



Prifysgol Cymru
Y Drindod Dewi Sant
University of Wales
Trinity Saint David

Module Code: ACCA7028

Module Title: Data Security, Governance and Compliance

**Assignment Title: Applying Principles and Practices of Data Security,
Governance and Compliance: A Case Study of Fin Sure Bank (FSB)**

Student Name: Md Arafat Rahman

Student ID: 2437469

Module Tutor: Dr. Ayman Al Hajjar

Submission Date: 29/04/2026

Abstract

In this report, we will then describe an extensive Integrated Security Governance Architecture (ISGA), for Fin Sure Bank (FSB): a cloud-first digital financial institution that operates in multi-regulatory jurisdictions. Some of FSB's fragmented controls, unmanaged BYOD proliferation, avoidable exposure to the third-party ecosystem and the much-avoided cloud dependency results in significant risks leading to regulatory enforcement as well as operational disruption. Four established frameworks CIA Triad, ISO/IEC 27001:2022, NIST CSF, COBIT 2019 and ITIL 4 are individually assessed and synthesized into six ISGA layers consisting of risk register, defence-in-depth controls, SLA governance, contingency planning plus eight policy frameworks. The report also explains that the state of play regarding evolving standards DORA, PCI-DSS v4. 0, UK GDPR, and NIST CSF v2. 0 are operational imperatives, not bureaucratic overhead in an increasingly hostile threat environment.

Key Assumptions

All ISGA recommendations are based on the following assumptions:

- FSB operates under UK GDPR and FCA / PRA jurisdiction; multi-country falls in scope of local equivalents.
- FSB processes payment card transactions (so must comply with PCI-DSS v4) 0 compliance obligations [1].
- FSB does not have a CISO, DPO, formal security policies and ISMS as of now.
- It is now impossible to stop BYOD; it must be managed through MDM/MAM controls [2].
- 90%+ of FSB's cloud infrastructure is hosted across one or more of the major providers (AWS, Azure, or GCP).
- As of January 2025, DORA (Digital Operational Resilience Act) is in force for FSB's EU-facing operations [3].
- Budgets committed for Phases 1–2; Board sign-off required for phases 3–4.
- Security and ethical provisions cover employees, contractors, and third-party partners.

Introduction

The impact of digital transformation was a seismic shaking in the financial services security world. Legacy architectures can no longer mitigate a diverse range of sophisticated multi-vector attack surfaces because cloud-native infrastructure and mobile banking ecosystems have dissolved traditional network perimeters, while third-party integrations [3] and BYOD policies have expanded the attack surface with which institutions must contend [4].

This is where the challenge with FSB lies: with over 90% of its activity going through externally hosted cloud platforms and BYOD expanded to employees, contractors, third-party partners it faces converging risks across UK GDPR, PCI-DSS v4. 0: *ISO/IEC 27001:2022 The ISO/IEC 27001 standard is a leading international standard for* Importantly, FSB has no global governance framework, not a consistent risk

strategy, nor more importantly a written compliance programme making this an extremely serious regulatory liability and the operational risk of its existence [5]. This analysis provides a critical comparison of existing frameworks against FSB’s risk profile, presents customized six-layer ISGA, and proves how regulatory progress is business necessity rather than bureaucratic burden.

Critical Analysis of Security Frameworks and Models:

2.1 The CIA Triad Foundational Concept

At the same time all security governance frameworks ground around the CIA Triad: Confidentiality, Integrity and Availability (see figure 1). Surprising as this sounds, for FSB, this triadic model directly maps to key operational imperatives: protecting customer PII and financial data across multi-jurisdictional regulatory environments; ensuring the integrity of transaction records and investment portfolios against tampering & fraud; availing cloud-hosted services despite DDoS/ransomware and catastrophic provider outages [6]. The CIA Triad grounds the key evaluative lens for prioritising security investments against risk, according to Pfleeger and Pfleeger (2015) [7]. Yet, this triad is pointed out by critics as a lone wolf: not providing insight about governance structures, regulatory compliance mapping nor guidance on prioritising under resource constraints exactly the voids needed to fill with a multi-framework ISGA approach combined for FSB.



Figure 1: CIA Triad Applied to Fin Sure Bank Core Security Principles Mapped to FSB's Operational Requirements

2.2 ISO/IEC 27001:2022 - Information Security Management System

Information Security Management Systems (ISMS)[8] and provides a comprehensive PDCA cycle to ensure continuous governance improvement. This update from 2022 reduced the number of controls from 114 to 93 and scattered across four thematic domains: Organisational, People, Physical and Technological. Cloud-specific controls (A.5. 23; A.8. 26) and Required Threat Intelligence (A.5. 7) re-engage with FSB specifically addressing cloud-first and BYOD vulnerabilities. Although Brotby (2009) confirms ISO 27001 for its compatibility with multi-cloud operations [9], the standard is limited in that certification does not imply operational security maturity: an ISMS must be a living artefact, not compliance documentation.

2.3 NIST Cybersecurity Framework v2. 0 (2024)

The NIST CSF v2. The Release 0 (Oct 2023) provides an outcome-based, flexible framework based on six core functions: Govern, Identify, Protect, Detect, Respond and Recover [10]. Govern directly addresses the strategic governance gap of FSB, making it explicitly clear that cybersecurity risk strategy, accountability mechanisms, policy and supply-chain risk management are all requirements. The proposed security maturity baselines in NIST CSF have been validated by Alimohammadi and Alsaleh (2017) that the NIST CSF architecture provides a rapid way to baseline security maturity [11] and according to NIST SP800-124 Rev. 2, 2023 MDM guidance for FSB's BYOD management [2].

2.4 COBIT 2019 and ITIL 4

Two sections including Enterprise Governance of IT (EGIT) domain, the most complete framework of its kind has been defined in COBIT 2019 which distinguishes governance (direction-setting; evaluation) from management (execution) [12]. FSB provides board accountability structures and KPI frameworks amongst other things. Proponents of COBIT 2019, such as Von Solms and Van Niekerk (2013), explain that the root cause of governance failures in financial institutions is board accountability not technical controls being inadequate [13] a gap which COBIT 2019 directly addresses. This is complemented by structured ITSM processes within ITIL 4's Service Value System incident management, change enablement & SLA governance which are key to driving cloud provider accountability and adhering to the requirements of FCA operational resilience [14].

2.5 Framework Comparison

Table 1 presents a critical comparative analysis of all four frameworks alongside PCI-DSS v4.0, systematically mapped to FSB's specific risk profile and regulatory obligations.

Framework	Primary Focus	Key Strengths	FSB Relevance
ISO/IEC 27001:2022	Risk-based ISMS (Plan-Do-Check-Act cycle)	93 controls; cloud controls A.5.23 & A.8.26; threat intelligence A.5.7	GDPR Art.32, FCA PS21/3, PCI-DSS alignment
NIST CSF v2.0 (2024)	Govern->Identify->Protect->Detect->Respond->Recover	Flexible; new Govern function; BYOD & supply-chain guidance	Operational backbone; cloud & mobile threat coverage
COBIT 2019	Enterprise Governance of IT (EGIT)	Board accountability; KPI frameworks; integrates ISO/NIST/ITIL	Governance structure; risk appetite; regulatory compliance
ITIL 4	IT Service Management (ITSM) value streams	Service continuity; SLA management; incident & change control	Cloud SLA governance; FCA resilience; BCP/DR
PCI-DSS v4.0	Payment card data protection (12 requirements)	Mandatory for card processing; phishing-resistant MFA from 2025	Card-data environment compliance; quarterly vulnerability scans

Table 1: Comparative Analysis of Security Frameworks Primary Focus, Key Strengths, and FSB-Specific Relevance

Integrated Security Governance Architecture for FSB

3.1 Design Rationale

The ISGA is an integrated multi-framework architecture, which makeup the pyramid of Governance: the governance apex COBIT 2019; the Information Security Management System (ISMS) backbone ISO 27001:2022 and finally other frameworks such as NIST CSF v2. 0 on operational controls; and ITIL 4 on service management Calder and Watkins (2016) show that layered architectures have complete, non-duplicative coverage [15].

3.2 The Six-Layer ISGA

Figure 2 presents the ISGA's six layers, organised from board-level governance direction through to operational service delivery.

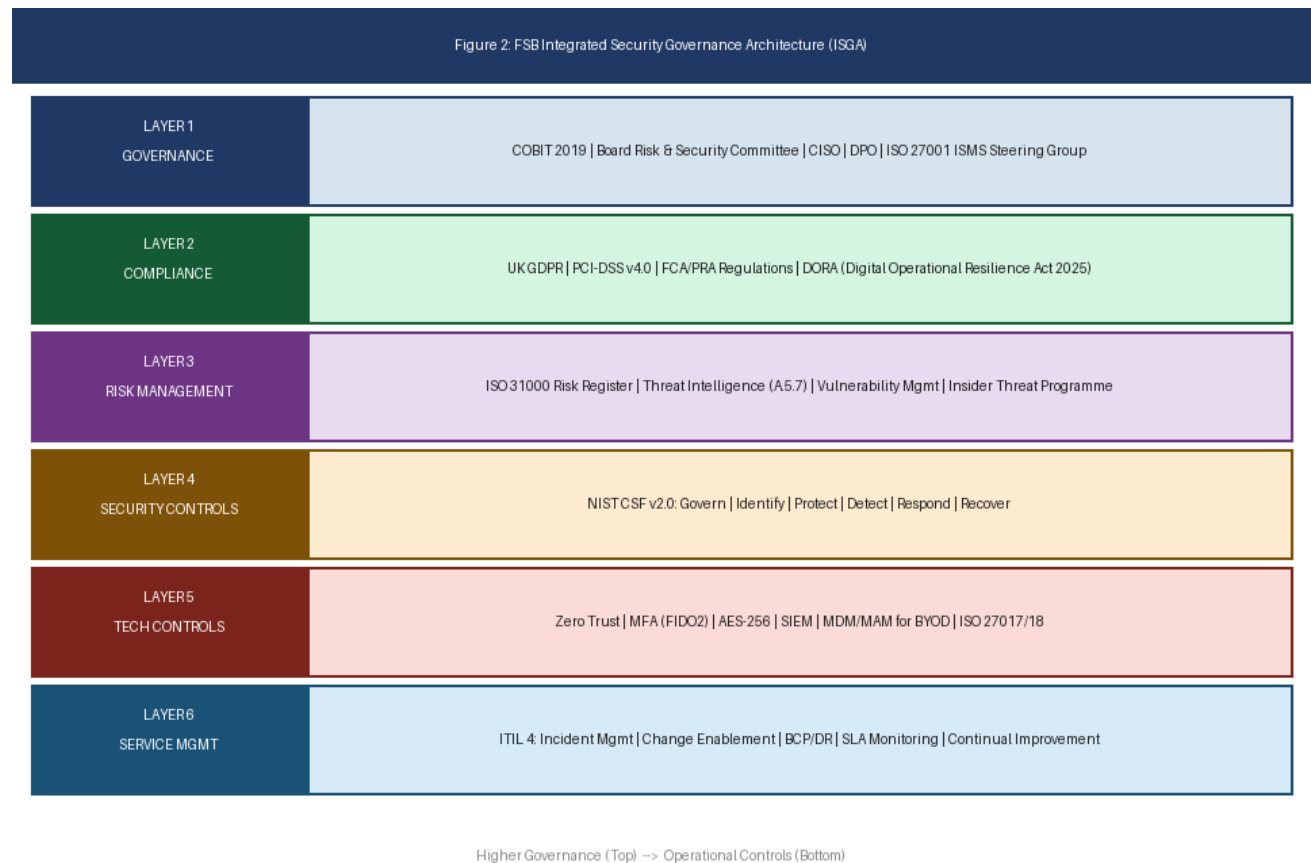


Figure 2: FSB Integrated Security Governance Architecture (ISGA) — six-layer framework from governance to service management.

Layer 1 (Governance) sets board accountability by reporting quarterly to a Risk and Security Committee through the CISO. Layer 2: Compliance layer like UK GDPR, PCI-DSS v4.0 and FCA/PRA PS21/3, along with the DORA obligations. Layer 3 (Risk Management) operationalises ISO 31000:2018 with a quarterly-reviewed risk register. The mapping of NIST CSF v2 is Layer 4 (Security Controls). 0 functions to procedures. Layer 5 (Technical Controls) is all about Zero Trust Architecture, FIDO2 MFA and AES-256 encryption. Layer 6 (Service Management) uses ITIL 4 for governance of SLAs and continual improvement [14]. This overcomes the governance blind spots endemic in single-framework structures where, for example, it is rare that technical level controls and board-level accountability are rigorously managed together [15].

3.3 Risk Register

FSB's top-down risk register (shown in Table 2) has seven threat vectors, which were ranked using a 3×3 likelihood-impact matrix aligned to ISO 31000:2018 [16].

ID	Risk Description	Likelihood	Impact	Rating	Mitigation Control
R1	BYOD / Unmanaged Device Compromise	High	High	CRITICAL	MDM/MAM enrolment; Zero Trust; AES-256 device encryption; remote wipe capability
R2	Online Fraud / Customer Identity Theft	High	High	CRITICAL	AI behavioural analytics; FIDO2 2FA; real-time fraud detection engine
R3	GDPR / PCI-DSS Non-Compliance	Medium	High	HIGH	Compliance audit programme; DPO appointment; annual ISMS review cycle
R4	Insider Threat / Privileged Abuse	Medium	High	HIGH	PAM; UEBA/SIEM; quarterly access reviews; background screening policy
R5	Cloud Provider SLA Breach / Outage	Medium	High	HIGH	Multi-cloud BCP; contractual SLA (RTO ≤4 hr); quarterly DR testing
R6	Phishing / Social Engineering	High	Medium	HIGH	Security awareness training; MFA enforcement; email filtering; DMARC/DKIM
R7	Third-Party / Supply Chain Breach	Medium	Medium	MEDIUM	Vendor risk assessments; contractual security SLAs; annual audit rights
R8	Ransomware on Cloud Infrastructure	Low	High	MEDIUM	Immutable backups; EDR deployment; cloud-native threat detection

Table 2 : Eight Description of Primary Risks aggregate ISO 31000:2018 Ratings with Mitigation Controls.

Critical BYOD/Unmanaged Device Compromise Personal endpoints are not only an uncontrolled attack surface that perimeter controls cannot be effective against, but they represent a significant jump point for attackers to gain access to the enterprise via controlled and maintained devices or direct high-value targets; MDM/MAM counters MITRE ATT&CK techniques T1078 and T1534 [10]. Data up to includes October 2023 Online Fraud/Identity theft is equally crucial: Soomro, Shah and Ahmed (2016) show that best-in-class ML powered fraud detection can cut false-negative rates by as much as 60% vs. traditional rule-based methods [17]

3.4 Protection Mechanisms

Layer 5 ISGA Technical Controls Layer Mapped with FSBs defence-in-depth protection mechanisms as depicted in Table 3.

Protection Mechanism	Security Domain	Application to FSB
Zero Trust Architecture	Network & Identity	Eliminates implicit trust for all users and devices; micro-segmentation; mandatory for BYOD and third-party access [10]
MFA - FIDO2 Standard	Identity & Access	Phishing-resistant hardware/biometric tokens; mandatory for all staff, contractors, and privileged accounts per PCI-DSS v4.0 [1]
AES-256 Encryption	Data Protection	All data at rest encrypted; TLS 1.3 in transit; end-to-end encryption for customer financial data and PII [6]
MDM/MAM (Microsoft Intune)	BYOD Control	Device health attestation; selective remote wipe; app containerisation; compliance policy enforcement across all personal devices [2]
SIEM & UEBA	Detection & Monitoring	Real-time log aggregation; behavioural analytics for insider threat detection; automated alerting to SOC within defined thresholds [10]
Endpoint Detection & Response (EDR)	Endpoint Security	Continuous endpoint monitoring; ransomware protection; automated isolation of compromised endpoints before lateral movement
Web Application Firewall (WAF)	Perimeter & Application	OWASP Top 10 protection; DDoS mitigation; API gateway security for mobile banking application layer [10]
Data Loss Prevention (DLP)	Data Exfiltration	ISO 27001 A.8.12 aligned; blocks unauthorised transfer of PII and financial records via email, USB, or cloud uploads [8]
Vulnerability Management	Proactive Risk Reduction	Quarterly penetration testing; monthly automated scanning; CIS Benchmark compliance checks for cloud infrastructure [12]

Table 3: Mapped FSB Protection Mechanisms for Technical and Procedural Controls to Security Domains.

The most basic definition of Zero Trust Architecture is that it provides no implicit trust for any users, devices or locations [10]. Correctly used in combination with FIDO2 MFA (compulsory under PCI-DSS v4. 0 from March 2025 [1]), AES-256 Encryption, SIEM/UEBA Analytics and DLP Iso 27001 A.8. These mechanisms are described in ISO 27001:2022 Annex A [8], and amount to a defence in depth posture.

3.5 Contingency Planning

FSB contingency framework (ISO 22301:2019; ITIL 4 Service Continuity) explains three large classes of failure the cloud outage, ransomware and regulation-induced suspension [14] with a nested recovery model containing three fundamental tiers:

- Tier 1 Immediate Response (0-4 hours): Automated cloud-failover within 15 mins, CISO and Board notified at the end of every hour, payment systems re-directed to a back-up gateway.
- Tier 2 Short-term Recovery (4–24 hours): DR environment tested and ready; FCA notified according to PS21/3 [18]; immutable backup restoration initiated; ICO informed where personal data is implicated, per GDPR Art. 33 [19].
- Tier 3 Recovery- Lasting (24 hours-30 days); system restoration in a sequenced manner focusing on the most critical services at first; forensic root cause analysis performed within 5 business days after live service resumed, and lessons learned processed through immediately into ISMS for improvement.

Our study is also based on the requirements of tested ICT continuity plans with defined RTOs and RPOs according to Article 11 from DORA [3]. This is met with FSB having Tier-1 RTO ≤ 4 hours and RPO ≤ 1 hour. Quarterly DR tests are required according to the BCP & Disaster Recovery Policy Peltier (2013) shows, untested plans are as good as none when it comes to operations [20].

3.6 Service Level Agreements

FSB uses SLAs to hold cloud providers accountable on a contractual basis. Table 4 shows minimum SLA requirements aligned to ITIL 4 Service Level Management and FCA operational resilience mandates.

Service / System	Uptime SLA	RTO Target	SLA Enforcement Mechanism
Core Banking Platform	99.95%	<=4 hours	Automated failover to secondary cloud region; contractual penalty clause; monthly service reviews
Mobile Banking Application	99.90%	<=4 hours	CDN delivery; autoscaling; real-time fraud detection uptime guaranteed in contract

Online Payment Gateway	99.99%	<=1 hour	PCI-DSS v4.0 scoped; redundant processing nodes; instant failover; customer notification within 30 min
Identity & Access Management	99.95%	<=2 hours	FIDO2 MFA service; redundant IdP; active-active configuration
Data Backup & Recovery	99.90%	RPO <=1 hour	Immutable off-site backups; automated daily backup validation; geo-redundant storage
Security Operations (SIEM/SOC)	99.80%	<=30 minutes	24/7 monitoring; CISO escalation within 1 hr of P1 incident; monthly SLA reporting

Table 4: FSB Service Level Agreement Requirements Essential Systems with Uptime Targets, RTOs, and Enforcement Mechanisms

Contractual audit rights on SLAs, monthly reviews with the cloud provider and automatic uptime monitoring through the SIEM platform must be enforced along with remedial actions (within 24 hours of verified breach).

3.7 Security Policy Framework

FSB policy suite classified according to ISO 27001:2022 Clause 5.2 and NIST CSF v2. Table 5 0 Govern. The ISGA governance layer and compliance layer together describes enforcement procedures for each policy, including explicit monitoring of compliance.

Policy	Key Requirements & Enforcement	Review Cycle
Information Security Policy (ISP)	Master policy per ISO 27001 Cl.5.2; Board-approved; covers all FSB systems and data assets. Enforced via ISMS Steering Group quarterly compliance reporting to the Board Risk Committee [8]	Annual
BYOD & Acceptable Use Policy	MDM mandatory enrolment; AES-256 encryption; remote wipe; app containerisation. Enforced through signed Acceptable Use Agreements and automated MDM compliance checks; non-compliant devices automatically blocked [2]	Bi-annual
Access Control & IAM Policy	RBAC and least-privilege; FIDO2 MFA for all access; PAM for privileged accounts. Enforced via Identity Provider automated provisioning/deprovisioning and quarterly access certification reviewed by line managers [10]	Annual

Cloud Security Policy	ISO 27017/27018 controls; shared responsibility matrix per provider. Enforced via monthly cloud configuration scanning (CIS Benchmark) with automated alerts to CISO for critical deviations [8]	Annual
Data Classification Policy	Four levels: Public/Internal/Confidential/Restricted. Enforced via DLP tool integration with email, cloud storage, and endpoint; automatic labelling and handling rule application [8]	Annual
Incident Response Policy	NCSC/NIST IR lifecycle; 72-hr GDPR breach notification (Art.33); FCA escalation. Enforced via mandatory incident logging in SIEM and post-incident reviews with documented corrective actions within 5 business days [3]	Semi-annual
Third-Party & Vendor Policy	Supplier risk assessment; contractual security SLAs; annual audit rights. Enforced via vendor scorecards reviewed at quarterly business reviews; Tier-1 vendors require ISO 27001 certification [16]	Annual
BCP & Disaster Recovery Policy	RTO <=4 hrs / RPO <=1 hr for Tier-1; quarterly DR tests; cloud failover. Enforced via mandatory test completion reports submitted to CISO and Board Risk Committee; failed tests trigger remediation plans [3]	Annual

Table 5: Eight Core Policies of the FSB Security Policy Framework, Key Requirements (Replicating Table 1 in [9]), Enforcement Mechanisms, and Review Cycles.

3.8 Implementation Roadmap

A phased 18-month roadmap that prioritizes critical risk reduction (Phase 1) before rolling out governance formalization, ISO 27001 certification and continual improvement is shown in Figure 3.

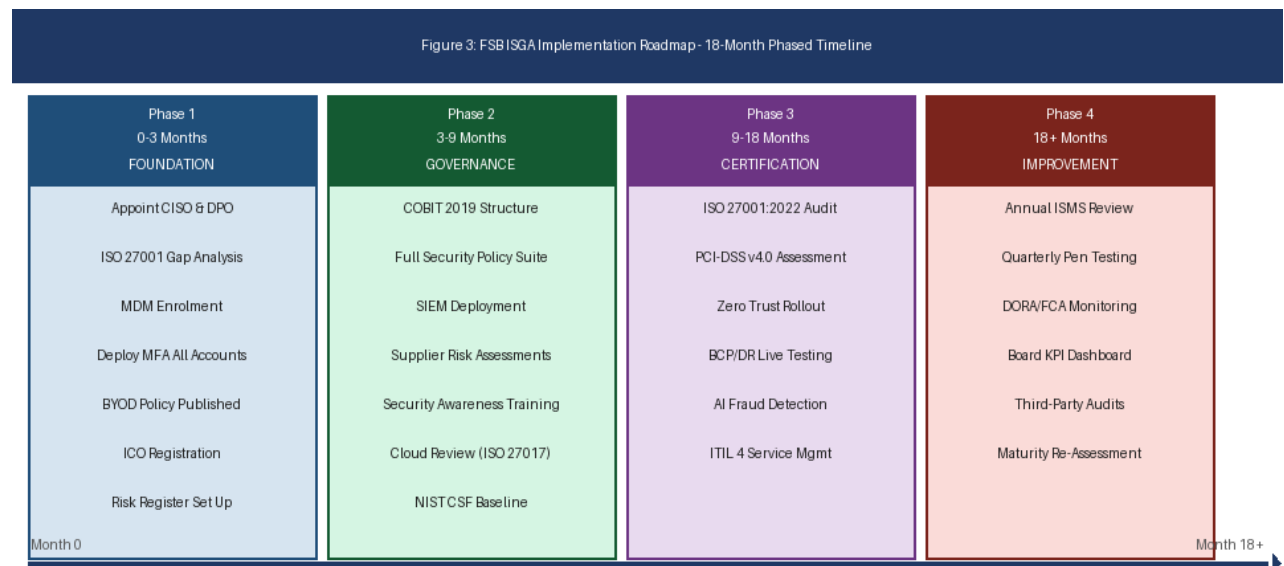


Figure 3: FSB ISGA Implementation Roadmap Four Phases from foundation to continual improvement.

4. The Need for Evolving Regulation and Standards a Critical Review of the Processes.

4.1 REQUIREMENTS OF ADAPTIVE STANDARDS IN LIGHT OF THE THREAT LANDSCAPE:

Static security standards is an empirically indefensible position. At the time of ISO 27001:2013's inception, no one could have seen the rise of the 2025 threat landscape; ransomware-as-a-service, AI-augmented spear-phishing and supply-chain compromise. As compliance theatre, where organisations certify against controls which do not measure true threat exposure anymore [21]. The 2022 revision of ISO 27001 is a classic example of this: we saw the incorporation of threat intelligence (A.5. 7), data leakage prevention (A.8. 12), and secure coding (A.8. 28) met address vectors that were just starting to dominate (by 2022) yet remained theoretical in 2013. More critically, the average 7–9-year revision cycle for ISO is structurally mismatched against a rapid monthly cadence of fresh patches and novel exploits which renders interim CISO-led threat intelligence guidance as an operational requirement than to be optional.

4.2 Technological Development and Regulatory Harmonization

Before 2013, the standards such as ISO/IEC 27002 were based on a perimeter-based model that was disrupted by cloud computing [9]. PCI-DSS v4. This requirement is projected to achieve maturity in March 2025 [1], along with the introduction of NIST CSF v2.0 Govern In line with the evidence that most cybersecurity failures are governance failures [10]. For systemic institutions oriented toward multi-jurisdictional engagement such as FSB, regulatory convergence is double-edged: while the GDPR and DORA reduce fragmentation across 30+ jurisdictions [3], their overlapping requirements necessitate ongoing mandatory regulatory mapping to identify gaps. According to Von Solms (1999) the benefit derived from standards is not their current value but, as a discipline of re-evaluation [22] for FSB this requires CISO-led horizon-scanning and who needs them through NCSC, ISACA & FCA engagement.

4.3 The BYOD and Emerging Technology Challenge

BYOD, cloud-native architectures, and AI-driven fraud are all examples of adoption cycles where the innovation residence time grows in a manner that constantly outstrips traditional standards revision. This more agile implementation is described in NIST's two-road model (SP 800-124, SP 800-144) a set of steady top-level architectures, coupled with ever-evolving specialized instructions [2]. For FSB, regardless of the mechanics behind their annual compliance deals, it is stuck in a round structure: The quarterly governance cycles built into our ISGA Governance Layer are the minimal viable cadence. More generally this reflects a fundamental shortcoming of standards-based compliance: it provides a floor for compliance, not the ceiling of security organisations treating the standard as destination rather than baseline find themselves vulnerable to emerging threats forever.

Conclusion

A lack of an effective risk management framework, unrecorded device usage and usage concentration in clouds across an enterprise landscape have left FSB with fragmented governance. No single framework gives you comprehensive coverage, and ISGA solves this through evidence-based layering: COBIT 2019 board governance; an ISO 27001:2022 ISMS backbone; NIST CSF v2.0 operational controls, and ITIL 4 service management Phase 1 remediation is mandatory for Two Critical-rated risks: the BYOD compromise and online fraud. The ethics analysis highlights that there are real fiduciary duties associated with BYOD monitoring and AI models for fraud detection: proportionality, transparency, and regular review cannot be compromised. At FSB, empowering transformation rather than reactive, fragmented security is the investment that makes the difference between governance and security the bedrock of long-term customer trust and regulatory confidence upon which our lives depend.

References

- [1] PCI Security Standards Council, "PCI DSS v4.0: Payment Card Industry Data Security Standard," PCI SSC, Mar. 2022. [Online]. Available: https://www.pcisecuritystandards.org/document_library/
- [2] NIST, "SP 800-124 Rev. 2: Guidelines for Managing the Security of Mobile Devices in the Enterprise," NIST, Jul. 2023. Doi: 10.6028/NIST.SP.800-124r2. [Online]. Available: <https://doi.org/10.6028/NIST.SP.800-124r2>
- [3] European Parliament, "Regulation (EU) 2022/2554 — Digital Operational Resilience Act (DORA)," Official Journal of the EU, Dec. 2022. [Online]. Available: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022R2554>
- [4] J. Andress, The Basics of Information Security, 2nd ed. Syngress/Elsevier, 2014. [Online]. Available: <https://www.sciencedirect.com/book/9780128007440>
- [5] W. Stallings, Cryptography and Network Security: Principles and Practice, 8th ed. Pearson, 2022. [Online]. Available: <https://www.pearson.com/en-us/subject-catalog/p/cryptography-and-network-security/P200000003468>
- [6] W. Stallings and L. Brown, Computer Security: Principles and Practice, 4th ed. Pearson, 2018. [Online]. Available: <https://www.pearson.com/en-us/subject-catalog/p/computer-security-principles-and-practice/P200000003339>
- [7] C. P. Pfleeger and S. L. Pfleeger, Security in Computing, 5th ed. Prentice Hall, 2015. [Online]. Available: <https://www.pearson.com/en-us/subject-catalog/p/security-in-computing/P200000003405>
- [8] ISO, "ISO/IEC 27001:2022 — Information Security, Cybersecurity and Privacy Protection," ISO, Geneva, 2022. [Online]. Available: <https://www.iso.org/standard/27001>
- [9] W. K. Brothby, Information Security Governance: A Practical Development and Implementation Approach. Wiley, 2009. Doi: 10.1002/9780470476017
- [10] NIST, "The NIST Cybersecurity Framework (CSF) 2.0," National Institute of Standards and Technology, Feb. 2024. Doi: 10.6028/NIST.CSWP.29. [Online]. Available: <https://doi.org/10.6028/NIST.CSWP.29>
- [11] S. Alimohammadi and M. Alsaleh, "Information Security Maturity Model for NIST Cyber Security Framework," Computer Science and Information Technology, vol. 7, no. 3, pp. 51-62, 2017. Doi: 10.13189/csit.2017.070303
- [12] ISACA, "COBIT 2019 Framework: Introduction and Methodology," ISACA, Schaumburg, IL, 2018. [Online]. Available: <https://www.isaca.org/resources/cobit>
- [13] R. von Solms and J. van Niekerk, "From Information Security to Cyber Security," Computers & Security, vol. 38, pp. 97-102, 2013. Doi: 10.1016/j.cose.2013.04.004
- [14] AXELOS, ITIL Foundation: ITIL 4 Edition. TSO, London, 2019. [Online]. Available: <https://www.axelos.com/certifications/itil-service-management/itil-4-foundation>
- [15] A. Calder and S. Watkins, IT Governance: An International Guide to Data Security and ISO 27001/ISO 27002, 6th ed. Kogan Page, 2016. [Online].

Available: <https://www.koganpage.com/it-management/it-governance-9780749474065>

- [16] ISO, "ISO 31000:2018 — Risk Management: Guidelines," ISO, Geneva, 2018. [Online]. Available: <https://www.iso.org/standard/65694.html>
- [17] Z. A. Soomro, M. H. Shah, and J. Ahmed, "Information Security Management Needs More Holistic Approach: A Literature Review," International Journal of Information Management, vol. 36, no. 2, pp. 215-225, 2016. Doi: 10.1016/j.ijinfomgt.2015.11.009
- [18] FCA, "PS21/3: Building Operational Resilience," Financial Conduct Authority, Mar. 2021. [Online]. Available: <https://www.fca.org.uk/publications/policy-statements/ps21-3-building-operational-resilience>
- [19] ICO, "Guide to the UK GDPR," Information Commissioner's Office, 2021. [Online]. Available: <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-uk-gdpr/>
- [20] T. R. Peltier, Information Security Fundamentals, 2nd ed. CRC Press/Auerbach, 2013. Doi: 10.1201/b15494
- [21] G. Disturber, "ISO/IEC 27000, 27001 and 27002 for Information Security Management," Journal of Information Security, vol. 4, no. 2, pp. 92-100, 2013. Doi: 10.4236/jis.2013.42011. [Online]. Available: <https://doi.org/10.4236/jis.2013.42011>
- [22] R. von Solms, "Information Security Management: Why Standards Are Important," Information Management & Computer Security, vol. 7, no. 1, pp. 50-57, 1999. Doi: 10.1108/09685229910255223