Future-Ready Cloud Strategy for FinBankX

Hybrid Multi-Cloud Adoption through Terraform, AI, and Zero-Trust Governance

DAbiodun_12696259

13th October 2025

MSc Enterprise IT Management

1. Executive Summary

FinBankX, a digital-first financial services provider, is expanding into the EU and Nigeria with a hybrid multi-cloud strategy ensuring secure, scalable, and compliant operations. Terraform-first IaC with policy-as-code and zero-trust enforces GDPR/NDPR, while AWS supports non-PII analytics (Bernstein et al., 2009; Alharkan and Aslam, 2021; Hashizume et al., 2013).

AI-driven fraud detection, CI/CD automation, and cloud-native orchestration enhance resilience and efficiency. The risk framework addresses residency, security, cost, and vendor lock-in, supported by ISO 27001 and NIST CSF standards (Shi et al., 2016; Preskill, 2018).

Anticipated outcomes include improved fraud resilience, faster delivery, cost optimisation with an expected 30% reduction, and more substantial regulatory confidence.

Looking ahead, FinBankX will adopt edge computing for low-latency payments, explore quantum pilots, and implement sustainable cloud practices to support ESG goals and long-term competitiveness (Masanet et al., 2020).

2. Cloud Solution Design (IaC-led, Hybrid/Multi-Cloud)

2.1 Business Needs → Cloud Mapping

Table 1: Cloud Capabilities Addressing FinBankX's Regulatory, Security, and Operational Needs

Need	Cloud capability (IaC-provisioned)
Regulatory compliance & data residency (GDPR/NDPR/FCA)	Regionalised data stores (Azure EU/UK South; AWS eu-west-2; AWS Africa/Cape Town as applicable), private endpoints, policy-as-code (Azure Policy, AWS Config)
24/7 payments uptime	Multi-AZ deployments, cross-region DR, active/active API layer behind global DNS
Fraud detection at scale	Event streaming (Kafka/MSK/Event Hubs), serverless inference (Lambda/Azure Functions), GPU node pools (AKS/EKS)
Cost control & transparency	FinOps tagging, budgets/alerts, autoscaling, spot for batch analytics, reserved capacity for steady workloads
Security by default	HSM/KMS/Key Vault, customer-managed keys, private networking, zero-trust, managed identities

2.2 Target Architecture

- **Hybrid core**: On-premises/colocation for high-sensitivity workloads and HSMs; **Azure** for core banking apps and data; **AWS** for analytics/fraud ML (Bernstein et al., 2009; Hashizume et al., 2013).
- **Network**: Hub-and-spoke VNets/VPCs, private link/endpoint access to PaaS, transit gateway/ExpressRoute/Direct Connect (via resilient MPLS/SD-WAN), unified DNS.
- **Platform runtime**: AKS (core APIs, mobile backend), EKS (fraud/analytics), Functions/Lambda for event-driven tasks, managed databases (Azure SQL MI, DynamoDB or Aurora Serverless for analytics sidecars).
- **Security & identity**: Azure AD/Entra ID as IdP, SSO to AWS via federated roles, Key Vault + AWS KMS/HSM.
- **Observability**: Azure Monitor/Log Analytics + Amazon CloudWatch, centralised SIEM (Microsoft Sentinel) via log forwarders.
- **Resilience**: Active/active API gateways (Azure Front Door + Amazon Route 53 failover), RPO ≤ 5 mins (streaming replication), RTO ≤ 1 hr (IaC redeploy + automated runbooks).

FinBankX also leverages SaaS (Microsoft 365, Dynamics 365, ServiceNow) federated through Entra ID and integrated into the zero-trust framework, ensuring GDPR/NDPR compliance with unified access controls across the hybrid multi-cloud estate.

2.3 IaC Strategy (Terraform-first)

- **Structure:** Mono-repo with versioned modules per domain (network, compute, data, security, observability).
- **State:** Remote backends with locking (Azure Storage + blob lock / S3 + DynamoDB).
- **Workspaces:** Dev, test, staging, and prod mapped to separate subscriptions/accounts.
- **Pipelines:** GitHub Actions/Azure DevOps — plan on PR, apply on protected branches with approvals; OPA/Conftest or Checkov for policy checks pre-merge.
- **Policy-as-Code:** Azure Policy (enforce private endpoints, CMK encryption) and AWS Config rules (block public S3/EBS), evaluated in CI (Guerriero et al., 2019).
- **2.4 Scalability**
- **Horizontal**: HPA on AKS/EKS for API workloads; KEDA for event-driven scale on queues/topics.
- **Autoscaling:** configured via VM Scale Sets (VMSS) or App Service Plans, with IaC ensuring consistent application of scaling rules across environments (Toka et al., 2020; Jamshidi, Ahmad and Pahl, 2016).
- **Serverless**: Functions/Lambda for KYC checks, card tokenisation webhooks, statement generation.
- **Data**: Autoscale databases (Azure SQL MI vCores), partitioned analytics stores (S3/ADLS + table formats).

- **Global entry**: Azure Front Door + CDN caching for mobile app content; Route 53 health-based failover.

2.5 Security-by-Design

Security-by-design aligns with the CIA triad (Confidentiality, Integrity, Availability), the cornerstone of information security (Ali, Al-Khalidi, & Al-Zaidi, 2024), ensuring that cloud controls address not only technical hardening but also regulatory compliance and resilience.

Network (Availability & Confidentiality): Private clusters with no public ingress; only WAF-fronted gateways are internet-facing, reducing exposure and ensuring service uptime.

Encryption (Confidentiality & Integrity): Customer-managed keys (Key Vault/KMS) protect data at rest, with TLS 1.2+ securing data in transit.

Identity (Confidentiality & Integrity): Workload identity/IRSA, JIT admin, least-privilege RBAC, and break-glass accounts with PIM strengthen access governance.

Zero Trust (Integrity & Confidentiality): Enforces least privilege, segmentation, and identity-based access controls across domains.

Supply chain (Integrity): Container image signing (Sigstore/Cosign), private registries (ACR/ECR), and SCA/SAST in CI safeguard against tampering.

Baseline (Availability & Integrity): CIS Benchmarks for AKS/EKS/VMs with daily drift detection via policy-as-code maintain consistent, secure states.

2.6 Cost Effectiveness (FinOps)

- **Tagging**: env, app, owner, cost_centre, pii_level.
- **Controls**: Budgets and anomaly alerts; rightsizing via advisor tools; reserved instances for steady services; **spot** for batch ML training.
- **Auto-off**: Schedules for non-prod clusters; lifecycle policies for cold data (S3/ADLS tiers), supported by cloud pricing model surveys that highlight the role of reserved and spot instances in reducing operational costs (Al-Roomi et al., 2013).

2.7 DR & SRE Guardrails

- **DR**: Cross-region replication (Geo-replicated storage, database replicas); IaC runbooks to rehydrate in secondary, supported by research on fault-tolerant and scalable replication schemes for cloud storage (Bonvin, Papaioannou and Aberer, 2010
- **SLOs/alerts**: Error budget policies, synthetic probes, golden signals (latency, traffic, errors, saturation).
- **Game days**: Chaos testing on non-prod; post-incident reviews feeding back into Terraform modules.

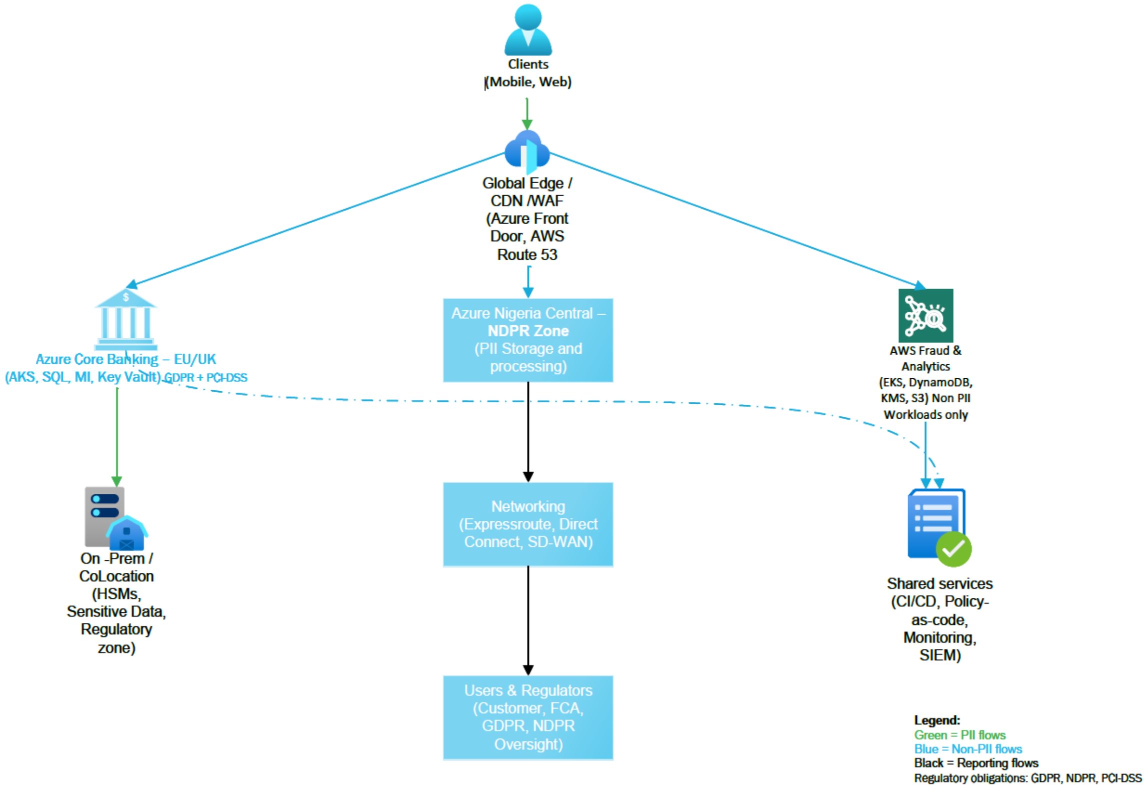

Clients
(Mobile, Web)
Global Edge / CDN /WAF (Azure Front Door, AWS Route 53
Azure Core Banking – EU/UK
(AKS, SQL, MI, Key Vault) GDPR + PCI-DSS
Azure Nigeria Central – NDPR Zone (PII Storage and processing)
AWS Fraud & Analytics
(EKS, DynamoDB, KMS, S3) Non PII Workloads only
On -Prem / CoLocation (HSMs, Sensitive Data, Regulatory zone)
Networking (Expressroute, Direct Connect, SD-WAN)
Shared services (CI/CD, Policy-as-code, Monitoring, SIEM)
Users & Regulators (Customer, FCA, GDPR, NDPR Oversight)
Legend:
Green = PII flows
Blue = Non-PII flows
Black = Reporting flows
Regulatory obligations: GDPR, NDPR, PCI-DSS

Figure 1: FinBankX Hybrid Multi-Cloud Architecture (GDPR/NDPR Aligned)

As shown in Figure 1, FinBankX's hybrid multi-cloud architecture separates GDPR and NDPR workloads across Azure and AWS, with active/active routing ensuring resilience and compliance

3. Integration of Advanced Cloud Technologies

To achieve resilience, efficiency, and regulatory alignment, FinBankX utilises advanced cloud technologies, including AI, automation, and hybrid-cloud orchestration, ensuring secure and adaptive service delivery.

3.1 Artificial Intelligence (AI) and Machine Learning (ML)

- Fraud detection and anomaly monitoring are critical differentiators for FinBankX, building on adaptive detection frameworks (Fawcett and Provost, 1997) and extended by recent Big Data-driven approaches to real-time anomaly detection and compliance (Popoola, 2023).
- **Model Training:** Anonymised, high-volume datasets are processed in AWS EKS GPU node pools and S3-based data lakes, supporting retraining while preserving data sovereignty.
- **Model Inference:** Fraud engines operate in serverless environments (AWS Lambda, Azure Functions) for low-latency checks on live payment streams, integrating with Kafka and Azure Event Hubs to handle millions of daily transactions.
- **Continuous Improvement:** Drift detection pipelines retrain and redeploy models via CI/CD, ensuring resilience against evolving fraud tactics.
- **KPIs:** <200 ms fraud check latency, ≥95% detection accuracy, ≤3% false positive rate.

3.2 Automation and Orchestration

Automation is central to FinBankX’s operational efficiency, enhancing consistency and reducing human error (Ajiga et al., 2024).

- **CI/CD Pipelines:** Secure deployments via Azure DevOps and GitHub Actions, with static and dynamic security testing (SAST/DAST) before release.
- **Infrastructure Automation:** Terraform modules executed through GitOps workflows, with peer review, policy checks (OPA/Conftest, Checkov), and approval gates.
- **Resource Optimisation:** Kubernetes HPA and KEDA dynamically scale compute resources, reducing costs while sustaining performance.
- **Self-Healing:** Automated runbooks and remediation workflows rehydrate failed services, lowering mean time to recovery (MTTR).
- **KPIs:** <1 hr MTTR, >95% pipeline success rate, and ≥20% cost savings through elastic scaling.

3.3 Hybrid Cloud and Multi-Cloud Synergy

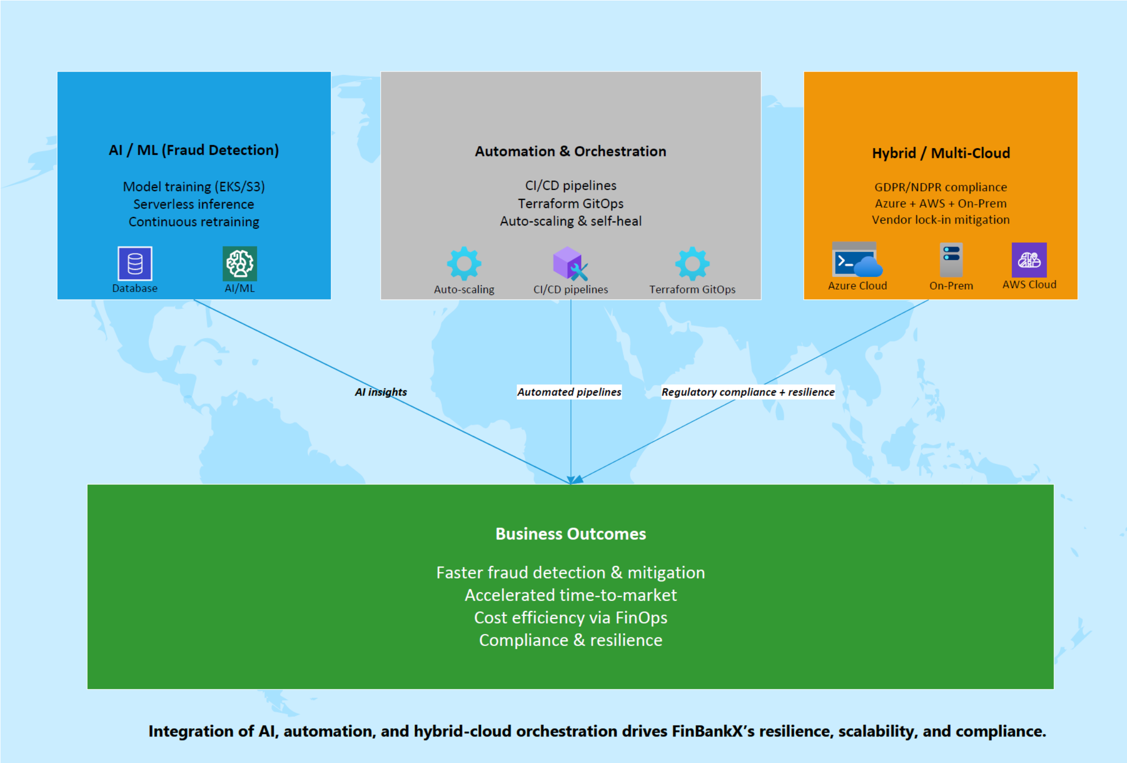
The hybrid/multi-cloud strategy (see Figure 1 and Appendix A) underpins compliance, optimisation, and continuity, aligning with findings that multi-cloud architectures improve resilience, avoid lock-in, and support regulatory alignment (Hiran and Hegde, 2018):

- **Regulatory Alignment:** PII is stored in compliance zones (Azure EU/UK for GDPR, Azure Nigeria Central for NDPR), while non-PII analytics are in AWS, ensuring legal compliance and flexibility.

- **Resilience and Interconnectivity:** ExpressRoute, Direct Connect, and SD-WAN overlays provide secure, low-latency links across cloud and on-premises domains.
- **Vendor Lock-in Mitigation:** Terraform-first IaC and open standards (Kubernetes, OpenTelemetry) ensure portability and resilience against dependency on proprietary services.
- **KPIs:** 99.95% cross-cloud uptime, <50 ms inter-cloud latency, and <3 months estimated migration time between providers.

3.4 Business Outcomes of Integration

- **Fraud Management:** Faster detection and mitigation, reducing losses and reputational risk.
- **Agility:** Accelerated time-to-market through automated deployments and continuous delivery.
- **Cost Efficiency:** Optimised resource use via elastic scaling and FinOps governance.
- **KPIs:** ≥95% fraud detection accuracy, <200 ms fraud check latency, <1 hr MTTR, and >20% cloud cost savings.



Integration of AI, automation, and hybrid-cloud orchestration drives FinBankX's resilience, scalability, and compliance.

Figure 2: Integration of AI, Automation, and Hybrid Multi-Cloud for Business Outcomes

As shown in Figure 2, the Terraform-driven pipeline integrates policy-as-code checks and CI/CD automation, reducing misconfiguration risks while enforcing consistent governance.

4. Risk and Compliance Considerations

As FinBankX expands into Nigeria and the EU, compliance with GDPR and NDPR is critical, alongside managing risks across security, cost, and vendor lock-in.

Table 2: Risk Analysis

Event	**Likelihood**	**Impact**	**Mitigation**
Misconfiguration	Medium	Data breach, service outage	Automated IaC validation, regular audits
Vendor lock-in	High	Migration difficulty, costs	Multi-cloud, open standards, contractual clauses
Cost Overruns	Medium	Profitability, project halt	FinOps monitoring, auto-scaling, anomaly detection
Compliance failure (GDPR)	Low	Fines, reputational damage	Policy-as-code, audits, zone-restricted storage
AI Model Drift/Bias	Medium	Fraud detection errors	Frequent retraining, monitoring, explainability

4.1 Data Residency and Sovereignty

- **Risk:** PaaS defaults may replicate PII outside approved jurisdictions, breaching GDPR/NDPR.
- **Impact:** Regulatory sanctions and reputational harm.

Mitigation:

Segregate workloads (Azure EU/UK for GDPR, Azure Nigeria Central for NDPR; AWS for non-PII) and enforce residency via policy-as-code, with audits ensuring compliance (Hummel et al., 2021).

4.2 Security Risk

- **Risk:** Misconfigurations in IaaS, PaaS, or SaaS may expose sensitive data.
- **Impact:** Breaches could disrupt payments and trigger penalties.

Mitigation:

Apply zero-trust networking, encryption with customer-managed keys, and continuous monitoring via centralised SIEM.

SaaS adoption introduces risks in data residency and vendor dependency, as platforms like Microsoft 365, Dynamics, and ServiceNow handle sensitive data in provider-controlled environments. Misconfiguration may cause unauthorised access or GDPR/NDPR breaches. Mitigation includes conditional access via Entra ID, customer-managed keys, and regular compliance audits.

Recent cloud breaches—such as the unsecured banking server leak which exposed over 273,000 records in 2025—highlight the importance of rigorous configuration and audit controls (Economic Times, 2025).

4.3 Vendor Lock-in Risk

Risk: Reliance on proprietary services may hinder migration and inflate costs (Opara-Martins, Sahandi and Tian, 2016).

Impact: Reduced agility and exposure to CSP pricing.

Mitigation:

Adopt Terraform-first IaC, Kubernetes for portability, open standards for observability/policy, and negotiate exit clauses.

4.4 Cost Management Risk

- **Risk:** Elastic AI/ML and SaaS adoption may exceed budgets (FinOps Foundation, 2022; Lanz and Nearon, 2022).
- **Impact:** Rising costs could undermine profitability.

Mitigation:

Apply FinOps tagging, anomaly detection, reserved/spot instances, SaaS governance, and automated cost reporting.

4.5 AI and Automation Integrity

- **Risk:** Fraud models may drift or show bias; IaC misconfigurations may spread vulnerabilities.
- **Impact:** Ineffective fraud detection or outages, breaching CBN compliance.

Mitigation:

Use drift/bias detection, secure DevOps guardrails, and chaos testing, reflecting best practice for managing bias and reliability in AI (Gichoya et al., 2023).

4.6 Compliance Monitoring / Governance Risk

- **Risk:** Evolving GDPR/NDPR and Nigeria’s Data Protection Act may outpace static controls.
- **Impact:** Non-compliance risks fines and restrictions on EU–Nigeria data flows.

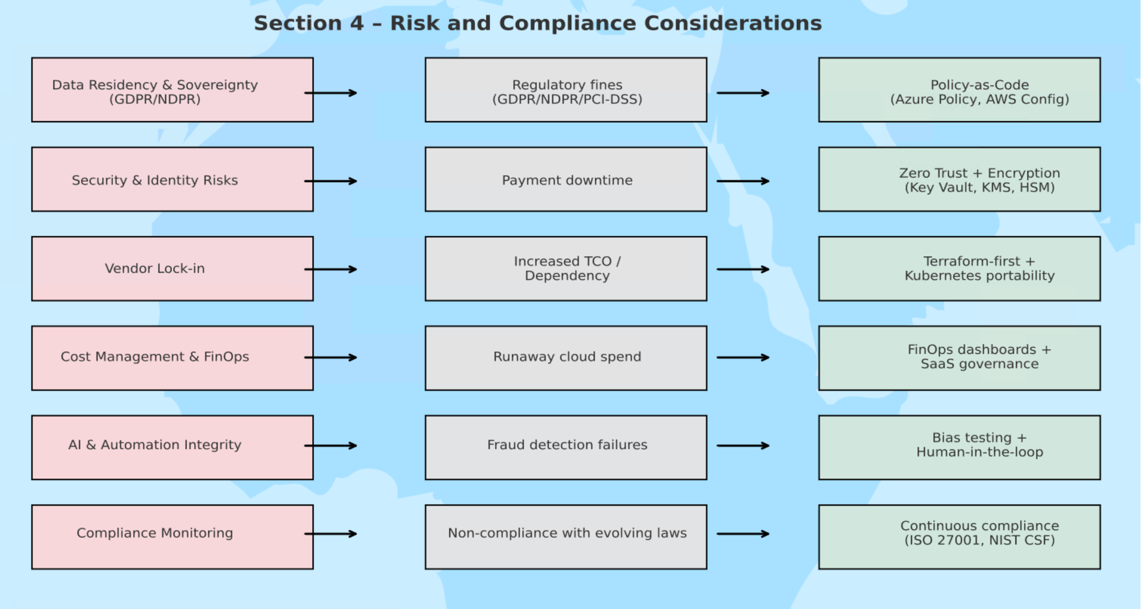
Mitigation:

Enable continuous compliance monitoring, align with ISO 27001/NIST CSF, and engage regulators proactively (Adekunle et al., 2023).

Summary of Risk Posture:

FinBankX’s risk strategy prioritises zero trust, FinOps, and policy-as-code to maintain GDPR/NDPR compliance, reduce lock-in, and manage costs while safeguarding customer trust and ensuring resilient 24/7 payments.

Figure 3: outlines FinBankX's key risks, impacts, and mitigation strategies, emphasising regulatory compliance and operational resilience.



Section 4 – Risk and Compliance Considerations

Data Residency & Sovereignty (GDPR/NDPR)	Regulatory fines (GDPR/NDPR/PCI-DSS)	Policy-as-Code (Azure Policy, AWS Config)
Security & Identity Risks	Payment downtime	Zero Trust + Encryption (Key Vault, KMS, HSM)
Vendor Lock-in	Increased TCO / Dependency	Terraform-first + Kubernetes portability
Cost Management & FinOps	Runaway cloud spend	FinOps dashboards + SaaS governance
AI & Automation Integrity	Fraud detection failures	Bias testing + Human-in-the-loop
Compliance Monitoring	Non-compliance with evolving laws	Continuous compliance (ISO 27001, NIST CSF)

Figure 3: Risk and Compliance Considerations with Mitigation Strategies

As shown in Figure 3, FinBankX’s risk posture is structured around regulatory, security, cost, and vendor lock-in categories, each linked to defined mitigations

5. Future Recommendations

FinBankX aims to strengthen its EU–Nigeria presence by advancing capabilities in latency-sensitive payments, risk analytics, and sustainable operations. Recommendations are phased to minimise risk while aligning with GDPR/NDPR obligations and key KPIs, such as fraud loss rate, authorisation latency, and cost-to-serve.

5.1 Edge Computing for Low-Latency Payments (0–12 months)

Deploy edge nodes in Lagos and Abuja to reduce mobile payment latency and enhance fraud detection. (Shi et al., 2016; Satyanarayanan, 2017).

KPIs: <150 ms authorisation latency, ≥5% uplift in fraud detection accuracy, 99.9% service availability.

Implementation Approach:

- Stand up an **Edge Gateway** pattern (K3s/AKS Edge) with local caching of non-PII features and tokenised identifiers.
- Use **privacy-preserving sync** (event sourcing; PII stays in approved regions).
- SLOs: p95 authorisation latency ≤ 150 ms in Nigeria; >99.95% local decisioning availability.

5.2 Quantum Cloud Pilots for Risk & Crypto Readiness (6–24 months)

Conduct bounded pilots using managed quantum services to explore two areas:

(1) Speeding up portfolio and credit risk Monte Carlo simulations.

(2) Preparing for post-quantum cryptography in key exchange and digital signatures. Focus on pragmatic pilots with classical–quantum hybrids (Preskill, 2018; Chen et al., 2022).

Implementation Approach:

- Establish a quantum sandbox using only synthetic data, benchmarking against classical baselines.
- Create a PQC roadmap: inventory cryptographic dependencies, test NIST candidate algorithms, and plan dual-stack transitions.

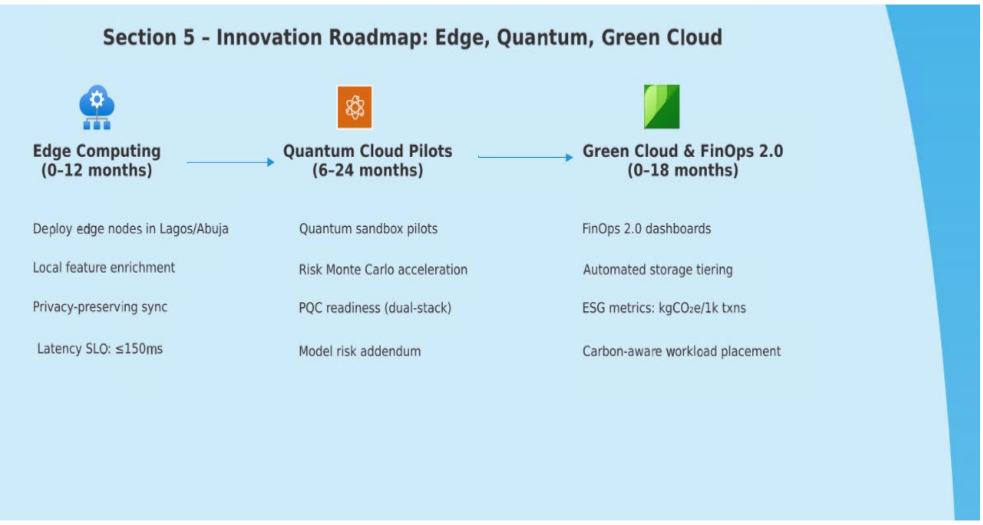
Extend governance with a model risk management addendum and conduct regulator briefings on pilot scope and data boundaries.

5.3 Green Cloud & FinOps 2.0 (0–18 months)

Adopt carbon-aware workload placement by prioritising energy-efficient regions and right-sizing services. Efficiency measures reduce data centre energy intensity (Masanet et al., 2020; Patel and Doshi, 2022). Coupling this with FinOps 2.0 practices (unit economics, anomaly detection, and automated rightsizing) will lower cost-to-serve while meeting ESG goals (FinOps Foundation, 2022).

Implementation Approach:

- Deploy carbon-intensity aware schedulers for workload placement.
- Automate rightsizing and storage tiering with FinOps 2.0 guardrails.
- Publish ESG dashboards combining cloud carbon data with financial KPIs.
- KPIs: ≤0.15 gCO_2eq per transaction, ≥15% reduction in cost-to-serve, and 100% workloads tagged for carbon and cost tracking.



Section 5 - Innovation Roadmap: Edge, Quantum, Green Cloud

Edge Computing (0-12 months)

Deploy edge nodes in Lagos/Abuja

Local feature enrichment

Privacy-preserving sync

Latency SLO: ≤150ms

Quantum Cloud Pilots (6-24 months)

Quantum sandbox pilots

Risk Monte Carlo acceleration

PQC readiness (dual-stack)

Model risk addendum

Green Cloud & FinOps 2.0 (0-18 months)

FinOps 2.0 dashboards

Automated storage tiering

ESG metrics: $kgCO_2e$/1k txns

Carbon-aware workload placement

Figure 4: Innovation Roadmap – Edge, Quantum, and Green Cloud Initiatives

5.4 Roadmap & Dependencies

- **People & skills:** Edge SRE rotation, PQC champions, FinOps analysts embedded with product teams.
- **Platform enablers:** Policy-as-code extensions for edge nodes; crypto-agility libraries; carbon/FinOps dashboards.
- **Regulatory engagement:** NDPC and EU DPA briefings on edge privacy controls and PQC timelines.

- **Exit criteria:** Measurable latency and fraud KPIs improved (5.1); documented PQC impact and migration plan (5.2); 15–25% unit cost reduction and published ESG baselines (5.3).

These recommendations extend FinBankX’s hybrid, policy-driven platform into a low-latency, crypto-agile, and sustainability-aware operating model—ensuring GDPR/NDPR compliance while improving resilience and cost efficiency (Bernstein et al., 2009; Hashizume et al., 2013; Alharkan and Aslam, 2021).

As shown in Figure 4, the phased roadmap highlights the adoption of edge computing, quantum pilots, and green cloud practices, positioning FinBankX for future innovation and ESG compliance.

Executive Conclusion

FinBankX’s cloud strategy demonstrates that a secure, scalable, and compliant hybrid multi-cloud design can directly support growth in the EU and Nigeria.

Terraform-led IaC, zero-trust, and AI automation strengthen resilience.

Future adoption of edge computing, quantum pilots, and sustainable cloud practices positions FinBankX for regulatory confidence, ESG alignment, and long-term competitiveness.

Word Count 2176

References

Adekunle, B.I., Chukwuma-Eke, E.C., Balogun, E.D. and Ogunsola, K.O. (2023) ‘Developing a digital operations dashboard for real-time financial compliance monitoring in multinational corporations’, *International Journal of Scientific Research in Computer Science, Engineering and Information Technology*, 9(3), pp. 728–746. Available at: https://doi.org/10.32628/IJSRCSEIT (Accessed: 4 October 2025).

Ajiga, D., Okeleke, P.A., Folorunsho, S.O. and Ezeigweneme, C. (2024) ‘The role of software automation in improving industrial operations and efficiency’, *International Journal of Engineering Research Updates*, 7(1), pp. 22–35. Available at: https://doi.org/10.53430/ijeru.2024.7.1.0031 (Accessed: 4 October 2025).

Ali, T., Al-Khalidi, M. and Al-Zaidi, R. (2024) ‘Information security risk assessment methods in cloud computing: comprehensive review’, *Journal of Computer Information Systems*, pp. 1–20. Available at: https://doi.org/10.1080/08874417.2024.2329985 (Accessed: 4 October 2025).

Alharkan, I. and Aslam, N. (2021) ‘A survey on GDPR compliance in cloud computing’, *Future Internet,* 13(9), pp. 1–22. Available at: https://doi.org/10.3390/fi13090224 (Accessed: 4 October 2025).

Al-Roomi, M., Al-Ebrahim, S., Buqrais, S. and Ahmad, I. (2013) ‘Cloud pricing models: a survey’, *International Journal of Grid and Distributed Computing*, 6(5), pp. 93–106. Available at: https://doi.org/10.14257/ijgdc.2013.6.5.09 (Accessed: 4 October 2025).

Bernstein, D., Ludvigson, E., Sankar, K., Diamond, S. and Morrow, M. (2009) ‘Blueprint for the Intercloud: Protocols and formats for cloud computing interoperability’, in *Fourth International Conference on Internet and Web Applications and Services*, IEEE, pp. 328–336. Available at: https://doi.org/10.1109/ICIW.2009.55 (Accessed: 4 October 2025).

Bonvin, N., Papaioannou, T.G. and Aberer, K. (2010) ‘A self-organized, fault-tolerant and scalable replication scheme for cloud storage’, in *Proceedings of the 1st ACM Symposium on Cloud Computing (SoCC’10)*. ACM, pp. 205–216. Available at: https://doi.org/10.1145/1807128.1807162 (Accessed: 4 October 2025).

Carugati, C. (2023) *The competitive relationship between cloud computing and generative AI*. Working Paper 19/2023. Brussels: Bruegel. Available at: https://www.jstor.org/stable/resrep55201 (Accessed: 4 October 2025).

Chen, J., Gheorghiu, V., Kashefi, E., Pappa, A. and Wallden, P. (2022) ‘Quantum cloud computing: recent progress and challenges’, *npj Quantum Information*, 8(1), pp. 1–13.

Economic Times (2025) ‘Data breach exposes 2.73 lakh bank records’. Available at: https://economictimes.com/tech/technology/data-breach-exposes-2-73-lakh-bank-records/articleshow/124184985.cms (Accessed: 28 September 2025).

European Parliament and Council of the European Union (2016) *Regulation (EU) 2016/679 (General Data Protection Regulation)*. *Official Journal of the European Union*.

Fawcett, T. and Provost, F. (1997) ‘Adaptive fraud detection’, *Data Mining and Knowledge Discovery*, 1(3), pp. 291–316. Available at: https://doi.org/10.1023/A:1009700419189 (Accessed: 4 October 2025).

FinOps Foundation (2022) *Cloud FinOps: Collaborative, Real-Time Cloud Financial Management*. Sebastopol, CA: O’Reilly Media.

George, J. (2022) ‘Optimising hybrid and multi-cloud architectures for real-time data streaming and analytics: Strategies for scalability and integration’,*World Journal of Advanced Engineering Technology and Sciences*, 7(1), pp. 174–185. Available at: https://doi.org/10.30574/wjaets.2022.7.1.0087 (Accessed: 4 October 2025).

Gichoya, J.W., Thomas, K., Celi, L.A., Safdar, N., Banerjee, I., Banja, J.D., Seyyed-Kalantari, L., Trivedi, H. and Purkayastha, S. (2023) ‘AI pitfalls and what not to do: mitigating bias in AI’, *British Journal of Radiology,* 96(1150), pp. 1–10. Available at: https://doi.org/10.1259/bjr.20230023 (Accessed: 4 October 2025).

Guerriero, M., Garriga, M., Tamburri, D.A. and Palomba, F. (2019) ‘Adoption, support, and challenges of infrastructure-as-code: insights from industry’, in *2019 IEEE International Conference on Software Maintenance and Evolution (ICSME).* IEEE, pp. 580–590. Available at: https://doi.org/10.1109/ICSME.2019.00092 (Accessed: 4 October 2025).

Hashizume, K., Rosado, D.G., Fernández-Medina, E. and Fernandez, E.B. (2013) ‘An analysis of security issues for cloud computing’, *Journal of Internet Services and Applications*, 4(5), pp. 1–13.

Hiran, K.K. and Hegde, V. (2018) *Multi-cloud architecture and governance*. Cham: Springer.

Hummel, P., Braun, M., Tretter, M. and Dabrock, P. (2021) ‘Data sovereignty: A review’, *Big Data & Society,* 8(1), pp. 1–17. Available at: https://doi.org/10.1177/2053951720982012 (Accessed: 4 October 2025).

Lanz, J. and Nearon, B. (2022) ‘Risk impacts of SaaS cloud computing’, *The CPA Journal*, July/August, pp. 52–57. Available at: https://www.cpajournal.com/2022/08/22/risk-impacts-of-saas-cloud-computing/ (Accessed: 4 October 2025).

Masanet, E., Shehabi, A., Lei, N., Smith, S. and Koomey, J. (2020) ‘Recalibrating global data center energy-use estimates’, *Science*, 367(6481), pp. 984–986.

National Information Technology Development Agency (NITDA) (2019) *Nigeria Data Protection Regulation (NDPR)*. Abuja: NITDA.

Nigeria Data Protection Commission (NDPC) (2023) *Nigeria Data Protection Act 2023*. Abuja: NDPC.

Opara-Martins, J., Sahandi, R. and Tian, F. (2016) ‘Critical analysis of vendor lock-in and its impact on cloud computing migration: a business perspective’, *Journal of Cloud Computing*, 5(4), pp. 1–18.

Patel, N. and Doshi, R. (2022) ‘Sustainable cloud computing: trends and research directions’, *Journal of Cloud Computing*, 11(42), pp. 1–19.

Popoola, N.T. (2023) ‘Big Data-driven financial fraud detection and anomaly detection systems for regulatory compliance and market stability’, *International Journal of Computer Applications Technology and Research*, 12(9), pp. 32–46. Available at: https://doi.org/10.7753/IJCATR1209.1004 (Accessed: 4 October 2025).

Preskill, J. (2018) ‘Quantum computing in the NISQ era and beyond’, *Quantum*, 2(79), pp. 1–22.

Satyanarayanan, M. (2017) ‘The emergence of edge computing’, *Computer*, 50(1), pp. 30–39.

Shi, W., Cao, J., Zhang, Q., Li, Y. and Xu, L. (2016) ‘Edge computing: Vision and challenges’, *IEEE Internet of Things Journal,* 3(5), pp. 637–646.

Toka, L., Dobreff, G., Fodor, B. and Sonkoly, B. (2020) ‘Adaptive AI-based auto-scaling for Kubernetes’, in *2020 20th IEEE/ACM International Symposium on Cluster, Cloud and Internet Computing (CCGRID)*. IEEE, pp. 599–608. Available at: https://doi.org/10.1109/CCGrid49817.2020.00-33 (Accessed: 4 October 2025).

Appendix A — Terraform Extract: Residency, Zero-Trust, and FinOps Guardrails

Appendix A provides a working Terraform extract that demonstrates the enforcement of GDPR/NDPR residency, customer-managed encryption keys, private endpoints, and FinOps guardrails across Azure and AWS.

```
terraform {
  required_version = ">= 1.6.0"
  required_providers {
    azurerm = { source = "hashicorp/azurerm", version = "~> 3.111" }
    aws     = { source = "hashicorp/aws",     version = "~> 5.0" }
  }
}

provider "azurerm" {
  features {}
  subscription_id = var.azure_subscription_id
}
provider "aws" {
  region = var.aws_region_non_pii   # e.g., eu-west-2
}

locals {
  tags = {
    env         = var.env
    app         = "FinBankX-Core"
    owner       = "Platform-Team"
    cost_centre  = "FINTECH-1001"
    pii_level    = "PII"
  }
}
```

```
# ------------------------
# Azure GDPR/NDPR PII Plane
# ------------------------
resource "azurerm_resource_group" "pii_rg" {
  name     = "rg-fbx-pii-${var.env}"
  location = var.azure_region_pii   # "uksouth" or "nigeria"
  tags     = local.tags
}

resource "azurerm_key_vault" "pii_kv" {
  name                = "kv-fbx-pii-${var.env}"
  location            = azurerm_resource_group.pii_rg.location
  resource_group_name = azurerm_resource_group.pii_rg.name
  tenant_id           = var.tenant_id
  sku_name            = "standard"

  purge_protection_enabled     = true
  soft_delete_retention_days   = 90
  enable_rbac_authorization    = true
  tags                         = local.tags
}

resource "azurerm_key_vault_key" "cmk" {
  name         = "cmk-storage"
  key_vault_id = azurerm_key_vault.pii_kv.id
  key_type     = "RSA"
  key_size     = 3072
}

resource "azurerm_storage_account" "pii_sa" {
  name                     = "stfbxpii${var.env}"
  resource_group_name      = azurerm_resource_group.pii_rg.name
  location                 = azurerm_resource_group.pii_rg.location
  account_tier             = "Standard"
  account_replication_type = "ZRS"

  enable_https_traffic_only       = true
  min_tls_version                 = "TLS1_2"
  allow_nested_items_to_be_public = false

  identity {
    type = "SystemAssigned"
  }

  customer_managed_key {
    key_vault_key_id = azurerm_key_vault_key.cmk.id
  }

  network_rules {
    default_action             = "Deny"
    virtual_network_subnet_ids = [var.subnet_id_private_paas]
  }

  tags = local.tags
}

resource "azurerm_private_endpoint" "pii_sa_pe" {
  name                = "pe-stfbxpii-${var.env}"
  location            = azurerm_resource_group.pii_rg.location
  resource_group_name = azurerm_resource_group.pii_rg.name
  subnet_id           = var.subnet_id_private_paas

  private_service_connection {
    name                           = "psc-stfbx"
    private_connection_resource_id = azurerm_storage_account.pii_sa.id
    subresource_names              = ["blob"]
  }

  tags = local.tags
}

# Guardrail: enforce Private Endpoints
resource "azurerm_policy_assignment" "enforce_private_endpoints" {
  name                 = "pa-enforce-private-endpoints-storage"
  scope                = azurerm_resource_group.pii_rg.id
  policy_definition_id = "/providers/Microsoft.Authorization/policyDefinitions/2d1d6b9d-59b4-4d1e-9f1d-3cf9c0fc5b7e"
  enforcement_mode     = true
}

# -----------------------
# AWS NON-PII Analytics
# -----------------------
resource "aws_kms_key" "analytics" {
  description             = "KMS key for non-PII analytics data"
  deletion_window_in_days = 30
  enable_key_rotation     = true
  tags                    = merge(local.tags, { pii_level = "NON-PII" })
}

resource "aws_s3_bucket" "analytics" {
  bucket = "fbx-analytics-${var.env}-${var.aws_account_suffix}"
  tags   = merge(local.tags, { pii_level = "NON-PII" })
}

resource "aws_s3_bucket_server_side_encryption_configuration" "analytics" {
  bucket = aws_s3_bucket.analytics.id
  rule {
    apply_server_side_encryption_by_default {
      kms_master_key_id = aws_kms_key.analytics.arn
      sse_algorithm     = "aws:kms"
    }
  }
}

resource "aws_s3_bucket_public_access_block" "analytics" {
  bucket                  = aws_s3_bucket.analytics.id
  block_public_acls       = true
  block_public_policy     = true
  ignore_public_acls      = true
  restrict_public_buckets = true
}

resource "aws_s3_bucket_lifecycle_configuration" "analytics" {
  bucket = aws_s3_bucket.analytics.id
  rule {
    id     = "tiering"
    status = "Enabled"
    transition { days = 30  storage_class = "STANDARD_IA" }
    transition { days = 90  storage_class = "GLACIER" }
  }
}

# -----------------------
# Variables (variables.tf)
# -----------------------
# variable "env" {}
# variable "tenant_id" {}
# variable "azure_subscription_id" {}
# variable "azure_region_pii" {}
# variable "subnet_id_private_paas" {}
# variable "aws_region_non_pii" {}
# variable "aws_account_suffix" {}
```