



UNIVERSITY OF WALES TRINITY SAINT DAVID

MSc Cybersecurity and Digital Forensics

Module: ACCA7028 — Data Security, Governance and Compliance

Data Security, Governance and Compliance Framework for FinSure Bank: An Applied Approach

Lecturer: Dr. Ayman Al Hajjar

Student Name: Md Ahasanul Kobir Opy

Student ID: 2522648

Submission Date: 28 April 2026

Table of Contents

Abstract	3
1. Introduction	4
2. Security Frameworks and Models.....	4
2.1 ITIL 4	4
2.2 ISO/IEC 27001 and ISO/IEC 27002	5
2.3 NIST CSF 2.0	5
2.4 COBIT 2019	6
3. Assumptions	7
4. Integrated Security Governance and Compliance Framework for FSB	7
4.1 Governance and Strategic Planning	8
4.2 Security Policies and Data Governance	8
4.3 Risk Management.....	9
4.4 Compliance, Ethics and Assurance	10
4.5 Protection Mechanisms and BYOD	11
4.6 Business Continuity, Third Parties and SLAs	11
4.7 Phased Implementation Roadmap	12
5. Why Regulations and Standards Must Be Updated	13
6. Conclusion	13
References	14

Abstract

FinSure Bank (FSB) is a digital-first financial institution that uses externally hosted cloud services but processes high amounts of personal and financial information in multiple jurisdictions. Its present stance is dangerous since the reliance on clouds, mobile banking, BYOD access and third-party connectivity are not accompanied by well-developed governance, policy, risk management or compliance assurance. This report examines four popular frameworks - ITIL 4, ISO/IEC 27001, NIST Cybersecurity Framework 2.0 and COBIT 2019 - and applies them to develop a custom security, governance and compliance model at FSB. The suggested solution will involve board-level responsibility, risk-based information security management framework, enhanced supplier and device control, and better alignment with the requirements of GDPR, PCI DSS and DORA. Another point the report makes is that regulations and standards have to continuously evolve due to the fact that threat actors, technologies and business models evolve at a faster rate than the rulebooks. The overall finding is that FSB requires a cohesive, constantly enhanced governance framework as opposed to fragmented technical solutions.

1. Introduction

Banks are good targets since they possess payment information, identity, credentials, transaction records and valuable intellectual property. The risk has increased because banking has shifted to cloud services, APIs and mobile apps, and the consequences of a failure now involve fraud, privacy damage and regulatory fines [1], [2]. FSB demonstrates the common vulnerabilities of a fast-growing digital company: disjointed governance, lack of formal risk approach, absence of formal compliance audit process, and mounting pressure to allow personal devices and third-party access. The fundamental issue is thus not merely technical vulnerability but the lack of a consistent operating model to decide on security.

This report appraises the existing security and governance frameworks, and suggests a practical model of FSB based on the factors listed in the brief: laws and ethics, governance, policy, risk management, contingency planning, protection mechanisms and service level agreements.

2. Security Frameworks and Models

A multinational cloud-first bank cannot be served by just one framework. FSB requires an integration of structures since each addresses a different governance issue. ITIL associates security with service delivery and continuous improvement; ISO/IEC 27001 offers the formal management-system structure and control logic; NIST CSF 2.0 presents a clear risk narrative that is built around Govern, Identify, Protect, Detect, Respond and Recover; and COBIT 2019 clarifies accountability between the board, executives and operational teams [3]-[6].

2.1 ITIL 4

ITIL 4 is practical as it views security as service value and not as a technical add-on. This is important at FSB since online banking, lending, identity verification and customer service all rely on reliable services. ITIL assists in integrating security in change enablement, incident management, service continuity and continual improvement [3]. It is limited by the fact that it does not specify a verifiable security foundation or a comprehensive set of controls. ITIL by itself would enhance process discipline but not offer sufficient assurance to a regulated bank.

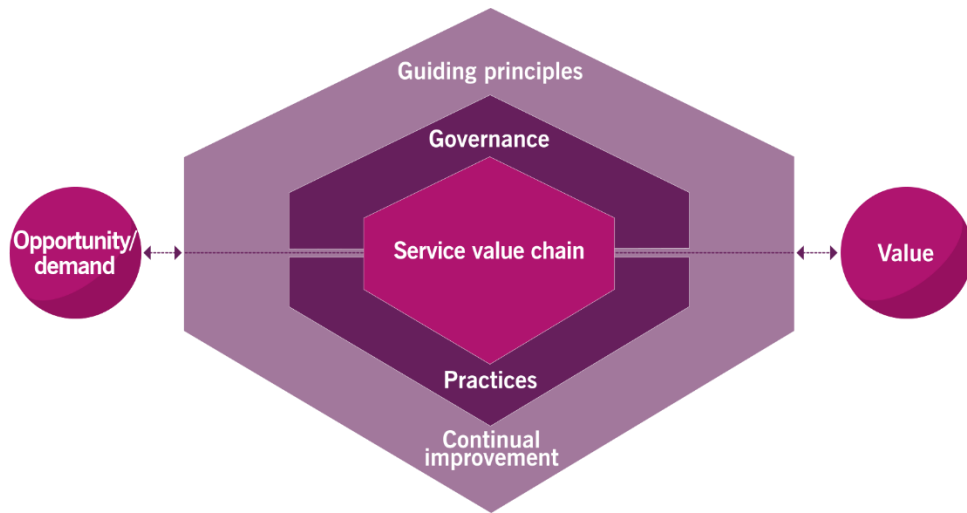


Figure 1: ITIL 4 Service Value System (SVS) Diagram. Source: QRP International [7].

2.2 ISO/IEC 27001 and Supporting Control Guidance

FSB has the best anchor in ISO/IEC 27001:2022 since it mandates the formal information security management system (ISMS), scope, commitment, risk assessment, treatment planning, documented policies and continuous improvement [4]. The corresponding control guidance can be used to support areas such as supplier relationships, threat intelligence, cloud services and access control measures. In the case of FSB, ISO is useful as it transforms security into a governance system that is repeatable. Its vulnerability is that certification will only motivate box-ticking unless controls are tied to business priorities and live operational metrics [8], [9].

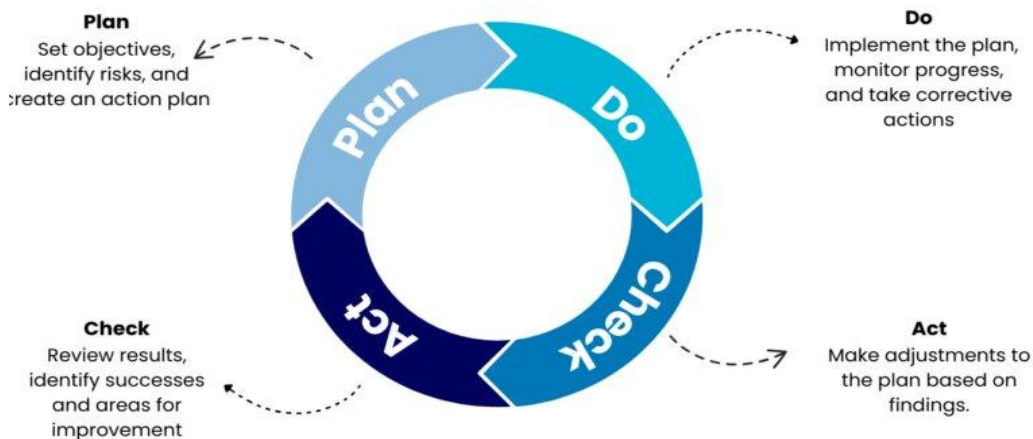


Figure 2: The Plan-Do-Check-Act (PDCA) Cycle Applied to ISO/IEC 27001 ISMS. Source: SF Trainings [10].

2.3 NIST CSF 2.0

In particular, NIST CSF 2.0 is particularly applicable since the new Govern role puts cybersecurity under leadership and not just the IT department [5]. The structure is adaptable and can be communicated to mixed audiences making it practical to a bank that needs to organize executives, engineers, risk personnel and third parties. NIST profiles may also assist FSB to compare its current

position with a target position and prioritise investment. Nevertheless, the CSF is not a certifiable standard and is more effective when aligned to more powerful control and audit tools like ISO 27001 and PCI DSS.



Figure 3: NIST Cybersecurity Framework 2.0 - Six Core Functions. Source: NIST [5].

2.4 COBIT 2019

The area of FSB that is weak nowadays, according to COBIT 2019, is the most useful: governance accountability. COBIT makes a distinction between governance and management and assists in determining who reviews risk, who sets direction, who implements controls and who monitors performance [6]. This separation is essential to a regulated bank since security failures are frequently caused by ambiguous ownership, as opposed to a shortage of technology. COBIT is not as available to the day-to-day operational teams as ITIL or NIST, and should be applied as the governance layer over them, not as the framework used throughout the organization.

Collectively, these frameworks imply a significant principle: efficient banking security is socio-technical. Controls are ineffective when there is a disconnect between strategy, ownership, process and assurance. FSB thus requires a framework that connects governance decisions with operational controls and evidence, as opposed to using a framework due to its popularity or certification.

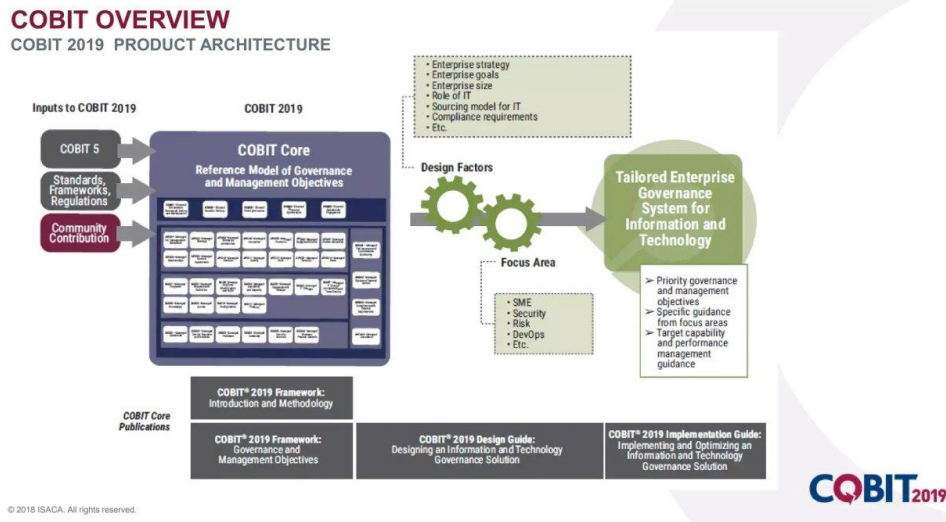


Figure 4: COBIT 2019 Product Architecture - Governance and Management Objectives. Source: ISACA [6].

3. Assumptions

- FSB is present in the UK and at least one EU market, thus both UK GDPR and EU GDPR are considered as relevant compliance drivers.
- FSB handles payment-card data, and thus needs to harmonize applicable systems and processes to the requirements of the PCI DSS.
- The majority of infrastructure is managed on one or more large cloud providers on a shared-responsibility basis.
- BYOD will still be required by certain workers and contractors and the solution should not block but regulate the use of personal devices.
- FSB lacks an established security operations capability, but the top management is open to establishing a CISO-based governance framework and ISO/IEC 27001 certification in two years.

4. Integrated Security Governance and Compliance Framework for FSB

The most appropriate design of FSB is a hybrid one: the management-system foundation is ISO/IEC 27001, the organizing structure of risk communication is NIST CSF 2.0, the governance accountability is COBIT 2019, and the ITIL practices are chosen to incorporate security into the service delivery. This is better than embracing one framework alone since FSB has to meet regulatory scrutiny, coordinate third-party services and enhance day-to-day operations simultaneously.

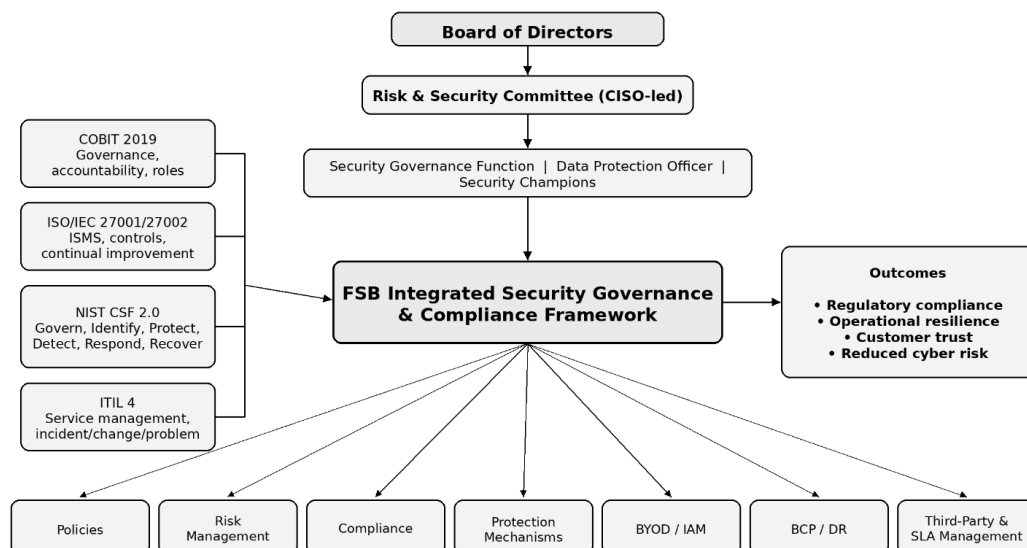


Figure 5: FSB Integrated Security Governance and Compliance Framework Overview (Used Draw.IO)

4.1 Governance and Strategic Planning

The board should be the first to govern security. The board is supposed to endorse a security plan, an official risk appetite statement and yearly security objectives. Under it, a Risk and Security Committee led by the CISO, must convene quarterly and consists of legal, compliance, operations, architecture and product leaders. Operational accountability must in turn be shared by system owners, data owners and security champions in every business unit. This framework helps to avoid the typical issue with digital companies where security is the responsibility of everyone in theory but practically no one in practice [6].

FSB is to monitor the following set of indicators: coverage of critical-asset inventory, coverage of MFA, compliance with patches of internet-facing systems, completion of privileged-access review, completion of supplier-assurance, mean time to detect, mean time to contain, and policy-training. These metrics are to be reported to the board and this would turn governance into an auditable control process.

4.2 Security Policies and Data Governance

FSB should have a small hierarchy of policies as opposed to having a huge library of unread policies. The basic list must also cover: Information Security Policy; Access Control and Identity Management Policy; BYOD and Remote Access Policy; Data Classification and Handling Policy; Incident Response Policy; Third-Party Security Policy; Business Continuity and Disaster Recovery Policy; and Secure Development Policy. Every policy must specify owner, scope, mandatory controls, exceptions process and review cycle.

It is adequate to have a four-level classification model - Public, Internal, Confidential and Restricted. Restricted data should include customer identity data, payment data, authentication secrets and regulatory evidence. The management of rules must require encryption during transit and rest, authorized repositories, only, privileged access logging, and the use of personal devices to store local data. Since FSB is cloud-heavy, shared-responsibility boundaries should be explicitly stated in the policy set to ensure that teams understand what controls are part of FSB and what are part of the provider.

4.3 Risk Management

The foundation of a successful security system is risk management. The standard approach to information security risk management is ISO/IEC 27005:2022, which is adopted in this case. It is a four-iteration process that includes risk identification, risk analysis and evaluation, risk treatment, and risk monitoring and review [11].

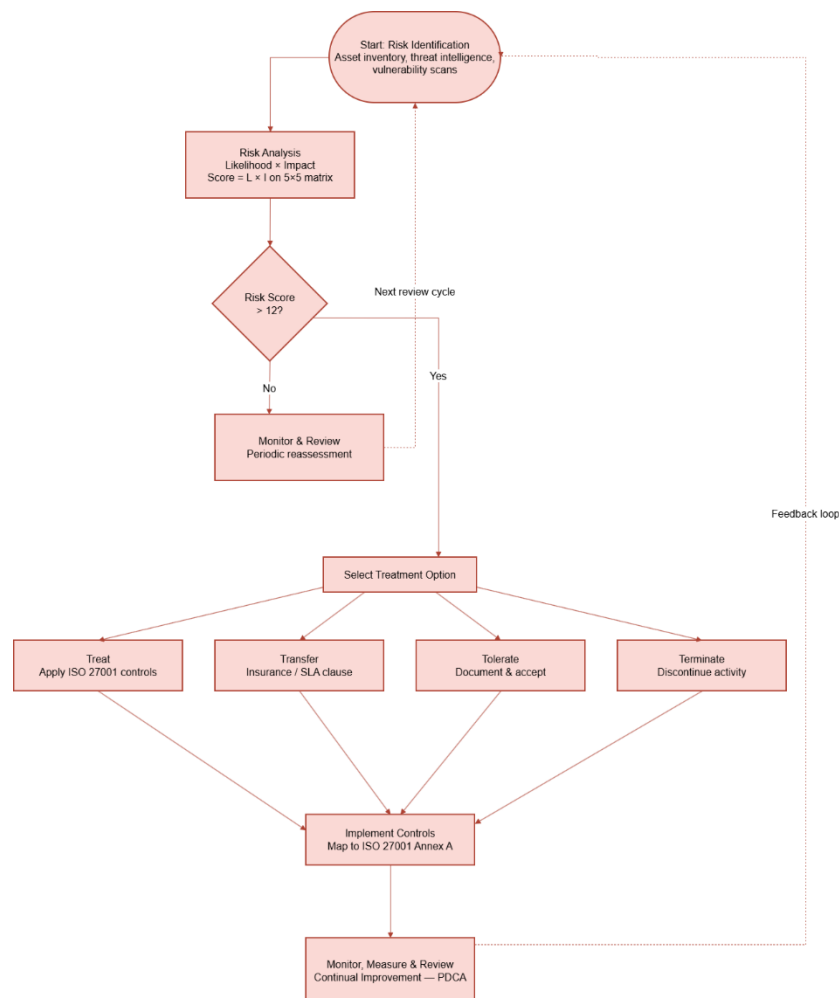


Figure 6: FSB Risk Management Process Flowchart (Used Draw.IO)

In the case of FSB, the CISO needs to create and maintain a risk register. Risks are rated on a likelihood-impact matrix of 5x5. Treatment choices are based on the ISO 27001 approach: Treat

(implement controls), Transfer (insurance, SLAs), Tolerate (accept within appetite), or Terminate (stop the activity). A sample risk register of the priority risks of FSB is given in Table 1.

Risk Description	Category	Likelihood (1-5)	Impact (1-5)	Risk Level	Treatment / Mitigation
Unauthorized access via compromised BYOD device	Technical	4	5	HIGH (20)	MDM deployment; MFA; network segmentation; endpoint encryption
Cloud provider outage causing service disruption	Operational	3	5	HIGH (15)	Multi-cloud redundancy; DRP with 4hr RTO; SLA with cloud provider
Insider threat — data exfiltration by employee/contractor	People	3	5	HIGH (15)	DLP tools; least-privilege IAM; user behaviour analytics (SIEM)
GDPR breach due to inadequate data handling	Compliance	4	4	HIGH (16)	Data classification policy; privacy impact assessments; staff training
Third-party supplier security failure	Supply Chain	3	4	MEDIUM (12)	Supplier security assessments; contract clauses; annual audits
Phishing/social engineering attack on staff	People	5	3	MEDIUM (15)	Security awareness training; anti-phishing email gateways; simulation exercises
Ransomware attack on cloud workloads	Technical	3	5	HIGH (15)	Immutable backups; endpoint detection & response (EDR); incident playbook

Table 1: FSB Priority Risk Register — Sample (Likelihood x Impact Matrix, 1=Low, 5=High)

4.4 Compliance, Ethics and Assurance

The compliance at FSB must be structured as a working discipline, rather than as an annual practice. The bank will need to at least implement security controls in accordance with the UK GDPR and EU GDPR specifications on proper technical and organisational controls, breach management and responsibility, and the PCI DSS specifications on payment-card environments [12], [13]. Since FSB is involved in financial services and transnational, the design must also be aware of the DORA focus on ICT risk management, resilience testing, incident reporting, and third-party ICT oversight [14].

It is important that there is a separation of roles in good compliance practice. Privacy obligations should be supervised by a Data Protection Officer, whereas security controls and security-risk treatment should be owned by the CISO. Policies in actual practice should be tested by internal audit, or independent assurance role. New high-risk products, particularly mobile features that are analytics-intensive or changes in cross-border processing, should be subject to DPIA. Ethics should be handled together with law: clear privacy disclosures, minimisation of data, justifiable retention term and privacy-by-design should be standard design principles as opposed to compliance as an afterthought [15].

4.5 Protection Mechanisms and BYOD

The defence-in-depth architecture that FSB should implement should be informed by the principles of Zero Trust. There should be no implicit trust in any user, device or application since banking staff, contractors and customers will be connecting to various networks and devices. It should have the minimum technical baseline, such as MFA to all users, phishing-resistant authentication to privileged and high-risk users where possible, centralised identity and access management, privileged access management, endpoint detection and response, secure configuration baselines, vulnerability scanning, network segmentation, SIEM-led monitoring, and immutable backups [5], [2].

BYOD needs to be strictly regulated. Corporate resources should be accessed by personal devices only via managed application or containerized workspaces, and devices must be checked prior to being given access. Local storage of Restricted data on unmanaged devices should be prohibited. Where third parties must have access, FSB must favor segregated accounts, just-in-time privileges and logging and review rights that are defined in a contract. These controls minimize fraud, credential theft and data leakage without impeding business.

4.6 Business Continuity, Third Parties and SLAs

Since FSB relies on services that are hosted externally, resilience planning is essential. The bank ought to have a business continuity plan, disaster recovery plan and cyber-incident response playbooks in line with business impact analysis. Recovery goals must be prioritized: the most important customer-facing banking and payment services must have strict recovery goals, and less important internal services can withstand longer outages. Tabletop exercises and periodic technical recovery tests must be done at least once a year; a plan which is never exercised is not a control.

Procurement and contract management should incorporate third-party assurance. Supplier due diligence must examine certifications, evidence of penetration testing, commitments on data-location, subcontracting, resilience, and incident-notification schedules. The availability, restoration

expectations, evidence rights, breach-notification times, exit support and secure data return or destruction should be specified in SLAs with critical providers. This is especially the case with cloud, payments, identity and managed security services, since the resilience of FSB cannot be decoupled with theirs.

The management of SLA must be considered as a security control, not just a procurement term. The critical providers must be committed to quantifiable criteria on uptime, recovery services, log retention, vulnerability disclosure, security incident notification and collaboration in investigations. Audit rights, data-residency clauses where applicable, secure exit and evidence requirements like annual assurance reports should also be contained in FSB. This is important since a bank that has adopted a cloud-first approach may be able to satisfy its internal controls, but still fail its customers in the event that the obligations of a particular provider are unclear or unenforceable. Powerful SLAs transform the external dependency into managed risk.

4.7 Phased Implementation Roadmap

Implementing it in stages is more realistic than trying to correct all the gaps at the same time. The first 90 days should be the basis of governance and basic coverage of control; the second 6-12 months should formalize the ISMS and build resilience and the second year should be regarding audit maturity and certification preparedness. This sequencing is important since the early wins instill confidence in the management and the later stages provide more profound assurance, audit evidence and certification preparedness. It also minimizes interference with live banking activities.

Phase	Priority actions	Primary owners	Evidence of completion
0-90 days	Appoint CISO and DPO; approve governance structure; identify critical assets; enforce MFA; launch BYOD policy and risk register	Board, CISO, Compliance	Committee terms of reference, asset inventory, MFA coverage report, approved policies
3-12 months	Implement MDM, SIEM, privileged access controls and supplier due diligence; perform DPIAs; test incident response and recovery	CISO, IT Operations, Procurement	Control implementation evidence, supplier assurance files, exercise reports
12-24 months	Mature ISMS, internal audit cycle, metrics reporting and certification readiness; refine SLAs and resilience testing	CISO, Internal Audit, Executive team	Management review outputs, audit results, certification gap-closure evidence

Table 2: Phased implementation roadmap for FSB

5. Why Regulations and Standards Must Be Updated

Rules and norms have to evolve since the systems that they apply to are not static. The emergence of new attack techniques, cloud operating models, AI-driven fraud, open banking integration and complex supply chains pose risks that older standards may not have been able to fully foresee. That is why such updates as ISO/IEC 27001:2022 and NIST CSF 2.0 are important: they represent a change in the paradigm of perimeter security to governance, resilience, cloud use and threat-informed risk management [4], [5]. Another example is DORA since the reliance of contemporary firms on ICT providers was not properly considered in the traditional financial regulation [14]. Learning effect is also present. The fact that the older rules were too broad, too limited, or too slow is shown by significant violations. Modifying standards enables regulators and the profession to transform lessons of incidents into improved base practice. The ever-evolving can be exhausting especially across jurisdictions, but the remedy is not regulatory stagnation. FSB must map overlapping obligations once and create shared control evidence to support multiple compliance regimes simultaneously, and to depend on ongoing monitoring. The issue of compliance would be especially threatening to FSB since its operating model is very dynamic. Risk can change more quickly than annual policy reviews due to new mobile features, contractor access patterns, outsourced services and data-sharing arrangements. The new standards must thus be seen as catalysts to governance review and not as administrative burdens.

6. Conclusion

FSB's main weakness is not the absence of security tools but the absence of an integrated governance model. A good response will thus entail more than the implementation of technologies but board supervision, ownership, formal risk treatment, improved control of devices and suppliers as well as an ongoing compliance process. The hybrid model proposed relies on ISO/IEC 27001 to offer structure, NIST CSF 2.0 to structure risk, COBIT 2019 to assign responsibility and ITIL 4 to integrate security in service provision. This combination is very appropriate to a cloud-first bank that has BYOD exposure and cross-border requirements.

The highest priority short-term measures include appointing responsible leaders, cataloging essential resources and data, implementing MFA and device controls, developing the risk register, and formalizing supplier assurance. Based on that, FSB can evolve into a certifiable ISMS and more robust, auditable operating model.

References

- [1] J. Address, *The Basics of Information Security: Understanding the Fundamentals of InfoSec in Theory and Practice*, 2nd ed. Waltham, MA, USA: Syngress/Elsevier, 2014.
- [2] M. E. Whitman and H. J. Mattord, *Principles of Information Security*, 6th ed. Boston, MA, USA: Cengage Learning, 2018.
- [3] AXELOS, *ITIL Foundation: ITIL 4 Edition*. London, U.K.: The Stationery Office, 2019.
- [4] International Organization for Standardization, *ISO/IEC 27001:2022, Information Security, Cybersecurity and Privacy Protection - Information Security Management Systems - Requirements*. Geneva, Switzerland: ISO, 2022.
- [5] National Institute of Standards and Technology, *The NIST Cybersecurity Framework (CSF) 2.0*, Gaithersburg, MD, USA: NIST, NIST CSWP 29, Feb. 2024. [Online]. Available: <https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf>
- [6] ISACA, *COBIT 2019 Framework: Governance and Management Objectives*. Schaumburg, IL, USA: ISACA, 2019.
- [7] QRP International, "What is ITIL?," n.d. [Online]. Available: <https://www.qrpinternational.be/blog/it-governance-and-service-management/what-is-til/>
- [8] G. Disterer, "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.
- [9] A. Calder and S. Watkins, *IT Governance: An International Guide to Data Security and ISO 27001/ISO 27002*, 7th ed. London, U.K.: Kogan Page, 2020.
- [10] SF Trainings, "PDCA in ISO 27001: A Practical Guide for Auditors," n.d. [Online]. Available: <https://www.sftrainings.org/pdca-in-iso-27001-a-practical-guide-for-auditors/>
- [11] International Organization for Standardization, *ISO/IEC 27005:2022, Information Security, Cybersecurity and Privacy Protection - Guidance on Managing Information Security Risks*. Geneva, Switzerland: ISO, 2022.
- [12] Information Commissioner's Office, "Guide to the UK General Data Protection Regulation (UK GDPR)," 2021. [Online]. Available: <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/>
- [13] PCI Security Standards Council, *Payment Card Industry Data Security Standard: Requirements and Testing Procedures, Version 4.0.1*. Wakefield, MA, USA: PCI Security

Standards Council, Jun. 2024. [Online]. Available:
https://www.pcisecuritystandards.org/document_library/.

- [14] European Parliament and Council of the European Union, *Regulation (EU) 2022/2554 of 14 December 2022 on Digital Operational Resilience for the Financial Sector, Official Journal of the European Union*, vol. L 333, pp. 1-79, Dec. 27, 2022.
- [15] A. Cavoukian, *Privacy by Design: The 7 Foundational Principles*. Toronto, ON, Canada: Information and Privacy Commissioner of Ontario, 2009. [Online]. Available:
<https://www.ipc.on.ca/wp-content/uploads/Resources/7foundationalprinciples.pdf>