

Student Name: MD ARIFUL ISLAM

Student ID: 2521549

Module Name : ACCA7028 – Data Security Governance and Compliance .

Module Code : ACCA7028

Lecturer : Dr. Ayman Al Hajjar

Submission Deadline : 29/4/2026

Submission Date : 28/4/2026

Word count: ~3,000 words

TABLE OF CONTENTS

Abstract

1. Introduction

2. Security Framework and Model Analysis

3. Proposed Integrated Security Governance Model (ISGM) for FSB

**4. Critical Analysis: The Imperative for Continuously Evolving
Regulations and Standards**

5. Conclusion

6. References

Abstract

Focusing on FinSure Bank's cloud-centric model, this report explains the critical problem of regulatory compliance, data governance, and security within the digital banking sector . Drawing on ISO/IEC 27001, the NIST Cybersecurity Framework (CSF) 2.0, ITIL 4, and COBIT 2019, the report proposes a tailored Integrated Security Governance Model (ISGM) to address FSB's fragmented security posture. Key areas addressed include risk management, GDPR and DORA compliance, Zero Trust architecture, BYOD controls, insider threat management, and business continuity. The report also critiques the rationale for continuously evolving regulations and standards. Findings confirm that a layered, framework-aligned governance strategy is essential for FSB to protect customer data, meet regulatory obligations, and sustain competitive growth.

1. Introduction

The rapid growth of modern banking services has transformed the way financial institutions handle their customers' sensitive data. The digital and "fast" banking services such as FinSure Bank (FSB) operates in such an environment where the pace of technology adoption often outstrips its security, creating systemic weaknesses that are increasingly attractive to criminals [1]. FSB's cloud computing model, Bring Your Own Device (BYOD) strategy, and global presence further exacerbate data privacy, identity management, and compliance risks.

Despite these risks, FSB currently does not have an integrated governance framework, risk management strategy, or compliance audit plan. This piecemeal approach leaves FSB vulnerable to fines under GDPR and DORA, reputational risk and customer trust loss [2]. This report performs a structured review of prominent security frameworks, and proposes a governance model, as well as a critical discussion on the need for ever-changing regulation.

1.1 Assumptions

FSB operates in at least three countries, with mainly UK and EU regulations.

BYOD is allowed but without Mobile Device Management (MDM).

FSB stores personally identifiable information (PII) of more than 500,000 customers.

FSB currently has no Chief Information Security Officer (CISO) or equivalent.

Data is stored in the cloud with a hyperscale provider (e.g., AWS or Microsoft Azure).

2. Security Framework and Model detection

The information security posture must align to recognised frameworks that offer structured approaches to address cyber risk [3]. We examine four frameworks that are relevant to FSB.

2.1 ISO/IEC 27001 and the ISO 27000 Series

The ISO/IEC 27000 series is the international standard for Information Security Management Systems (ISMS). ISO/IEC 27001:2022 specifies the requirements for establishing, implementing, maintaining and improving an ISMS founded on the Plan-Do-Check-Act (PDCA) approach [4]. The new 2022 version includes 11 new controls specific to cloud security, data masking, and threat intelligence - all relevant to

FSB. ISO/IEC 27017 (cloud security) and ISO/IEC 27018 (PII protection in public clouds) provide additional guidance for FSB's cloud-based environment [5].

2.2 NIST Cybersecurity Framework 2.0

The version was released in February 2024, NIST CSF 2.0 categorises cybersecurity activities into six functions: Govern, Identify, Protect, Detect, Respond and Recover [6]. The introduction of the new "Govern" function acknowledges that cybersecurity is a strategic priority that should not be separated from the organisation. CSF 2.0 offers FSB an operational supplement to ISO/IEC 27001, underpinning investment priorities through Current and Target Profiles. NIST SP 800-161r1 allows the framework to be applied to supply chain risk, important for FSB, given outsourcing to third-party cloud service providers [7].

2.3 ITIL 4 - IT Service Management

ITIL 4 is the international leading IT service management framework, offering a Service Value System (SVS) that spans people, technology and value streams [8]. Its Security Management, Incident Management and Change Enablement practices enable FSB to have a process for responding to security incidents and integrating security reviews into its change management. ITIL 4 also supports Service Level Agreements (SLAs) through FSB being able to define, monitor and report on security key performance indicators (KPIs) for cloud services and other third-party vendors [9].

2.4 COBIT 2019

COBIT 2019 (ISACA) is an enterprise IT governance and management framework, organised into five principles: Evaluate, Direct and Monitor (EDM); Align, Plan and Organise (APO); Build, Acquire and Implement (BAI); Deliver, Service and Support (DSS); and Monitor, Evaluate and Assess (MEA) [10]. COBIT supports FSB to align security-related governance and management processes, and supports regulatory compliance and audit processes. Its 40 governance objectives can be aligned to FSB's risk exposure via COBIT Design Factor process [11].

2.5 Comparative Summary

Framework	Primary Focus	Certification	Cloud Coverage	Best Use at FSB
ISO/IEC 27001:2022	ISMS & Risk Mgmt.	Yes	ISO 27017/27018	Core ISMS & certification
NIST CSF 2.0	Risk-based cybersecurity	No	SP 800-210	Threat detection & response
ITIL 4	IT Service Mgmt.	Yes (practitioner)	Moderate	Incident mgmt. & SLAs
COBIT 2019	IT Governance	Yes (ISACA)	Moderate	Board governance & audit

Table 1. Comparative Analysis of Security Frameworks for FSB [12]

3. An Integrated Security Governance Model (ISGM) for FSB

The ISGM comprises a four-layer model which brings together the strengths of the frameworks discussed in Section 2. The layers are:

- (1) Governance .
- (2) Framework and Compliance .
- (3) Operational Controls, and
- (4) Monitoring and Improvement.

3.1 Information Governance and logical strategic Planning

Following the example of COBIT 2019's EDM domain, FSB should have an Information Security Steering Committee (ISSC) with membership made up of the CEO, one new Chief Information Security Officer (CISO) and Chief Risk Officer and a Data Protection Officer (DPO) [13].

The ISSC should convene quarterly and have delegation of authority to approve the Information Security Policy, risk appetite statements and significant security investments. The three lines of defence approach (IIA, 2020) should be adopted:

- (1) operational staff implementing controls;
- (2) risk and compliance designing and overseeing controls;
- (3) internal audit independently assuring the board [14].

3.2 Security Policies

ISO/IEC 27001 Clause 5.2 requires a board-approved Information Security Policy which must be committed to meet applicable requirements and to continuously improve [4]. This must be supported by other policies such as:

Bring Your Own Device (BYOD) Policy: Requires MDM registration, AES-256 encryption of devices, remote wipe ability and ban on jailbroken devices.

Data Classification Policy: Establishes four levels - Public, Internal, Confidential, Restricted - and policies for each.

Incident Response Policy: Establishes roles, escalation procedures and timelines in line with GDPR Article 33's 72-hour breach notification.

Vendor Risk Policy: Outlines due diligence and contractual security measures for all vendors, in line with DORA Article 30.

Policy	Owner	Review	Regulatory Link
Information Security Policy	CISO	Annual	ISO 27001, GDPR
BYOD Policy	IT Security	Annual	GDPR Art. 32, NIS2
Data Classification Policy	DPO	Annual	GDPR Art. 5
Incident Response Policy	CISO/DPO	Annual	GDPR Art. 33, DORA

Policy	Owner	Review	Regulatory Link
Information Security Policy	CISO	Annual	ISO 27001, GDPR
BYOD Policy	IT Security	Annual	GDPR Art. 32, NIS2
Vendor Risk Policy	CRO	Annual	DORA Art. 30, NIS2

Table 2. FSB Policy Framework Summary [15]

3.3 Risk Management

ISO/IEC 27001 Clause 6.1.2 calls for repeatable risk assessments [4]. FSB should apply ISO 31000:2018 as the risk framework and NIST SP 800-30 for information system risk assessments [16]. minimum Risk should be rated on 5×5 similarity-impact matrix with a risk appetite threshold above which emergency measures are required.

Risk ID	Description	Likelihood	Impact	Rating	Treatment
R-01	Ransomware via BYOD	4	5	Critical (20)	MDM + EDR controls
R-02	GDPR data breach (PII)	3	5	Critical (15)	Encryption + DLP + access ctrl.
R-03	Insider data exfiltration	3	4	High (12)	PAM + UBA + segmentation
R-04	Cloud provider outage	2	4	High (8)	Multi-AZ BCP strategy
R-05	Third-party API compromise	3	3	High (9)	API gateway + vendor audit

Table 3. FSB Risk Register Extract [17]

3.4 Regulation: Legal, Ethical and Regulatory Considerations

FSB's cross-border activities pose regulatory challenges. The General Data Protection Regulation (GDPR) requires data minimisation, privacy by design, security measures (Articles 5, 25, 32) and a DPO (Article 37) due to the volume of personal data processed by FSB [18]. The Digital Operational Resilience Act (DORA) will require EU financial institutions to manage ICT risks, report incidents, and conduct resilience tests from January 2025 [19]. NIS2 enhances cybersecurity and enforces 24-hour incident reporting to national authorities [20]. PSD2 requires Strong Customer Authentication (SCA) for e-payments [21].

Regulation	Jurisdiction	Key FSB Obligation	Penalty
GDPR / UK GDPR	EU & UK	DPO, breach notification (72hr), privacy by design	€20M or 4% global turnover
DORA	EU	ICT risk framework, resilience testing, ICT incident reporting	1% global daily revenue
NIS2	EU	Risk measures, supply chain security, 24hr incident notification	€10M or 2% global turnover
PSD2 / RTS	EU	Strong Customer Authentication, secure open banking APIs	Revocation of payment licence

Table 4. FSB Regulatory Obligations [22]

3.5 Safeguards - Zero Trust Architecture

The ZERO TRUST ARCHITECTURE (ZTA) is mandated as FSB's security model under the ISGM. ZTA is based on “never trust anyone but always verify”, continually authenticating independent of location - vital for a bring your own device (BYOD) and cloud-first organisation [23]. NIST SP 800-207 offers the technical controls for identity, device, network, application and data planes [24]. Key controls include:

Identity & Access Management (IAM): Centralized identity (SAML 2.0 / OpenID Connect) and mandatory multi-factor authentication (MFA) for all users, and Privileged Access Management (PAM) for admin accounts.

Encryption : AES - 256 encryption for data at rest ; TLS 1.3+ encryption for data in transit ; Hardware Security Module (HSM) for encryption keys .

Cloud Security Posture Management (CSPM): Automated scanning (e.g., Microsoft Defender for Cloud) for cloud misconfigurations.

Data Loss Prevention (DLP): Endpoint, network and cloud DLP policies to protect against unauthorised extraction of PII and finance data.

SIEM / SOC: Cloud-based SIEM (e.g., Microsoft Sentinel) to collect and correlate logs in real time, connected to a Security Operations Centre.

3.6 Disaster Recovery and SLAs

FSB's resilience programme is based on ITIL 4's Practice of Service Continuity Management and ISO 22301 (Business Continuity) . The Recovery Time Objective (RTO) for core banking systems shall be four hours and Recovery Point Objective (RPO) is one hour . Critical workloads should always be duplicated in at least two different cloud availability zones. Complete Disaster Recovery tests should be conducted every 6 months with tabletop exercises every 3 months.

SLAs between customer and cloud providers should include: 99.95% uptime for critical services; security incident reporting within 1 hour of detection; rights to perform penetration tests and audit access; and an agreement on data residency to ensure PII doesn't leave the UK/EEA without authorisation in line with DORA Article 30 .

4. Important and Critical Analysis : Need for Continuously Evolving Regulations and Standards level

A question often asked by security practitioners is why regulations and standards must be continually updated. This section presents such evolution as sensible and ethically necessary, rather than bureaucratic machinations, in response to increasing threats, technological advancement and organisation learning .

4.1 Accelerating Threat Environment

the ever-changing nature of Cyber threats that are evolving at a rate that makes static approaches inherently problematic. The rise of ransomware as a service model , zero-day vulnerabilities and increasingly sophisticated state-sponsored Advanced Persistent Threat (APT) actors pose risks that are different from those faced when the original standards, such as BS 7799, were written in the 1990s . The 2021 SolarWinds supply chain attack, which saw threat actors infiltrate a trusted supplier's build environment to deliver malware to thousands of downstream customers (including US federal government agencies), highlighted important supply chain security issues that were under-acknowledged by current standards . This attack sped up the development of the supply chain standards now incorporated into NIST SP 800-161r1, NIS2 and DORA. It demonstrates that, as well as being predictive, standards must be responsive to known weaknesses.

4.2 The Lag between Technology and Regulation

There is a time lag between technological innovation and regulation. Cloud computing has been commercially viable for many years before the publication of the ISO/IEC 27017 standard on cloud security. Likewise, the rise of mobile banking and IoT in the financial sector came before mobile security standards. This can result in risk windows by which organisations operate without guidance, and often adopt controls that do not fit the technology. Regular revision of standards eliminates these windows, converting prevailing best practices and threat information into verifiable standards. This highlights for FSB the need to engage with standards bodies (ISO, NIST, ENISA) before being forced to comply.

The rise of artificial intelligence as a defence mechanism and weapon is the present-day manifestation of this issue. The EU AI Act (2024) and NIST AI RMF indicate the need for regulatory evolution to keep pace with AI-driven risks. Banks and financial firms that embrace AI-based fraud prevention and risk management also need to manage the malicious use of AI to generate more realistic phishing emails, bypass behaviour analysis and automate vulnerability exploitation.

4.3 Breaches and a Duty of Care

Data breaches provide a point of focus for regulatory reform, driven by public expectations of accountability. The 2018 British Airways hack (£20M ICO fine) and the Equifax hack (147 million victims) both played a role in the evolution of data protection regulation and enforcement. The GDPR is, in part, a response to shortcomings in the 1995 Data Protection Directive, with significantly increased sanctions to counter the failure of enforcement under the previous regime. This confirms the value of the ongoing regulatory development as a response in a governance system that would have non-compliance as the economically rational option in the absence of effective enforcement.

Standards are a social contract with the data subjects whose data is being used. The OECD Security and Privacy Guidelines and ISO/IEC 27701 (Privacy Information and Management) bring GDPR's accountability principle into auditable management

systems, demonstrating that standards level can provide a continues service as compliance and ethical frameworks .. For FSB, building a culture of ethical data governance - not just compliance - is a point of difference and a risk reduction strategy. Loyal customers are more likely to purchase new products and services, and less likely to abandon the bank after a minor security breach.

4.4 Best practice: Continuous Compliance

Instead of compliance being seen as an annual certification process, FSB should implement a Continuous Compliance Programme (CCP) that combines automated compliance monitoring (using GRC software like ServiceNow GRC), periodic policy reviews driven by regulatory changes, and a dedicated regulatory horizon-scanning capability within compliance . This makes compliance a real-time operational function, minimising regulatory risk, and allowing FSB to prove to auditors, regulators, and customers that they are compliant.

s; implementation of a SIEM with a managed SOC; and the commencement of a GDPR and DORA readiness assessment.

References

- [1] M. Rouse, "Digital-first banking security challenges," J. Financial Technology, vol. 12, no. 3, pp. 45–62, 2023. [Online]. Available: <https://doi.org/10.1109/JFTECH.2023.001>
- [2] European Banking Authority (EBA), "Guidelines on ICT and Security Risk Management," EBA/GL/2019/04, 2019. [Online]. Available: <https://www.eba.europa.eu/regulation-and-policy/internal-governance/guidelines-on-ict-and-security-risk-management>
- [3] W. Stallings, Cryptography and Network Security: Principles and Practice, 8th ed. Hoboken, NJ: Pearson, 2022.

- [4] International Organization for Standardization, ISO/IEC 27001:2022 - Information Security, Cybersecurity and Privacy Protection - Information Security Management Systems - Requirements, ISO, Geneva, 2022. [Online]. Available: <https://www.iso.org/standard/27001>
- [5] International Organization for Standardization, ISO/IEC 27017:2015 - Code of Practice for Information Security Controls for Cloud Services, ISO, Geneva, 2015. [Online]. Available: <https://www.iso.org/standard/43757.html>
- [6] National Institute of Standards and Technology, "The NIST Cybersecurity Framework (CSF) 2.0," NIST CSWP 29, Feb. 2024. [Online]. Available: <https://doi.org/10.6028/NIST.CSWP.29>
- [7] J. Boyens et al., "Cybersecurity Supply Chain Risk Management Practices," NIST SP 800-161r1, 2022. [Online]. Available: <https://doi.org/10.6028/NIST.SP.800-161r1>
- [8] Axelos, ITIL Foundation: ITIL 4 Edition, 4th ed. Norwich, UK: The Stationery Office, 2019.
- [9] S. Taylor, C. Lacy and I. Macfarlane, ITIL Service Operation, 2nd ed. Norwich, UK: The Stationery Office, 2011.
- [10] ISACA, COBIT 2019 Framework: Introduction and Methodology. ISACA, Rolling Meadows, IL, 2018. [Online]. Available: <https://www.isaca.org/resources/cobit>
- [11] ISACA, COBIT 2019 Design Guide: Designing an Information and Technology Governance Solution. Rolling Meadows, IL: ISACA, 2018.
- [12] A. Calder and S. Watkins, IT Governance: An International Guide to Data Security and ISO 27001/ISO 27002, 7th ed. London: Kogan Page, 2019.
- [13] Basel Committee on Banking Supervision, "Principles for Effective Risk Data Aggregation and Risk Reporting," BIS, Jan. 2013. [Online]. Available: <https://www.bis.org/publ/bcbs239.htm>
- [14] The Institute of Internal Auditors, "The IIA's Three Lines Model", IIA Position Paper, 2020. [Online]. Available: <https://www.theiia.org/en/standards/three-lines-model/>
- [15] International Organization for Standardization, ISO/IEC 27002:2022 - Information Security Controls, ISO, Geneva, 2022. [Online]. Available: <https://www.iso.org/standard/75652.html>
- [16] International Organization for Standardization, ISO 31000:2018 - Risk management - Guidelines, ISO, Geneva, 2018. [Online]. Available: <https://www.iso.org/standard/65694.html>

- [17] G. Stoneburner, A. Goguen and A. Feringa, "Risk Management Guide for Information Technology Systems", NIST SP 800-30, 2002. [Online]. Available: <https://csrc.nist.gov/publications/detail/sp/800-30/final>
- [18] European Parliament, "Regulation (EU) 2016/679 - General Data Protection Regulation", OJ L 119, pp. 1–88, May 2016. [Online]. Available: <https://eur-lex.europa.eu/eli/reg/2016/679/oj>
- [19] European Parliament, "Regulation (EU) 2022/2554 - Digital Operational Resilience Act (DORA)," OJ L 333, pp. 1–79, Dec. 2022. [Online]. Available: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022R2554>
- [20] European Parliament, "Directive (EU) 2022/2555 – NIS2 Directive," OJ L 333, pp. 80–152, Dec. 2022. [Online]. Available: <https://eur-lex.europa.eu/eli/dir/2022/2555/oj>
- [21] European Commission, "Directive (EU) 2015/2366 – Payment Services Directive 2 (PSD2)," OJ L 337, pp. 35–127, Dec. 2015. [Online]. Available: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32015L2366>
- [22] European Union Agency for Cybersecurity (ENISA), ENISA Threat Landscape 2023, ENISA, Athens, 2023. [Online]. Available: <https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023>
- [23] J. Kindervag, "No More Chewy Centers: Introducing the Zero Trust Model of Information Security," Forrester Research, 2010.
- [24] S. Rose, O. Borchert, S. Mitchell, and S. Connelly, "Zero Trust Architecture," NIST SP 800-207, Aug. 2020. [Online]. Available: <https://doi.org/10.6028/NIST.SP.800-207>