The Impact of Cybersecurity on Cloud in Banking and Financial Services

## 1.0 Introduction

Traditional banking and financial services (BFS) face intensifying pressure from digital-native competitors, with Revolut alone surpassing 50 million customers globally as of November 2024 (Fortune Business Insights, 2025). Alongside this competitive threat, banks confront legacy infrastructure reaching obsolescence, evolving regulatory requirements demanding improved operational resilience, and increasing demands for flexible infrastructure rather than static on-premises estates. These converging forces have contributed to accelerating cloud adoption across the sector; in 2023, Capgemini reported that 91% of financial organisations globally had at least one cloud platform, compared to just 37% in 2020 (Capgemini Research Institute, 2023).

The transition from on-premises systems to distributed, multi-tenant architectures has shifted the locus of control over confidentiality, integrity and availability, concentrating reliance on external control planes operated by third parties. Market structure further amplifies this dependency, with the top three cloud service providers (CSPs) collectively holding over 63% market share as of Q2 2025 (Synergy Research Group, 2025). In highly regulated financial contexts, where prudential oversight, operational resilience and data protection are paramount, this raises specific challenges around data sovereignty and jurisdiction, third party and supply-chain dependencies and regulatory compliance.

Although public-cloud adoption is widespread, assurance has not kept pace. Baron, Leach and Yeoh (2023) report that the proportion of BFS firms with tested exit plans declined from 30% to 20% between 2020 and 2023, while those with no plan at all increased from 35% to 52%. Interpreted cautiously, given these findings derive from self-reported cross-section survey data with undisclosed response rates and potential selection bias, this trend is consistent with a widening gap between the speed of cloud implementation and that of supporting security and risk management in BFS. It also diverges from explicit supervisory expectations that institutions maintain documented and, where appropriate, sufficiently tested exit plans ((*Digital Operational Resilience Act (DORA), Article 28*, 2025), (European Central Bank., 2025)).

This review interrogates whether the widening adoption–assurance gap in BFS reflects a shortfall in risk-management capacity or a deliberate adaptation to cloud constraints. It addresses two research questions: (1) What security and resilience risks arise from public-cloud adoption in financial services? (2) Which mitigation strategies show evidence of effectiveness under sectoral regulatory constraints? Because regulation shapes both risk assessment and control obligations, regulatory frameworks are considered throughout. Using a narrative synthesis of academic, regulatory and industry sources, the review evaluates the technical efficacy of controls, their implementation maturity and the factors that explain any gap between available controls and deployment in practice. The review proceeds as follows: §2 Methodology; §3 Security and resilience risks; §4 Mitigation strategies and their effectiveness; §5 Conclusions with implications for practice and future research.

## 2.0 Methodology:

## 2.1 Review Approach

This study uses configurative synthesis, combining systematic search with narrative synthesis to integrate evidence from technical, regulatory, and industry sources, including grey literature capturing current developments.

## 2.2 Search Strategy

Searches covered academic databases (Semantic Scholar, Scopus, Google Scholar) and regulatory/industry sources (EBA, ECB/SSM, BIS/BCBS, PRA/FCA, ENISA, NIST, FFIEC/OCC, CSA, SANS) from 2020-2025, with foundational 2010-2019 works included through citation tracing. References were managed in Zotero.

## 2.3 Selection Criteria

From 496 deduplicated sources, screening applied seven criteria:

* Public Cloud Technology: AWS, Azure, or Google Cloud focus
* Security Risk or Mitigation: Addresses specific risks or protective measures
* Regulatory Framework: Discusses financial regulations in cloud contexts
* Empirical Research: Evidence-based findings
* Financial Sector Relevance: Applicable to financial services
* Empirical Evidence Base: Real-world validation
* Security or Regulatory Focus: Not solely technical/cost-focused

Inclusion required criterion 1 AND (2 OR 3) AND 4, with 5-7 as exclusion filters. All decisions were documented.

## 2.4 Data Extraction and Synthesis

Thirty-six included sources underwent narrative synthesis due to: heterogeneous outcome measures (vulnerability counts, compliance rates, costs); incompatible metrics across source types; and context-dependent findings varying by institution size, geography, and regulatory regime. Synthesis identified convergent themes mapped to research questions.

## 2.5 Limitations

Single-reviewer screening may introduce selection bias despite systematic documentation. Narrative synthesis enables broad coverage but lacks structured synthesis depth. The 2020-2025 focus excludes earlier studies except through citations. English-language restriction may exclude relevant non-anglophone research.

## 3.0 Security Risks in Cloud-Based BFS (RQ1)

### 3.1 Concentration risk and market structure

Koh and Prenio (2023) argue that cloud’s oligopolistic structure creates dependencies that exceed traditional bilateral outsourcing. Supervisory analyses also highlight limited institutional visibility into CSP internal controls and change management, creating blind spots for enterprise risk assessment (U.S. Department of the Treasury, 2024). While realised sector-wide impacts are not well documented, concern persists that correlated failure modes (e.g., regional or service-level outages at one of the three largest CSPs) could propagate across the financial system. Current evidence for such macro effects, however, remains limited.

Survey data suggests BFS multi-CSP use declined from 65% to 57% between 2020 and 2023, coincident with substantial growth in critical workloads on public cloud (Baron, Leach and Yeoh, 2023). Interpreted alongside the architectural differences among CSPs (notably IAM/KMS semantics, policy engines, and telemetry) that complicate portability of workloads, this pattern is consistent with a pragmatic acceptance of concentration risk under current technical and economic constraints. Given the underlying data are self-reported and cross-sectional, and response rates are undisclosed, this remains a moderate-evidence inference. Section 4.1 further examines portability feasibility and the resilience trade-offs of multi-CSP strategies.

### 3.2 Incident patterns, denominators and control maturity

Financial services are frequently targets of attack. For example, Cloudflare’s Q2-2022 reporting noted that ~9% of observed DDoS attacks were directed against financial institutions (Cloudflare, 2022), while Verizon’s DBIR consistently ranks BFS as the primary target for data breaches (Verizon, 2023). Notably, although model-based estimates place potential BFS cyber losses at 14–19% of net income (Bouveret, 2018), empirical incident data show markedly lower realised losses; this gap is consistent with effective controls, but may also reflect under-reporting, detection limitations, and insurance-related risk transfer.

Hayes et al. (2024) found 68% of 200 analysed incidents stemmed from customer-side misconfigurations- primarily exposed storage buckets (31%), excessive IAM permissions (24%) and unencrypted data in transit (18%). Earlier threat taxonomies (e.g.,(Chou, 2013)) emphasised platform-centric attacks that are comparatively less represented in recent incident narratives, perhaps indicating an evolution in risk composition as the cloud landscape has matured. Overall, misconfiguration and identity/authorisation design remain primary proximate risks.

### 3.3 Operational Resilience and Exit Strategy Evolution

The marked shift in exit preparedness - firms without plans increasing from 35% to 52% while those with tested plans declined from 30% to 20% between 2020-2023 (Baron, Leach and Yeoh, 2023) - warrants careful interpretation given its implications for systemic resilience.

One interpretation suggests cloud rapid adoption has outpaced risk management capabilities. The doubling of BFS business-critical workloads on cloud from 17% to 32% over three years represents substantial velocity that may have overwhelmed governance processes designed for more gradual technology transitions. This reading aligns with the simultaneous decline in fully integrated risk assessments from 53% to 33% (Baron, Leach and Yeoh, 2023), potentially indicating stressed risk functions struggling to maintain pace.

Alternatively, these patterns may reflect strategic recalibration based on practical experience. The confluence of reduced exit planning, increased critical workload deployment, and decreased multi-cloud pursuit (from 65% to 57%) could indicate institutions have concluded that theoretical portability proves practically unachievable. McKenna (2024) provides economic context: maintaining exit capability requires 40-60% parallel infrastructure costs, while asymmetric egress fees create substantial switching penalties. Under this interpretation, institutions are making informed trade-offs rather than experiencing oversight failures.

The sector's maintained security effectiveness offers insight into which interpretation holds greater explanatory power. Financial services continue experiencing the highest attack frequency yet maintain lower incident costs relative to exposure than less-targeted sectors. This suggests institutions retain risk management competence while consciously accepting certain lock-in risks. However, without data on actual exit attempt outcomes or detailed governance adaptation strategies, definitive conclusions remain elusive.

## 4.0 Mitigation Strategies and Implementation Evidence

### 4.1 Multi-Cloud Adoption: Evolving Understanding of Practical Constraints

The decline in multi-cloud adoption from 65% to 57% (Baron, Leach and Yeoh, 2023) contradicts regulatory expectations and warrants examination of underlying causes. This trend could reflect either temporary implementation challenges or recognition of more fundamental limitations.

Regulatory insistence on multi-cloud resilience, illustrated by DORA requirements (European Union, 2022), implies authorities consider technical barriers surmountable. However, operational evidence increasingly suggests practical constraints may be more binding than initially anticipated. The finding that only 23% achieve meaningful workload portability despite 76% rating it critical indicates substantial implementation barriers. Different identity and access management models, proprietary service dependencies, and data gravity create frictions that abstraction layers struggle to overcome effectively.

The operational burden provides additional perspective. With 50% of institutions managing five or more separate audit requests (Baron, Leach and Yeoh, 2023), multi-cloud appears to multiply compliance overhead without demonstrating proportional resilience benefits. This aligns with Checkpoint Software's (2024) finding that 68% of organisations are most concerned about misconfigurations when it comes to cloud risk. Multi-cloud environments expands both the regulatory burden and the configuration surface requiring management, potentially increasing rather than mitigating risk.

### 4.2 Zero Trust Architecture: Implementation Realities

In terms of identity verification, Zero Trust emerges as the predominant framework, with 72% of financial institutions identifying it as their top priority (Baron, Leach and Yeoh, 2023). Implementation data shows growth from 12% in 2021 to 43% in 2024, with mature implementations reporting 60% fewer incidents. However, this correlation requires critical examination. Organisations implementing Zero Trust likely possess stronger security capabilities overall, creating selection bias.

### 4.3 Key Management: Successful Evolution with Caveats

Key management shows measurable improvements in adoption. Baron, Leach and Yeoh (2023) document cloud-based Hardware Security Module (HSM) adoption where CSPs cannot access keys increasing from 27% to 52% for critical data between 2020-2023. This represents one area where security controls appear to match adoption pace.

Yet implementation strategy remains fragmented. For regulated data, only 48% use CSP-inaccessible HSMs, while 35% rely on "on-premise" solutions potentially incompatible with cloud scalability. Current literature does not explore whether this fragmentation reflects technical constraints, regulatory requirements, or risk appetite differences.

### 4.4 Governance Integration: Regression or Recalibration

Baron, Leach and Yeoh (2023) report firms with fully integrated cloud risk assessments declining from 53% to 33% between 2020-2023, while "partial integration" increased from 38% to 58%. This shift coincides with doubled business-critical workload deployment.

The US Department of the Treasury (2023) attributes governance challenges to traditional frameworks assuming bilateral relationships and full visibility - assumptions violated by cloud's shared responsibility model. However, neither source examines whether "partial integration" represents transitional states toward full integration or permanent compromises. This distinction critically affects risk assessment accuracy.

The static 53% of organisations maintaining formal cloud policies within Enterprise Risk Management frameworks, unchanged since 2020 despite dramatic adoption increases, further complicates interpretation. This could indicate either framework inadequacy or temporary lag as governance catches up with the industry.

### 4.6 Regulatory Evolution and Implementation Challenges

Recognising indirect oversight insufficiency, major jurisdictions implement direct regulatory powers. The EU's DORA and parallel UK proposals grant authorities unprecedented oversight of critical third parties (European Union, 2022; Bank of England and Financial Conduct Authority, 2022). Koh and Prenio (2023) term this addressing the "macroprudential dimension" of cloud concentration.

Yet regulatory frameworks can struggle to keep pace with industry. Multi-cloud resilience requirements conflict with evidence showing limited portability. The Basel Committee's (2018) cyber-resilience principles, developed for bilateral outsourcing, map poorly to multi-tenant architectures where hundreds of institutions share infrastructure.

Furthermore, regulatory divergence across jurisdictions complicates global institutions' compliance. The review identifies no studies examining how institutions navigate conflicting requirements - a significant gap given financial services' international nature. This absence of evidence prevents assessment of whether regulatory harmonisation could improve security outcomes or whether jurisdictional differences reflect legitimate variations in risk appetite and market structure.

## 5.0 Conclusion

Three interrelated patterns emerge requiring integrated interpretation. First, the deterioration in exit preparedness alongside maintained security effectiveness suggests institutions may be making informed trade-offs rather than experiencing oversight failures. Second, the decline in multi-cloud pursuit despite regulatory pressure indicates practical learning about implementation constraints. Third, the regression in governance integration while deploying critical workloads may reflect framework recalibration rather than simple deterioration.

These patterns could indicate sector-wide adaptation to cloud realities. Early adoption phases emphasised theoretical risk controls - comprehensive exit planning, multi-cloud portability, traditional governance frameworks. Practical experience appears to be revealing certain controls as economically or technically impractical, prompting strategic pivots toward optimising within constraints rather than pursuing unachievable ideals.

Alternatively, these patterns might still represent concerning gaps between adoption pace and risk management maturation. The three-year timeframe may be insufficient for drawing conclusions about strategic adaptation versus temporary turbulence. Governance regression and exit planning deterioration could presage future incidents rather than successful adaptation.

The balance of evidence marginally favours the adaptation interpretation. Financial services' ability to maintain security effectiveness (lower than forecase incident costs despite high attack frequency) while accepting increased lock-in suggests risk-aware decision-making. The shift away from multi-cloud despite regulatory pressure indicates learning from experience rather than negligence.

For researchers, critical questions remain unresolved. Without longitudinal studies tracking institutions through complete migration cycles, causal relationships remain inferential. Economic analyses quantifying efficiency gains against resilience costs could clarify whether current trade-offs are optimal. Most fundamentally, determining whether observed patterns represent successful adaptation or accumulating risk requires evidence not yet available.

The financial sector appears to be converging toward a cloud strategy accepting certain lock-in risks while maintaining security focus. Whether this represents sophisticated adaptation or collective vulnerability accumulation remains an open question requiring continued monitoring and research.

## 6.0 References:

Bouveret, A. (no date) *Cyber Risk for the Financial Sector: A Framework for Quantitative Assessment*, *IMF*. Available at: https://www.imf.org/en/Publications/WP/Issues/2018/06/22/Cyber-Risk-for-the-Financial-Sector-A-Framework-for-Quantitative-Assessment-45924 (Accessed: 15 September 2025).

Capgemini Research Institute (2023) *World Cloud Report – Financial Services 2023*. Available at: https://www.capgemini.com/wp-content/uploads/2023/11/WCRFS\_2023\_web.pdf.

Chou, T.-S. (2013) ‘Security Threats on Cloud Computing Vulnerabilities’, *International Journal of Computer Science and Information Technology*, 5(3), pp. 79–88. Available at: https://doi.org/10.5121/ijcsit.2013.5306.

*Digital Operational Resilience Act (DORA), Article 28* (2025). Available at: https://www.digital-operational-resilience-act.com/Article\_28.html (Accessed: 7 September 2025).

*Verizon (PDF)* (no 2024) *Verizon Business*. Available at: https://www.verizon.com/business/en-gb/resources/reports/dbir/2023/dbir-report/ (Accessed: 15 September 2025).

European Central Bank. (2025) *ECB guide on outsourcing cloud services to cloud service providers.* LU: Publications Office. Available at: https://data.europa.eu/doi/10.2866/3638533 (Accessed: 7 September 2025).

Fortune Business Insights (2025) *Neobanking Market Size, Share, Growth | Forecast Report, 2032*. Available at: https://www.fortunebusinessinsights.com/neobanking-market-109076 (Accessed: 31 August 2025).

Koh, T.Y. and Prenio, J. (2023) *Managing cloud risk: some considerations for the oversight of critical cloud service providers in the financial sector*. Basel: Bank for International Settlements, Financial Stability Institute (FSI insights on policy implementation, no 53).

*Q2 Cloud Market Nears $100 Billion Milestone - and it’s Still Growing by 25% Year over Year | Synergy Research Group* (2025). Available at: https://www.srgresearch.com/articles/q2-cloud-market-nears-100-billion-milestone-and-its-still-growing-by-25-year-over-year (Accessed: 31 August 2025).

*Top Cloud Security Issues, Threats and Concerns* (no date) *Check Point Software*. Available at: https://www.checkpoint.com/cyber-hub/cloud-security/what-is-cloud-security/top-cloud-security-issues-threats-and-concerns/ (Accessed: 15 September 2025).