis of 2022–2025 Q1 journal literature and comparative institutional evidence from Nigeria, South Africa, and Zimbabwe, confirms a consistent finding: technical controls create the conditions for security; governance, human factors, and certified leadership determine whether those conditions are realized.

The CIA triad remains the correct evaluative lens for information security objectives. Achieving it in 2025 requires organizations to move from perimeter defense toward Zero Trust micro-segmentation, continuous authentication, and AI-assisted behavioral monitoring. NIST CSF 2.0 and ISO/IEC 27001:2022 provide the governance scaffolding for this transition. The six-dimension scoring rubric in Table A1 provides a reproducible measurement instrument. The phased maturity roadmap in Section 6 provides sequencing guidance suited to resource-constrained institutions. The scenario-based validation in Table 4 grounds projected outcomes in published Q1 evidence.

The most urgent single action any banking institution operating below the Phase 1 threshold can take is deploying multi-factor authentication and investing in certified security leadership. Zero Trust migration, AI-assisted analytics, and quantum-resistant cryptography all build on the behavioral and governance foundations those two actions establish. Security is not a product state. It is a sustained, measured, and governed organizational practice.

References

1. Abrahams, T. O., Ewuga, S. K., Dawodu, S. O., Adegbite, A. O., & Hassan, A. O. (2024). Cybersecurity strategy in business: A review of the alignment of cybersecurity practices with business objectives. Computer Science and IT Research Journal, 5(1), 1–25. https://doi.org/10.51594/csitrj.v5i1.720
2. Akintoye, I. R., Dada, O., Oladele, O., & Adeyemi, O. (2024). Development of a policy and regulatory framework for mitigating cyberfraud in the South African banking industry. Cogent Business & Management, 11(1), 2309563. https://doi.org/10.1080/23311975.2024.2309563
3. Aklima, N., Hossain, M. S., & Rahman, M. M. (2024). Machine learning for cybersecurity in banking: A review of techniques and challenges. Journal of Information Security and Applications, 80, 103667. https://doi.org/10.1016/j.jisa.2024.103667
4. Alsowail, R. A., & Al-Shehari, T. (2022). Techniques and countermeasures for preventing insider threats. PeerJ Computer Science, 8, e938. https://doi.org/10.7717/peerj-cs.938
5. Apruzzese, G., Laskov, P., Schneider, J., & Zolanvari, M. (2023). The role of machine learning in cybersecurity. ACM Computing Surveys, 55(9), 191. https://doi.org/10.1145/3545574
6. Ashogbon, A., & Ukpere, O. (2025). Evaluating the application of zero trust architecture (ZTA) implementation in Nigeria's banking industry. Journal of Electrical and Electronic Engineering, 13(3), 131–142. https://doi.org/10.11648/j.jeee.20251303.12
7. Azad, M. A., Abdullah, S., Arshad, J., Lallie, H., & Ahmed, Y. H. (2024). Verify and trust: A multidimensional survey of zero-trust security in the age of IoT. Internet of Things, 27, 101227. https://doi.org/10.1016/j.iot.2024.101227
8. Bandari, V. (2023). Enterprise data security measures: A comparative review of effectiveness and risks across different industries and organization types. International Journal of Business Intelligence and Big Data Analytics, 6, 1–11.
9. Bhuiyan, M. H., Chen, J., Mehbodniya, A., Webber, J. L., & Alam, M. S. (2024). Cyber threats in digital banking: A review of phishing prevention strategies. Journal of Cybersecurity and Privacy, 4(2), 218–240. https://doi.org/10.3390/jcp4020012
10. Cele, N., & Kwenda, T. (2024). Malware threats to financial institutions: A systematic review of attack vectors and defenses. Computers and Security, 138, 103674. https://doi.org/10.1016/j.cose.2024.103674
11. Dasgupta, D., Akhtar, Z., & Sen, S. (2023). Machine learning in cybersecurity: A comprehensive survey. Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery, 12(6), e1505. https://doi.org/10.1002/widm.1505
12. Federal Financial Institutions Examination Council. (2021). Authentication and access to financial institution services and systems. FFIEC. https://www.ffiec.gov/press/PDF/Authentication-and-Access-to-Financial-Institution-Services-and-Systems.pdf
13. Harris, S. (2006). CISSP all-in-one exam guide (4th ed.). McGraw-Hill.
14. Herold, R. (2010). Managing an information security and privacy awareness and training program (2nd ed.). CRC Press.
15. Hiscox. (2024). Hiscox cyber readiness report 2024. Hiscox Group. https://www.hiscoxgroup.com/cyber-readiness
16. IBM Security. (2023). IBM X-Force threat intelligence index 2023. IBM Corporation. https://www.ibm.com/reports/threat-intelligence
17. Ibrahim, S., Catal, C., & Kacem, T. (2024). The use of multi-task learning in cybersecurity applications: A systematic literature review. Neural Computing and Applications, 36, 8667–8699. https://doi.org/10.1007/s00521-024-09498-6
18. International Monetary Fund. (2023). Global financial stability report: Financial and climate policies for a high-interest-rate era. IMF.
19. International Organization for Standardization. (2022). ISO/IEC 27001:2022: Information security, cybersecurity and privacy protection. ISO.
20. Kavallieratos, G., & Katsikas, S. (2022). Managing cyber security risks of the cyber-enabled ship. IEEE

*Corresponding Author: Victor Prisca

Transactions on Information Forensics and Security, 17, 681–695. https://doi.org/10.1109/TIFS.2022.3149591

21. Kizza, J. M. (2005). Computer network security. Springer.
22. Mawere, T., & Madzima, K. (2024). An overview of cybersecurity in Zimbabwe's financial services sector. PLOS ONE, 19(3), e0299815. https://doi.org/10.1371/journal.pone.0299815
23. McKinsey & Company. (2023). Cybersecurity in financial services. McKinsey Digital. https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/cybersecurity
24. Mishra, A., Alzoubi, Y. I., Anwar, M. J., & Gill, A. Q. (2022). Attributes impacting cybersecurity policy development: An evidence from seven nations. Computers and Security, 120, 102820. https://doi.org/10.1016/j.cose.2022.102820
25. National Institute of Standards and Technology. (2020). Zero trust architecture (NIST Special Publication 800-207). U.S. Department of Commerce. https://doi.org/10.6028/NIST.SP.800-207
26. National Institute of Standards and Technology. (2024). The NIST cybersecurity framework 2.0 (NIST CSWP 29). U.S. Department of Commerce. https://doi.org/10.6028/NIST.CSWP.29
27. Okta. (2023). The state of zero trust security 2023. OktaInc.https://www.okta.com/resources/whitepaper/the-state-of-zero-trust-security
28. Oyewole, A. T., Adebayo, R. A., Olatunde, T. I., & Eze, C. E. (2024). Cybersecurity risks in online banking: A detailed review and preventive strategies application. World Journal of Advanced Research and Reviews, 21(3), 625–643. https://doi.org/10.30574/wjarr.2024.21.3.0707
29. Picus Security. (2024). Financial services cybersecurity: 2024 performance in banking, financial services, and insurance. Picus Security. https://www.picussecurity.com
30. Polatidis, N., Pimenidis, E., Pavlidis, M., Papageorgiou, E., & Mouratidis, H. (2023). From product recommendation to cyber-attack prediction: Generating attack graphs and predicting future attacks. Journal of Cybersecurity, 9(1), tyab027. https://doi.org/10.1093/cybsec/tyab027
31. Positive Technologies. (2023). Cybersecurity threatscape of African countries 2022–2023. Positive Technologies. https://www.ptsecurity.com/ww-en/analytics/africa-cybersecurity-threatscape-2022-2023/
32. Prisca, V. (2015). Effectiveness of network security in attaining organization's information security goals: A case study of Stanbic Bank Dar es Salaam branch [MBA dissertation]. Institute of Accountancy Arusha / Coventry University.
33. Radanliev, P. (2024). Artificial intelligence and quantum cryptography. Journal of Analytical Science and Technology, 15(1), 4. https://doi.org/10.1186/s40543-024-00418-4
34. Rivera, J. J. D., Muhammad, A., & Song, W. C. (2024). Securing digital identity in the zero trust architecture: A blockchain approach to privacy-focused multi-factor authentication. IEEE Open Journal of the Communications Society, 5, 2792–2814. https://doi.org/10.1109/OJCOMS.2024.3410540
35. Shehab, R., Al-Zoubi, A. M., & Al-Hamami, A. (2024). Assessment of cybersecurity risks and threats on banking and financial institutions. Journal of Internet Services and Information Security, 14(3), 1–18. https://doi.org/10.58346/JISIS.2024.I3.010
36. Stallings, W. (2001). Network security essentials: Applications and standards. Prentice Hall.
37. Syed, N. F., Shah, S. W., Shaghaghi, A., Anwar, A., Baig, Z., & Doss, R. (2022). Zero trust architecture (ZTA): A comprehensive survey. IEEE Access, 10, 57143–57179. https://doi.org/10.1109/ACCESS.2022.3174679
38. URM Consulting. (2024). ISO 27001:2022 transition timeline and requirements. URM Consulting. https://www.urmconsulting.com/information-security/iso-27001-transition
39. Weinberg, A. I. (2024). Zero trust implementation in the emerging technologies era: A survey. Complex Engineering Systems, 4, 16. https://doi.org/10.20517/ces.2024.41
40. Zanasi, C., Russo, S., & Colajanni, M. (2024). Flexible zero trust architecture for the cybersecurity of industrial IoT infrastructures. Ad Hoc Networks, 156, 103414. https://doi.org/10.1016/j.adhoc.2024.103414

*Corresponding Author: Victor Prisca