AI-Driven Multi-Cloud Governance: A Framework for Automated Regulatory Compliance in the Financial Sector

MSc Research Proposal Presentation Transcript

DAbiodun_12696259

11th January 2026

MSc Enterprise IT Management

Slide 1: Introduction and Context

Financial institutions increasingly operate across multiple cloud platforms, most commonly Amazon Web Services, Microsoft Azure, and Google Cloud Platform. This multi-cloud approach is often adopted to improve resilience and scalability and reduce dependence on a single vendor. However, while multi-cloud offers clear technical and operational benefits, it also introduces significant governance and security complexity.

Each cloud provider implements security controls, identity models, logging mechanisms, and compliance tooling differently. For regulated organisations, particularly in the financial sector, this creates challenges when attempting to demonstrate consistent regulatory compliance across environments. Regulators are not concerned with which cloud platform is used; rather, they focus on accountability, transparency, and assurance.

At the same time, regulatory expectations continue to evolve, with regulators increasingly strengthening data protection standards and adapting legal frameworks to address emerging technologies such as artificial intelligence and cross-border data processing (Bakare et al., 2024).

This creates a set of fundamental tensions.

The first tension is between automation and accountability.

The second tension is between innovation and compliance.

The third tension concerns AI opacity versus transparency as AI-driven controls become more complex

Slide 2: Problem Context

From a regulatory perspective, compliance is assessed at the organisational level rather than at the platform level. Regulators require firms to demonstrate consistent accountability, transparency, and assurance across all operational systems, regardless of underlying technology.

In multi-cloud environments, this often results in fragmented compliance evidence, inconsistent audit trails, and increased reliance on manual processes to reconcile control gaps.

Manual and reactive compliance approaches are resource-intensive, error-prone, and poorly aligned with the scale and dynamism of cloud-native infrastructures. As organisations increasingly introduce automation and AI-driven controls to manage complexity, additional challenges emerge around the explainability and traceability of security and risk-related decisions. These factors collectively increase operational risk and reduce confidence in governance outcomes, highlighting a structural mismatch between traditional compliance approaches and modern multi-cloud operating models.

Slide 3: Proposed Framework for Automated Regulatory Compliance

Regulatory frameworks such as the General Data Protection Regulation (GDPR), the Financial Conduct Authority's Operational Resilience requirements, GDPR (European Union, 2016) and operational resilience guidance (FCA, 2022) the Monetary Authority of Singapore's Technology Risk Management guidelines, and the EU Artificial Intelligence Act emphasise transparency, accountability, and auditability of organisational systems and decisions. However, prior research indicates that cloud-based compliance processes are frequently fragmented, provider-specific, and difficult to scale across complex multi-cloud environments (Saunders, Lewis and Thornhill, 2023).

As automation and AI-driven controls become increasingly prevalent in regulatory compliance, the literature highlights growing concerns regarding explainability, accountability, and ethical governance. Studies in AI ethics caution that opaque or poorly governed automated decision-making can introduce legal, ethical, and operational risks, particularly in regulated sectors where human accountability remains a regulatory expectation (Schneider, 2018; Corrêa et al., 2023). This creates a structural tension between the efficiency gains of automation and regulatory demands for transparency, traceability, and oversight.

This research addresses this gap by proposing an AI-driven, provider-agnostic governance framework that enables consistent policy interpretation, explainable decision-making, and regulator-ready evidence across heterogeneous cloud environments, while preserving meaningful human oversight.

Slide 4: Proposed Framework for Automated Regulatory Compliance

The research question guiding this study is: How can an explainable, AI-driven governance framework enhance regulatory compliance across multi-cloud environments in the financial sector?

The research aims to design and evaluate a governance framework that improves compliance accuracy, transparency, and accountability in heterogeneous cloud environments.

The proposed framework adopts a layered approach.

A regulatory interpretation layer translates regulatory obligations into technology-agnostic control objectives while embedding accountability and explainability requirements.

A control orchestration layer maps these objectives to cloud-native controls and coordinates consistent enforcement across multiple cloud service providers.

An evidence and assurance layer collects identity-linked logs and decisions, producing audit-ready evidence to support regulatory reporting, review, and human oversight.

The research objectives include reviewing relevant governance and AI literature, identifying gaps in existing compliance approaches, designing and prototyping the proposed framework, evaluating the artefact using explicit criteria, and examining associated ethical and professional implications.

Slide 5: Literature Review and Research Gap

Existing literature recognises that multi-cloud adoption improves resilience and reduces dependence on single providers, while platform-native compliance tools enhance scalability within individual clouds. However, these solutions are typically siloed, leading to fragmented identity management, logging, and control enforcement in multi-cloud environments.

Vendor-native tools lack provider-agnostic regulatory abstractions, consistent accountability mechanisms, and explainable mappings between technical controls and regulatory obligations.

Explainability is essential for accountable AI adoption, as unguided decisions cannot be governed. No provider-agnostic framework currently enables automated multi-cloud compliance with human oversight. This research addresses this gap through a Design Science approach.

Slide 6: Methodology – Design Science Research

This study adopts a Design Science Research (DSR) methodology, which is well-suited to addressing applied problems through the systematic design and evaluation of artefacts.

DSR enables the development of practical solutions while maintaining methodological rigour and academic validity (Saunders, Lewis and Thornhill, 2023).

The research follows established DSR phases, including problem identification, artefact design and development, demonstration, evaluation, and communication. This iterative approach supports continuous refinement of the proposed governance framework in response to regulatory, technical, and organisational requirements. The decision to employ rule-based, explainable logic rather than opaque machine-learning models is consistent with prior financial-sector research, which demonstrates that model-specific explainability enables stronger regulatory compliance, auditability, and human accountability than post-hoc explanation techniques (Adams and Hagras, 2020).

Recent FinTech and RegTech literature highlights the growing use of AI-driven compliance automation, alongside persistent challenges in transparency, accountability, and governance (IJSRA, 2024). Design Science Research addresses these challenges by combining artefact construction with explicit evaluation, ensuring the solution is both theoretically grounded and operationally relevant for complex multi-cloud financial environments.

Slide 7: Project Progression, Ethics & Risk Management

The project follows three phases: research, design and prototyping, and final evaluation before submission.

Ethical and governance principles are applied continuously across all stages of the project. These include human oversight, the explainability and transparency of automated decisions, alignment with regulatory requirements, the avoidance of production data by utilising synthetic configurations, and the maintenance of accountability and auditability.

Several risks are identified and mitigated.

From a technical perspective, overly complex automation could reduce interpretability; this is mitigated by using rule-based, explainable logic.

Ethically, automation may reduce accountability, which is addressed by embedding human review and override mechanisms.

From a project management perspective, time constraints are mitigated by setting August as the internal completion milestone, allowing sufficient time for evaluation and refinement before submission.

Slide 8: Artefact Design

The artefact developed in this research consists of a conceptual AI-driven governance framework, supported by a lightweight prototype to demonstrate feasibility. The framework is designed to model regulatory interpretation, cloud control alignment, and compliance decision logic across heterogeneous cloud platforms, including AWS, Microsoft Azure, and Google Cloud Platform.

Regulatory requirements are translated into control objectives, which are then mapped to cloud-native security and governance controls. Rule-based, explainable AI logic is used to assess compliance configurations and generate auditable, human-readable outputs. This approach prioritises transparency and traceability over opaque automation.

The prototype will employ rule-based, explainable AI techniques, implemented as a rule engine using decision tables to evaluate compliance configurations against mapped control objectives. Where useful, decision-tree representations may be used to visualise rule paths; however, the logic remains deterministic and fully traceable to explicit rules.

A human-in-the-loop mechanism is embedded within the framework to enable oversight, challenge, and validation of automated decisions. This design choice mitigates the risks of over-automation and supports accountability, aligning the artefact with ethical AI and trustworthiness principles appropriate for regulated financial environments (Lincoln and Guba, 1985).

Slide 9: Internal Regulatory Translation Logic

It is important to emphasise that this evaluation is conducted at a proposal stage and focuses on conceptual and scenario-based assessment rather than a production deployment.

A core contribution of this research is the explicit internal regulatory translation logic embedded within the artefact. Regulatory texts are systematically decomposed into discrete compliance obligations, which are then translated into control objectives aligned with governance domains such as access management, audit logging, and data protection.

These control objectives are mapped to equivalent cloud-native implementations across different providers, enabling consistent interpretation despite underlying platform differences. Rule-based, explainable AI logic evaluates configuration data against these mappings and produces compliance assessments that remain traceable to specific regulatory requirements.

By maintaining a clear linkage between regulation, technical controls, and evidence, the framework addresses a key limitation of existing cloud compliance approaches in regulated financial environments.

Slide 10: Evaluation Framework

We evaluate across explainability, alignment, consistency, and ethics – but the key focus is traceability.

The evaluation begins by examining explainability and transparency. This assesses whether automated decisions can be traced back to explicit rules, supported by interpretable evidence, and clearly justified rather than operating as opaque, black-box processes.

Regulatory alignment evaluates the accuracy and completeness of mappings between regulatory obligations and implemented control objectives, ensuring that outputs are audit-ready and aligned with regulatory expectations.

Technical consistency ensures uniform control enforcement across cloud platforms.

Together, these criteria provide a structured and ethically grounded basis for evaluation

Slide 11: Contributions, Limitations & Future Work

This research contributes an explainable, AI-driven governance framework for multi-cloud compliance in regulated financial environments.

Using a Design Science approach, it shows how regulatory requirements can be translated into technology-agnostic controls and evaluated through transparent, rule-based logic.

Ethical risks are addressed through explainability and human oversight, while evaluation is limited to a scenario-based prototype.

Future work will focus on real-world validation and broader regulatory coverage.

Conclusion

In conclusion, this research presents an explainable, AI-driven governance framework to strengthen compliance and accountability in multi-cloud financial environments.

By translating regulatory obligations into technology-agnostic controls and generating audit-ready evidence through rule-based logic, the framework improves consistency while preserving human oversight.

Despite being evaluated through a scenario-based prototype, the findings establish a robust foundation for trustworthy automated compliance and future regulator-aligned governance research.

Word Count 1648

Slide 12: References

Lincoln, Y. S. and Guba, E. G. (1985) Naturalistic Inquiry. Newbury Park, CA: Sage.

Saunders, M., Lewis, P. and Thornhill, A. (2023) Research Methods for Business Students. 9th edn. Harlow: Pearson Education Limited.

Schneider, C. (2018) Making the case: A qualitative approach to studying social media documents. In Bryman, A. and Buchanan, D. (eds.) Unconventional Methodology in Organization and Management Research. Oxford: Oxford University Press.

Bakare, S.S., Adeniyi, A.O., Akpuokwe, C.U. and Eneh, N.E. (2024) *Data privacy laws and compliance: A comparative review of the EU GDPR and USA regulations*. **Computer Science & IT Research Journal**, 5(3), pp. 528–543. https://doi.org/10.51594/csitrj.v5i3.859

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

Financial Conduct Authority (FCA) (2022) *Operational resilience: Impact tolerances for important business services.* London: FCA.

Corrêa, N.K., Galvão, C., Santos, J., et al. (2023) 'Worldwide AI ethics: A review of 200 guidelines and recommendations for AI governance', *Nature Machine Intelligence*, 5(3), pp. 238–249.

International Journal of Scientific Research and Analysis (IJSRA) (2024) *Automating financial compliance with AI: A new era in regulatory technology (RegTech)*. **International Journal of Scientific Research and Analysis**, 11(1), pp. 1–10.

Adams, A. and Hagras, H. (2020) *A Type-2 Fuzzy Logic Approach to Explainable AI for Regulatory Compliance, Fair Customer Outcomes and Market Stability in the Global Financial Sector*. IEEE Transactions on Emerging Topics in Computational Intelligence, 4(6), pp. 852–865. https://doi.org/10.1109/TETCI.2020.3004990