UNIVERSITY OF SURREY

Data Security and Governance Challenges in FinTech

Student ID : 6859062

Module: MANM492 – FinTech and Policy Project

MSc FinTech and Policy

29th August 2025

Table of Contents

Chapter 3 – Methodology

Chapter 4 – Findings and Analysis

Chapter 5 – Discussion

Abstract (Executive Summary)

Financial technology (FinTech) has rapidly transformed the global financial ecosystem by leveraging digital infrastructures, cloud computing, artificial intelligence (AI), distributed ledger technologies (DLT), and open banking platforms. This exponential growth, however, introduces significant governance and security challenges, particularly concerning the stewardship of sensitive financial data, regulatory compliance, and resilience against evolving cyber threats. This dissertation critically examines these data governance and security challenges in FinTech, focusing on the intersection of regulatory requirements, organisational practices, and technological innovation.

The study adopts a desk-based mixed-methods methodology, synthesizing insights from academic research, regulatory frameworks, industry reports, and case studies of leading FinTech firms such as Monzo, Revolut, Starling Bank, Zopa, and incumbent banks including Barclays and HSBC. The analysis employs a comparative benchmarking framework, guided by the ISO/IEC 27001:2022 standard, the NIST Cybersecurity Framework 2.0 (2024), and supervisory regimes such as the EU's Digital Operational Resilience Act (DORA, 2022), the UK Financial Conduct Authority (FCA) Consumer Duty (2023), and the General Data Protection Regulation (GDPR, 2018).

The findings highlight critical vulnerabilities in third-party and vendor risk management, algorithmic governance, and API security, while also recognizing the potential of RegTech to enhance compliance and resilience. Emerging threats such as ransomware, supply-chain compromise, and identity based cyberattacks underscore the urgency for holistic governance mechanisms that integrate ethical oversight, security by design engineering, and regulatory alignment.

This dissertation contributes to both academic theory and industry practice by:

- Developing an integrated conceptual framework that links external drivers (regulation, standards, market forces) to governance mechanisms and security outcomes.

- Providing a comparative regulatory analysis of data governance requirements across the UK, EU, and global standards.
- Benchmarking governance maturity in FinTech firms relative to incumbent banks.
- Offering actionable recommendations for boards, regulators, and engineering leaders, including adopting control-as-code, continuous assurance, and algorithmic fairness testing.

Ultimately, robust data governance and security practices are framed not merely as compliance imperatives but as strategic differentiators that enhance customer trust, operational resilience, and competitive positioning in a rapidly evolving financial ecosystem.

Chapter 1 – Introduction

1.1 Background and Context

The financial services industry is in the midst of unprecedented digital transformation, largely driven by the rise of financial technology (FinTech). FinTech encompasses a broad range of firms and business models challenger banks, peer-to-peer lenders, robo-advisors, cryptocurrency exchanges, and RegTech vendors all leveraging digital technologies to disrupt traditional financial intermediation (Zetzsche et al., 2020). These innovations have created efficiencies and expanded access to financial services, but they have also introduced novel risks associated with the governance, security, and ethical use of financial data.

Financial data is among the most sensitive categories of personal and transactional information, and its misuse or compromise can have catastrophic consequences for individuals, firms, and systemic stability (BCBS, 2021). At the same time, regulators and policymakers are intensifying scrutiny of how these firms handle data, as evidenced by initiatives such as the EU's Digital Operational Resilience Act (DORA, 2022), the UK Financial Conduct Authority's (FCA) Consumer Duty (2023), and global standard-setting by the International Organization for Standardization (ISO) and the National Institute of Standards and Technology (NIST).

The convergence of innovation and regulation underscores the importance of data governance as a strategic capability for FinTechs. Data governance is defined by the DAMA

DMBOK (2021) as the exercise of authority and control (planning, monitoring, and enforcement) over the management of data assets. In practice, this involves ensuring data quality, lineage, security, availability, and ethical use across the product lifecycle. Within FinTech, data governance is intertwined with cybersecurity, requiring the integration of technical, organisational, and regulatory measures (FCA, 2021).

1.2 Problem Statement

While FinTech innovation has accelerated, the maturity of data governance and security frameworks has not always kept pace. Many FinTech firms face resource constraints, rapid scaling pressures, and fragmented regulatory environments, leading to inconsistent practices in areas such as:

- **Third-party risk management**: Dependence on cloud and API providers introduces vulnerabilities in vendor ecosystems (ENISA, 2022).
- **Algorithmic governance**: Increasing reliance on machine learning in credit scoring and fraud detection raises concerns around bias, explainability, and accountability (CDEI, 2022).
- **Cross-jurisdictional compliance**: Firms operating internationally must reconcile conflicting data protection regimes, such as GDPR, CCPA/CPRA, and PDPA, creating operational complexity (BIS, 2023).
- **Cyber resilience**: The rise in ransomware and supply-chain attacks demonstrates gaps in incident response and recovery mechanisms (NIST, 2024).

These challenges create risks not only for individual firms but also for consumer trust and systemic stability. Addressing them requires a holistic understanding of the interplay between governance, technology, and regulation.

1.3 Research Aim and Objectives

The aim of this dissertation is to critically evaluate data governance and security challenges in FinTech and to develop a framework for strengthening resilience and compliance.

The specific objectives are to:

- Synthesize academic, regulatory, and industry perspectives on data governance and security in FinTech.
- Compare and contrast regulatory and standards frameworks relevant to FinTech data governance.
- Develop a conceptual framework linking external drivers, governance mechanisms, and security outcomes.
- Benchmark governance maturity across representative FinTechs and incumbent banks.
- Provide actionable recommendations for FinTech boards, regulators, and technology leaders.

1.4 Research Questions

This study is guided by the following research questions:

- What governance structures and security practices are most effective in managing data within FinTech firms?
- How do regulatory frameworks such as GDPR, DORA, and FCA rules shape data governance in FinTech?
- What are the critical risks and vulnerabilities in FinTech operations, and how can they be mitigated?
- What role can RegTech and automation play in enhancing governance and compliance?
- How can FinTechs reconcile the tension between innovation, regulatory compliance, and consumer trust?

1.5 Scope and Delimitations

The scope of the study is defined by the following:

- **Geographical scope**: The primary focus is on the UK and EU contexts, with reference to global standards where relevant.

- **Thematic scope**: The analysis focuses on data governance, cybersecurity, and regulatory compliance in FinTech.
- **Empirical scope**: The study is desk-based, relying on secondary data from academic sources, regulatory frameworks, and industry reports.

Limitations include the reliance on publicly available data, the dynamic nature of cyber threats, and the heterogeneity of FinTech business models, which may limit the generalisability of findings.

1.6 Significance of the Study

This dissertation contributes to both academic literature and industry practice. Academically, it bridges gaps in the literature by integrating insights from data governance, cybersecurity, and financial regulation into a unified framework. Practically, it provides FinTech firms, regulators, and policymakers with actionable guidance for enhancing governance and resilience. In doing so, it underscores the role of data governance and security as not merely compliance burdens but as strategic assets that foster trust, innovation, and competitive advantage.

Chapter 2 – Literature Review & Conceptual Framework

2.1 Theoretical Foundations

2.1.1 Data Governance as a Strategic Capability

Data governance is defined by the DAMA DMBOK (2021) as the exercise of authority and control over the management of data assets. In FinTech, data governance extends beyond compliance to become a dynamic capability that enables firms to reconfigure resources under uncertainty (Teece, 2007). Dynamic capabilities theory is particularly relevant because FinTechs operate in volatile environments shaped by regulatory flux, technological innovation, and cyber threats (Zetzsche et al., 2020).

Data governance encompasses several dimensions:

- Data quality management: ensuring accuracy, completeness, and timeliness.

- Metadata management: maintaining data lineage and traceability.
- Access control: defining roles and entitlements.
- Privacy and ethics: ensuring lawful and fair processing.
- Security: maintaining confidentiality, integrity, and availability. Academic research underscores that effective governance requires board-level accountability, cross-functional coordination, and integration into product design (Khatri & Brown, 2010).

2.1.2 Cybersecurity Foundations

Cybersecurity frameworks traditionally emphasize the CIA triad confidentiality, integrity, availability. However, more recent models expand to resilience, detection, response, and recovery (NIST, 2018). For financial institutions, resilience is critical, given the systemic implications of disruptions (BCBS, 2021).

ISO/IEC 27001:2022 emphasizes risk-based controls embedded into an Information Security Management System (ISMS). NIST CSF 2.0 (2024) introduces “Governance” as a core function, reflecting the need to integrate cybersecurity with corporate strategy. This highlights a shift from reactive security to proactive, risk-based governance.

2.1.3 RegTech and Compliance Automation

Regulatory Technology (RegTech) represents the use of AI, machine learning, and automation to streamline compliance tasks (Arner et al., 2017). RegTech aligns with theories of institutional isomorphism (DiMaggio & Powell, 1983), as firms adopt similar practices under regulatory and market pressures. Empirical studies report RegTech can reduce compliance effort by up to 30% while improving anomaly detection (Deloitte, 2022). However, governance must oversee model risk and ethical implications (CDEI, 2022).

2.2 Regulatory and Standards Landscape

2.2.1 European Union and United Kingdom

GDPR (2018): Establishes obligations for lawful processing, transparency, consent, data minimization, and cross-border transfers. Non-compliance risks fines of up to €20 million or 4% of turnover.

- **UK Data Protection Act (2018)**: Implements GDPR principles domestically, overseen by the Information Commissioner's Office (ICO).
- **FCA Rules**: The FCA imposes governance requirements under SYSC and operational resilience (PS21/3, 2021). The Consumer Duty (2023) adds obligations for firms to deliver good consumer outcomes, with implications for data fairness and transparency.

2.2.2 International Standards

- **ISO/IEC 27001:2022**: Provides requirements for ISMS, with updated Annex A controls aligned to threat trends.
- **NIST Cybersecurity Framework 2.0 (2024)**: Expands functions to Identify, Protect, Detect, Respond, Recover, and Governance.
- **Basel Committee on Banking Supervision (BCBS, 2021)**: Principles for operational resilience emphasize third-party risk, scenario testing, and board accountability.

2.2.3 Comparative Analysis Table (Textual)

Table 2.1: Key Regulatory and Standards Frameworks in FinTech Data Governance

Framework	**Scope & Coverage**	**Enforcement**	**Relevance to FinTech**
GDPR (2018)	EU personal data	National data protection authorities	Lawful processing, DPIAs, data portability
UK DPA (2018)	UK GDPR implementation	ICO fines up to £17.5m	Domestic rules with UK-specific nuances
FCA SYSC & Consumer Duty (2023)	Governance & conduct	FCA supervision	Operational resilience, consumer fairness

PSD2 (2015)	Open Banking APIs	National authorities	API security, strong customer authentication
ISO/IEC 27001:2022	ISMS	Certification audits	Assurance to partners/regulators
NIST CSF 2.0 (2024)	Cybersecurity maturity	Voluntary guidance	Benchmarking and uplift roadmap

2.3 Data Governance Challenges in FinTech

Several challenges are unique to FinTech compared to traditional banks:

- Cloud-native architectures: Outsourced hosting and SaaS providers fragment data lineage, complicating governance (ENISA, 2022).
- Third-party risk: FinTechs rely heavily on cloud, analytics, and payments vendors. Continuous monitoring is often immature (PwC, 2023).
- Algorithmic governance: AI models for credit scoring or fraud detection risk bias and opacity (CDEI, 2022).
- Cross-jurisdictional compliance: Global FinTechs face fragmented regimes GDPR (EU), CPRA (California), PDPA (Singapore) creating conflicting requirements (BIS, 2023).
- Resource constraints: Many FinTechs are startups with limited compliance budgets.

2.4 Threat Landscape

2.4.1 Technical Threats

- API exploitation: Poor authentication and insecure coding of Open Banking APIs have been exploited (FCA, 2022).
- Identity-based attacks: Compromised credentials account for the majority of breaches in cloud environments (Verizon, 2023).
- Ransomware: Attacks on payment processors and crypto exchanges highlight systemic vulnerabilities (Europol, 2022).

- Supply-chain compromise: Incidents such as SolarWinds show how third-party tools can cascade risk (NIST, 2024).

2.4.2 Organisational Threats

Insider threats, weak governance culture, and inadequate incident readiness exacerbate technical risks (EY, 2022).

2.5 Best Practice Models

Emerging models of best practice include:

- Board-level accountability: Assigning Chief Data Officers and governance councils (FCA, 2021).
- DevSecOps: Embedding security in development pipelines (Deloitte, 2022).
- Third-party oversight: Enhanced due diligence, right to audit clauses, and continuous monitoring (ENISA, 2022).
- Algorithmic transparency: Bias testing, explainability, and audit trails (CDEI, 2022).
- Incident response: Quarterly exercises and lessons-learned integration (BCBS, 2021).

2.6 Conceptual Framework

The conceptual framework integrates three layers:

- **External Drivers**: Regulation (GDPR, DORA, FCA), Standards (ISO, NIST), Market Forces (consumer trust).
- **Governance Mechanisms**: Data stewardship, technical controls, third-party oversight, incident response, RegTech automation.
- **Outcomes**: Compliance, resilience, trust, competitive advantage.

2.7 Literature Gaps

While literature is growing, key gaps remain:

- Limited comparative studies across multiple FinTechs and incumbents.

- Few empirical studies on RegTech effectiveness beyond pilot deployments (PwC, 2023).
- Lack of integrated models linking governance, cybersecurity, and consumer trust.
- Insufficient longitudinal data on post-DORA and post-NIST CSF 2.0 adoption impacts. This dissertation addresses these gaps by synthesizing diverse perspectives into an integrated framework and applying structured benchmarking to industry cases.

Chapter 3 – Methodology

3.1 Research Philosophy

The study adopts a pragmatist philosophy, which is appropriate for applied fields such as FinTech where practical problem-solving and multi-paradigm integration are necessary (Creswell & Plano Clark, 2018). Pragmatism allows the researcher to employ both interpretivist and positivist approaches:

- **Interpretivist**: for understanding organisational cultures, governance behaviours, and ethical dilemmas.
- **Positivist**: for assessing regulatory requirements, cybersecurity controls, and benchmarking standards. This philosophical stance aligns with the objective of generating actionable recommendations that are both theoretically grounded and practically applicable.

3.2 Research Design

The research design combines systematic literature review, regulatory benchmarking, and thematic analysis. The design process follows four stages:

- Defining objectives and research questions: Aligned to Chapter 1.
- Systematic literature review: Identifying peer-reviewed articles, regulatory documents, and industry white papers.
- Data extraction and thematic coding: Categorizing findings into themes such as regulatory drivers, governance mechanisms, threat vectors, and outcomes.

- Comparative analysis and synthesis: Benchmarking FinTech practices against incumbent banks and mapping results onto the conceptual framework. This approach ensures breadth (coverage across multiple domains) and depth (detailed analysis within each theme).

3.3 Data Sources

3.3.1 Academic Literature

Sources include peer-reviewed journals in finance, information systems, cybersecurity, and law, accessed via databases such as Scopus, Web of Science, and SSRN. Seminal works include governance frameworks (Khatri & Brown, 2010), dynamic capabilities (Teece, 2007), and cybersecurity resilience (NIST, 2018; 2024).

3.3.2 Regulatory and Standards Frameworks

Primary documents include:

- GDPR (2018), UK DPA (2018), FCA Consumer Duty (2023).
- EU DORA (2022), Basel Committee Operational Resilience Principles (2021).
- ISO/IEC 27001:2022, NIST CSF 2.0 (2024). These provide authoritative benchmarks against which FinTech practices are assessed.

3.3.3 Industry Reports

Big Four consultancies (PwC, Deloitte, EY, KPMG), cyber agencies (ENISA, Europol), and central banks (BIS, ECB, BoE) provide practical insights into emerging threats and best practices.

3.3.4 Case Studies

Illustrative case studies focus on UK challenger banks (Monzo, Starling, Revolut, Zopa) and incumbents (Barclays, HSBC). These were selected due to data availability, regulatory relevance, and representativeness of different FinTech maturity levels.

3.4 Data Collection

A systematic review protocol was followed:

- **Search strings**: “FinTech” AND “data governance” OR “cybersecurity” OR “regulation” (2017–2024).
- **Inclusion criteria**: English-language, peer-reviewed, regulatory relevance, or practitioner credibility.
- **Exclusion criteria**: Non-financial contexts, outdated pre-2017 sources unless seminal.
- **Selection process**: Titles, abstracts, and full-text screening, consistent with PRISMA guidelines (Moher et al., 2009). Industry and regulatory sources were triangulated against academic evidence to mitigate bias.

3.5 Data Analysis

3.5.1 Thematic Analysis

Thematic coding was applied to extract recurring patterns (Braun & Clarke, 2006). Codes included: “third-party risk,” “algorithmic bias,” “cloud dependency,” “incident response,” “regulatory compliance,” “consumer trust.”

3.5.2 Benchmarking

A benchmarking framework mapped FinTech practices against ISO/IEC 27001:2022 and NIST CSF 2.0 controls. This revealed governance maturity gaps relative to incumbents.

3.5.3 Comparative Analysis

Cross-case comparison identified commonalities and differences among firms. For example, challenger banks often excel in agile incident detection but lag in third-party oversight compared to incumbents.

3.6 Research Design Matrix

Table 3.1: Research Design Matrix

Research Objective	**Data Source**	**Method of Analysis**	**Expected Output**
Synthesize academic/regulatory perspectives	Journals, laws, standards	Systematic literature review	Thematic synthesis
Compare regulatory frameworks	GDPR, DORA, FCA, ISO, NIST	Documentary analysis	Comparative table
Develop conceptual framework	Synthesized literature	Conceptual modeling	Framework (Figure 2.1)
Benchmark governance maturity	Case studies (Monzo, Revolut, Barclays)	Cross-case benchmarking	Governance maturity assessment
Recommend improvements	Academic + industry evidence	Critical synthesis	Actionable recommendations

3.7 Methodology Flow

The research process is illustrated in Figure 3.1 (to be embedded in Word): Research Objectives & Questions↓ Systematic Literature Review↓ Data Extraction & Thematic Coding↓ Benchmarking & Comparative Analysis↓ Synthesis & Recommendations This structured flow ensures logical progression from problem framing to actionable outputs.

3.8 Reliability and Validity

To ensure rigor:

- **Construct validity**: Use of multiple data sources and frameworks (triangulation).
- **Reliability**: Clear inclusion/exclusion criteria and repeatable review process.
- **External validity**: Focus on UK/EU FinTechs limits generalisability globally but aligns with regulatory focus.

3.9 Ethical Considerations

Although the study is desk-based and uses only secondary sources, ethical issues arise in interpreting sensitive topics such as cyber incidents and consumer trust. Care has been taken to:

- Accurately represent sources without bias.
- Ensure transparency in attribution via Harvard referencing.
- Avoid misrepresentation of regulatory obligations.

3.10 Limitations

Key limitations include:

- Reliance on secondary data may omit confidential practices.
- The rapidly evolving threat landscape means findings may age quickly.
- Benchmarking relies on publicly available disclosures, which may understate weaknesses.

3.11 Summary

This chapter has outlined the pragmatic, desk-based mixed-methods design underpinning the dissertation. It demonstrated how systematic review, thematic analysis, and benchmarking are combined to critically evaluate data governance and security in FinTech. The next chapter applies this methodology to present findings and analysis.

Chapter 4 – Findings and Analysis

The analysis proceeds in three stages:

- Benchmarking findings: comparing FinTech and incumbent practices against international frameworks (ISO/IEC 27001:2022, NIST CSF 2.0, DORA 2022).
- Thematic findings: highlighting recurring governance and security challenges.
- Case-based findings: drawing insights from illustrative firm-level practices.

4.1 Benchmarking Governance Maturity

A comparative benchmarking exercise assessed firms across five categories aligned with ISO/IEC 27001:2022 and NIST CSF 2.0:

- Governance structures (board oversight, policies, accountability).
- Third-party/vendor risk management.
- Cybersecurity controls (access, encryption, monitoring).
- Incident detection and response.
- Regulatory compliance and reporting.

Table 4.1: Governance Maturity Benchmark (Simplified)

Category	**Challenger Banks (Monzo, Starling, Revolut, Zopa)**	**Incumbents (Barclays, HSBC)**
Governance structures	Agile, product-centric governance; limited board cybersecurity expertise	Mature risk committees; board-level CISOs
Third-party/vendor risk	High cloud/API reliance; limited continuous monitoring	Established vendor management programmes
Cybersecurity controls	Advanced encryption, strong MFA; gaps in legacy integration	Mature layered security; sometimes slowed by legacy IT
Incident detection/response	Agile detection, automated response; less formal resilience testing	Formal response plans, extensive resilience testing
Regulatory compliance	Good open banking compliance; challenges in cross-jurisdiction	Extensive compliance functions, global coordination

The findings show that challenger banks excel in agility and technology-native controls but face weaknesses in third-party governance and resilience testing. Incumbents demonstrate stronger structural governance and compliance maturity but are constrained by legacy IT and slower innovation cycles.

4.2 Thematic Findings

From the thematic analysis, five cross-cutting themes emerged:

4.2.1 Third-Party Risk as a Critical Weakness

All FinTechs studied are cloud-native and dependent on third-party providers such as AWS, Google Cloud, and Microsoft Azure. While these providers are resilient, concentration risk (i.e., systemic reliance on a small number of hyperscalers) creates vulnerabilities (ENISA, 2022). Unlike incumbents, FinTechs have weaker continuous monitoring and limited contractual leverage for audits.

4.2.2 Algorithmic Governance and Model Risk

AI-driven credit scoring, fraud detection, and customer support automation are widely used in challenger banks. However, limited model governance exposes risks of bias, explainability failures, and regulatory non-compliance (CDEI, 2022). Incumbents are beginning to embed model risk management (MRM) frameworks, but FinTechs often lack comparable oversight.

4.2.3 Cyber Resilience and Incident Response

While FinTechs are quick at incident detection, their resilience frameworks are less robust. Incumbents regularly conduct scenario-based stress testing, mandated by regulators (BCBS, 2021). Challenger banks, in contrast, have agile but less formal recovery testing. This gap risks prolonged downtime during sophisticated attacks such as ransomware.

4.2.4 Regulatory Complexity and Compliance Costs

FinTechs face disproportionate compliance burdens, particularly when operating internationally. GDPR, CPRA (California), and PDPA (Singapore) impose conflicting obligations, which can overwhelm resource-constrained firms. Incumbents absorb compliance more easily due to scale and established legal/compliance functions.

4.2.5 Consumer Trust as a Governance Outcome

Consumer surveys highlight persistent trust gaps between FinTechs and incumbents (EY, 2022). Data protection incidents, such as Revolut's 2022 breach (affecting 50,000 EU/EEA customers), amplify perceptions of vulnerability. Trust is a critical governance outcome, reinforcing the importance of transparent communication and ethical practices.

4.3 Case-Based Findings

4.3.1 Monzo

Monzo demonstrates strong API security and agile detection but has faced scrutiny regarding third-party controls. Its emphasis on user-friendly data portability aligns with GDPR but creates risks if APIs are misconfigured.

4.3.2 Revolut

Revolut suffered a data breach in September 2022, exposing weaknesses in insider access management (TechCrunch, 2022). While its rapid response was commended, the incident highlighted the gap between technological agility and structural governance maturity.

4.3.3 Starling Bank

Starling has prioritized in-house technology development over third-party outsourcing, which strengthens governance control. However, this strategy creates resource intensity and scaling limitations.

4.3.4 Zopa

Zopa's reliance on credit algorithms raises model risk concerns. While the firm has adopted bias-testing initiatives, the governance framework remains underdeveloped relative to incumbents.

4.3.5 Barclays and HSBC

Both incumbents have embedded comprehensive operational resilience frameworks aligned with FCA PS21/3 (2021). However, legacy IT integration challenges reduce agility. Barclays'

"Fusion Centre" provides real-time monitoring, a best-practice model absent in most challengers.

4.4 Mapping Against NIST CSF 2.0

Table 4.2: NIST CSF 2.0 Benchmark

Function	**FinTechs**	**Incumbents**
Identify	Informal asset catalogues	Comprehensive inventories
Protect	Strong MFA, encryption; API focus	Legacy gaps, but layered controls
Detect	Agile SIEM, AI-enabled detection	Mature SOCs with global reach
Respond	Automated playbooks	Structured crisis management
Recover	Limited resilience testing	Formal disaster recovery and testing
Govern	Emerging, product-centric governance	Formalized board oversight

The analysis shows that FinTechs excel in the Protect and Detect functions but lag in Govern and Recover, exposing significant resilience gaps.

4.5 Comparative Regulatory Readiness

Findings show a divergence in regulatory readiness:

- FinTechs often comply reactively, adapting after FCA or ICO scrutiny.
- Incumbents adopt proactive compliance cultures, embedding legal teams in product design.
- DORA (2022) is expected to disproportionately impact FinTechs, requiring costly third-party monitoring upgrades.

4.6 Summary of Findings

- FinTechs demonstrate agility and innovation in controls but face governance maturity gaps.
- Incumbents show robust governance and compliance but are hindered by legacy IT.

- Third-party/vendor risk is the most critical vulnerability across both groups.
- Algorithmic governance is underdeveloped, especially in FinTechs.
- Consumer trust remains fragile, highlighting governance as a driver of reputation.

Chapter 5 – Discussion

The discussion proceeds in four stages:

- Situating findings within theoretical frameworks (dynamic capabilities, institutional theory, socio-technical systems).
- Comparing outcomes against regulatory and standards expectations (GDPR, DORA, NIST CSF 2.0, ISO/IEC 27001:2022).
- Exploring implications for FinTechs, incumbents, policymakers, and consumers.
- Reflecting on contributions to research and practice.

5.1 Interpretation of Findings Through Theoretical Lenses

5.1.1 Dynamic Capabilities Theory

The benchmarking results demonstrated that FinTechs excel in agility and technology-native controls but lag in structural governance maturity. This reflects the dynamic capabilities perspective (Teece, 2007), where FinTechs are strong in “sensing” and “seizing” opportunities (e.g., adopting MFA, agile detection) but weaker in “reconfiguring” resources to institutionalize governance.

Incumbents, conversely, illustrate robust ordinary capabilities formalized committees, board level CISOs, compliance functions yet struggle with dynamic reconfiguration due to legacy IT. This validates the dual challenge in data governance: agility without resilience (FinTechs) and resilience without agility (incumbents).

5.1.2 Institutional Theory

The thematic finding that FinTechs often adopt reactive compliance strategies aligns with institutional isomorphism (DiMaggio & Powell, 1983). Under regulatory scrutiny, FinTechs conform to normative and coercive pressures (e.g., adapting after ICO investigations).

Incumbents, however, embody mimetic isomorphism, embedding compliance deeply as a legitimacy mechanism.

This suggests that governance in FinTech is less institutionalized and more ad hoc, creating vulnerabilities when regulations such as DORA require systemic, continuous oversight.

5.1.3 Socio-Technical Systems Theory

Cyber resilience challenges illustrate the interdependence of people, processes, and technology (Trist, 1981). For instance, Revolut's 2022 breach resulted not from technical encryption failures but from insider access weaknesses a socio-technical gap. Similarly, FinTechs' automated incident detection is undercut by insufficient human-led resilience exercises. This supports socio-technical systems theory, which holds that sustainable governance requires alignment across technical and organizational subsystems.

5.2 Findings in Relation to Regulatory and Standards Frameworks

5.2.1 GDPR and Data Protection Principles

FinTechs demonstrate strong alignment with GDPR's data portability and consent management provisions (e.g., Monzo's user-friendly app interfaces). However, the Revolut breach reveals gaps in GDPR's integrity and confidentiality principle. Incumbents, though less innovative, generally maintain stronger GDPR audit trails and DPIA practices.

5.2.2 DORA (Digital Operational Resilience Act)

DORA (2022) will disproportionately challenge FinTechs, given its emphasis on third-party oversight and resilience testing. Findings in Chapter 4 confirmed FinTechs' reliance on hyperscaler cloud providers without robust continuous monitoring. DORA requires harmonized oversight across the EU, meaning non-compliance could become a barrier to market access. Incumbents, already aligned with BCBS (2021) resilience principles, are better positioned.

5.2.3 NIST CSF 2.0 and ISO/IEC 27001:2022

The benchmarking against NIST CSF 2.0 revealed that FinTechs score highly in Protect and Detect functions but weakly in Govern and Recover. This confirms NIST's rationale for introducing "Govern" in its 2024 update, recognizing governance gaps as systemic vulnerabilities. ISO/IEC 27001:2022 further reinforces the need for information security governance as a board-level issue, which most FinTechs have yet to embed fully.

5.3 Implications for Stakeholders

5.3.1 For FinTech Firms

FinTechs must prioritize:

- Embedding governance at the board level: appointing CISOs with voting rights and integrating governance councils.
- Third-party monitoring: shifting from reactive vendor risk assessments to continuous oversight, leveraging RegTech tools.
- Resilience exercises: expanding beyond automated detection to include stress-testing and recovery simulations. These steps are essential for meeting DORA and FCA Consumer Duty requirements, as well as for building long-term consumer trust.

5.3.2 For Incumbent Banks

Incumbents should:

- Address legacy IT constraints: adopting modular upgrades and "tech debt reduction" programs.
- Leverage RegTech collaboration: partnering with FinTechs to integrate agile detection with established governance.
- Promote cultural agility: shifting compliance from a bureaucratic burden to a proactive innovation enabler.

5.3.3 For Policymakers and Regulators

Findings highlight a regulatory challenge:

- **Proportionality**: ensuring DORA and FCA enforcement do not stifle small FinTechs through disproportionate compliance costs.
- **Standardization**: promoting interoperability of cross-border privacy and resilience regimes.
- **Transparency**: mandating clearer disclosures of third-party reliance to regulators and consumers.
- **Support RegTech adoption**: Encourage integration of supervisory technology (SupTech) and industry RegTech solutions to streamline compliance.

5.3.4 For Consumers

Consumer trust remains fragile. Regulators and firms must address:

- Transparency in breach disclosure.
- Clarity in consent and data sharing (e.g., Open Banking APIs).
- Education on digital security practices to reduce susceptibility to phishing and credential theft.

5.4 Contributions to Knowledge

This study contributes to the growing literature on FinTech governance by synthesising insights from regulatory frameworks (e.g., GDPR, DORA, NIST CSF 2.0) with practical challenges faced by emerging firms. Unlike earlier studies that focused narrowly on cybersecurity (Arner et al., 2017), this dissertation integrates **data governance maturity models**, **third-party risk management**, and **consumer trust mechanisms** into a comprehensive conceptual framework. Furthermore, by incorporating recent policy interventions such as the UK FCA’s 2023 guidance on operational resilience and the EU’s 2022 Digital Operational Resilience Act (DORA), the research updates existing knowledge with the **latest regulatory developments**. This provides both academics and practitioners with a **holistic understanding** of governance gaps in FinTech ecosystems.

5.5 Limitations of Discussion

Despite its depth, this research has several limitations.

- First, the analysis is primarily **desk-based**, relying on secondary data, regulatory documents, and case studies. The absence of **primary empirical research** (e.g., interviews with FinTech executives or regulators) constrains the ability to capture lived organisational experiences.
- Second, given the rapid pace of regulatory reform, findings may become **time-sensitive**; new legislation could reshape governance practices within months.
- Third, the geographical scope is weighted towards the **UK and EU**, limiting generalisability to regions such as Asia or Africa where FinTech adoption models differ.
- Finally, while the research identifies gaps in governance maturity, it does not test a **quantitative model** of operational resilience or consumer trust, which could be explored in future studies.

5.6 Summary

The contributions highlight how this dissertation advances theory and practice in data governance, while the limitations acknowledge methodological and contextual boundaries. This sets the stage for Chapter 6, which presents the **conclusions and actionable recommendations** for stakeholders.

Chapter 6 – Conclusion and Recommendations

6.1 Recap of Research Aim and Objectives

The primary aim was to examine the **data governance and security challenges in FinTech** and evaluate how these impact regulatory compliance, consumer trust, and competitive advantage. The objectives included:

1. Reviewing the evolution of data governance frameworks in financial services.
2. Analysing the unique vulnerabilities of FinTech ecosystems.
3. Benchmarking FinTech practices against incumbents and global regulatory standards.
4. Proposing practical and policy recommendations.

All objectives were addressed through systematic literature review, regulatory analysis, and case synthesis.

6.2 Summary of Key Findings

The study identified five overarching findings:

1. **Governance Maturity Gaps** – Many FinTechs lack structured governance models compared to banks.
2. **Third-Party Risk Concentration** – Heavy reliance on cloud providers introduces systemic risk.
3. **Regulatory Fragmentation** – Diverging national rules (e.g., GDPR vs. US privacy laws) complicate cross-border operations.
4. **Algorithmic Governance Issues** – AI/ML models raise transparency and bias challenges, with limited oversight mechanisms.
5. **Consumer Trust Dynamics** – Despite high adoption, consumers remain concerned about data misuse and breaches.

6.3 Practical Recommendations

6.3.1 For FinTech Firms

- Adopt **privacy-by-design** principles (Cavoukian, 2019) and embed governance frameworks early in the scaling process.
- Conduct **regular third-party audits** of cloud and API partners.
- Establish **AI governance boards** to oversee model transparency and fairness.

6.3.2 For Incumbent Banks

- Collaborate with FinTechs via **regulatory sandboxes** to harmonise data practices.
- Leverage their advanced compliance systems to **mentor smaller firms** in governance maturity.
- Invest in **joint cyber-resilience exercises** with FinTech partners.

6.3.3 For Policymakers and Regulators

- Promote **cross-jurisdictional regulatory harmonisation** (e.g., G20, BIS initiatives).
- Enforce **mandatory resilience testing** (DORA, FCA guidelines).
- Issue **guidance on algorithmic accountability** for financial services AI models.

6.3.4 For Consumers

- Enhance digital financial literacy to improve understanding of consent and data usage.
- Encourage use of **multi-factor authentication** and personal data management tools.
- Demand **greater transparency** from FinTech providers regarding data storage and sharing.

6.4 Contributions of the Study

6.4.1 Academic Contributions

- Expands theoretical models of **data governance maturity** into the FinTech domain.
- Links **regulatory theory** (responsive regulation, risk-based supervision) with **practical governance challenges** in startups.
- Provides a **synthesised conceptual framework** that integrates cybersecurity, consumer trust, and regulatory alignment.

6.4.2 Practical Contributions

- Offers **actionable governance recommendations** tailored to FinTechs at different stages of growth.
- Provides **benchmarking insights** for incumbents on collaboration and resilience.
- Supplies regulators with a **roadmap for supervisory innovation**, particularly regarding AI and third-party risk.

6.5 Future Research Agenda

While this study is comprehensive, further work is needed:

- **Empirical validation**: Conducting interviews and surveys with FinTech executives to validate findings.
- **Cross-regional comparisons**: Expanding analysis to Asia-Pacific and North America to explore regulatory and cultural differences.
- **Quantitative resilience modeling**: Developing models that quantify the economic cost of governance immaturity.
- **Behavioral insights**: Investigating consumer responses to breaches and transparency strategies.
- **AI governance in FinTech**: Future research should assess how the EU AI Act (2024) will reshape algorithmic accountability.

6.6 Final Reflection

Data governance and security represent both existential risks and strategic opportunities for FinTechs. Weak governance can result in catastrophic breaches, loss of trust, and regulatory sanctions. Conversely, robust governance can serve as a competitive differentiator, enabling firms to scale responsibly while maintaining consumer trust.

The findings of this dissertation underscore the importance of moving beyond compliance-driven approaches toward governance as a core strategy. In a financial ecosystem increasingly mediated by data, algorithms, and platforms, the firms that thrive will be those that embed governance and security not as peripheral obligations but as core elements of innovation and value creation.

References

- Aldasoro, I., Gambacorta, L., Giudici, P. and Leach, T., 2022. The drivers of cyber risk. BIS Quarterly Review, September 2022. Available at: https://www.bis.org/publ/work865.pdf [Accessed 21 Jul. 2025].
- Arner, D.W., Barberis, J. and Buckley, R.P., 2017. FinTech, RegTech, and the reconceptualization of financial regulation. Northwestern Journal of International Law & Business, 37(3), pp.371–413. Available at: https://scholarlycommons.law.northwestern.edu/njilb/vol37/iss3/2/ [Accessed 22 Jul. 2025].
- Arner, D.W., Barberis, J. and Buckley, R.P., 2017. The evolution of FinTech: A new post-crisis paradigm? Georgetown Journal of International Law, 48(4), pp.1271–1318. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2676553[Accessed 23 Jul. 2025].
- Basel Committee on Banking Supervision (BCBS), 2019. Guiding principles for operational resilience. Basel: BIS. Available at: https://www.bis.org/bcbs/publ/d516.pdf [Accessed 24 Jul. 2025].
- Basel Committee on Banking Supervision (BCBS), 2021. Principles for operational resilience. Basel: BIS. https://www.bis.org/bcbs/publ/d516.pdf [Accessed 25 Jul. 2025].
- Bank for International Settlements (BIS), 2024. Digitalisation and cyber resilience in the financial system: An international perspective. Basel: BIS. https://www.bis.org/bcbs/publ/d575.pdf [Accessed 26 Jul. 2025].
- Boot, A., Hoffmann, P., Laeven, L. and Ratnovski, L., 2021. Fintech: What's old, what's new? Journal of Financial Stability, 53, p.100836. Available at: https://www.sciencedirect.com/science/article/abs/pii/S157230892030139X [Accessed 27 Jul. 2025].
- Bouveret, A., 2018. Cyber risk for the financial sector: A framework for quantifying operational risk losses. IMF Working Paper WP/18/143. Available at: https://www.imf.org/en/Publications/WP/Issues/2018/06/22/Cyber-Risk-for-the-Financial-Sector-A-Framework-for-Quantitative-Assessment-45924 [Accessed 28 Jul. 2025].

- Braun, V. and Clarke, V., 2006. Using thematic analysis in psychology. Qualitative Research in Psychology, 3(2), pp.77–101. https://psychology.ukzn.ac.za/?mdocs-file=1176 [Accessed 29 Jul. 2025].
- Centre for Data Ethics and Innovation (CDEI), 2022. Governing AI in the financial servicessector.London:CDEI.https://assets.publishing.service.gov.uk/media/64d360415cac65000dc2dc8d/Britainthinks_Report_-_CDEI_AI_Governance.pdf [Accessed 30 Jul. 2025].
- Chen, Y., Dube, K. and Banerjee, P., 2021. Secure open banking APIs: Threats, best practices, and standards. Computer Standards & Interfaces, 76, p.103525. [Accessed 31 Jul. 2025].
- Cornelli, G., Frost, J., Gambacorta, L., Rau, R. and Wardrop, R., 2020. Fintech and big tech credit: A new database. BIS Working Papers No. 887. Available at: https://www.bis.org/publ/work887.pdf [Accessed 1 Aug. 2025].
- Creswell, J.W. and Plano Clark, V.L., 2018. Designing and conducting mixed methods research.https://www.scirp.org/reference/referencespapers?referenceid=2697821 [Accessed 2 Aug. 2025].
- DAMA International, 2021. The DAMA guide to the data management body of knowledge (DAMA-DMBOK 2). 2nd ed. Technics Publications. Available at: https://dama.org/dmbok2r-infographics/ [Accessed 3 Aug. 2025].
- Deloitte,2024.RegTechUniverse.https://www.deloitte.com/lu/en/Industries/technology/analysis/regtech-companies-compliance.html [Accessed 4 Aug. 2025].
- Denzin, N.K., 2012. Triangulation 2.0. In: J.A. Holstein and J.F. Gubrium, eds. The handbook of constructionist research. New York: Guilford Press, pp.58–69. https://www.researchgate.net/publication/26524868_Handbook_of_Constructionist_Research [Accessed 5 Aug. 2025].
- DiMaggio, P.J. and Powell, W.W., 1983. The iron cage revisited: Institutional isomorphism and collective rationality in organizational fields. American Journal of Sociology,48(2),pp.147–160. https://www.researchgate.net/publication/224892279_'The_Iron_Cage_Revisited_Isomorphism_in_Organizational_Fields' [Accessed 6 Aug. 2025].

- ENISA (European Union Agency for Cybersecurity), 2022.Threat landscape for the financialsector.Athens:ENISA.https://www.enisa.europa.eu/sites/default/files/publications/ENISA%20Threat%20Landscape%202022.pdf [Accessed 7 Aug. 2025].
- Ernst & Young (EY), 2022. Global FinTech Adoption Index. London: EY. https://www.ey.com/content/dam/ey-unified-site/ey-com/en-uk/insights/banking-capital-markets/documents/ey-fintech-scale-up-handbook-interactive.pdf [Accessed 8 Aug. 2025].
- Europol, 2025. Internet Organised Crime Threat Assessment (IOCTA). The Hague: Europol.https://www.europol.europa.eu/publications-events/main-reports/iocta-report [Accessed 9 Aug. 2025].
- FCA (Financial Conduct Authority), 2021. Operational resilience: Impact of disruption on firms,markets,andconsumers.PS21/3.https://www.fca.org.uk/publication/policy/ps21-3-operational-resilience.pdf [Accessed 10 Aug. 2025].
- FCA (Financial Conduct Authority), 2022. Consumer Duty Final Rules and Guidance. London: FCA. Available at: https://www.fca.org.uk/publication/policy/ps22-9.pdf [Accessed 11 Aug. 2025].
- FCA (Financial Conduct Authority), 2023. Business Plan 2023/24. London: FCA. Available at: https://www.fca.org.uk/publication/corporate/business-plan-2023-24.pdf [Accessed 13 Aug. 2025].
- FCA (Financial Conduct Authority), 2023. Consumer Duty. London: FCA. https://www.fca.org.uk/firms/consumer-duty [Accessed 14 Aug. 2025].
- Goodman, B. and Flaxman, S., 2017. European Union regulations on algorithmic decision-making and a “right to explanation”. AI Magazine, 38(3), pp.50–57. Available at: https://ojs.aaai.org/aimagazine/index.php/aimagazine/article/view/2741/2647 [Accessed 15 Aug. 2025].
- ICO (Information Commissioner’s Office), 2023. Monetary penalty notices issued for GDPR violations. Available at: https://ico.org.uk/media2/for-organisations/documents/2619985/ico-opinion-the-use-of-lfr-in-public-places-20210618.pdf [Accessed 16 Aug. 2025].

- ISO/IEC, 2022. ISO/IEC 27001:2022 – Information security, cybersecurity and privacy protection — Information security management systems — Requirements. Geneva: International Organization for Standardization. Available at: https://www.iso.org/standard/27001 [Accessed 17 Aug. 2025].
- Khatri, V. and Brown, C.V., 2010. The roles of data governance in achieving and sustaining data quality. Journal of Data and Information Quality (JDIQ), 1(1), pp.1–25. https://www.scirp.org/reference/referencespapers?referenceid=3916458 [Accessed 18 Aug. 2025].
- Moher, D., Liberati, A., Tetzlaff, J. and Altman, D.G., 2009. Preferred reporting items for systematic reviews and meta-analyses: the PRISMA statement. PLoS Medicine, 6(7),e1000097.https://www.researchgate.net/publication/51156625_Moher_D_Liberati_A_Tetzlaff_J_Altman_DG_Group_PPreferred_reporting_items_for_systematic_reviews_and_meta-analyses_the_PRISMA_statement_PLoS_Med_6_e1000097 [Accessed 19 Aug. 2025].
- Monzo Bank, 2022. Transparency and security reports. Available at: https://monzo.com/static/docs/monzo-annual-report-2022.pdf [Accessed 20 Aug. 2025].
- NIST (National Institute of Standards and Technology), 2018. Framework for improving critical infrastructure cybersecurity. Gaithersburg: NIST. Available at: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf [Accessed 21 Aug. 2025].
- NIST (National Institute of Standards and Technology), 2024. NIST Cybersecurity Framework(CSF)2.0.Gaithersburg:NIST.https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf [Accessed 21 Aug. 2025].