Literature Review Outline

Proposed Title:

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

1. Background and Rationale

Cloud computing has become a foundational element of digital transformation in the financial sector, enabling agility, scalability, and AI-driven innovation **(Kunduru, 2023)**. However, these advancements introduce heightened risks, including data breaches, misconfigurations, adversarial attacks on AI systems, and cross-border governance challenges **(NIST, 2020)**. Regulatory frameworks such as the UK GDPR and Data Protection Act 2018 impose stringent security and accountability requirements **(UK Government, 2018; FCA, 2023)**.

AI integration strengthens threat detection but simultaneously creates new vulnerabilities (e.g., model bias, poisoning attacks, opaque decision-making) **(Corrêa et al., 2023)**. This review will critically synthesise academic, regulatory, and ethical literature to evaluate the effectiveness of cloud-security mitigation approaches within financial services and identify where current governance mechanisms fall short.

2. Aim and Objectives

Aim:

To critically analyse academic, regulatory, and ethical literature on cloud-security risks in financial services, assessing how technological, regulatory, and governance frameworks mitigate or exacerbate these risks.

Objectives:

1. Identify and classify major cloud-security risks affecting financial organisations.

2. Evaluate key regulatory and legal frameworks, including GDPR, the Data Protection Act 2018, and FCA obligations.

3. Assess AI-enabled mitigation technologies, including their benefits and limitations.

4. Analyse ethical issues relating to accountability, fairness, transparency, and automated decision-making.

5. Propose an integrated governance model that balances innovation, compliance, and risk reduction.

3. Proposed Thematic Structure (Chapter Plan)

1. Introduction & Rationale

2. Cloud Adoption in the Financial Sector: Opportunities and Risks

3. Regulatory and Compliance Frameworks

4. Technological Threat Landscape

5. AI-Driven Mitigation Tools

6. Governance and Ethical Considerations

7. Synthesis of Debates and Identified Gaps

8. Recommendations for Policy and Practice

9. Conclusion

4. Key Themes

- Regulatory Compliance grounded in GDPR and the Data Protection Act **(European Union, 2016; UK Government, 2018)**.

- Technological Risks

- AI and Security Augmentation

- Ethics and Accountability

- Governance Models (ISO 27005, NIST)

5. Research Approach and Methodology

Approach:

A primarily deductive approach, using established regulatory and governance frameworks (NIST, 2020) as analytical lenses, combined with inductive identification of emerging patterns in literature. The combination of deductive and inductive reasoning aligns with established research methodology principles **(Miessler, 2018)**.

Method:

Qualitative secondary-data synthesis using thematic analysis, conceptual comparison, and framework mapping.

Source Selection and Justification:

Peer-reviewed articles for rigour; regulatory texts for accuracy; ISO/NIST standards for operational relevance.

6. Ethical Considerations

Secondary data only, no human participants. Adherence to the University of Essex Online Research Ethics Framework and Cite Them Right Harvard referencing.

7. Expected Contribution

The review will:

- Highlight gaps between regulatory expectations and practical implementation.

- Identify contradictions in AI-security literature.

- Propose an integrated governance model combining technical, regulatory, and ethical controls.

- Provide insights for policymakers, compliance teams, and cloud-governance practitioners.

- Support future MSc project work on enterprise cloud governance.

References

Corrêa, N.K., Galvão, C., Santos, J.W. *et al.* (2023) 'Worldwide AI ethics: A review of 200 guidelines and recommendations for AI governance', *Patterns*, 4(100857).

European Union (2016) *General Data Protection Regulation (GDPR)*. Available at: https://eur-lex.europa.eu (Accessed: 12 November 2025).

Financial Conduct Authority (2023) *Guidance on cloud outsourcing and operational resilience*. London: FCA.

Kunduru, A.R. (2023) 'Artificial Intelligence Advantages in Cloud FinTech Application Security', *Central Asian Journal of Mathematical Theory and Computer Sciences*, 4(8), pp. 48–53.

Miessler, D. (2018) 'The Difference Between Deductive and Inductive Reasoning'. Available at: https://danielmiessler.com/blog/the-difference-between-deductive-and-inductive-reasoning (Accessed: 12 November 2025).

NIST (2020) *Risk Management Framework (SP 800-37 Revision 2)*. Gaithersburg: National Institute of Standards and Technology.

UK Government (2018) *Data Protection Act 2018*. London: The Stationery Office.