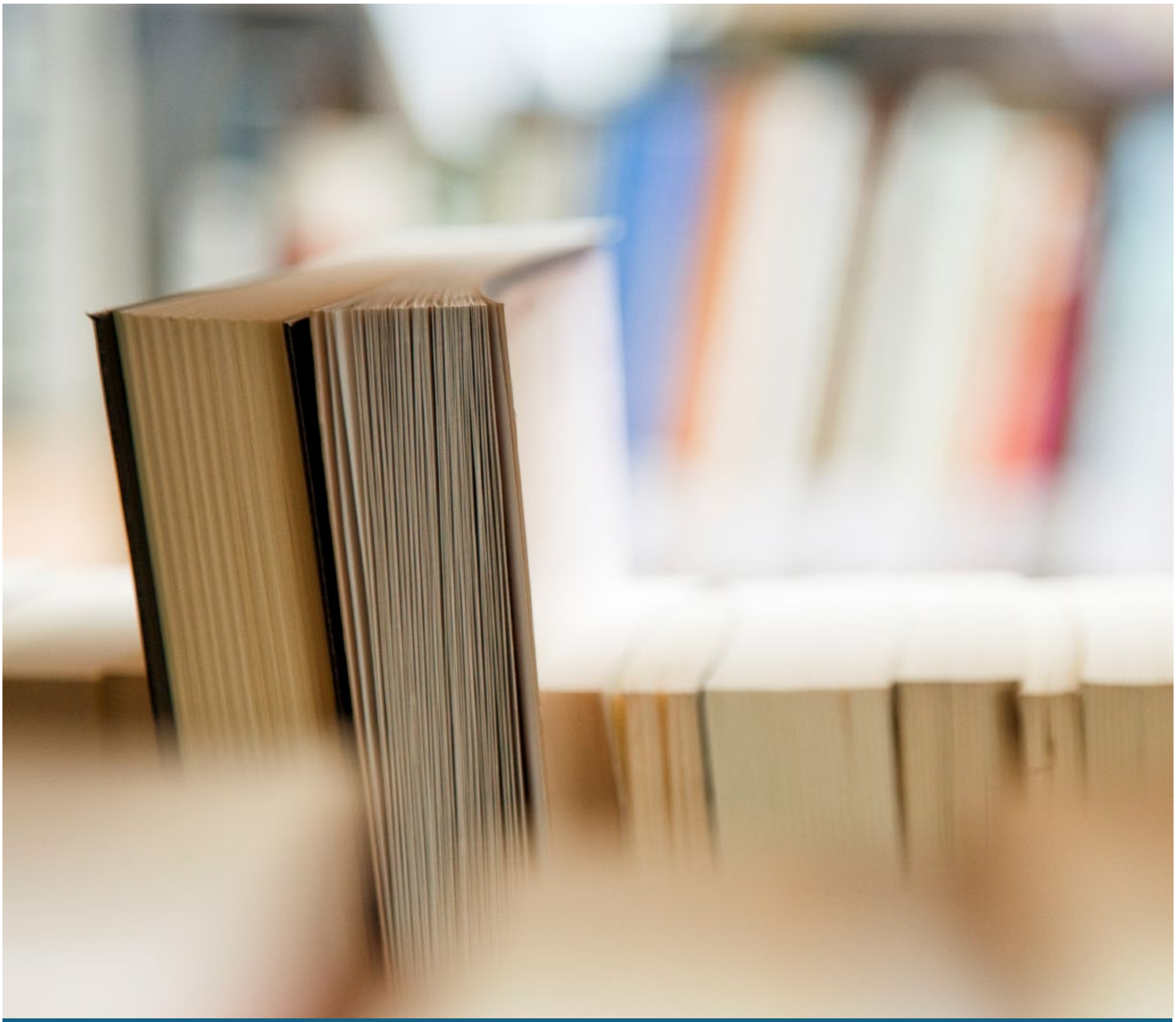


# Literature Review

## A Critical Review of Cloud Security Risks in the Financial Sector: Regulatory, Technological, and Ethical Perspectives

David Abiodun

7th December 2025

MSc Enterprise IT Management

# Introduction

Interconnected technological, regulatory and ethical pressures shape cloud security in financial services. Existing literature consistently identifies misconfiguration, identity compromise and API vulnerabilities as leading causes of cloud breaches (Shahzad, 2020; Alharthi et al., 2021). However, the empirical evidence base is constrained by underreporting of incidents and limited transparency from cloud service providers, which reduces the methodological reliability of many findings (Woods, 2022). Regulatory expectations continue to evolve, with frameworks such as GDPR, FCA operational-resilience guidance and the EU's DORA imposing increasingly stringent requirements for accountability, data governance and ICT third-party risk, although authors diverge on whether these measures adequately mitigate systemic concentration risks (Bank of England, 2022; Corrêa et al., 2023).

A further area of contention concerns the role of AI within cloud-security architectures. Studies position AI both as a potential threat vector—through model exploitation and data-poisoning attacks—and as a mechanism for improving detection and policy enforcement, raising unresolved questions about explainability and accountability in high-stakes environments (Corrêa et al., 2023).

These debates highlight the need for a critical synthesis of technological, regulatory and governance perspectives. The following thematic review evaluates converging and conflicting viewpoints to assess how cloud-security risks are conceptualised and where significant gaps remain in understanding their implications for financial institutions.

## Cloud Adoption in the Financial Sector: Opportunities and Risks

Cloud adoption in financial services is powerfully shaped by regulatory expectations for resilience, scalable analytics and cost efficiency. Cloud platforms support real-time fraud detection and global service delivery, particularly for FinTechs and digitally native banks (Woods, 2022). However, these benefits introduce dependencies on third-party CSPs and distributed architectures, altering organisational and sector-wide risk exposure. Misconfiguration persists as a dominant vulnerability, with errors in access rules, storage settings and identity policies frequently implicated in breaches (Alharthi, Alassafi and Walters, 2021). This prevalence highlights the operational complexity of cloud provisioning and the need for automated baselines aligned to NIST CSF and ISO 27001 configuration and access-control standards.

Shared-responsibility misunderstandings further exacerbate exposure. Firms often assume CSPs handle controls that remain their responsibility, leaving gaps in IAM, encryption and monitoring that stem from governance maturity rather than technical constraints (Shahzad, 2020).

Methodological variability across the literature complicates interpretation. Incident-based studies rely on disclosed breaches, conceptual papers provide limited empirical grounding, and regulatory assessments—such as FCA operational-resilience reviews—offer sectoral insights but little technical depth (Bank of England, 2022).

These disparities shape the debate around concentration risk. While DORA and the Bank of England warn that reliance on a small number of hyperscale providers could lead to systemic disruption, Woods (2022) frames the issue as an organisational vulnerability stemming from limited visibility and uneven capabilities. This contrast reinforces that cloud dependency constitutes both an institutional and systemic risk.

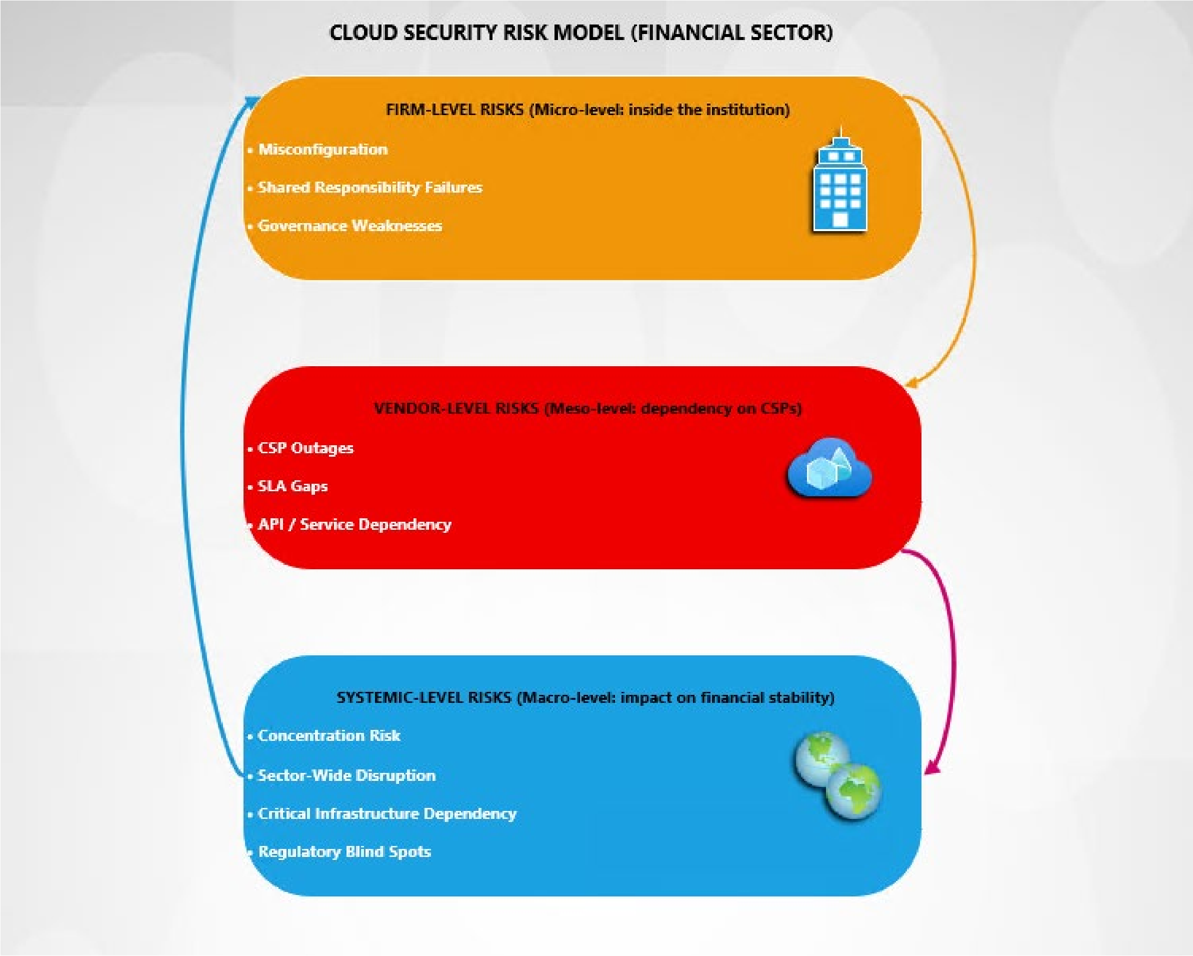

CLOUD SECURITY RISK MODEL (FINANCIAL SECTOR)
FIRM-LEVEL RISKS (Micro-level: inside the institution)
• Misconfiguration
• Shared Responsibility Failures
• Governance Weaknesses
VENDOR-LEVEL RISKS (Meso-level: dependency on CSPs)
• CSP Outages
• SLA Gaps
• API / Service Dependency
SYSTEMIC-LEVEL RISKS (Macro-level: impact on financial stability)
• Concentration Risk
• Sector-Wide Disruption
• Critical Infrastructure Dependency
• Regulatory Blind Spots

*Figure 1: Regulator-Focused Cloud Risk Escalation Model*

## Regulatory and Compliance Frameworks

Financial institutions operate within stringent regulatory frameworks governing cloud adoption. UK GDPR (2021) and the Data Protection Act 2018 impose requirements for data minimisation, privacy by design and accountability, obliging firms to embed robust data-governance and privacy-engineering controls within cloud architectures. FCA outsourcing and operational-resilience expectations emphasise auditability, exit planning and third-party oversight, yet smaller FinTechs often struggle to meet these requirements due to limited resources and constrained visibility into CSP environments (Woods, 2022). Frameworks such as NIST RMF and ISO 27001 provide structured control baselines. Still, several authors argue that they were designed for relatively static systems and remain imperfectly aligned with dynamic, multi-tenant, or serverless cloud architectures (Alharthi et al., 2021). DORA further extends accountability by imposing direct oversight of critical ICT third-party providers, although its practical implementation remains contested.

Cross-border data transfers introduce additional complexity. Schrems II (2020) invalidated the EU–US Privacy Shield, highlighting geopolitical and surveillance risks. Kuner (2021) argues that mechanisms such as SCCs cannot fully mitigate jurisdictional exposure, reinforcing the need for cautious region selection and encryption-by-default practices.

Regulatory literature itself exhibits methodological limitations. GDPR case law provides normative guidance but limited operational insight, while FCA and Bank of England materials rely on firm self-assessments that lack technical depth. These constraints—legal abstraction, supervisory opacity and limited empirical evidence—create gaps between regulatory expectations and feasible cloud-security architectures. A central contradiction emerges: regulators prioritise transparency and auditability, whereas CSPs maintain inherently opaque multi-tenant environments, leaving firms to reconcile compliance obligations with structural constraints on visibility.

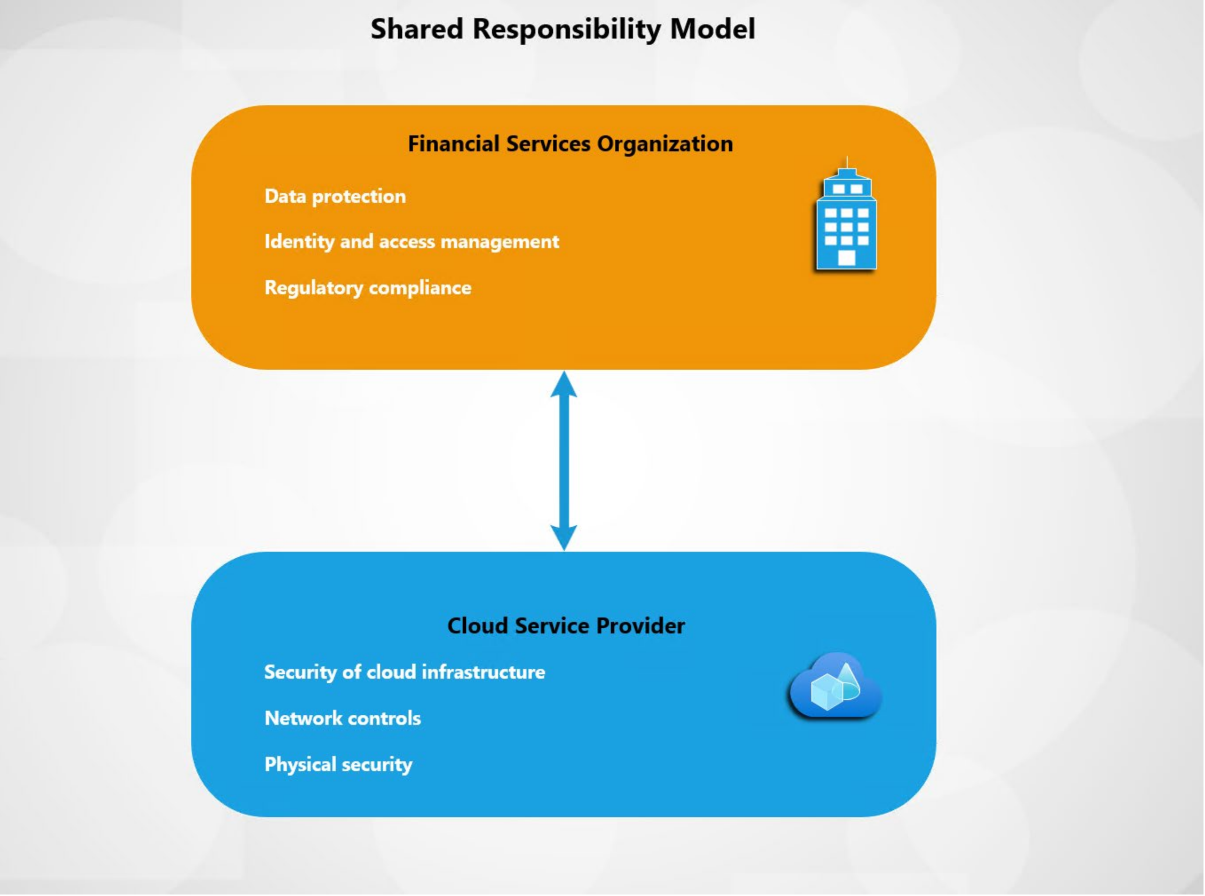

Shared Responsibility Model
Financial Services Organization
Data protection
Identity and access management
Regulatory compliance
Cloud Service Provider
Security of cloud infrastructure
Network controls
Physical security

*Figure 2: Illustration of the shared responsibility model in financial services.*

## Technological Threat Landscape

The cloud-security threat landscape encompasses misconfiguration, identity compromise, API exploitation, supply-chain vulnerabilities and emerging AI-driven attack vectors. Misconfiguration is consistently identified as the most common breach vector, with Shahzad (2020) attributing most recent incidents to errors in access controls, storage policies and identity settings. This pattern suggests that internal governance weaknesses frequently outweigh external threats, reinforcing the need for automated configuration baselines aligned with NIST and ISO 27001 control requirements.

API exploitation is an escalating concern as open banking, identity and payment APIs expand the attack surface. Weak authentication, token mismanagement and insufficient rate limiting can enable sophisticated intrusions (Alharthi et al., 2021), making API governance and continuous monitoring central to resilience. Identity compromise presents similarly high impact: attackers increasingly target cloud IAM systems through credential theft, OAuth manipulation and privilege escalation (Woods, 2022), underscoring that identity, not network perimeter, is now the primary control plane.

Hypervisor and CSP supply-chain risks are less empirically evidenced but potentially severe. Due to CSP operational secrecy, research relies on theoretical modelling rather than observed incidents. However, Woods (2022) argues that a hypervisor compromise could expose multiple tenants simultaneously, highlighting structural opacity and the need for regulatory transparency under FCA and DORA.

Evidence strength varies across threats: misconfiguration is strongly validated through investigations; API and IAM risks have moderate empirical support; hypervisor and supply-chain vulnerabilities remain largely hypothetical. This hierarchy clarifies where controls can be evidence-driven and where precautionary principles are necessary.

The Capital One breach provides empirical confirmation of these patterns, with MIT's analysis showing that a misconfigured WAF and over-privileged IAM role enabled large-scale data exfiltration (Khan et al., 2022).

Diagram 3: Cloud Threat Landscape Map

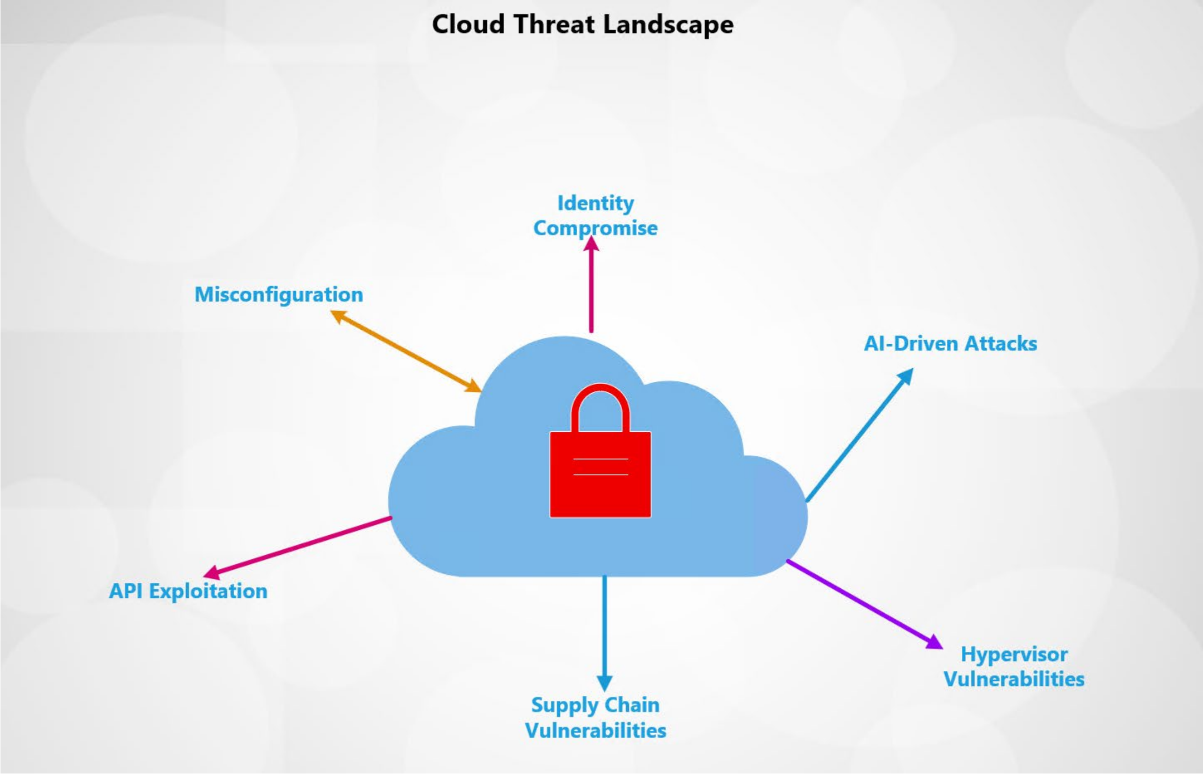
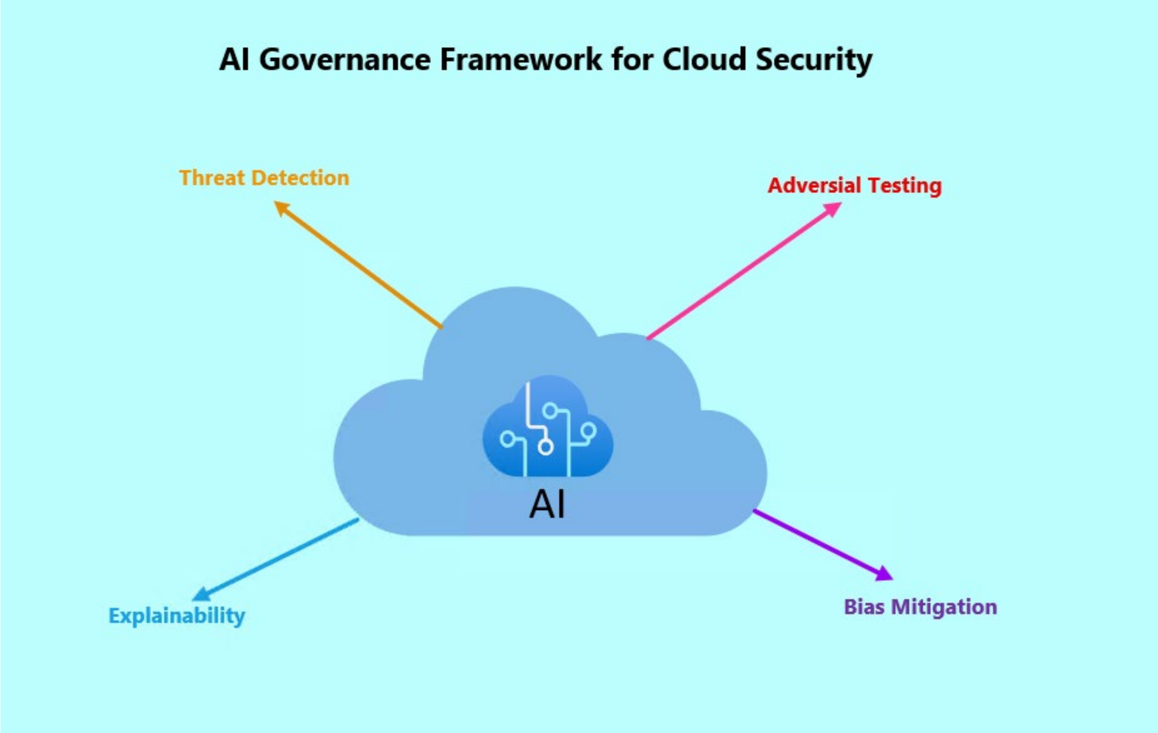


*Figure 3: Cloud Threat Landscape Map identifying key attacks.*

## AI-Driven Mitigation Tools

AI is increasingly embedded in cloud-security operations, enhancing anomaly detection, threat intelligence and fraud analytics. Studies report 30–50% precision gains over rule-based systems (Kunduru, 2023), and AI's capacity to analyse high-volume telemetry has made it central to monitoring and incident response. However, these benefits introduce parallel vulnerabilities. Corrêa et al. (2023) highlight risks such as model poisoning, adversarial examples and data-integrity manipulation, showing how attackers can exploit the exact data-driven mechanisms that strengthen detection. Opaque model behaviour also raises ethical concerns: fairness, accountability and bias in automated fraud-scoring systems remain contested issues (Mittelstadt, 2019), reinforcing the importance of explainability, oversight and alignment with emerging standards such as the NIST AI RMF and ISO 42001.

Confidence in AI-driven security tools is undermined by limited independent validation. Vendor performance claims are rarely reproducible due to confidentiality constraints, restricting scrutiny by regulators, academics and firms. Most evaluations rely on synthetic or proprietary datasets, meaning reported gains may not generalise to adversarial cloud environments. Similarly, adversarial-testing research tends to occur under controlled laboratory conditions, overlooking distributed architectures and the real-world operational pressures typical of financial services. These methodological constraints—closed datasets, constrained reproducibility and artificial testing environments—limit the evidentiary strength of AI-security claims and may overstate practical effectiveness.



.

*Figure 4: AI Governance Framework for Cloud Security.*

## Governance and Ethical Considerations

Ethical concerns such as transparency, accountability and fairness are central to cloud security in financial services. Opaque cloud infrastructure and AI-driven decision systems undermine trust when outcomes cannot be explained or independently validated (Corrêa et al., 2023), necessitating the integration of responsible AI and explainability principles into cloud governance frameworks. Accountability gaps persist because CSPs restrict access to internal infrastructure and telemetry data, creating “black-box” environments in which financial institutions retain regulatory responsibility despite having limited operational visibility (Kuner, 2021). This misalignment between responsibility and control challenges established notions of due diligence and risk ownership.

Cross-border data transfers introduce additional ethical and operational tensions. Schrems II (2020) demonstrated how weaker foreign surveillance protections may expose financial data to disproportionate risks, forcing firms to balance cloud efficiency with duties of care related to confidentiality, sovereignty and client trust.

Ethical analyses within the literature are themselves constrained. AI-ethics research often relies on normative argument rather than empirical validation, while CSP accountability work is mainly grounded in legal interpretation rather than operational evidence. These limitations mirror wider methodological weaknesses: limited transparency prevents researchers and regulators from verifying risk claims, generating epistemic opacity that affects incident detection, forensic analysis and resilience planning. Ethical issues, therefore, function not as abstract principles but as material operational vulnerabilities, underscoring the need for governance models that integrate ethical, technological and regulatory evidence.

## Synthesis of Debates and Gaps

Across the literature, there is a broad consensus that cloud adoption delivers operational efficiencies while simultaneously introducing significant vulnerabilities. Misconfiguration, IAM weaknesses, API exposure and limited CSP visibility consistently emerge as dominant risks, while AI enhances detection but adds complexity through opacity, fairness concerns and adversarial manipulation. However, the evidence base underpinning these insights remains thin: incident datasets are incomplete, regulatory transparency is constrained, research on AI auditability is still emerging and privacy obligations vary across jurisdictions, producing uneven analytical foundations.

These tensions reflect methodological divergence across disciplines. Technical studies rely heavily on simulations or underreported incidents; regulatory analyses are predominantly normative and emphasise systemic stability; and ethical scholarship focuses on legitimacy, fairness and accountability. Cloud-governance frameworks often lack empirical validation and are rarely tested in live financial environments (Rebollo et al., 2015), reinforcing the fragmented nature of current knowledge.

A clear pattern therefore emerges: technological literature examines micro-level vulnerabilities, regulatory sources frame macro-level systemic risks, and ethical work interrogates the legitimacy of opaque infrastructures and AI-driven decisions. Because these perspectives seldom converge, cloud-security governance in financial services remains siloed. This review identifies the absence of an integrated, multi-level framework linking technical controls, regulatory expectations, and ethical principles as a central gap limiting the sector’s ability to formulate coherent, evidence-based responses to cloud risk.

## Recommendations

### *For Regulators*

- Mandate greater CSP transparency and independent technical audits. Addressing the opacity and information asymmetry identified across the literature and echoed in global regulatory critiques (Jones & Knaack, 2019).

- Harmonise international cloud-security and financial-data regulations.

  Addressing jurisdictional fragmentation and enhancing cross-border operational resilience requires proportionate, coherent standards aligned with emerging calls for more harmonised digital-finance regulation. Liu and Tiwari (2023) underscore how divergent regulatory frameworks complicate cloud-based data governance, reinforcing the need for coordinated international oversight.

### *For Financial Institutions*

- Adopt identity-first security architectures.

  IAM is consistently identified as a core safeguard against account hijacking and the enforcement of least-privilege access in cloud environments (Rebollo *et al.*, 2015).
  Strengthening IAM enhances resilience against the dominant threat vectors observed in financial-sector breach patterns.

- Implement automated configuration baselines and continuous telemetry.

  Continuous monitoring and vulnerability scanning improve early detection of misconfigurations and anomalous activity in cloud systems (Ahmadi, 2024), reducing human error and strengthening configuration integrity across dynamic multi-cloud environments.

- Conduct independent validation of AI models.

  AI enhances threat detection but remains vulnerable to opacity, bias and adversarial manipulation, requiring oversight beyond vendor assurances (Corrêa, Galvão and Santos, 2023; Mittelstadt, 2019). Independent model validation strengthens trustworthiness and helps institutions meet regulatory expectations for fairness, transparency and robust decision-making.

### *For CSPs*

- Publish standardised, verifiable security attestations

  Including configuration integrity, applied controls and audit evidence—to bridge current visibility gaps and support regulatory oversight.

***For AI Vendors***

- Provide transparent robustness, bias and testing documentation, enabling financial institutions to meet regulatory expectations for explainability and model governance.

These recommendations respond directly to the gaps identified across the literature, particularly the lack of empirical validation, methodological transparency and cross-jurisdictional coherence. By grounding governance improvements in the limitations of observed evidence, this review not only summarises existing research but also outlines concrete directions for future scholarly investigation.

## Conclusion

Cloud computing is now integral to financial services but continues to present intertwined technological, regulatory and ethical challenges. Persistent risks—such as misconfiguration, IAM weaknesses, API exposure and restricted visibility into CSP environments—mirror patterns observed in other highly regulated sectors where organisations lack complete control over underlying infrastructure (Sharma, 2024). AI enhances detection and operational resilience yet introduces vulnerabilities related to adversarial manipulation, opacity and fairness (Corrêa, Galvão and Santos, 2023; Mittelstadt, 2019). Across financial, healthcare and public-sector domains, technological innovation routinely outpaces regulatory adaptation, resulting in fragmented oversight and inconsistent compliance expectations (Sharma, 2024).

The literature converges on the view that secure and accountable cloud adoption requires integrated governance that blends technical controls, regulatory alignment, privacy-by-design practices, ethical oversight and significantly greater transparency from CSPs. Without such convergence, cloud-dependent financial institutions will continue to face elevated operational, legal and systemic risks.

This review contributes to the field by demonstrating how evidence gaps, regulatory opacity and ethical constraints collectively hinder the development of robust cloud-security governance. It highlights the absence of a unified, multi-level framework capable of synthesising technological, regulatory, and ethical perspectives. This gap limits the sector's ability to develop coherent, empirically grounded responses to evolving cloud risks.

**Word Count** 2195

## References

Ahmadi, S. (2024)‘Systematic literature review on cloud computing security: Threats and mitigation strategies’, Journal of Information Security, 15, pp. 148–167.

Alharthi, A., Alassafi, M. and Walters, R. (2021)‘Addressing security misconfigurations in cloud computing’, Journal of Cloud Computing, 10(1), pp. 1–15. https://doi.org/10.1186/s13677-021-00257-6

Alouffi, B., Hasnain, M., Alharbi, A., Alosaimi, W., Alyami, H. and Ayaz, M. (2021) ‘A systematic literature review on cloud computing security: Threats and mitigation strategies’, IEEE Access, 9, pp. 57792–57807.

Bank of England (2022) Operational resilience: Impact tolerances for essential business services. London: Bank of England.

Corrêa, N.K., Galvão, C. and Santos, J.W. (2023)‘Worldwide AI ethics: A review of 200 guidelines’, Patterns, 4(100857), pp. 1–20. https://doi.org/10.1016/j.patter.2023.100857

Court of Justice of the European Union (2020) Data Protection Commissioner v Facebook Ireland and Maximillian Schrems (C-311/18). Luxembourg: CJEU.

FCA (2023) FG16/5: Guidance for firms outsourcing to the cloud and other third-party IT services. London: Financial Conduct Authority.

Jones, E. and Knaack, P. (2019) ‘Global financial regulation: Shortcomings and reform options’, Global Policy, 10(2), pp. 193–206. https://doi.org/10.1111/1758-5899.12656

Khan, S., Kabanov, I., Hua, Y. and Madnick, S. (2022) *A systematic analysis of the Capital One data breach: Critical lessons learned*. ACM Transactions on Privacy and Security, 26(1), pp. 1–29. doi:10.1145/3546068.

Kunduru, A.R. (2023) ‘Artificial intelligence advantages in cloud FinTech application security’, Central Asian Journal of Mathematical Theory and Computer Sciences, 4(8), pp. 48–53.

Kuner, C. (2021) Transborder data flows and data privacy law. Oxford: Oxford University Press.

Liu, Y. and Tiwari, A. (2023) ‘Unravelling cross-country regulatory intricacies of data governance’, Journal of Global Information Policy and Governance, 8(2), pp. 115–134.

Mittelstadt, B. (2019) ‘Principles alone cannot guarantee ethical AI’, Nature Machine Intelligence, 1(11), pp. 501–507. https://doi.org/10.1038/s42256-019-0114-4

NIST (2020) Risk Management Framework for Information Systems and Organizations (SP 800-37, Rev. 2). Gaithersburg, MD: National Institute of Standards and Technology.

Rebollo, O., Mellado, D., Fernández-Medina, E. and Mouratidis, H. (2015) ‘Empirical evaluation of a cloud computing information security governance framework’, Information and Software Technology, 58, pp. 44–57. https://doi.org/10.1016/j.infsof.2014.09.008

Shahzad, F. (2020) ‘Comparative analysis of cloud security issues’, International Journal of Advanced Computer Science and Applications, 11(3), pp. 405–412.

Sharma, L. (2024) Compliance and regulatory challenges in cloud computing: A sector-wise analysis. Delhi: University of Delhi.

Woods, M. (2022) ‘Operational resilience and cloud computing in UK financial services’, Journal of Financial Regulation and Compliance, 30(2), pp. 123–139.