SCIENCE SET
OPEN ACCESS PUBLISHERS

Research Article

International Journal of Blockchain Applications and Financial Technology

Toward Unified Information Security Governance in Banking: Integrating Policy Evaluation and Cyber Risk Management for Online Services

Adil Omar Yousif Mohamed[1], Zahra.I.Mahmoud[2], Mawahib Elamin[3], Amel H. Abdalla[4] & Abdulnaser Rashid[5]

[1]Department of Computer Science, College of Computer, Qassim University, Saudi Arabia
[2]College of Public Health and Health Informatic ,Hail University ,Saudi Arabia
[3]Department of Mathematics, College of Science, Qassim University, Buraydah, 51452, Saudi Arabia
[4]Department of Mathematics, College of Science, Qassim University, Buraydah, Saudi Arabia
[5]Department of Computer Science, College of Computer, Qassim University, Buraydah 51452, Saudi Arabia

***Corresponding author:** Mohamed, A. O. Y., Department of Computer Science, College of Computer, Qassim University, Saudi Arabia.

Submitted: 05 January 2026 **Accepted:** 12 January 2026 **Published:** 18 January 2026

Citation: *Mohamed, A. O. Y., Mawahib Elamin, Z. I., Abdalla, A. H., & Rashid, A. (2026). Toward Unified Information Security Governance in Banking: Integrating Policy Evaluation and Cyber Risk Management for Online Services. I Jou of Bloc App nd Fina Tech, 2(1), 01-06.*

Abstract

Banking institutions face dynamic information security (IS) challenges, requiring a balance between stringent confidentiality and privacy mandates and the operational demands of digital banking. Recent research has contributed significantly to this domain through three key strands: (i) the development and validation of an ISO/NIST-aligned framework for assessing confidentiality and privacy in bank security policies, (ii) a systematic review of IS policy risks, benefits, and emerging trends across U.S. and global banking sectors, and (iii) the proposal of an integrated cyber-risk management framework tailored for online banking environments [1-3]. Building on these foundations, this paper introduces a unified approach that bridges policy evaluation with technical risk assessment and treatment [4, 5]. The proposed model integrates multiple layers: policy conformance checks against ISO 27001 and NIST SP 800-series standards, threat modeling using STRIDE and TVRA methodologies, vulnerability classification aligned with OWASP and CWE taxonomies, and iterative risk scoring and treatment cycles. This holistic design addresses the persistent gap between "written policy" and operational security controls in digital channels. Empirical findings—such as variability in confidentiality and privacy readiness among banking institutions and the influence of regulatory and cultural factors on compliance—inform the model's architecture and adoption strategies [6]. Implementation guidance includes structured steps, governance checkpoints, and measurement artifacts such as maturity indices and control coverage maps. These tools enable banks to progress from policy alignment toward demonstrable control effectiveness and, ultimately, from static compliance to continuous assurance. By linking governance frameworks with technical safeguards, this approach enhances resilience against evolving cyber threats while ensuring regulatory conformity and customer trust.

Keywords: Information Security Policy, Confidentiality, Privacy, Online Banking, Cyber Risk Management, ISO 27001, NIST CSF, Stride.

Introduction

Financial institutions are among the most targeted sectors for cyberattacks due to the sensitivity and value of customer data and transaction flows. While banks have long maintained formal Information Security Policies (ISPs), the critical challenge is ensuring these documents—covering confidentiality, privacy, identity verification, secure development, and network/email security—are both complete and continuously translated into effective controls across online-banking ecosystems. Without this alignment, ISPs risk becoming static guidelines rather than actionable frameworks for mitigating cyber risks [7, 8].

Recent research highlights three complementary needs for strengthening security in this domain. First, there is a demand for repeatable evaluation frameworks to assess whether confidentiality and privacy requirements in ISPs meet ISO/NIST expectations and to locate gaps that could expose institutions to

vulnerabilities. Second, sector-level evidence is essential to map the evolving risk landscape—including phishing, ransomware, insider threats, and regulatory non-compliance—and to demonstrate the benefits of robust information security programs, such as improved customer trust, AI-enabled fraud reduction, and operational stability. Third, integrated cyber-risk management approaches must be adopted for online channels. These approaches should combine threat identification, vulnerability cataloguing, risk scoring, and treatment planning, while considering cascading effects among interconnected security features [9, 10].

This paper proposes a unified methodology that connects policy evaluation with operational cyber-risk management for online banking. By bridging compliance assessment and proactive risk mitigation strategies, the framework aims to help financial institutions of varying sizes and maturity levels strengthen their security posture. Practical adoption guidelines are also provided to support implementation, ensuring that banks can effectively translate policy into action and maintain resilience against emerging cyber threats [11].

Related Work

Policy Evaluation Frameworks in Banking:

AL feel et al. developed and implemented a policy evaluation framework tailored for banking institutions, focusing on confidentiality and privacy requirements. The framework aligns with international standards such as ISO and NIST, enabling systematic assessment of compliance and security posture. Applied across multiple banks, the approach identified strengths and weaknesses in policy implementation and introduced automated reporting mechanisms. Their findings underscore the importance of periodic reviews—typically every 6 to 12 months—and the establishment of dedicated working groups to ensure continuous improvement in policy effectiveness.

Systematic Reviews of IS Policies and Practices

Ullah et al. conducted a comprehensive review of information security (IS) policies and practices within U.S. and global banking sectors. Their synthesis highlights key regulatory anchors, including the Gramm-Leach-Bliley Act (GLBA), and collaborative mechanisms such as the Cybersecurity and Infrastructure Security Agency (CISA) and the Financial Services Information Sharing and Analysis Centre (FS-ISAC). The study emphasizes the critical role of multi-factor authentication (MFA), the integration of AI/ML techniques for fraud detection and fostering a robust security culture as essential complements to formalized policy frameworks.

Integrated Cyber-Risk Management for Online Banking

Azura et al. proposed a holistic cyber-risk management framework for online banking environments. The model incorporates STRIDE-based threat modeling, OWASP and CWE vulnerability classifications, and ISO 27005-inspired risk matrices that combine likelihood and impact assessments. This integrated approach supports a recurring risk treatment cycle and accounts for cascading dependencies among security features such as encryption, authentication, and monitoring. Furthermore, the framework aligns with zero-trust principles, reinforcing resilience against evolving cyber threats.

Standard Sand Good Practices

International standards and best practices provide foundational guidance for banking cybersecurity. ISO/IEC 27001 and 27005 outline Information Security Management Systems (ISMS) and risk management processes, while the NIST Cybersecurity Framework (CSF) organizes activities into five core functions: Identify, Protect, Detect, Respond, and Recover. Additionally, OWASP Top 10 and CWE Top 25 catalog prevalent web and software vulnerabilities, and CIS Controls v8 offer prioritized safeguards for mitigating risks.

Methodology

This study integrates three complementary streams: (i) policy evaluation for confidentiality and privacy compliance, (ii) sector-level insights into information security (IS) policies, and (iii) technical cyber-risk management tailored for online banking. The unified approach unfolds across four iterative phases: (1) Policy Conformance Mapping, which benchmarks organizational policies against regulatory and industry standards; (2) Threat and Vulnerability Cataloguing, involving systematic identification of potential attack vectors and weaknesses; (3) Risk Assessment, applying likelihood–impact matrices to prioritize risks; and (4) Risk Treatment and Assurance, which develops mitigation strategies and validates control effectiveness. Each phase generates structured artifacts—such as compliance checklists, maturity indices, threat scenarios, and control-to-weakness mappings—that evolve through feedback loops. Risk quantification leverages standardized scoring models, while treatment planning incorporates coverage maps and remediation backlogs. Designed for scalability, the methodology supports banks at varying maturity levels and facilitates partial automation through tools like vulnerability scanners and Security Information and Event Management (SIEM) systems. Governance integration is achieved via policy committees and risk boards, ensuring alignment with strategic objectives and regulatory mandates.

Unified Model: From Policy to Controls and Risk Treatment

Policy Conformance and Maturity Index

Starting from the ISP corpus, we assess the presence, clarity, and recency of confidentiality/privacy provisions and related poli-

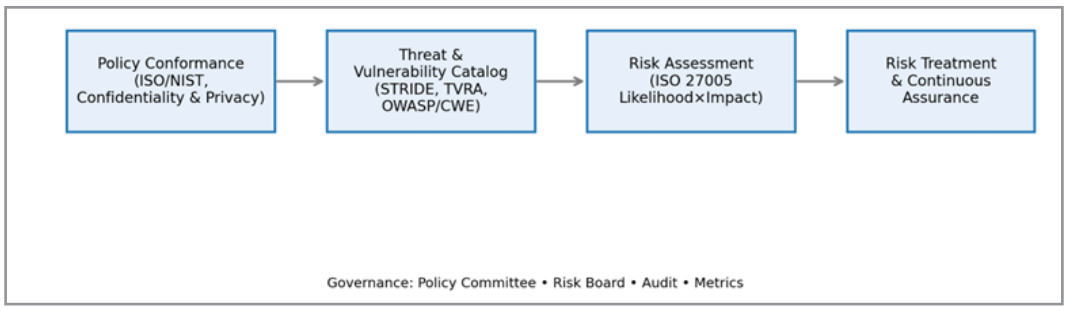

Figure 1: Unified workflow from policy conformance to continuous assurance.

Threat and Vulnerability Catalog for Online Banking

We construct threat scenarios using STRIDE/TVRA principles and categorize vulnerabilities using OWASP Top 10 (e.g., broken access control, injection) and CWE Top 25 (e.g., buffer overflows, improper authentication). Threat agents span bank environments, customer endpoints, and third-party providers (TPPs). Cascading effects among security features are explicitly modeled (e.g., certificate validation → authentication bypass → session hijacking).

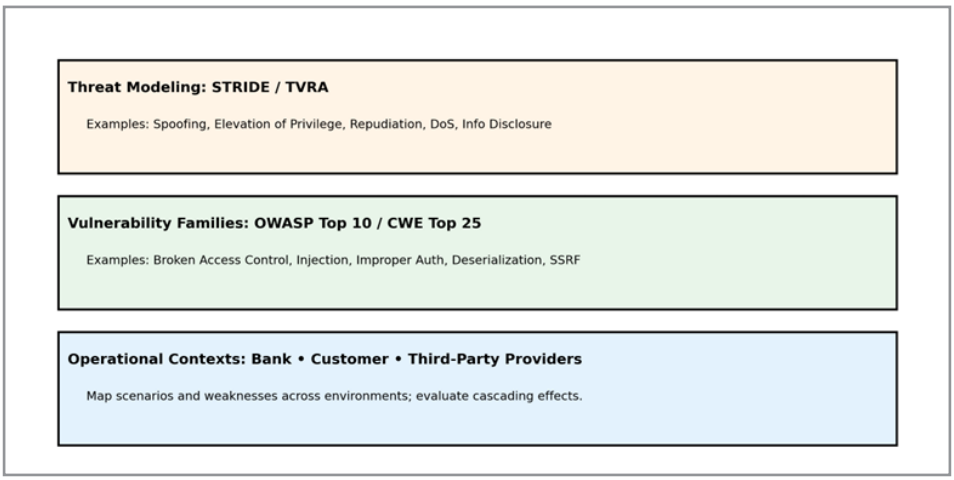

Figure 2: Layered mapping: threats, vulnerabilities, and operational contexts.

Risk Assessment Matrix

We score risk as a function of Likelihood and Impact (ISO 27005-style), yielding severity 0–8: Low (0–2), Medium (3–5), High (6–8).

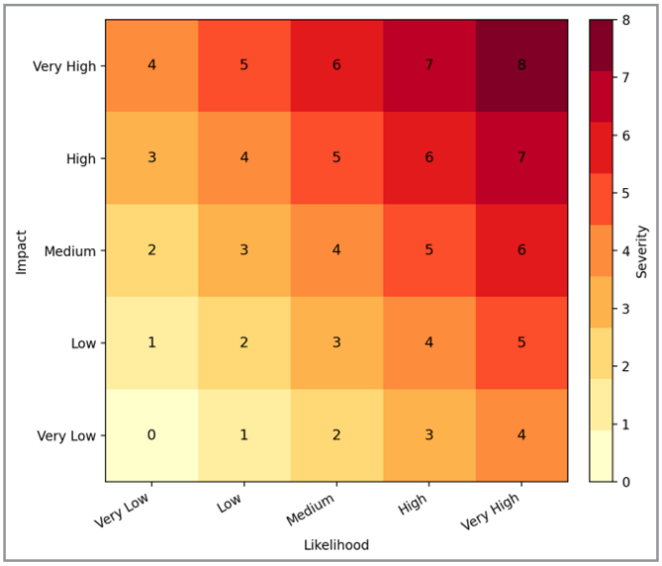

Figure 3: Risk assessment matrix (likelihood × impact) with severity scale.

Risk Treatment and Continuous Assurance

Risk treatment options include modification (hardening, patching, configuration review), avoidance, retention, and transfer (insurance). Pre-defined tasks accelerate response (code review, incident response, vulnerability scanning, penetration testing, IAM reviews, provider governance). Continuous assurance aligns monitoring (SIEM, SOAR), audits, and metrics to track control effectiveness and policy-to-control coverage.

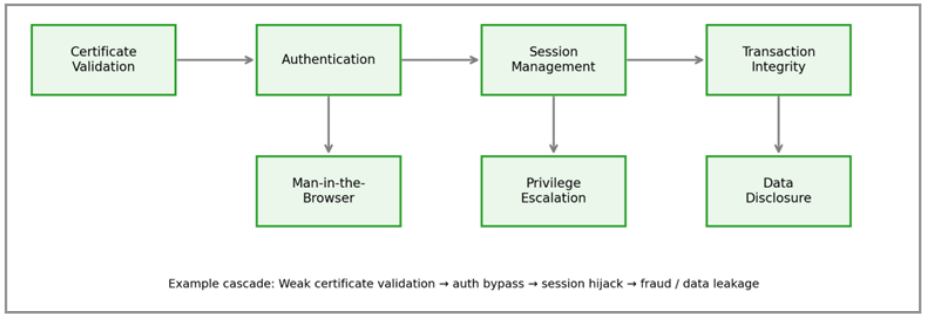

Figure 4: Example cascading effects among security features and attack scenarios.

Implementation Guidance

Governance: Establish an IS policy committee and a cyber risk board; define owners for confidentiality, privacy, and online-banking controls. Technology: Enforce MFA and adaptive authentication; validate certificates (PKI/CA); encrypt data in transit and at rest; instrument session monitoring. Process: Set review cadences (semiannual/annual); integrate third-party risk management; run red-team/pen tests; ensure patch and configuration hygiene. Culture: Conduct recurring security awareness for staff and customers; share intelligence via sector bodies (e.g., FS-ISAC).

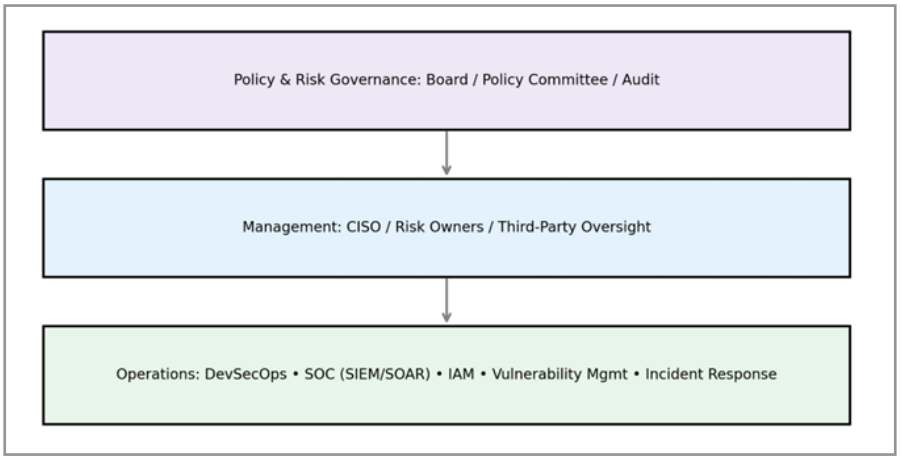

Figure 5: Governance operating model for policy–risk–operations alignment.

Evaluation and Case Insights

Policy Readiness Variability: Applied policy-evaluation results in prior work show confidentiality/privacy readiness ranging from ~65% to ~71% across banks, demonstrating benchmarking value and guiding remediation priorities. Threat/Vulnerability Coverage: Integrated frameworks improve detection of scenarios such as spoofing, privilege escalation, man-in-the-browser, and session hijacking, enabling targeted control tuning. Regulatory and Cultural Factors: Systematic reviews indicate that regulatory compliance (GLBA/PCI DSS) and coordinated threat intelligence (CISA/FS-ISAC) materially influence preparedness and response quality.

T Table 1: Comparative View of GLBA, PCI DSS, and ISO/NIST for Banking Cybersecurity Governance

Aspect	GLBA (Gramm Leach Bliley Act)	PCI DSS	ISO 27001 / NIST CSF
Jurisdiction & Type	U.S. federal financial privacy law	Global industry standard (card brands)	ISO 27001: international standard; NIST CSF: U.S. voluntary framework
Scope of Coverage	"Financial institutions" offering consumer financial products/services; covers customer personal financial information	Entities that store, process, or transmit payment card data (merchants, processors, issuers)	ISO 27001: any organization's Information Security Management System (ISMS) NIST CSF: cybersecurity risk across sectors
Applicability to Banks	Mandatory for U.S. banks, credit unions, lenders, insurers, etc.	Mandatory for any bank handling cardholder data, with compliance levels based on transaction volume	ISO 27001: voluntary but widely adopted globally by banks; NIST CSF: voluntary but endorsed by U.S. regulators (OCC uses it in exam programs)
Primary Objectives	• Financial Privacy Rule: disclosure/opt out of data sharing • Safeguards Rule: protect non-public personal information • Pretexting Rule: prevent social engineering	• Secure cardholder data • Prevent fraud • Maintain a baseline for data protection	ISO 27001: Establish/manage ISMS to ensure confidentiality, integrity, availability NIST CSF: Guided by five functions—Identify, Protect, Detect, Respond, Recover
Key Requirements	• Privacy notices • Risk assessments • Written safeguards program • Oversight, vendor management, training	• 12 core requirements: firewalls, config management, encryption, access control, vulnerability management, monitoring, security policies	ISO 27001: Risk assessment, security policies, asset management, access control, incident management, continual monitoring NIST CSF 2.0: Adds governance, supply chain risk; aligns to Identify–Recover lifecycle

Standards & Certification	Enforced by regulators (FTC, FFIEC, state agencies); no formal certification, but subject to audits and penalties	Validated via Self-Assessment Questionnaires, Qualified Security Assessors (QSAs), Approved Scanning Vendors (ASVs); non-compliance triggers fines, card brand penalties	ISO 27001: Certification by accredited audit bodies NIST CSF: No certification; implementation is audited by regulators/tools in examinations
Enforcement & Penalties	FTC/Regulator enforcement; fines, orders, reputational loss for non-compliance	Card brands/acquirers can impose fines up to hundreds of thousands per breach, plus suspension of processing privileges	ISO 27001: Certification failure leads to reputational risk but no legal mandate NIST CSF: Recommendations by OCC, FFIEC; non-adoption may lead to supervisory action
Best Fit Use Cases	U.S.-based banks handling consumer financial data, with focus on privacy and internal safeguards	Banks with significant card processing needs, issuance, merchant relationships	ISO 27001: Holistic ISMS framework; suitable for global/regional compliance synergy NIST CSF: Risk-based cybersecurity management; helpful for aligning to regulatory expectations
Unique Emphasis	Consumer privacy, disclosure and protection of non-public financial info, vendor oversight	Focused on payment data security, encryption, access, vulnerability management	ISO 27001: Continual improvement (PDCA), international alignment NIST CSF: Governance and supply chain risk, sector-specific tailoring

Summary and Applicability

- GLBA is essential for U.S. financial institutions focusing on customer privacy, with regulation-driven compliance programs.
- PCI DSS is critical for banks in the payment card ecosystem, enforcing strict, transactional data-focused controls.
- ISO 27001 and NIST CSF serve as complementary frameworks offering broad information security management:
- ISO 27001 is a global certification targeting organizational risk management and security.
- NIST CSF provides a flexible, sector-aligned model, increasingly mandated by U.S. financial regulators.

Discussion

Bridging Policy and Practice: The unified model ensures that policy statements drive concrete control implementations and that control telemetry feeds continuous policy improvement. Cascading Effects: Modeling dependencies among security features helps anticipate compound failures (e.g., certificate weaknesses enabling authentication bypass). Adoption Challenges: Smaller banks may face resource constraints; prioritization via risk scoring and use of shared services (managed detection/response) can mitigate. Limitations: This synthesis relies on published studies and standards; institution-specific constraints (legacy systems, undisclosed vulnerabilities) may require tailored adjustments [11-13].

Conclusion

We present a unified approach that connects policy evaluation for confidentiality/privacy with integrated cyber-risk management for online banking. By aligning ISP conformance to ISO/NIST, structuring threat/vulnerability catalogs with OWASP/CWE, and operationalizing risk scoring and treatment cycles, banks can move from static compliance to continuous assurance. Future work includes automating artifact generation (risk matrices, coverage maps), enriching sector-specific threat intelligence, and validating outcomes via longitudinal studies [14, 15].

References

1. Alfeel, M. I., Alhalangy, A., Mohamed, A. O. Y., & Abdalaa, O. M. (2025). Designing a Framework for Evaluating Information Security Policies for Banking Institutions. International Journal of Environmental Sciences. 11: 310-321.
2. Ullah, M. W., Alam, M. T., Sultana, T., Rahman, M. M., Faraji, M. R., & Ahmed, M. F. (2024). A Systematic Review on Information Security Policies in the USA Banking System and Global Banking: Risks, Rewards, and Future Trends. Edelweiss Applied Science and Technology. 8: 8437-8453.
3. Azura, Y. T. Y., Azad, M. A., & Ahmed, Y. (2025). An Integrated Cyber Security Risk Management Framework for Online Banking Systems. Journal of Banking and Financial Technology. 9: 85-104.
4. International Organization for Standardization. (2024). ISO/IEC 27001:2013—Information security management systems (2022 update). ISO.
5. National Institute of Standards and Technology. (2012). Guide for conducting risk assessments (NIST Special Publication 800-30 Rev. 1). U.S. Department of Commerce.
6. OWASP Foundation. (2023). OWASP API security top 10. OWASP.
7. Federal Trade Commission. (2024). Safeguards rule amendments: Gramm-Leach-Bliley Act compliance. FTC.
8. Kaspersky. (2024). Financial cybersecurity report. Kaspersky Lab.
9. PCI Security Standards Council. (2025). Payment Card Industry data security standard: Version 4.0.1 (PCI DSS v4.0.1). PCI SSC.
10. International Organization for Standardization. (2013). ISO/IEC 27001:2013—Information security management

systems—Requirements. ISO.
11. International Organization for Standardization. (2018). ISO/IEC 27005:2018—Information security risk management. ISO.
12. National Institute of Standards and Technology. (2018). Framework for improving critical infrastructure cybersecurity (NIST Cybersecurity Framework). U.S. Department of Commerce.
13. OWASP Foundation. (2021). OWASP top 10: The ten most critical web application security risks. OWASP.
14. MITRE. (2022). CWE top 25 most dangerous software weaknesses. MITRE Corporation.
15. Center for Internet Security. (2021). CIS critical security controls v8. CIS.