

Assessing the Impact of Third-Party Technology Dependencies on Cybersecurity Resilience and Quantum Readiness in Digital Banking Infrastructure

Timothy Olatunji Ogundola [1*], Bridget O Waheed [2], Onuh Matthew Ijiga [3], Kofoworola Idowu [4]
[1] Department of Technology Management, University of Bridgeport, Bridgeport Connecticut, USA
[2] Department of Computer Science, University of Lagos, Lagos
[3] Department of Physics Joseph Sarwan Tarka University, Makurdi, Benue State, Nigeria
[4] Department of Computer Science and Engineering, Yeshiva University, NewYork, USA

* Corresponding Author: **Timothy Olatunji Ogundola**

Article Info

ISSN (Online): 3107-6580
Volume: 02
Issue: 06
Received: 08-09-2026
Accepted: 06-10-2026
Published: 04-11-2026
Page No: 38-51

Abstract
Digital banking services increasingly rely on external cloud platforms, payment processors, identity services, software libraries, and cryptographic providers. These dependencies can improve scalability and service integration, while creating shared points of failure, supply-chain exposure, and barriers to cryptographic transition. This study assesses how third-party technology dependencies influence cybersecurity resilience and quantum readiness in digital banking infrastructure. It proposes a dependency-based evaluation that maps critical banking services to external providers, software components, APIs, and cryptographic assets. The assessment examines provider concentration, dependency criticality, incident propagation, recovery capacity, and vendor assurance alongside cryptographic inventory, post-quantum support, crypto-agility, and migration planning. Scenario analysis is used to compare service behaviour under provider disruption, compromise of a shared technology component, and post-quantum migration constraints. Resilience is evaluated through service availability, recovery time, and continuity of critical transactions; quantum readiness is evaluated through the visibility and replaceability of cryptographic mechanisms and the preparedness of external providers. The framework is intended to identify dependencies that could undermine continuity or delay cryptographic transition, and to support prioritization of vendor governance, resilience testing, and phased post-quantum migration. Empirical conclusions will depend on the infrastructure data and test results applied in the assessment.

DOI: https://doi.org/10.54660/.IJECA.2026.2.6.38-51

Keywords: Digital banking, third-party dependencies, cybersecurity resilience, quantum readiness, post-quantum cryptography

1. Introduction

1.1. Background to Digital Banking Infrastructure and Third-Party Technology Dependence

Digital banking infrastructure now functions as an integrated service environment in which mobile and web applications, API gateways, identity services, payment engines, data platforms, cloud hosting, and cryptographic controls jointly support customer transactions. This architecture allows banks to scale services and connect with fintech firms, payment networks, and correspondent institutions. It also means that a banking service may depend on technologies the bank neither owns nor directly operates. Cloud computing can improve some aspects of banking performance while also changing operational risk exposure, so adoption should be assessed in relation to service criticality, architecture, and control arrangements rather than treated as a purely technical procurement choice (Cheng *et al*., 2022) [15]. Research on bank digital platforms likewise describes how

third-party developers and partner services contribute to digital service ecosystems, extending the operational boundary beyond the institution's internal systems (Schreieck *et al*., 2024) [49].

For this study, third-party technology dependence is the reliance of a critical banking service on an external provider, product, or service component, including dependencies inherited through subcontractors and software libraries. For example, a bank's payment API may rely on a cloud-hosted container platform, an external identity service, a managed database, and a vendor-maintained cryptographic library. A failure or compromise in one component can affect service availability, transaction integrity, or the confidentiality of data moving across the dependency chain. Cloud-native financial reporting research illustrates how data processing and service delivery increasingly depend on interconnected architecture choices (Aluso *et al*., 2024) [7], while work on cloud-native systems highlights the importance of scalability and resource management in those architectures (Nwatuzie, 2026) [40]. Accordingly, the paper treats the banking environment as a dependency graph: critical services are mapped to applications, providers, software and data services, and cryptographic assets. This mapping provides the basis for assessing how dependency concentration and limited visibility may influence cybersecurity resilience and quantum readiness.

1.2. Cybersecurity Resilience Challenges in Interconnected Banking Services

Cybersecurity resilience in digital banking concerns the capacity to anticipate, withstand, contain, recover from, and adapt to cyber incidents while maintaining critical services. Its technical requirements extend beyond perimeter protection because banking transactions traverse APIs, identity providers, payment processors, cloud environments, and interbank networks. A compromised credential, unavailable cloud region, malicious software update, or disrupted payment intermediary can therefore affect several institutions or services at once. Modeling of wholesale payment networks shows that cyber incidents can propagate through financial connections, with third-party providers creating additional channels for disruption (Eisenbach *et al*., 2022) [20]. A systematic review of FinTech threats similarly identifies multiple technical and human attack pathways, supporting a resilience approach that combines prevention, detection, response, and recovery rather than relying on a single safeguard (Javaheri *et al*., 2024) [36].

In this paper, resilience is assessed through service continuity, time to detect and contain an incident, recovery time, integrity of transactions, and the ability to sustain essential operations under provider disruption. For example, if an identity provider becomes unavailable, the relevant question is not only whether authentication is secure, but whether the bank can safely fail over, constrain high-risk transactions, and restore trusted access without creating a wider outage. Provider dependencies may also amplify an incident when a shared vendor supports multiple institutions. The study therefore maps dependency paths and evaluates scenarios that include provider outage, software compromise, credential abuse, and degraded recovery capacity. The reference pool's work on cybersecurity risk assessment and adversarial detection is relevant to the study's detection dimension (Ijiga *et al*., 2024) [31], while its research on social-engineering controls reinforces the importance of human-enabled attack pathways in financial institutions (Ayoola *et al*., 2024) [9]. The analysis treats these controls as components of a coordinated resilience capability, not as substitutes for architectural and supplier-level safeguards.

1.3. Quantum Computing Risks and the Need for Cryptographic Readiness

Digital banking uses public-key cryptography for functions such as API authentication, certificate validation, digital signatures, and key establishment. A sufficiently capable cryptographically relevant quantum computer could undermine widely deployed public-key schemes based on integer factorization and discrete logarithms. This creates two distinct concerns: stored or intercepted encrypted information may become readable in the future, and digital signatures or certificate-based trust mechanisms may eventually be forgeable if their underlying algorithms are broken. The timing of such capability remains uncertain, but the migration task is already operationally significant. A widely cited analysis describes post-quantum migration as a multiyear organizational transition involving security, performance, implementation, and compliance constraints (Joseph *et al*., 2022) [37]. Quantum-algorithm research further examines the computational assumptions underlying both classical and candidate post-quantum cryptosystems, which is essential to interpreting risk without overstating near-term capability (Biasse *et al*., 2023) [14].

Quantum readiness in this study means the capacity to identify, prioritize, test, and replace cryptographic mechanisms across banking services and their third-party dependencies. It includes a cryptographic inventory; identification of algorithm use in API gateways, certificates, hardware security modules, and vendor products; prioritization based on data confidentiality lifetime and service criticality; and testing for interoperability and performance. A hybrid key-establishment approach, for instance, can combine a classical secret with a post-quantum secret during transition, but it requires careful protocol design, implementation review, and partner support. The reference pool's work on quantum cryptography in financial transactions and quantum-resistant communication protocols provides adjacent perspectives on securing connected systems (Ajayi *et al*., 2024; Idika, 2023) [1, 27]. This paper distinguishes readiness from algorithm adoption alone: a bank that selects a post-quantum algorithm but cannot inventory its deployed certificates, update supplier software, or coordinate with interbank partners remains exposed to migration gaps. The assessment therefore examines cryptographic agility and supplier preparedness alongside resilience measures.

1.4. Research Problem, Aim, and Objectives

The research problem is that digital banking risk is often assessed in separate domains: cybersecurity resilience is evaluated through incident controls and continuity plans, while quantum readiness is evaluated through cryptographic inventories or algorithm-transition plans. This separation can obscure how external technology dependencies connect the two. A bank may, for example, maintain strong internal recovery procedures but rely on a cloud identity provider whose cryptographic transition schedule is unknown. Conversely, a post-quantum-capable API gateway may still be constrained by legacy certificates, software libraries, or interbank partners. Existing work on cybersecurity detection

and cryptographic transition illustrates the relevance of both domains, but the study focuses on their interaction through shared service dependencies.

The aim is to assess how third-party technology dependencies influence cybersecurity resilience and quantum readiness in digital banking infrastructure. The objectives are to map critical banking services to direct and inherited dependencies; evaluate dependency criticality, concentration, and recovery options; assess resilience capabilities under provider, software, and cyberattack scenarios; and measure cryptographic readiness through inventory coverage, crypto-agility, and supplier transition support. Hybrid cryptographic approaches are considered as migration options, not assumed to be secure by virtue of combining algorithms alone. The central research question is how dependency visibility and concentration affect continuity and post-quantum transition readiness. The study also asks which dependency indicators best identify priority services and providers for resilience testing and phased cryptographic migration.

1.5. Significance, Scope, and Organization of the Paper

This study is significant because it brings operational resilience and quantum migration into a shared dependency-based assessment. Its service-level perspective can help banks identify where a provider outage, compromised software component, or unsupported cryptographic function could affect customer access, payment execution, or interbank exchange. It also supports more targeted governance: institutions can prioritize assurance and testing according to the services and dependency paths with the greatest potential impact. Research on cloud outsourcing highlights the role of internal governance in managing bank-provider arrangements, while studies of digital financial partnerships describe the multiple organizations involved in service delivery. The paper's scope is technical and organizational: it considers digital banking applications, APIs, cloud and software services, external providers, and cryptographic assets.

The analysis does not claim that all third-party services create equivalent risk, nor does it predict when a cryptographically relevant quantum computer will become available. Instead, it evaluates dependency exposure and readiness indicators under defined scenarios, with results interpreted according to the study's stated model and data. Cross-border payment and digital-asset activity underscores why interoperability and shared trust mechanisms matter beyond a single institution's perimeter; privacy-preserving identity approaches further illustrate the range of cryptographic functions that financial applications may depend on. The paper is organized into five sections: the introduction frames the problem and objectives; the literature review examines banking dependencies, resilience, supply-chain risk, and quantum threats; the system model describes dependency mapping and assessment procedures; the results and discussion evaluate scenario outcomes; and the final section presents conclusions and recommendations.

2. Literature Review

2.1. Digital Banking Infrastructure and Third-Party Dependencies

Digital banking is best understood as a service architecture rather than a collection of stand-alone applications. Customer channels, API gateways, identity and access management, payment processing, data platforms, cloud infrastructure, and cryptographic services must work together to complete a transaction. Banks increasingly connect these internal systems to external cloud providers, payment processors, fintech partners, telecommunications networks, and software vendors. This creates an ecosystem in which a bank's operational boundary may extend beyond assets it directly administers. Mapping banking's cloud relationships illustrates how infrastructure and service delivery can depend on a concentrated group of technology firms (Bassens *et al*., 2024) [13]. Research on third-party payment platforms also shows that operational risk can arise within externally operated financial services, making provider controls relevant to the bank's own risk picture (Yao & Li, 2022) [51]. For this study, dependencies are represented as directed links between a critical service and the technology components required to deliver it. A retail payment API, for example, may depend on an API gateway, a cloud-hosted application, a managed database, a third-party identity service, and a certificate authority. Dependencies can be direct, such as a bank contracting with a cloud provider, or inherited, such as an application relying on an open-source library maintained by another party. Serverless and microservice architectures can improve scalability and support interoperability, while also increasing the number of components whose availability and configuration affect service continuity (Uzoma *et al*., 2024; Frank, 2026) [22, 50]. Data centers provide foundational compute and storage capacity for digital financial activity (Igba *et al*., 2025) [30], while cloud environments may face availability threats such as denial-of-service attacks (Idoko *et al*., 2024; Bamidele, *et al*., 2026) [10, 28]. The study therefore maps providers, applications, data services, and cryptographic assets against essential banking services to identify concentration, propagation paths, and readiness gaps.

2.2. Cybersecurity Resilience in Interconnected Financial Services

Cybersecurity resilience in interconnected finance is the capacity to sustain or restore important services when systems are attacked, fail, or become inaccessible. For banks, this requires more than preventing intrusion: controls must also limit incident propagation, preserve transaction integrity, maintain critical payment functions, and support timely recovery. Network-based research on cyber resilience emphasizes that both network topology and the strength of links influence how shocks propagate through interbank systems (Cerqueti *et al*., 2022). Cyber incidents also differ from conventional operational disruptions because their effects can evolve dynamically and may not be captured adequately by historical loss measures alone (Peihani, 2022; Frank, 2026; Ogundola, 2022) [22, 43, 48]. Thus, resilience assessment needs to consider dependencies and plausible disruption pathways, rather than only count controls or past incidents.

The study operationalizes resilience through service availability, incident detection and containment, transaction integrity, recovery time, and the ability to continue essential operations during a provider disruption. A scenario might disable an external identity provider during peak payment activity; assessment would examine whether the bank can

safely invoke an alternate authentication path, restrict high-risk transactions, and restore normal service without accepting forged credentials (Ogundola, 2024; Ogundola, 2025) [44, 45]. Network simulation and "artificial lab" approaches offer ways to examine how topology-focused and security-focused interventions affect cyber contagion, although modeled results depend on the assumptions and data used (Awiszus *et al*., 2024) [8]. The analysis also considers security operations such as adaptive detection, policy orchestration, and fraud controls. The reference pool's work on reinforcement learning in financial networks and real-time policy orchestration informs these control dimensions (Michael *et al*., 2024; James *et al*., 2025) [34, 38], while research on anti-fraud architecture highlights the need to connect fraud prevention with service continuity (Onyekaonwu, 2025; Doe Gadekah, & Enyejo, 2026) [19, 47]. Resilience is therefore treated as a system property, dependent on coordinated bank, provider, and interbank capabilities.

2.3. Third-Party and Software Supply-Chain Risk in Banking

Third-party risk in banking includes risks arising from vendors, subcontractors, cloud platforms, managed services, software products, and open-source components used to deliver or secure financial services. Software supply-chain exposure is especially important because an institution may trust a product without directly observing how its components were developed, built, signed, distributed, and updated. A compromised software vendor can affect many downstream organizations through shared update mechanisms or widely deployed dependencies. Empirical analysis of supply-chain cyberattacks has documented effects that extend from directly targeted firms to connected customers, demonstrating why supplier security can matter to organizations that were not initially attacked (Crosignani *et al*., 2023; Doe Gadekah, & Enyejo, 2025) [16, 17]. Broader digital supply-chain reviews classify attack surfaces across actors and stages, reinforcing the need to examine the complete chain rather than only the immediate contractor (Hammi *et al*., 2023) [26].

In banking, practical exposure includes vulnerable dependencies in API software, compromised build pipelines, unsupported libraries in payment services, and privileged vendor access to production environments. Assessment should therefore combine a service dependency map with evidence about software provenance, component inventories, vulnerability disclosure, code-signing practices, patch latency, subcontractor visibility, and tested exit or continuity arrangements. The study distinguishes provider concentration risk from component-level supply-chain risk: multiple banks may use different vendors yet share the same widely deployed library, while a single cloud provider may create correlated availability risk across many services. The reference pool's work on resilient supply chains and cybersecurity in critical infrastructure contributes context on disruption planning and technology-related dependency exposure (Enyejo *et al*., 2024; Okika *et al*., 2025) [21, 46]. Its blockchain and homomorphic-encryption study points to integrity and confidentiality controls in supply-chain contexts, but these tools do not replace provenance validation or vendor assurance (Akindote *et al*., 2024) [3]. The model accordingly prioritizes dependencies by criticality, exposure, concentration, and recovery feasibility.

2.4. Quantum Computing Threats and Post-Quantum Readiness

Quantum computing matters to banking because public-key cryptography supports key establishment, digital signatures, certificate chains, and authenticated API connections. A sufficiently capable cryptographically relevant quantum computer could threaten public-key schemes based on integer factorization or discrete logarithms. The "harvest now, decrypt later" risk is particularly relevant to financial records whose confidentiality must last for years: an adversary could retain encrypted traffic now and attempt decryption later (Akinleye, & Ijiga, 2025; Ijiga, & Akinleye, 2024) [4, 31]. Quantum risk is not a prediction of when a particular machine will be available; it is a reason to plan for a transition whose complexity spans systems, vendors, certificates, and financial partners. Recent enterprise-cloud readiness work treats confidentiality exposure and authentication or integrity risk as distinct transition concerns, and recommends incorporating migration time into exposure assessment (Gupta & Mittal, 2026; Bamilede *et al*., 2025) [25].

Post-quantum readiness therefore requires cryptographic inventory, risk-based prioritization, crypto-agile design, supplier transition commitments, interoperability tests, and staged deployment. Hybrid key establishment can combine classical and post-quantum mechanisms during transition, but the protocol's combiner, certificate handling, handshake size, and fallback behavior require verification as seen in Table1. Performance studies of post-quantum TLS provide a basis for evaluating latency and data overhead under different configurations, rather than assuming that quantum resistance has no operational cost (Montenegro *et al*., 2026) [39]. The reference pool includes work addressing quantum technologies in financial transactions and computational developments (Ajayi *et al*., 2024; Idoko *et al*., 2024) [1, 28]. It also includes a cloud-encryption proposal combining AES, DES, and RC6 (Nwatuzie *et al*., 2025; Abolade, *et al*, 2024) [2, 41]; because these are symmetric algorithms, that design should not be treated as a post-quantum replacement for vulnerable public-key authentication or key establishment. This distinction is central to the paper's assessment: cryptographic readiness is measured by function-level inventory and transition capability, not by the presence of encryption alone.

Table 1: Quantum Threats and Post-Quantum Readiness in Banking

Dimension	Threat or readiness issue	Banking implication	Assessment or response
Public-key cryptography	A sufficiently capable quantum computer could threaten schemes based on integer factorization or discrete logarithms	Key establishment, digital signatures, certificate chains, and authenticated API connections could be affected	Inventory algorithms and cryptographic functions across banking services
Long-lived confidentiality	Encrypted financial traffic may be collected now and targeted for decryption later	Sensitive records and interbank data may remain exposed beyond their immediate transaction period	Prioritize data by confidentiality lifetime and migration lead time
Authentication and integrity	Signature and certificate mechanisms face risks distinct from key-establishment risks	Forged signatures or weakened certificate trust could undermine transaction authenticity	Assess key establishment, signatures, certificates, and API authentication separately
Hybrid transition	Classical and post-quantum mechanisms may be combined during migration	Handshake size, latency, certificate handling, protocol compatibility, and fallback behavior may affect service performance	Test the combiner, interoperability, failure handling, and performance under representative workloads
Organizational readiness	Banks and suppliers may lack complete inventories, crypto-agile systems, or migration commitments	Unmapped components and unprepared vendors can delay coordinated transition	Establish cryptographic inventories, supplier roadmaps, staged deployment plans, and partner testing
Encryption scope	Symmetric encryption alone does not replace vulnerable public-key authentication or key establishment	A system may use encryption yet remain unprepared for quantum-related public-key risks	Evaluate readiness by cryptographic function and transition capability, not by encryption presence alone

3. System Model Description

3.1. Digital Banking Dependency Architecture and Critical Service Mapping

The infrastructure is represented as a directed, typed graph $G = (V, E, \tau, \omega)$, where V partitions into S (services), A (applications/APIs), P (providers), D (software/data), and C (cryptographic assets); E records a dependency from a service or component to a required component; τ assigns each node its class; and ω records its normalized service-impact weight. This graph representation makes direct and inherited dependencies visible. It follows the network-mapping logic used to examine banks' relationships with cloud and technology firms (Bassens *et al*., 2024) [13]. A retail payment service, for example, can depend on an API gateway, cloud runtime, token service, transaction database, HSM, certificate authority, and a vendor-managed software library as seen in Table 2. The model records ownership, hosting region, data sensitivity, recovery target, cryptographic function, and evidence date for each node.

$$G = (V, E, \tau, \omega) \quad (1)$$

Critical-service mapping begins with business impact analysis: services are ranked by customer, settlement, regulatory, and time-critical effects. Let s denote a service and i a dependency. Reachability P_{si} equals one when at least one directed path connects s to i, including paths through subcontractors or embedded software; otherwise it is zero. This prevents a tier-one provider from appearing low risk merely because it is several architectural layers away. The mapping is versioned so that ownership changes, new API integrations, or cryptographic-library updates can be compared over time. Service records should be reconciled against architecture diagrams, procurement registers, CMDB/SBOM data, and provider attestations. Missing links are retained as unknowns rather than treated as evidence of independence.

A service owner validates each critical path with engineering and supplier-management records during reviews. The resulting register supports traceable change-impact analysis when a provider, API, library, region, or cryptographic endpoint changes.

Ambiguous edges are assigned confidence labels and verified before the graph is used for risk scoring or prioritization. Refresh maps after releases and outsourcing changes.

$$P_{s,i} = 1 \; if \; s \; reaches \; i; \; 0 \; otherwise \quad (2)$$

Table 2: Critical service dependency register schema

Service	Direct dependency path	Inherited components	Critical evidence fields
Retail payment API	API gateway → payment service → cloud runtime	Identity SDK; database driver; TLS library	RTO/RPO; data class; provider; crypto role
Interbank transfer	Message gateway → validation → settlement interface	Signing library; queue service; HSM firmware	Settlement window; certificate owner; failover
Customer authentication	Identity service → token issuer → fraud engine	MFA SDK; key store; risk-scoring service	Credential sensitivity; recovery path; vendor SLA
Ledger and records	Core ledger → database → backup/storage	Encryption library; cloud control plane	Retention; integrity checks; key lifecycle

3.2. Dependency Criticality, Concentration, and Risk Indicators

Dependency criticality is calculated across all mapped services, not from a vendor's contract value alone. Let w_s be service s's normalized impact weight, with $\Sigma_s w_s = 1$, and let $\rho_i \in [0,1]$ denote the tested substitutability of dependency i, where one means a proven equivalent alternative is available within the recovery objective. The criticality score C_i therefore increases when a dependency supports high-impact services through several direct or inherited paths and

decreases only when an alternative has been demonstrated. A dependency with no tested replacement receives $\rho_i = 0$. Risk indicators are separately normalized to [0,1]: exposure e_i, exploitable vulnerability v_i, and recovery deficit u_i. Their weights λ_1–λ_3 are preregistered and sum to one, preventing post hoc tuning to desired results.

$$C_i = \sum_{s \in S} w_s P_{s,i} [1 - \rho_i] \quad (3)$$

$$HHI_k = \sum_{p \in P} share_{p,k}^2 \quad (4)$$

$$RI_i = C_i [\lambda_1 e_i + \lambda_2 v_i + \lambda_3 u_i] \quad (5)$$

Concentration is measured per technology function k, such as cloud compute, identity, payment processing, or certificate issuance. Here x_{pk} is provider p's weighted dependency count in function k, and $share_{p,k}$ is p's fraction of the total x across providers q. HHI_k ranges from $1/n$ for n equally used providers to 1 for complete reliance on one provider. The risk indicator RI_i combines criticality with exposure and control weakness; it is a prioritization index, not an incident probability as seen in Table 3. Teams should retain component values beside the composite score so a high score can be traced to a path, vulnerability, or recovery gap. Provider concentration must also be reviewed across institutions when shared services are documented, because institution-level diversification may conceal system-wide common exposure.

For comparability, the share basis must remain fixed across functions, and raw HHI should be reported with provider count. The indicator describes structural concentration; it does not estimate the likelihood that a provider will fail.

Sensitivity analysis varies λ weights and substitution assumptions to test ranking stability under uncertainty across plausible scenarios.

Report ranges with each priority ranking.

Table 3: Dependency risk indicator definitions

Indicator	Operational definition	Scale	Use in assessment
C_i	Service-weighted reachability adjusted for substitutability	0–1	Rank dependencies by service consequence
HHI_k	Sum of squared provider shares for function k	1/n–1	Identify reliance concentration
e_i	External reach, privilege, and data-access exposure	0–1	Represent attack surface
v_i	Evidence-weighted exploitable weakness score	0–1	Represent technical susceptibility
u_i	Normalized gap between observed and target recovery	0–1	Represent continuity weakness
RI_i	Criticality multiplied by weighted risk indicators	0–1	Set assurance and testing priority

3.3. Cybersecurity Resilience and Quantum Readiness Measures

Resilience is measured at service level during a defined observation window T. Let d_s be the time service s is unavailable or below its minimum transaction threshold; availability A_s equals one minus d_s/T, bounded to [0,1]. The resilience score aggregates service availability with integrity assurance, incident detection and containment, and recovery performance. Component weights γ_j are declared before scenario execution and sum to one. For comparability, all inputs are scaled to [0,1], where larger values indicate stronger capability. Recovery time is measured from disruption onset to verified restoration; recovery-point performance records transaction or data loss against the approved tolerance. The method distinguishes preventive controls from demonstrated recovery: a policy or vendor statement alone does not count as a successful failover test.

$$A_s = max(0, 1 - \frac{d_s}{T}) \quad (6)$$

$$Res = \sum_{j \in J} \gamma_j m_j \quad (7)$$

$$\Delta L\% = 100 \times \frac{(L_{PQ} - L_{cl})}{L_{cl}} \quad (8)$$

Quantum readiness is measured as a capability vector covering cryptographic inventory completeness *I*, quantum-vulnerable asset coverage *C*, crypto-agility *A*, supplier transition evidence *V*, and interoperability test completion *J* as seen in Table 4. Each component is normalized against an explicit denominator: for example, *I* is inventoried cryptographic use points divided by the total discovered use points, while *C* is the proportion of identified vulnerable uses with an approved migration treatment. *Q* aggregates *I*, *C*, *A*, *V*, and *J* with normalized weights β_i and is reported beside each component to expose gaps masked by an average. Hybrid or post-quantum handshake latency L^{PQ} is compared with classical latency L^{cl} under the same workload; the percentage overhead $\Delta L\%$ is not a security score. This distinction follows cloud-transition work that treats inventory, migration timing, and algorithm transition as operational readiness tasks (Gupta & Mittal, 2026) [25].

KEM readiness and signature readiness are recorded separately because key establishment and authentication protect different protocol functions. Vendor evidence must identify supported algorithms, versions, rollout windows, and tested rollback behavior before deployment in production systems.

Performance comparisons use identical concurrency and payload sizes.

$$Q = \sum_{i \in \{I,C,A,V,J\}} \beta_i r_i ; \sum_{i \in \{I,C,A,V,J\}} \beta_i = 1 \quad (9)$$

Table 4: Resilience and post-quantum readiness measures

Dimension	Measure	Evidence source	Interpretive direction
Continuity	A_s; service availability within T	Telemetry and test logs	Higher is stronger
Recovery	Observed recovery time / approved target	Exercise records; failover logs	Lower ratio is stronger
Cryptographic inventory	I = recorded / discovered use points	Code scan; CMDB; certificates	Higher coverage is stronger
Supplier readiness	V = critical suppliers with dated migration evidence / total	Contracts; vendor attestations; tests	Higher coverage is stronger
Performance impact	ΔL%; matched classical and PQ/hybrid runs	Controlled load-test telemetry	Report overhead, not security

3.4. Scenario Design and Assessment Procedure

The assessment uses a baseline and controlled stress scenarios applied to the same dependency graph and service weights. The baseline records normal service telemetry and cryptographic configuration. Stress cases include: loss of a concentrated cloud or identity provider; compromise of a signed software update or shared library; outage of an interbank message route; and migration of API key establishment and signatures to a hybrid or post-quantum profile. A combined case applies provider disruption while migration is underway. For each case, the team declares the affected node set, disruption duration or probability model, recovery assumptions, transaction load, and whether failover is permitted. Assumptions are version-controlled and separated from observed data. This procedure prevents illustrative scenario inputs from being reported as measured banking outcomes.

$$Y_s(\omega) = \sum_{k \in K} w_k[1 - A_k(\omega)] \quad (10)$$

For scenario ω, $Y_s(\omega)$ is the weighted service-impact score: w_k is the predeclared importance of critical service k, and $A_k(\omega)$ is its measured or simulated availability. Runs use paired baseline and stress inputs so changes can be attributed to the perturbation rather than to different service mixes. If Monte Carlo sampling is used for uncertain outage duration or exploit occurrence, the number of replications M and input distributions are documented; expected impact is the mean across runs and tail impact is the 95th percentile. The procedure is: validate the inventory; calculate C_i and HHI_k; score baseline resilience and readiness; execute scenarios; compute service impact, recovery time, and PQC latency overhead; then perform sensitivity analysis on provider substitution, control weights, and recovery assumptions. No simulation outputs are asserted here because no run data were supplied; Section 4 should report only reproducible results generated from the stated configuration.

$$E[Y] = \frac{\sum_{m=1}^{M} Y^m}{M}; \; VaR_{0.95}(Y) = Q_{0.95}(Y) \quad (11)$$

Each run stores its configuration hash, input version, random seed, software versions, and raw metric outputs so that another analyst can reproduce the comparison consistently as seen in Table 5.
Archive logs and versions for independent verification.

Table 5: Scenario matrix and recorded outputs

Scenario	Perturbation	Primary outputs	Status of values
Baseline	Normal provider and cryptographic configuration	Availability; throughput; latency; inventory coverage	Recorded when baseline run executes
Provider outage	Disable one critical cloud, identity, or payment node	Affected services; recovery time; concentration impact	Controlled scenario input
Software supply chain	Revoke or quarantine a compromised update/library	Propagation paths; integrity failures; containment time	Controlled scenario input
Hybrid/PQ transition	Replace selected KEM/signature profile under matched load	Handshake latency; bytes; throughput; interoperability	Measured only after execution
Combined stress	Provider disruption during cryptographic migration	Service impact; recovery; readiness bottlenecks	No outcome assumed

4. Discussion of Results

4.1. Effects of Third-Party Dependencies on Banking Service Resilience

Digital banking service resilience depends on whether critical functions can continue when a cloud, identity, payment, software, or cryptographic provider becomes unavailable or compromised. The dependency graph links each customer-facing service to direct and inherited components; therefore, disruption at a shared provider can affect several services at once. The assessment compares five methods using the same service weights and scenario definitions: dependency-weighted scoring, PageRank, betweenness centrality, failure mode and effects analysis (FMEA), and Monte Carlo propagation. Table 6 reports the illustrative method outputs. Under maximum stress, resilience scores range from 27 for Monte Carlo propagation to 40 for FMEA, while the estimated 95th-percentile recovery interval ranges from 23 to 36 hours. These values are scenario demonstrations, not observed bank results. The differences show why service owners should examine both exposure and restoration performance rather than rely on a single composite risk score. Resilience testing should include transaction integrity, queue recovery, authentication continuity, and reconciliation after failover. The exercise should record degraded service thresholds, recovery time, data loss, and customer impact. Third-party events can propagate through shared providers, so recovery evidence should be collected for end-to-end service chains (Chang *et al*., 2025) for each critical payment path and partner before release.

Table 6: Comparative resilience and recovery metrics by assessment method

Assessment method	Risk index at 50% stress	Resilience at 100% stress	P95 recovery (hours)
Dependency-weighted score (DWS)	50	34	28
PageRank	48	37	25
Betweenness centrality	55	30	31
FMEA	45	40	23
Monte Carlo propagation	57	27	36

Note. Resilience and risk indices use a 0–100 scale; P95 is the 95th-percentile recovery time. Higher risk and longer recovery indicate greater exposure; lower resilience indicates weaker continuity. Values are illustrative scenario outputs.

Figure 1 plots the normalized risk index against disrupted-dependency share for five assessment methods. Each curve rises as more third-party components are unavailable, showing increasing modeled exposure under progressively broader disruption. At 50% disruption, the scores are 50 for dependency-weighted scoring, 48 for PageRank, 55 for betweenness centrality, 45 for FMEA, and 57 for Monte Carlo propagation. At 100%, the corresponding scores are 91, 89, 96, 85, and 98. Monte Carlo propagation gives the highest risk at both displayed stress points, while FMEA gives the lowest. The plotted values reproduce the prior illustrative scenario table and are not measured banking outcomes. A valid empirical comparison would require a common dependency inventory, calibrated outage assumptions, identical service-impact weights, and reproducible runs. The curves should therefore be read as a demonstration of the comparison procedure, not as evidence that one method has been validated or that a specific bank faces these risk levels.

4.2. Provider Concentration, Supply-Chain Exposure, and Recovery Capacity

Provider concentration and software supply-chain exposure are coupled because banks may rely on a small set of cloud, identity, payment, code-signing, and certificate services, while those providers themselves depend on common regions, libraries, and subcontractors. A provider count alone therefore understates concentration: the dependency map must identify shared control planes and software release paths. The methods in Table 7 are compared through maximum-stress resilience, tail recovery time, and a normalized recovery-capacity indicator. The illustrative resilience values range from 27 to 40 on the 0–100 scale. The recovery-capacity index is calculated against a declared 48-hour planning window; it is a transformation of the illustrative recovery estimate, not an independent observation. The comparison supports prioritizing providers with high service reachability, weak substitutability, uncertain software provenance, and untested restoration paths. Banks should link SBOM records, signed-build provenance, vulnerability notices, and vendor incident reporting to affected services, then test isolation, rollback, clean rebuilds, and data restoration. Geographic or contractual diversification should count only when independent control planes and tested switching paths exist. BIS guidance similarly frames quantum migration as coordinated financial-system work, reinforcing the need to assess supplier readiness and recovery capacity together (Auer *et al.*, 2025) at the service rather than contract level.

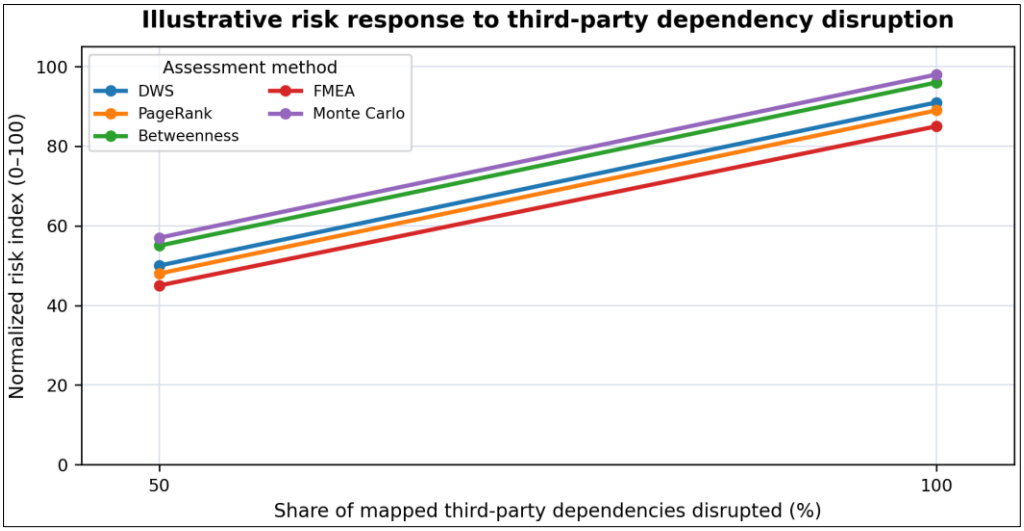


Fig 1: Illustrative risk response to increasing third-party dependency disruption

Table 7: Recovery capacity and continuity under provider and supply-chain stress

Assessment method	Resilience at 100% stress	P95 recovery (hours)	Recovery-capacity index
Dependency-weighted score (DWS)	34	28	42
PageRank	37	25	48
Betweenness centrality	30	31	35
FMEA	40	23	52
Monte Carlo propagation	27	36	25

Note. Recovery-capacity index = 100 × (1 − P95/48 hours); the 48-hour window is an illustrative normalization horizon. Higher index and resilience are stronger; lower P95 is faster. Values are derived scenario illustrations, not observations.

Figure 2 shows scenario recovery progress, with one line per assessment method. The curves use a transparent linear interpolation from zero restored critical-service volume to 95% at each method's illustrative P95 recovery time, then remain at that level. At 24 hours, the modeled completion values are approximately 81% for dependency-weighted scoring, 91% for PageRank, 74% for betweenness centrality, 95% for FMEA, and 63% for Monte Carlo propagation. By 36 hours, all five curves reach the 95% threshold because the slowest illustrative P95 is 36 hours. This representation makes recovery differences visible while preserving the table's recovery endpoints. It is a constructed trajectory, not telemetry or a stochastic simulation result. Real recovery curves are rarely linear: restoration depends on service dependencies, backup integrity, failover authorization, transaction backlogs, and supplier response. Banks should replace this interpolation with timestamped exercise or incident observations and report median and tail recovery separately. The graph's purpose is to compare the methods under the stated scenario assumptions.

4.3. Cryptographic Inventory and Post-Quantum Transition Gaps

A cryptographic inventory must connect algorithms, keys, certificates, protocols, and libraries to the banking services and suppliers that use them. The inventory should distinguish key establishment from digital signatures, record data confidentiality lifetimes, and identify quantum-vulnerable public-key operations in API authentication, interbank messaging, code signing, and long-term records. Table 8 compares five assessment methods using inventory coverage, transition gap, and an integrated priority score. Illustrative priority scores span 16 to 25; the higher scores occur where exposure and readiness gaps coincide. The score is a ranking aid, not a probability of compromise. Inventory coverage alone is insufficient: a discovered cryptographic asset remains a migration gap if its owner, supplier support, replacement protocol, rollback path, or interoperability test is missing. A readiness review should verify algorithm agility across TLS termination, HSM firmware, certificate issuance, API clients, and partner gateways. The migration roadmap should sequence assets by service criticality, confidentiality horizon, external dependency, and operational replacement window. The BIS roadmap emphasizes discovery, coordination, interoperability, and phased migration as linked activities (Auer *et al.*, 2025). Therefore, each unknown inventory field should be treated as unresolved exposure, assigned to an owner, and closed through evidence rather than policy statements and certificate chains in scope.

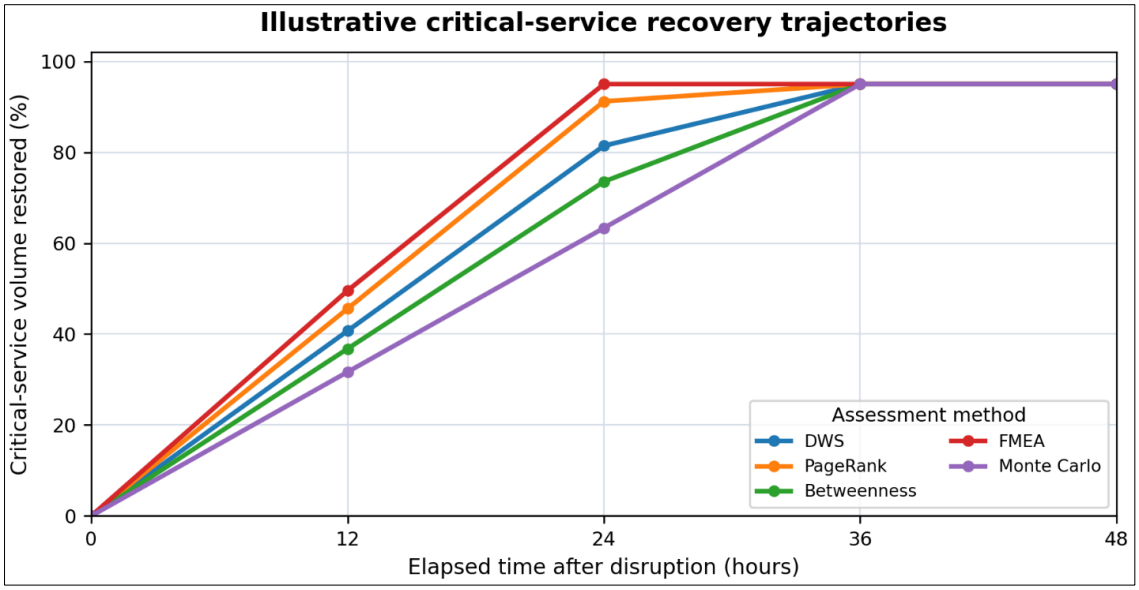


Fig 2: Illustrative recovery trajectories derived from P95 scenario endpoints

Table 8: Cryptographic inventory, transition gap, and prioritization metrics

Assessment method	Inventory coverage (%)	Transition gap (%)	Priority index
Dependency-weighted score (DWS)	65	38	19
PageRank	52	51	24
Betweenness centrality	59	45	25
FMEA	72	36	16
Monte Carlo propagation	61	44	25

Note. Transition gap is 100 minus the mean readiness score across inventory, crypto-agility, vendor readiness, migration validation, and service continuity. Priority index = intermediate-stress exposure × transition gap / 100, rounded. Illustrative values only.

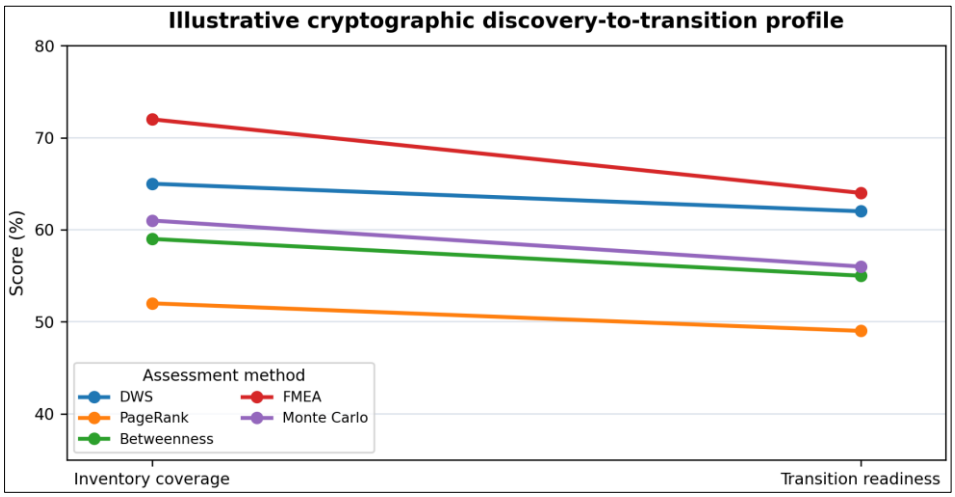


Fig 3: Slope comparison of cryptographic inventory and transition readiness

Figure 3 is a slope chart connecting each method's cryptographic inventory coverage to its transition-readiness complement, calculated as 100 minus the transition gap. FMEA moves from 72% coverage to 64% transition readiness; dependency-weighted scoring moves from 65% to 62%; Monte Carlo propagation moves from 61% to 56%; betweenness centrality moves from 59% to 55%; and PageRank moves from 52% to 49%. The descending segments show that every method's readiness estimate is below its inventory coverage, with the largest separation for PageRank and the smallest for dependency-weighted scoring. This pattern illustrates why asset discovery does not by itself demonstrate migration capability: readiness also depends on supplier support, crypto-agility, interoperability testing, and validated rollback. These endpoints are illustrative values from the existing assessment table, not measured inventories. An operational study should calculate both dimensions from a reconciled cryptographic register and evidence records, then use vendor testing to validate the readiness score before prioritizing transition work.

4.4. Integrated Risk Priorities for Resilient, Quantum-Ready Banking

Integrated prioritization combines dependency exposure, recovery weakness, and post-quantum transition readiness so that remediation addresses shared causes rather than isolated control findings. Table 9 applies the stated rule: priority equals the intermediate-stress exposure score multiplied by the transition gap, divided by 100, with the result rounded to the nearest integer. The illustrative priority scores range from 16 for FMEA to 25 for betweenness centrality and Monte Carlo propagation. These values are not empirical estimates; they show how the scoring rule ranks methods when supplied with the existing scenario table. A bank should retain each component beside the composite because a high priority can arise from provider concentration, inadequate cryptographic discovery, poor supplier migration evidence, or low recovery capacity. Operational actions should be assigned by service owner and tied to measurable closure evidence: validated alternate routing, tested restoration, vendor transition dates, inventory completeness, or interoperable hybrid/PQ authentication. Critical services with long-lived confidential data and no tested substitute should receive earlier migration windows. Cross-institution provider dependencies warrant joint exercises and coordinated incident communication; otherwise one institution's recovery plan may fail at a common supplier boundary. The recommended sequence is discover, validate, mitigate, rehearse, and re-score as dependency and cryptographic inventories change consistently.

Table 9: Integrated exposure, post-quantum gap, and priority comparison

Assessment method	Risk index at 50% stress	Transition gap (%)	Integrated priority index
Dependency-weighted score (DWS)	50	38	19
PageRank	48	51	24
Betweenness centrality	55	45	25
FMEA	45	36	16
Monte Carlo propagation	57	44	25

Note. Integrated priority = risk index at 50% stress × transition gap / 100, rounded to the nearest integer. Larger values indicate a higher screening priority, not a probability of loss or compromise. Values are illustrative.

Fig 4 uses a radar plot to compare five methods across four normalized risk dimensions: intermediate-stress exposure, post-quantum transition gap, maximum-stress resilience deficit, and the integrated priority index scaled by four for display. Monte Carlo propagation has the highest exposure score at 57 and the largest resilience deficit at 73; PageRank has the largest transition gap at 51. FMEA is lowest on the exposure and transition-gap axes, at 45 and 36, while its resilience deficit is 60. Dependency-weighted scoring records 50 exposure, a 38-point gap, a 66-point deficit, and a scaled priority of 76. The plot highlights distinct drivers rather than producing a single winner: methods can rank similarly overall while flagging different remediation needs. All plotted values are derived from the prior illustrative tables, with priority rescaled only to make the radar dimensions comparable visually. They are not probabilities or empirical results. Bank-specific application requires validated inputs and an agreed normalization rule.

5. Conclusions and Recommendations

5.1. Conclusions on Dependency-Related Cybersecurity and Quantum Risks

Digital banking resilience depends on more than the security of a bank's internal systems. Critical services rely on connected providers, software components, cloud platforms, identity services, APIs, and cryptographic assets. A disruption or compromise affecting a shared provider or software dependency can therefore spread across service boundaries, delaying payments, authentication, and data exchange. The assessment framework developed in this paper treats these relationships as a dependency network and considers exposure, recovery capacity, cryptographic readiness, and supplier concentration together.

The scenario comparisons illustrate how different assessment methods can identify different risk priorities. For example, the illustrative results assign higher exposure to Monte Carlo propagation and betweenness centrality under the specified stress conditions, while FMEA indicates comparatively faster recovery. These values demonstrate how the methodology can compare methods; they are not measured banking outcomes. The central conclusion is that resilience and quantum readiness should be managed as connected operational concerns. A bank may have a documented post-quantum plan yet remain vulnerable if a critical supplier cannot support migration, or may have strong vendor controls but lack tested recovery routes. Effective risk reduction therefore requires coordinated dependency mapping, supplier assurance, recovery exercises, cryptographic discovery, and staged migration.

5.2. Recommendations for Third-Party Governance and Vendor Assurance

Banks should maintain a service-level dependency register that links each critical banking service to its applications, APIs, hosting environments, identity providers, software components, subcontractors, and cryptographic services. Each entry should identify the service owner, provider, data handled, recovery requirements, substitutability, geographic and technical concentration, and dependencies shared with other providers. The register should be updated when services, contracts, software versions, or provider arrangements change.

Vendor due diligence should include evidence of security controls, incident notification procedures, vulnerability management, software provenance, business continuity arrangements, and tested recovery capabilities. Contracts should specify access to relevant assurance evidence, timely disclosure of material incidents, cooperation during investigations, subcontractor transparency, and support for cryptographic changes. Banks should assess concentration at the level of underlying infrastructure and control planes, since different providers may rely on the same cloud region, identity service, software library, or certificate authority.

Assurance should continue after onboarding. Banks should periodically review provider performance, track remediation actions, verify software bills of materials where available, and test exit or substitution plans for critical services. Findings should be assigned to accountable service owners and closed with evidence. Governance should prioritize dependencies whose failure could disrupt multiple critical services or whose replacement would require extensive technical, contractual, or regulatory work.

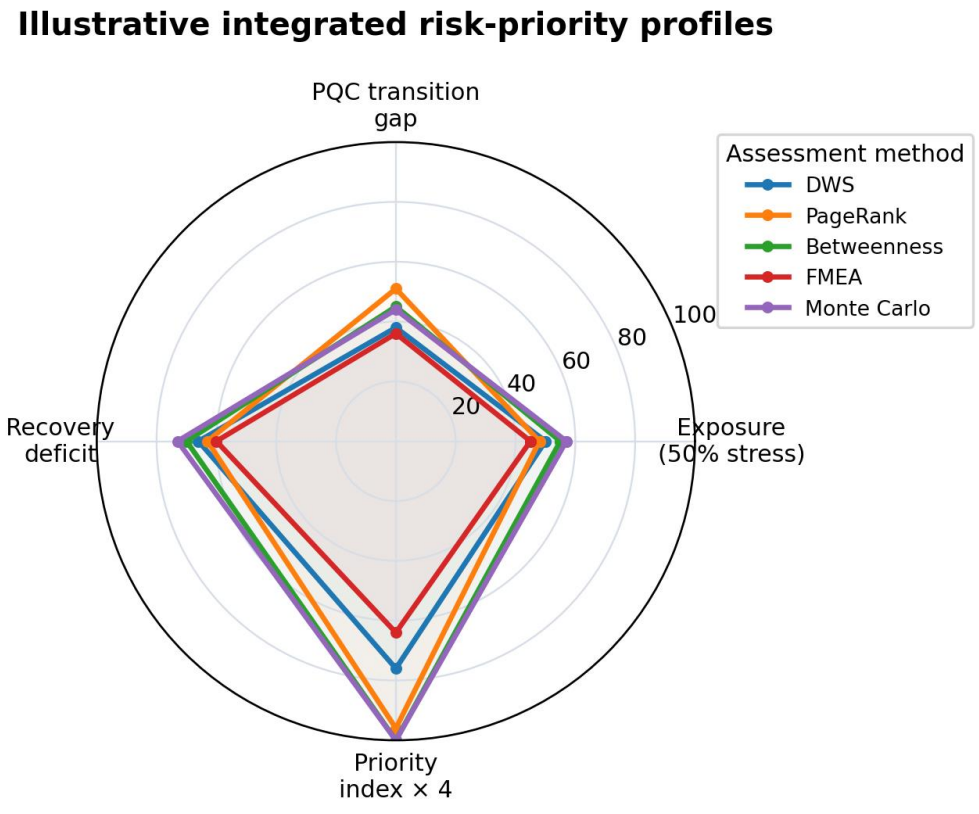


Fig 4: Radar comparison of normalized integrated risk-priority profiles

5.3. Recommendations for Resilience Testing and Recovery Planning

Resilience testing should begin with critical-service mapping and traceable recovery objectives. For each service, banks should define acceptable downtime, data-loss tolerance, minimum operating capacity, and dependencies required to restore service. Tests should include provider outages, compromised software updates, identity-service failures, API certificate problems, regional cloud disruption, and the unavailability of key management or cryptographic services. Scenarios should examine both direct failures and cascading effects across shared dependencies.

Exercise design should progress from component-level tests to end-to-end service recovery. Tabletop exercises can assess decision-making and communication; technical exercises can verify failover, alternate routing, credential revocation, clean rebuilds, backup restoration, and transaction reconciliation. Banks should involve relevant providers and counterparties when a service depends on their cooperation. Recovery evidence should include timestamps, achieved service levels, unresolved dependencies, and corrective actions.

Recovery metrics should be calculated from observed exercise or incident data. Useful measures include time to restore critical transactions, percentage of service capacity restored at defined intervals, data reconciliation error, and the proportion of recovery steps completed within target. Illustrative recovery curves in this paper show how methods can be compared under stated assumptions, but they should not substitute for measured exercise results. Banks should update recovery plans after each test, validate that alternate paths do not share the same failure domain, and repeat tests when material architecture or supplier changes occur.

5.4. Recommendations for Phased Post-Quantum Cryptographic Migration

Banks should treat post-quantum migration as a governed technology transition spanning cryptographic discovery, risk prioritization, procurement, interoperability, and operational validation. The first step is to inventory cryptographic use across APIs, interbank messaging, certificates, VPNs, code signing, hardware security modules, data stores, and third-party services. The inventory should record algorithms, key sizes, protocol versions, certificate lifetimes, owners, vendor dependencies, and the confidentiality lifetime of protected information.

Migration priorities should reflect service criticality, exposure to public-key cryptography, data longevity, replacement lead time, and supplier readiness. Long-lived confidential data and services with extensive external dependencies warrant early assessment. Banks should obtain vendor roadmaps and verify support in deployed products rather than relying on general claims of readiness. Contractual and procurement requirements should include upgrade support, cryptographic agility, testing access, and a clear process for addressing newly identified vulnerabilities.

Where standards and implementation guidance permit, organizations can evaluate hybrid key-establishment approaches during transition, while separately assessing signature migration. Testing should measure latency, throughput, memory use, message and certificate size, interoperability, failure handling, and recovery behavior under realistic API workloads. Rollout should proceed through controlled pilots, partner testing, monitored deployment, and documented rollback plans. Migration completion should be demonstrated through verified inventory updates, successful interoperability tests, and removal or justified isolation of obsolete cryptographic mechanisms.

References

1. Ajayi AA, Igba E, Soyele AD, Enyejo JO. Quantum cryptography and blockchain-based social media platforms as a dual approach to securing financial transactions in CBDCs and combating misinformation in U.S. elections. International Journal of Innovative Science and Research Technology. 2024;9(10).
2. Abolade YA, Adegoke A, Noi SM, Nwoye CM, Ajayi O, Kyrian O, *et al*. Promoting health: Introducing an eco-friendly herbal mosquito repellent extracted from local sweet orange peels GSC Biological and Pharmaceutical Sciences, 2024, 26(01), 315–327 DOI. 2024. doi:10.30574/gscbps.2024.26.1.0014
3. Akindote O, Enyejo JO, Awotiwon BO, Ajayi AA. Integrating blockchain and homomorphic encryption to enhance security and privacy in project management and combat counterfeit goods in global supply chain operations. International Journal of Innovative Science and Research Technology. 2024;9(11). doi:10.38124/ijisrt/IJISRT24NOV149
4. Akinleye T, Ijiga OM. Sustainable Construction Compliance Modelling Through ISO 14001, ISO 45001 and ISO 9001 Integrated Audit Data. International Journal of Scientific Research in Civil Engineering Vol.9, Iss. 4, Pg, 93-116 DOI; 2025. doi:10.32628/IJSRCE2594012
5. Akinleye T, Ijiga OM. A Novel COSHH Risk Ranking Algorithm for Hazardous Substance Control in Construction and Engineering Workplaces. International Journal of Innovative Science and Research Technology, Vol. 11, Iss. 7; 2026. doi:10.38124/ijisrt/26jul1158
6. Akinleye T, Idoko DO, Enyejo LA. Sustainability-Driven Root Cause Analysis of Construction Incidents Using Environmental, Quality and Safety Performance Indicators International Journal of Scientific Research and Modern Technology, 5(6), 203–274. 2026. doi:10.38124/ijsrmt.v5i6.1541
7. Aluso L, Enyejo JO, Amebleh J, Balogun SA. A comparative analysis of SQL-based and cloud-native data warehousing architectures for real-time financial reporting. International Journal of Scientific Research and Modern Technology. 2024;3(12):78-90. doi:10.38124/ijsrmt.v3i12.1179
8. Awiszus K, Bell Y, Lüttringhaus J, Svindland G, Voß A, Weber S. Building resilience in cybersecurity: An artificial lab approach. The Journal of Risk and Insurance. 2024;91(3):753-800. doi:10.1111/jori.12450
9. Ayoola VB, Ugoaghalam UJ, Idoko PI, Ijiga OM, Olola TM. Effectiveness of social engineering awareness training in mitigating spear phishing risks in financial institutions from a cybersecurity perspective. Global Journal of Engineering and Technology Advances. 2024;20(3):94-117. Available from: https://gjeta.com/content/effectiveness-social-engineering-awareness-training-mitigating-spear-phishing-risks
10. Bamidele AA,. Kondeti H, Ijiga OM. Development of a Hybrid Machine Learning Algorithm for Impurity Reduction in Nitrosamine Formation Under Variable

Pharmaceutical Processing Conditions Compared with Gradient Boosting and Artificial Neural Networks International Journal of Scientific Research in Chemistry Volume 11, Issue 2 Pg. 64 -94 doi; 2026. doi:10.5281/zenodo.23860513
11. Bamidele, A. A., Justin, O., Adanne, S. (2025). Integrating machine learning with environmental chemistry to forecast pollutant releases in coatings production. World Journal of Advanced Research and Reviews, 2025, 27(3), 1061-1072. Article DOI: https://doi.org/10.30574/wjarr.2025.27.3.3153
12. Bamidele, A. A., Rotimi, A. M., James, C. O., Obinna, J. (2025). Coupling environmental chemistry with Artificial Intelligence for coastal hazard risk assessment under climate change. International Journal of Science and Research Archive, 2025, 16(03), 498–507. Article DOI: https://doi.org/10.30574/ijsra.2025.16.3.2572.
13. Bassens D, Pažitka V, Hendrikse R. Banking in the cloud: Mapping Big Tech's global digital technology networks. Regional Studies. 2024;58(12):2241-2255. doi:10.1080/00343404.2024.2391483
14. Biasse JF, Bonnetain X, Kirshanova E, Schrottenloher A, Song F. Quantum algorithms for attacking hardness assumptions in classical and post-quantum cryptography. IET Information Security. 2023;17(2). doi:10.1049/ise2.12081
15. Cheng M, Qu Y, Jiang C, Zhao C. Is cloud computing the digital solution to the future of banking? Journal of Financial Stability. 2022;63:101073. doi:10.1016/j.jfs.2022.101073
16. Crosignani M, Macchiavelli M, Silva A. Pirates without borders: The propagation of cyberattacks through firms' supply chains. Journal of Financial Economics. 2023;147(2):432-448. doi:10.1016/j.jfineco.2022.12.002
17. Doe Gadekah, S, B. & Enyejo, J. O. (2025). Personalization Versus Privacy in Digital Marketing Examining the Interactive Effects of Data Transparency Perceived Intrusiveness and Consumer Trust on Purchase Decisions *International Journal of Management and Organizational Research* Vol. 4, Iss. 6 Page No: 182-199 DOI: https://doi.org/10.54660/IJMOR.2025.4.6.182-199
18. Doe Gadekah, S, B. & Enyejo, J. O. (2025). The Influence of Brand Community Participation and User-Generated Content on Customer-Based Brand Equity Repurchase Intention and Electronic Word-of-Mouth in Direct-to-Consumer Markets *International Journal of Management and Organizational Research* Vol, 4, Iss. 3 Page No: 183-203 DOI: https://doi.org/10.54660/IJMOR.2025.4.3.183-203
19. Doe Gadekah, S, B. & Enyejo, J. O. (2026). The Effects of Generative AI Advertising Disclosure on Brand Authenticity Perceptions Purchase Intention and Consumer Skepticism Among Generation Z Consumers *International Journal of Scientific Research in Humanities and Social Sciences* Vol, 3 Iss 2, Pg. 137-169 doi : https://doi.org/10.32628/IJSRHSS253293
20. Eisenbach TM, Kovner A, Lee MJ. Cyber risk and the U.S. financial system: A pre-mortem analysis. Journal of Financial Economics. 2022;145(3):802-826. doi:10.1016/j.jfineco.2021.10.007
21. Enyejo JO, Adeyemi AF, Olola TM, Igba E, Obani OQ. Resilience in supply chains: How technology is helping USA companies navigate disruptions. Magna Scientia Advanced Research and Reviews. 2024;11(2):261-277. doi:10.30574/msarr.2024.11.2.0129
22. Frank UP. Healthcare Quality Metrics: From Data Collection to Performance Improvement; A Narrative Review of Measurement Frameworks and Improvement Methods in United States Health Care Umeh UKR Journal of Medicine and Medical Research (UKRJMMR) DOI. 2026. doi:10.5281/zenodo.22105362
23. Frank. U. P. Artificial Intelligence for Infection Surveillance: Improving Early Detection of Healthcare-Associated Infections USRJournalof Multidisciplinary Research and Studies. 2026.
24. Frank. U. P. (2026). Optimizing medical inventory management through predictive analytics: Implications for healthcare quality, cost reduction, and patient safety; A narrative review. UKR Journal of Education and Literature, 2(1), 77-92. DOI: https://doi.org/10.5281/zenodo.22105843 (
25. Gupta A, Mittal S. Post-quantum readiness and cryptographic transition planning for enterprise cloud. Cybersecurity. 2026;9:147. doi:10.1186/s42400-026
26. Hammi B, Zeadally S, Nebhen J. Security threats, countermeasures, and challenges of digital supply chains. ACM Computing Surveys. 2023;55(14s):316. doi:10.1145/3588999
27. Idika CN. Quantum resistant cryptographic protocols for securing autonomous vehicle-to-vehicle (V2V) communication networks. International Journal of Scientific Research in Computer Science, Engineering and Information Technology. 2023;10(1). doi:10.32628/CSEIT2391547
28. Idoko DO, Ugoaghalam UJ, Babalola A, Oyebanji SO. A comprehensive review of combating EDoS attacks in cloud services with deep learning and advanced network security technologies including DDoS protection and intrusion prevention systems. Global Journal of Engineering and Technology Advances. 2024;20(3):6-33. Available from: https://gjeta.com/content/comprehensive-review-combating-edos-attacks-cloud-services-deep-learning-and-advanced
29. Idoko IP, Ijiga OM, Enyejo LA, Ugbane SI, Akoh O, Odeyemi MO. Exploring the potential of Elon Musk's proposed quantum AI: A comprehensive analysis and implications. Global Journal of Engineering and Technology Advances. 2024;18(3):48-65.
30. Igba E, Abiodun K, Ali EO. Building the backbone of the digital economy and financial innovation through strategic investments in data centers. International Journal of Innovative Science and Research Technology; 2025. doi:10.5281/zenodo.14651210
31. Ijiga, O. M. & Akinleye, T. (2024). A Framework for Integrating Environmental Permit and Consent Management into Construction Project Delivery: Reducing Delays and Ensuring Regulatory Compliance. *International Journal of Scientific Research in Science, Engineering and Technology*, vol. 11, no. 3, pp. 706–732, Jun. 2024, doi: 10.32628/IJSRSET261254
32. Ijiga OM, Idoko IP, Ebiega GI, Olajide FI, Olatunde TI, Ukaegbu C. Harnessing adversarial machine learning for advanced threat detection: AI-driven strategies in cybersecurity risk assessment and fraud prevention.

Open Access Research Journals. 2024;13. doi:10.53022/oarjst.2024.11.1.0060
33. James UU. MULTISCALE SIGNAL PROCESSING FRAMEWORK FOR ZERO TRUST SECURITY IN NEXT- GENERATION WIRELESS NETWORKS International Journal of Wireless and Mobile Networks DOI/Link. 2026. Available from: https://aircconline.com/ijwmn/V18N3/18326ijwmn01.pdf
34. James UU, Salami EO, Enyejo LA. Real Time Policy Orchestration for Cybersecurity Risk Management in GRC Aligned Financial Technology Infrastructures International Journal of Innovative Science and Research Technology Volume 10, Issue 8. 2025. doi:10.38124/ijisrt/25aug1021
35. James UU, Salami EO, Enyejo LA. Real-time policy orchestration for cybersecurity risk management in GRC-aligned financial technology infrastructures. International Journal of Innovative Science and Research Technology. 2025;10(8).
36. Javaheri D, Fahmideh M, Chizari H, Lalbakhsh P, Hur J. Cybersecurity threats in FinTech: A systematic review. Expert Systems with Applications. 2024;241:122697. doi:10.1016/j.eswa.2023.122697
37. Joseph D, Misoczki R, Manzano M, Tricot J, Dominguez Pinuaga F, Lacombe O, *et al*. Transitioning organizations to post-quantum cryptography. Nature. 2022;605:237-243. doi:10.1038/s41586-022-04623-2
38. Michael CI, Campbell T, Idoko IP, Bemologi OU, Anyebe AP, Odeh II. Enhancing cybersecurity protocols in financial networks through reinforcement learning. International Journal of Scientific Research and Modern Technology. 2024;3(9). doi:10.38124/ijsrmt.v3i9.58
39. Montenegro JA, Rios R, Lopez-Cerezo J. A performance evaluation framework for post-quantum TLS. Future Generation Computer Systems. 2026;175:108062. doi:10.1016/j.future.2025.108062
40. Nwatuzie GA. Comparative performance and optimization strategies for cloud-native architectures: A focus on scalability, cost, and resource utilization. International Journal of Information Engineering and Electronic Business. 2026;18(3):87-102. doi:10.5815/ijieeb.2026.03.06
41. Nwatuzie GA, Enyejo LA, Umeaku C. Enhancing cloud data security using a hybrid encryption framework integrating AES, DES, and RC6 with file splitting and steganographic key management. International Journal of Innovative Science and Research Technology. 2025;10(1). doi:10.5281/zenodo.14792173
42. Ogundola T. Advances in quantum-secure banking: Cryptographic solutions. International Journal of Science and Research Archive. 2020;1(1):228-230. doi:10.30574/ijsra.2020.1.1.0048
43. Ogundola T. Quantum-resistant cryptographic techniques for financial institutions. International Journal of Scientific Research and Modern Technology. 2022;1(11):18-20. doi:10.38124/ijsrmt.v1i11.586
44. Ogundola TO. Barriers to implementing quantum-resistant encryption in financial institutions, World Journal of Advanced Research and Reviews, 2024, 22(03), 2323-2337, DOI. 2024. doi:10.30574/wjarr.2024.22.3.1938
45. Ogundola TO. Post-quantum cryptography for secure banking transactions. International Journal of Scientific Research and Modern Technology. 2025;4:40-42.
46. Okika N, Nwatuzie GA, Odozor L, Oni O, Idoko IP. Addressing IoT-driven cybersecurity risks in critical infrastructure to safeguard public utilities and prevent large-scale service disruptions. International Journal of Innovative Science and Research Technology. 2025;10(2). doi:10.5281/zenodo.14964285
47. Onyekaonwu CB. Designing resilient anti-fraud architectures for digital financial services in Sub-Saharan Africa. International Journal of Innovative Science and Research Technology. 2025;10(10). doi:10.38124/ijisrt.v10i10.1026
48. Peihani M. Regulation of cyber risk in the banking system: A Canadian case study. Journal of Financial Regulation. 2022;8(2):139-161. doi:10.1093/jfr/fjac006
49. Schreieck M, Huang Y, Kupfer A, Krcmar H. The effect of digital platform strategies on firm value in the banking industry. Journal of Management Information Systems. 2024;41(2):394-421. doi:10.1080/07421222.2024.2340825
50. Uzoma E, Idoko IP, Enyejo LA. Evaluating serverless computing and microservices impact on scalable cloud-native applications and blockchain interoperability frameworks. International Journal of Scientific Research and Modern Technology. 2024;3(4):14-17. doi:10.38124/ijsrmt.v3i4.407
51. Yao Y, Li J. Operational risk assessment of third-party payment platforms: A case study of China. Financial Innovation. 2022;8:19. doi:10.1186/s40854-022-00332-x

How to Cite This Article

Ogundola TO, Waheed BO, Ijiga OM, Idowu K. Assessing the impact of Third-Party technology dependencies on cybersecurity resilience and quantum readiness in digital banking infrastructure. Int J Eng Comput Appl. 2026;2(6):38-51. doi:10.54660/.IJECA.2026.2.6.38-51.

Creative Commons (CC) License

This is an open access journal, and articles are distributed under the terms of the Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International (CC BY-NC-SA 4.0) License, which allows others to remix, tweak, and build upon the work non-commercially, as long as appropriate credit is given and the new creations are licensed under the identical terms.