International Journal of Scientific Research and Modern Technology (IJSRMT)
Volume 4, Issue 11, 2025
DOI: https://doi.org/10.38124/ijsrmt.v4i11.954
ijsrmt.com

Designing a Cloud-Native DevOps Framework for Risk Management in Digital Financial Service

Oreoluwa Omoike[1]

Publication Date: 2025/11/08

Abstract

The complexity of digital financial services (DFS) and the adoption of cloud-native infrastructures have boosted the demand for well-built, automated and compliant risk management frameworks. The paper argues that the Cloud-Native DevOps Framework for Risk Management (CNDF-RM) is aimed at implementing the principles of automation and constant monitoring as well as compliance-as-code in financial system lifetimes. Using recent studies on cloud-native DevOps, model deployment, and financial compliance (Kanimetta, 2025; Tambi, 2024; Ugwueze, 2024; Mittal, 2025), the paper highlights how cloud-native DevOps changes the traditional risk governance approach in the context of risk regulatory mechanisms being directly implemented into the CI/CD pipeline and infrastructure orchestration. The framework connects Infrastructure as Code (IaC), continuous security validation, and observability layers with the workflows to minimise vulnerabilities and regulatory violations related to digital finance. Finally, this paper introduces a holistic model of the integration of resilience, scalability, and governance in multi-cloud financial ecosystems through a design-science conceptual approach. Findings show that a cloud-native DevOps system can help financial institutions to recover faster in the event of disruption, have higher levels of compliance assurance, and real-time operational transparency, which remain key requirements to maintain trust in the digital financial ecosystems.

Keywords: *Cloud-Native DevOps; Risk Management; Digital Financial Services; Compliance-as-Code; CI/CD; Cloud Security; FinTech Resilience.*

I. INTRODUCTION

The digital landscape in the financial service has transformed the manner in which institutions create value, manage risk, and stay in line with regulatory standards. As the reliance on distributed infrastructures, pipelines of automation, and multi-cloud ecosystems has increased, they have imposed the necessity on risk-management architectures that can be changed and adapted to emerging threats and opportunities. The current environment of financial institutions is fast-paced and secure: the ability to implement the quickly changing digital offerings and simultaneously comply with a high level of compliance standards, including PCI-DSS, GDPR, and ISO/IEC 27001 (Tambi, 2024). The traditional models of risk management, which tend to rely on fixed infrastructure and manual governance controls, are becoming less and less suitable in managing the pace or changeability of contemporary digital operations.

In this context, the advent of the cloud-native DevOps offers a paradigm shift of strategy. The concept of cloud-native technology is based on microservice, container, orchestration, and continuous integration/continuous deployment (CI/CD) technologies, allowing organisations to create scalable and fault-tolerant systems that are portable (Ugwueze, 2024). These technologies do not just enhance operational efficiency, but when coupled with DevOps practices that have focused on collaboration, automation, and monitoring, they become tools for preventive risk management. By implementing risk controls into CI/CD lines in the form of compliance-as-code and infrastructure-as-code (IaC), financial institutions can dynamically identify, mitigate and respond to risks, minimising errors by humans and time to response (Kumbhani, 2025).

However, the integration of DevOps and risk management is not conceptualised sufficiently in the scholarly literature and practice. Although the current body of literature has reported on cloud-native DevOps in the context of product delivery (Mittal, 2025) and model deployment (Tambi, 2024), frameworks (related to the systematic risk governance in digital financial ecosystems) have been largely lacking. Moreover, most FinTech organisations are unable to reconcile innovation and agility and regulatory responsibility, which introduces gaps in the operation of automated deployment settings.

This paper fills this gap by developing a Cloud-Native DevOps Framework of Risk Management in Digital Financial Services (CNDF-RM). The framework combines the cloud-native architecture, DevOps automation, and risk-governance mechanisms into a single model that contributes to the improvement of compliance, resilience, and observability throughout the financial software lifecycle.

➢ *The Key Objectives are to:*

- Examine existing limitations and issues of the traditional risk-management frameworks within cloud-based financial contexts.
- Develop best practices from cloud-native DevOps, security automation, and compliance engineering.
- Establish a conceptual framework, which incorporates risk-management mechanisms.

Hence, this study, through the design-science approach, provides a strategic blueprint that reinvents the perception and management of risk in the era of continuous delivery and distributed cloud infrastructures.

II. LITERATURE REVIEW

➢ *FinTech Cloud-Native Architecture and Digital Transformation*

Cloud-native architecture has become one of the paradigms of digital transformation because it enables systems to be scaled, resilient, and agile through microservices, containerization, and orchestration technologies (Kubernetes and Docker) (Ugwueze, 2024). As opposed to traditional monolithic infrastructures, which are based on rigid, vertically scaled infrastructures, cloud-native environments support distributed, modular infrastructures, which can dynamically scale horizontally and survive failures. This change, in a financial sense, is allowing institutions to deploy and iterate services quickly and maintain operational reliability, which is a very important consideration in high-volume environments like mobile banking and digital payments (Tambi, 2024).

Cloud-native design also promotes continuous integration and deployment (CI/CD), making it possible to make changes iteratively without interfering with the services. Ugwueze (2024) states that CI/CD pipelines are conducive to automation and minimise human intervention as software releases can be faster and more reliable. Non-compliance, security vulnerabilities, and system drift are, however, more likely to occur as the deployment velocity increases. This has prompted researchers to support the idea of incorporating security and compliance controls into the development pipeline itself and make governance more of a design principle, rather than a control mechanism (Kanimetta, 2025).

➢ *DevOps Methodology and Risk Management Integration*

DevOps, which has its roots in the merger of development and operations, is concerned about breaking the organisational silos with the help of automation, collaboration, and constant feedback (Humble and Farley, 2010). In the financial services sector, it has enhanced the frequency of deployment, decreased the lead time of changes, and minimised the failure rates (Mittal, 2025). However, the deployment of DevOps in highly regulated industries has to deal with a complex compliance environment and requires the adoption of so-called DevSecOps or RiskOps strategies that directly integrate governance, security, and risk management controls into automated processes.

Kanimetta (2025) notes that cloud-native DevOps approaches have been specifically revolutionary in financial messaging like SWIFT, where there can be operational blockages and delays in compliance with conventional manual configuration processes. The way cloud-native DevOps can transform regulatory compliance into a competitive edge can be illustrated by integrating Azure-native automation, Infrastructure as Code (IaC), and CI/CD pipelines with embedded risk validations. On the same note, Tambi (2024) argues that the speed and fault tolerance of machine learning (ML) models are improved by CI/CD-driven orchestration using tools like Kubernetes and Kubeflow in the financial context- especially fraud detection and credit score models.

➢ *Cloud-Native Risk Management and Compliance Automation*

Traditional risk management of digital financial services is based on a fixed governance structure and regular audits. But with systems becoming cloud-native, the dynamic threats or regulatory changes cannot be responded to with swiftness using static controls (Tambi, 2024). Modern models have shifted focus to continuous monitoring, compliance-as-code and automated policy enforcement to make financial applications safe and compliant during their lifecycle (Syed, 2024).

Compliance-as-code, in which regulatory rules are formalised and automatically checked at the time of deployment, is used to make sure that configuration, data processing, and access control rules are compliant with regulatory standards, including PCI-DSS and GDPR. This paradigm will change compliance into a post-deployment process into an inseparable component of system design and delivery (Kanimetta, 2025). Similarly, AI-based anomaly detection and predictive analytics-based continuous monitoring solutions give early notifications of possible risk exposures. According to Mittal (2025), the increasing use of machine learning in the DevOps pipeline, which is also called MLOps, is where smart monitoring facilitates the proactive prediction of failures, threat detection, and prevention of incidents. However, despite these developments, studies have shown that most financial institutions are struggling to operationalise these principles. Such issues as the management of data sovereignty in hybrid or multi-cloud environments, the explainability of automated decision-making systems, and the alignment of different regulatory demands across jurisdictions are the challenges (Tambi, 2024). To resolve these problems, there is a need to have structures that integrate technical agility and governance-by-design concepts so that the institutions can integrate compliance and security controls at the infrastructure level.

➢ *Research Gap and Theoretical Implications*

Despite the evidence of the previous studies, which indicate a high level of advancement in the implementation of cloud-native DevOps, it is still possible to observe the lack of unified frameworks that would help to balance the principles of DevOps with the risk-management and compliance goals in digital finance. Most studies are more concerned with operational or technological approaches, including the automation of CI/CD (Ugwueze, 2024) or AI-based monitoring (Mittal, 2025), but do not fully explain how these practices form a coherent risk-management architecture. Moreover, the empirical validation of the DevOps-based compliance models in financial systems is still a limited aspect because of the regulatory limitations on experimentation and data sensitivity. This paper bridges this gap by proposing a Cloud-Native DevOps Framework of Risk Management (CNDF-RM) that integrates the concepts of automation, compliance-as-code and observability.

III. METHODOLOGY

In this research, the design science research (DSR) approach is used to conceptualise and create a Cloud-Native DevOps Framework of Risk Management in Digital Financial Services (CNDF-RM). The design science is suitable in this research since it aims at producing an artefact, in this case, a conceptual framework, which can solve a real-world problem through an iterative synthesis and validation (Hevner et al., 2004). In contrast to empirical or purely theoretical research, DSR focuses on solution-oriented research based on practical relevance and theoretical rigour.

The CNDF-RM framework was designed in a cyclic process of integrating a systematic literature review with a comparative analysis of the available cloud-native and DevOps frameworks. Peer-reviewed articles on cloud-native DevOps (Kanimetta, 2025), AI-enabled DevOps pipelines (Mittal, 2025), model deployment in financial applications (Tambi, 2024), and best practices in cloud-native application development (Ugwueze, 2024) were considered primary source materials. Additional sources like Syed (2024) on disaster recovery and compliance optimisation were also used to make sure that the framework covered the needs of resilience and risk mitigation.

➢ *Conceptual Approach*

The design process followed three core phases:

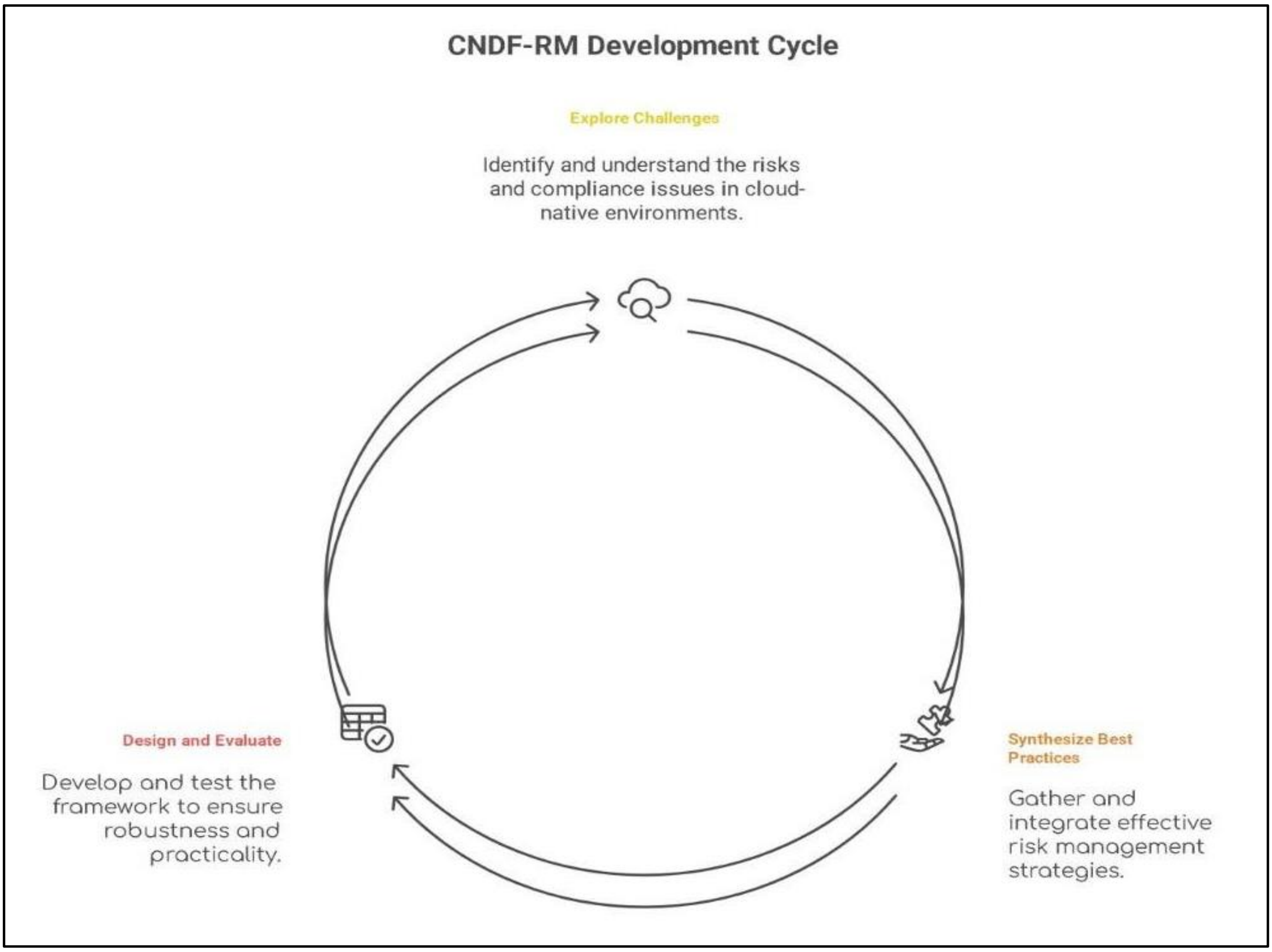
CNDF-RM Development Cycle
Explore Challenges
Identify and understand the risks and compliance issues in cloud-native environments.
Synthesize Best Practices
Gather and integrate effective risk management strategies.
Design and Evaluate
Develop and test the framework to ensure robustness and practicality.

Fig 1 Design Process for Developing the Cloud-Native DevOps Framework for Risk Management (CNDF-RM)

- *Framework Design Principles*

The design of the CNDF-RM was conducted using six core design principles:

- *Automation by Design:*

The CI/CD lifecycle. Automate all risk-checks and compliances with Infrastructure as Code (IaC) and Compliance as Code (CaC).

- *Continuous Governance:*

The risk management must be shifted from periodic audit-based evaluations to continuous embedded monitoring.

- *Observability and Traceability:*

The observability of the real-time system, logging, and event correlation should provide visibility to the auditors and regulators (Ugwueze, 2024).

- *Resilience by Redundancy:*

The framework should facilitate fault-tolerant and self-healing to reduce financial service disruption (Syed, 2024).

- *Security Integration:*

The DevSecOps principles, with the implementation of the security testing, vulnerability scanning, and policy enforcement, should be integrated into the automated deployment pipelines (Kanimetta, 2025).

- *Regulatory Alignment:*

The system must be able to trace to compliance requirements (PCI-DSS, GDPR, etc., ISO/IEC 27001) so that operational processes can be audited.

IV. CONCEPTUAL FRAMEWORK

Cloud-Native DevOps Framework of Risk Management (CNDF-RM) is a structured framework for integrating automated risk and compliance controls into the life cycle of digital financial services. The framework, which combines three interdependent areas: DevOps automation, cloud-native architecture, and risk governance, can guarantee a secure, compliant, and resilient financial application, both during design and deployment. It is consistent with the DevSecOps and Compliance-as-Code ideas, which transform regulatory rules into programmable rules that are automatically executed on multi-cloud and hybrid infrastructures, where distributed systems and regulatory heterogeneity are significant obstacles to operational control and information integrity (Kanimetta, 2025; Tambi, 2024).

- *Conceptual Diagram Description*

As illustrated in Figure 1, the CNDF-RM structure is a multilayered structure that consists of five layers that are horizontally stacked and linked to each other. The Governance and Compliance Layer stipulates regulatory policies and compliance templates in the form of code, which guarantees compliance with standards like PCI-DSS, GDPR, and ISO 27001. Traceable governance is made possible through automated audit trails and policy mapping. Risk Intelligence and Monitoring Layer is an AI-based tool that captures telemetry data, identifies anomalies, and predicts compliance violations in real time (Mittal, 2025). CI/CD Automation Layer is an automation of the integration, testing, and deployment systems with security scanners and policy validators to ensure that the risk thresholds are kept at predefined levels (Ugwueze, 2024). Infrastructure-as-Code and Configuration Layer is a framework that handles infrastructure provisioning with declarative code (e.g., Terraform, CloudFormation), ensures resilience by replicating, encrypting, and failing over (Syed, 2024). Finally, the Observability and Feedback Layer is where all the components are consolidated to provide logs, traces and metrics to support continuous visibility and adaptive risk governance. These interrelated layers create a feedback ecosystem that creates cycles of compliance and minimisation of risk exposure.

- *Functional Dynamics of the CNDF-RM*

The CNDF-RM model works in a feedback loop where governance is incorporated in all stages of the DevOps cycle. During the Code Commit Phase, security and compliance analysis of new code is carried out automatically. In the Build and Test Phase, automated pipelines check artefacts and roll back in the event of non-compliance. During the Deployment Phase, infrastructure is deployed through IaC templates with controls (encryption and segmentation) embedded. The monitoring and Learning Phase uses AI-based analytics to identify risks in real-time, whereas the Governance Feedback Phase streamlines compliance regulations and changes policies dynamically. Such a cyclical process will turn risk management into a living and automated discipline that is part of the cloud-native DevOps processes.

- *Strategic Value of the Framework*

The CNDF-RM framework has great strategic benefits for digital finance. It improves regulatory assurance through automation of compliance checks, which reduces non-conformities and delays in audits (Kanimetta, 2025). Its operational resilience is enhanced by its continuous monitoring mechanisms, which keep the systems up and self-healing in the event of disruptions (Syed, 2024). Reduction of manual approvals allows fast innovation without governance being jeopardised. The framework also facilitates cross-cloud consistency with policy-based provisioning, which guarantees consistency of heterogeneous infrastructures (Tambi, 2024). Finally, its built-in observability and analytics encourage a data-driven risk culture, enabling financial DevOps teams to make evidence-based proactive decisions.

V. DISCUSSION

The transition to a cloud-native DevOps paradigm and the abandonment of traditional risk management have become the major paradigm shift in the operations of financial services. In the past, risk management was reactive with a greater focus on post-incident reviews and audits. Nonetheless, according to Mittal (2025), DevOps facilitates continuous governance, which makes compliance part of the day-to-day operations. The CNDF-RM supports this model with the introduction of compliance-as-code and automated risk validation into CI/CD pipelines to make regulatory enforcement a normal operational activity and not an independent oversight role. In the example, encryption or access control may be checked by automated scripts before deployment, which minimises policy violations (Kanimetta, 2025). This shift in the concept of separation of duties to the shared responsibility model encourages the collaboration of the developers, engineers, and compliance officers by codifying governance tools.

Furthermore, digital financial resilience relies on smart surveillance and redundancy. Syed (2024) highlights that backup and disaster recovery on multi-clouds must be optimised to ensure continuity. This is actualised in the CNDF-RM framework, which gathers metrics, logs and traces together into a single observable layer, where AI analytics identify anomalies (latency spikes or unauthorised access) and cause an automated remediation. This is in line with the deployment strategies proposed by Tambi (2024) to achieve resilience by design, which guarantees the self-healing operations that minimise downtime and financial vulnerability. Moreover, the observability of real-time is conducive to regulatory transparency through the provision of continuous, verifiable audit trails, and compliance is turned into a quantifiable value of operational integrity.

More so, ensuring cross-jurisdictional alignment is one of the greatest challenges to global FinTechs. The slow pace of regulation is a common issue with manual audits, which enables systems to get ahead of certification (Ugwueze, 2024). The CNDF-RM handles this by standardising policies of compliance at the infrastructure level by Compliance-as-Code, and applying uniform standards (such as GDPR and PCI-DSS) across geographical areas. Because compliance is incorporated into the Azure DevOps pipelines, as illustrated by Kanimetta (2025), it improves the synchronisation of the technological processes with the regulatory frameworks. Nonetheless, this automation involves an initial cost on policy modelling and interdisciplinary teamwork that can convert legal regulations to programmable logic.

In spite of the potential, there are technical and cultural obstacles to the adoption of CNDF-RM. Traditional systems of existing financial institutions are frequently not modular in order to deploy microservices, preventing automation (Mittal, 2025). The resisting organisational elements also remain, with traditional compliance teams being based on hierarchies that are supported by documents (Tambi, 2024). Additionally, the governance across multi-clouds presents risks in terms of non-uniformity in the enforcement of policies and interoperability. Lastly, AI-based decision-making is questionable in matters of ethics and explainability - automated risk responses should be transparent and auditable to hold them accountable (Syed, 2024).

VI. CONCLUSION

Managing digital financial services (DFS) has radically evolved due to the shift to cloud-native infrastructures and operations that are driven by DevOps, to achieve agility, scalability, and innovation. This transformation has, however, also brought in new aspects of operational, regulatory, and cybersecurity risks, which require constant, smart, and automated management. These challenges were considered in this study, and thus, the Cloud-Native DevOps Framework on Risk Management (CNDF-RM), a structured and multi-layered framework that has risk governance, compliance automation, and resilience directly integrated into the DevOps lifecycle was designed.

The CNDF-RM is based recent studies on risk management as an open and dynamic approach is a part of the operational and daily development practice. Hence, the framework provides real-time evolution of the governance mechanisms along with system deployments through alignment of Compliance-as-Code, Infrastructure-as-Code, and continuous observability. Its stratified structure, which encompasses governance, monitoring, automation, configuration, and feedback, forms a feedback loop of detection, validation and responsiveness, as well, compliance and resilience become persistent and automated disciplines, instead of response event-driven actions.

The CNDF-RM is a contributor to theoretical and practical risk-concerned DevOps progress. It theoretically reinvents risk management in the form of a dynamic ecosystem sitting inside the framework of cloud-native design. In practice, it provides financial institutions with an effective channel of reaching compliance by design and resilience by automation, allowing them to innovate without jeopardising the integrity of governance. The focus of the framework on closed-loop automation and real-time intelligence can uphold the continuity of operation and regulatory transparency, which are important requirements in the field of digital finance due to its growing decentralisation and data-driven character.

Finally, empirical proof of CNDF-RM with pilot studies in a financial institution or a FinTech start-up should be included in further research to investigate how effectively the technique minimises operational risks and improves compliance results. Furthermore, further partnership between financial bodies and technology providers and regulators will be necessary to ensure that the model will be fine-tuned in application in various jurisdictions and other financial ecosystems.

REFERENCES

[1]. Tambi, V. K. (2025). Cloud-native model deployment for financial applications. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.5366158

[2]. Kanimetta, D. K. (2025). Cloud-native DevOps for SWIFT deployments on Azure: Redefining

operational agility in financial messaging. *Journal of Computer Science and Technology Studies, 7*(6), 959–966. https://doi.org/10.32996/jcsts.2025.7.113

[3]. Ugwueze, V. (2024). Cloud native application development: Best practices and challenges. *International Journal of Research Publication and Reviews, 5*, 2399–2412. https://doi.org/10.55248/gengpi.5.1224.3533

[4]. Mittal, A. (2025). *AI-driven DevOps automation for cloud-native application modernization*. TechRxiv. https://doi.org/10.36227/techrxiv.175339625.55743194/v1

[5]. Kumbhani, J. (2025). *DevOps in FinTech: Ensuring compliance & security in agile development*. Zymr. https://www.zymr.com/blog/devops-in-fintech

[6]. Hevner, A. R., March, S. T., Park, J., & Ram, S. (2004). Design science in information systems research. *MIS Quarterly*, *28*(1), 75–105.

[7]. Syed, A. (2024). Disaster recovery and data backup optimization: Exploring next-gen storage and backup strategies in multi-cloud architectures. *International Journal of Emerging Research in Engineering and Technology, 5*, 32–42. https://doi.org/10.63282/3050-922X.IJERET-V5I3P104