A Security Framework for Modern Cloud-Based Financial Software

Lalit Agarwal
University of Maryland
lagarwa1@umd.edu

***Abstract*—Financial firms are moving more of their software, data, and customer-facing services into cloud environments. The move is understandable: cloud platforms make it easier to scale systems, release products quickly, and support digital banking experiences that customers now expect. The same move, however, also changes the security problem. A bank is no longer protecting only a set of internal servers; it is managing identity, configuration, data movement, third-party platforms, regulatory obligations, and operational resilience across a much larger technology ecosystem. This paper proposes the Financial Cloud Cybersecurity Framework (FCCF), a practical model for securing cloud-based financial software. The framework is organized around three connected layers: technical controls, regulatory alignment, and organizational governance. Technical controls include encryption, identity and access management, zero trust, configuration monitoring, segmentation, and continuous detection. Regulatory alignment connects those controls to requirements such as PCI-DSS, GDPR, CPPA, OCC expectations, audit readiness, and data residency. Organizational governance addresses the people and decision-making structures that often determine whether security controls work in practice, including board oversight, CISO accountability, employee training, incident response, and vendor-risk management. Drawing on case examples from Capital One, JPMorgan Chase, Wells Fargo, and European financial institutions, the paper argues that financial cloud security failures rarely come from a single missing tool. More often, they emerge when technical decisions, compliance responsibilities, and leadership accountability are not joined together. FCCF is presented as an integration framework that can help financial institutions evaluate risk, strengthen resilience, and adopt cloud software without losing sight of customer trust.**

***Index Terms*—cloud security, financial software, cybersecurity framework, risk governance, compliance, zero trust**

I. Introduction

Cloud computing has become part of the basic operating model for modern financial institutions. Banks, payment networks, lenders, insurers, and fintech firms use cloud platforms to process transactions, store customer information, support analytics, and deliver digital products at a pace that older infrastructure often cannot match. The appeal is clear. Cloud environments give financial firms the ability to scale quickly, experiment with new services, and reduce some of the operational burden associated with maintaining physical data centers.

Yet the security stakes are unusually high in finance. A cloud-based financial application may hold personal information, payment data, account records, credit information, transaction histories, and internal decisioning logic. A failure in such a system can create more than a technical outage. It can damage customer confidence, trigger regulatory scrutiny, expose sensitive data, and interrupt services that people and businesses depend on every day.

Existing standards such as NIST, ISO/IEC 27001, PCI-DSS, and GDPR provide useful starting points, but they do not always speak directly to the way financial institutions experience cloud risk. Some standards focus heavily on security controls; others emphasize privacy, payment data, or management systems. In practice, however, a financial cloud program has to bring these concerns together. A secure architecture is not enough if the organization cannot prove compliance. Compliance documentation is not enough if the cloud environment is poorly configured. Governance is not enough if engineering teams lack automated controls and clear ownership.

This paper proposes the Financial Cloud Cybersecurity Framework (FCCF) as a sector-specific model for closing that gap. FCCF is built around three layers: technical controls, regulatory alignment, and organizational governance. The central argument is straightforward: financial institutions need a framework that reflects how cloud security actually fails and how it must be managed in practice. The paper is guided by three research questions: How can financial institutions strengthen cybersecurity while adopting cloud-based software? How can technical controls, compliance requirements, and leadership accountability be combined into one usable model? What lessons can be drawn from financial institutions such as Capital One, JPMorgan Chase, Wells Fargo, and European banks?

II. Literature Review

The recent literature on cloud cybersecurity points to a common theme: cloud risk is not only a matter of tools or infrastructure. It is a combination of technical design, organizational behavior, vendor dependency, and regulatory pressure. This is especially true in financial services, where cloud adoption touches sensitive data, payment systems, audit obligations, and customer trust.

Ahmadi~[1] identifies recurring cloud security threats such as data breaches, account compromise, malware,

denial-of-service activity, unauthorized access, and weak configuration practices. The review also emphasizes common safeguards, including encryption, identity and access management, vulnerability management, monitoring, employee awareness, and the use of artificial intelligence for threat detection. For financial institutions, this reinforces the need for security controls that are continuous rather than occasional. A quarterly review cannot keep up with cloud environments that change every day through deployments, permission updates, and infrastructure automation.

Research focused on banking cybersecurity reaches a similar conclusion. Tran~[2] explains that banks are moving from older, isolated forms of defense toward more integrated cybersecurity models shaped by artificial intelligence, blockchain, automation, cloud platforms, and connected digital services. At the same time, the review notes persistent barriers: cost, scale, resource constraints, and increasingly sophisticated threat actors. In other words, technology has improved, but the environment has also become harder to defend. This supports the need for a framework that does not treat security tools as a complete answer.

Regulation is another major force in the literature. The Digital Operational Resilience Act, or DORA, reflects a broader shift in financial regulation: supervisors are no longer concerned only with whether a firm has controls on paper. They are also concerned with whether the firm can withstand, respond to, and recover from technology disruptions. DORA's focus on information and communication technology risk, incident reporting, resilience testing, and third-party providers shows how cloud dependency has become part of systemic financial risk [3], [4].

Industry guidance also points toward a more integrated approach. KPMG~[5] highlights zero trust, identity-centered security, micro-segmentation, AI-enabled monitoring, and vendor-risk oversight as priorities for financial services. These areas are not separate workstreams in a mature security program. They are connected. A zero-trust model depends on identity controls. Identity controls depend on governance. Vendor oversight depends on legal, compliance, procurement, and engineering teams sharing the same risk picture.

The case examples in the source article strengthen this argument. Capital One illustrates the danger of misconfiguration and unclear accountability. JPMorgan Chase shows how governance, security investment, red-team testing, and zero-trust practices can support a stronger posture. Wells Fargo highlights the influence of regulatory scrutiny on technology choices, while European banks show how data sovereignty and cross-border compliance shape cloud strategy [6]. Taken together, the literature and case evidence suggest that financial cloud security needs a unified model. FCCF attempts to provide that model by linking technical safeguards, regulatory obligations, and governance structures in one framework.

III. Problem Statement and Research Objectives

The main problem addressed in this paper is the gap between the speed of cloud adoption in financial services and the maturity of cybersecurity governance around that adoption. Financial firms are under pressure to modernize. Customers expect fast digital services, business teams want shorter release cycles, and technology teams want the scalability of cloud platforms. But the same speed that makes cloud attractive can also create risk when access rules, configurations, vendor responsibilities, and audit expectations are not managed carefully.

Many financial institutions already use recognized standards. The challenge is that these standards are often applied in pieces. One team may focus on PCI-DSS, another on cloud architecture, another on privacy, and another on enterprise risk. When these efforts are disconnected, security gaps can fall between organizational boundaries. A cloud misconfiguration may look like an engineering issue, but it can quickly become a regulatory, legal, customer trust, and board-level issue.

The objective of this research is to develop a practical framework that helps financial institutions view cloud cybersecurity as an integrated operating model. Specifically, the paper aims to identify recurring cybersecurity risks in financial cloud software; compare those risks across selected institutional cases; map the risks to technical, regulatory, and governance dimensions; and propose FCCF as a structured model for assessing and improving cloud cyber resilience.

IV. Methodology and Approach

This study uses a qualitative framework-development approach. That choice fits the purpose of the paper because the goal is not to measure one narrow technical control in isolation. Instead, the goal is to understand how different forms of risk appear across standards, regulations, case examples, and financial-sector cloud practices, and then organize those findings into a practical framework.

Data were collected from three main sources. First, established cybersecurity and compliance frameworks were reviewed, including NIST, ISO/IEC 27001, PCI-DSS, GDPR, and shared-responsibility guidance used in cloud environments. These sources helped identify baseline security expectations such as encryption, access control, audit logging, incident response, and management accountability.

Second, the study reviewed case examples discussed in the source material, including Capital One, JPMorgan Chase, Wells Fargo, and European financial institutions. These cases were useful because they show cloud risk from different angles. Capital One highlights configuration and accountability gaps. JPMorgan Chase emphasizes heavy security investment and governance maturity. Wells Fargo reflects a compliance-driven approach shaped by regulatory pressure. European banks demonstrate how data sovereignty and cross-border rules affect cloud design (FCCF, n.d.).

Third, recent scholarly and industry literature was reviewed to connect the framework to current discussions about cloud security, banking cybersecurity, operational resilience, and financial regulation. The goal was to avoid building FCCF from one incident or one standard. Instead, the framework was developed by looking for patterns across multiple sources.

The analysis used thematic coding. Recurring ideas were grouped into categories such as identity control, encryption, configuration management, monitoring, shared responsibility, vendor risk, regulatory reporting, data sovereignty, incident response, and executive oversight. These themes were then organized into the three FCCF layers: technical controls, regulatory alignment, and organizational governance.

A structured comparison matrix was used as the main analytic tool. Each institutional case was mapped against the three layers to identify where the organization appeared strong, where it faced challenges, and what lessons could be drawn. The matrix was not intended to rank institutions. Its purpose was to make the framework concrete by showing how different cloud security issues appear in real financial environments.

TABLE I
FCCF Layer Summary

Layer	Focus	Controls or Practices
Technical Controls	Protect software, data, and infrastructure	Encryption, IAM, zero trust, configuration scanning, segmentation, SIEM, threat intelligence.
Regulatory Alignment	Connect controls to financial obligations	PCI-DSS, GDPR, CPPA, OCC expectations, audit trails, data residency, incident reporting.
Organizational Governance	Create accountability and operating discipline	Board oversight, CISO accountability, training, incident response, vendor-risk management, responsibility matrix.

V. Framework and Case Application

FCCF is designed as a layered model rather than a checklist. This is important because financial cloud security is not solved by completing a list of controls once. It requires an operating rhythm in which engineering, compliance, risk, and leadership teams understand how their responsibilities connect.

The first layer, technical controls, covers the safeguards closest to the software and cloud environment. These include encryption and tokenization for sensitive data, identity and access management, multi-factor authentication, least privilege, role-based access control, configuration scanning, segmentation, blast-radius reduction, continuous monitoring, and threat intelligence. This layer asks a practical question: if an attacker gains access, a developer makes a configuration mistake, or a service behaves unexpectedly, how quickly can the institution detect, contain, and recover?

The second layer, regulatory alignment, connects those controls to financial-sector obligations. Payment security, privacy rules, auditability, data residency, operational resilience, and third-party oversight must be built into the cloud program instead of being treated as paperwork after deployment. In this layer, compliance becomes evidence-based. Logs, access reviews, configuration records, incident exercises, vendor assessments, and control mappings become part of the institution's ability to prove that it is managing risk responsibly.

The third layer, organizational governance, focuses on the people and decision-making structures behind the technology. Board reporting, CISO and CIO accountability, employee training, incident response playbooks, red-team exercises, and vendor-risk management all belong here. The reason is simple: even strong controls can fail if responsibility is unclear, security exceptions are poorly governed, or leadership does not receive meaningful risk information.

The Capital One case shows why FCCF must include both technical and governance dimensions. The lesson is not that cloud platforms are inherently unsafe. The more useful lesson is that cloud environments require disciplined configuration management, clear responsibility boundaries, and meaningful oversight. A single weak configuration can become a major institutional event when sensitive data, regulatory obligations, and customer trust are involved.

JPMorgan Chase provides a different lesson. Its approach illustrates the value of investing in layered security, zero-trust practices, vendor oversight, and active testing. In FCCF terms, this case demonstrates that governance is not separate from engineering. Strong governance helps ensure that technical controls are funded, tested, monitored, and improved over time.

Wells Fargo and European financial institutions show how regulation shapes cloud adoption. A slower or more cautious cloud strategy is not necessarily a sign of weak innovation. In heavily regulated environments, the ability to demonstrate control, data residency, audit readiness, and operational resilience can determine how quickly cloud adoption can proceed. FCCF therefore treats regulatory alignment as a core design layer rather than a final review step.

VI. Findings and Discussion

The first major finding is that financial cloud cybersecurity depends on balance. Technical tools matter, but they are not enough by themselves. A firm may have encryption, monitoring, and identity controls, yet remain exposed if no one has clear ownership of cloud risk or if leadership receives only shallow security reporting. The opposite is also true. A firm may have strong policies and committees, but if cloud permissions, configurations, and vendor integrations are not continuously tested, the policy environment will not protect the system in practice.

The second finding is that misconfiguration remains one of the most serious cloud risks for financial institutions.

Cloud services can be secure, but they are also easy to change quickly. That flexibility creates room for mistakes. Permissions can become too broad, storage can be exposed, logging can be incomplete, and temporary exceptions can become permanent. In finance, these mistakes carry outsized consequences because the affected data and services are often highly sensitive.

The third finding is that compliance has become a design constraint, not a separate reporting activity. Financial institutions cannot wait until the end of a project to ask whether the system satisfies PCI-DSS, GDPR, OCC expectations, CPPA, or data-sovereignty requirements. In a cloud environment, regulatory expectations must influence architecture, vendor selection, data placement, logging, encryption, access control, and incident response from the beginning.

The fourth finding is that the shared-responsibility model needs to be made explicit. Cloud providers secure parts of the underlying infrastructure, but financial institutions remain responsible for their data, users, applications, configurations, monitoring, and regulatory obligations. Many problems arise in the space between those responsibilities. FCCF addresses this by encouraging institutions to maintain a responsibility matrix for each major cloud provider and vendor relationship.

The fifth finding is that cybersecurity should be treated as business resilience. When a financial software platform fails, the harm is not limited to the security team. Customers may lose access to services, regulators may ask for explanations, executives may face reputational damage, and business operations may slow down. FCCF is useful because it gives leaders a way to discuss cloud security in business terms without losing the technical detail needed by engineering teams.

These findings also point to a cultural issue. Some organizations still treat cybersecurity as a hurdle to clear before launch. That mindset is risky in cloud environments because the system continues to change after launch. A healthier approach is to treat security as part of the product lifecycle. Access reviews, configuration checks, vendor reassessments, incident exercises, and regulatory evidence should be part of normal operations. In that sense, FCCF is less about adding bureaucracy and more about making the right responsibilities visible before a failure forces attention.

VII. Conclusion and Future Research

This paper argues that financial cloud cybersecurity must be managed as an integrated discipline. Financial institutions are adopting cloud software because it helps them move faster, scale more easily, and support modern digital services. But speed and flexibility bring new responsibilities. Sensitive customer data, payment systems, regulated records, and critical business processes cannot be protected through isolated technical controls or last-minute compliance reviews.

FCCF offers a practical way to organize this challenge. Its three layers - technical controls, regulatory alignment, and organizational governance - reflect the reality that cloud security succeeds or fails across multiple levels at once. The technical layer protects systems and data. The regulatory layer ensures that controls meet financial-sector obligations. The governance layer makes sure people, leaders, and vendors are accountable for how cloud risk is managed. The framework's value is not that it replaces NIST, ISO 27001, PCI-DSS, GDPR, or DORA. Its value is that it helps financial institutions connect those requirements into a model that is easier to apply to cloud-based financial software.

The broader message is that customer trust is built through discipline. A financial institution may not be able to prevent every attempted attack or every operational disruption, but it can build systems that reduce exposure, detect issues quickly, limit damage, and recover with transparency. That kind of resilience requires more than technology. It requires leadership attention, regulatory awareness, engineering rigor, and a culture that treats security as part of everyday work.

Future research should test FCCF in live financial institutions through interviews, surveys, maturity assessments, or detailed case studies. Researchers could also develop a scoring model that allows institutions to measure their maturity across the three FCCF layers. Additional work should examine how FCCF applies to AI-driven banking, real-time payments, open banking APIs, multi-cloud environments, and fintech partnerships. These areas are likely to increase both innovation and risk. As financial services become more digital and interconnected, future cybersecurity research should focus not only on how to stop attacks, but also on how to design financial software that is trustworthy, resilient, and accountable from the start.

References

[1] S. Ahmadi, "Systematic literature review on cloud computing security: Threats and mitigation strategies," *Journal of Information Security*, vol. 15, no. 2, pp. 148–167, 2024, doi: 10.4236/jis.2024.152010.

[2] T. N. Tran, "Systematic review of cybersecurity in banking: Evolution from pre-Industry 4.0 to post-Industry 4.0 in artificial intelligence, blockchain, policies and practice," *arXiv preprint arXiv:2503.00070*, 2025, doi: 10.48550/arXiv.2503.00070.

[3] European Securities and Markets Authority, "Digital Operational Resilience Act (DORA)," 2025. [Online]. Available: https://www.esma.europa.eu/esmas-activities/digital-finance-and-innovation/digital-operational-resilience-act-dora

[4] European Insurance and Occupational Pensions Authority, "Digital Operational Resilience Act," 2025. [Online]. Available: https://www.eiopa.europa.eu/digital-operational-resilience-act-dora_en

[5] KPMG, "Cybersecurity considerations 2025: Financial services sector," 2025. [Online]. Available: https://kpmg.com/cn/en/insights/2025/05/cybersecurity-considerations-2025/financial-services.html

[6] L. Agarwal, "Financial Cloud Cybersecurity Framework (FCCF)," unpublished manuscript, 2026.