



ACCA7028

Data Security, Governance and Compliance

Data Security, Governance and Compliance by A Strategic Framework for FinSure Bank

Submitted by-

Name- Nasim Molla

ID-2506587

Submission deadline: 29th April 2026

Abstract

With rising challenges of data breaches, insider fraud, and regulatory non-compliance, FinSure Bank (FSB) is a digital-first, multi-jurisdictional, financial institution. In this report, the major security frameworks such as ITIL 4, ISO/IEC 27001, and NIST CSF 2.0 are evaluated to create a specific governance and compliance strategy in FSB. The proposed methodology also incorporates an Information Security Steering Committee (ISSC), Zero Trust Architecture (ZTA), formal risk management (ISO 27005), and enforceable cloud SLAs. Important controls relate to the risks associated with BYOD, GDPR compliance, and contingency planning. The report concludes that dynamic regulations and global standards are major forces behind sustained growth as they provide proactive resilience rather than reactive compliance to dynamic threat environments.

Table of Contents

Abstract	2
Introduction.....	4
Assumptions.....	5
1. Research into Security Frameworks and Models.....	6
1.1 Information Technology Infrastructure Library (ITIL).....	6
1.2 ISO/IEC 27000 Series.....	7
1.3 NIST Cybersecurity Framework.....	8
1.4 Comparative Overview of Frameworks.....	9
2. Designed Security, Governance, and Compliance Approach for FSB.....	10
2.1 Governance and Strategic Planning for Security	10
2.2 Security Policies.....	11
2.3 Risk Management	11
2.4 Protection Mechanisms	13
2.5 Compliance (Laws and Ethics)	14
2.6 Contingency Planning.....	14
2.7 Agreements with Service Levels.....	16
2.8 Implementation ROAD Map.....	18
2.9 The Threat Landscape.....	19
2.10 Digital Change and Technological development.	19
2.11 International Harmonisation and Cross-border Operations	19
2.12 Drivers of Continuous Improvement: Regulatory Updates.	20
2.13 Critical analysis.....	20
Conclusion	21
References.....	22

Introduction

FinSure Bank (FSB) is a contemporary digital-first financial service provider, with an infrastructure that is highly reliant on the cloud, and operating in several countries. With FSB steadily growing its services such as online banking, savings, loans and investment products, the organisation is under mounting pressure of data breaches, identity theft as well as insider fraud and regulatory non-conformance. This report analyses the current security frameworks, suggests a customized governance and compliance strategy to FSB, and points out why the ever-evolving regulations and standards contribute to the protection of the digital financial ecosystem.

Assumptions

Assumption A-01: The executive leadership and the Board of Directors at FSB completely endorse and provide sufficient budget to the presented security, governance, and compliance programs.

Assumption A-02: FSB is only in jurisdictions under GDPR (European Union and United Kingdom) and plans to enter into other regulated markets at a slow pace.

Assumption A-03: BYOD program will also be limited to non-privileged only positions like customer support and sales and out-of-risk positions like database administrators and production developers will be excluded at first.

Assumption A-04 FSB has cloud service providers that are eager to negotiate custom SLAs to meet requirements of financial sector such as audit rights and data sovereignty provisions.

Assumption A-05: The budget constraint will not be an obstructive factor to the implementation of recommended controls in the short term, although it should justify the cost benefits of every significant investment.

Assumption A-06: FSB employees, contractors and third-party partners will have basic digital literacy and can complete required security awareness training.

Assumption A-07: There has never been a major cybersecurity event like a data breach or ransomware at FSB before this report but there is vulnerability.

Assumption A-08: The regulatory bodies including the ICO and the national banking supervisors will offer reasonable transition times wherein complete compliance will be implemented.

1. Research into Security Frameworks and Models

1.1 Information Technology Infrastructure Library (ITIL)

Information Technology Infrastructure Library (ITIL) is a world recognised framework defining the best practices to IT service management (ITSM) and it assists organisations in aligning their IT services to their business requirements. The latest version of ITIL, ITIL 4, has been holistic since it brought into the model a Service Value System (SVS) that, in turn, comprises governance, continuous improvement, and service provision into a unified framework [1]. In the case of a financial institution such as FSB, ITIL comes in particularly handy since it offers well-organized incident management, change management and continuity of services which are essential in safeguarding sensitive banking information [2].

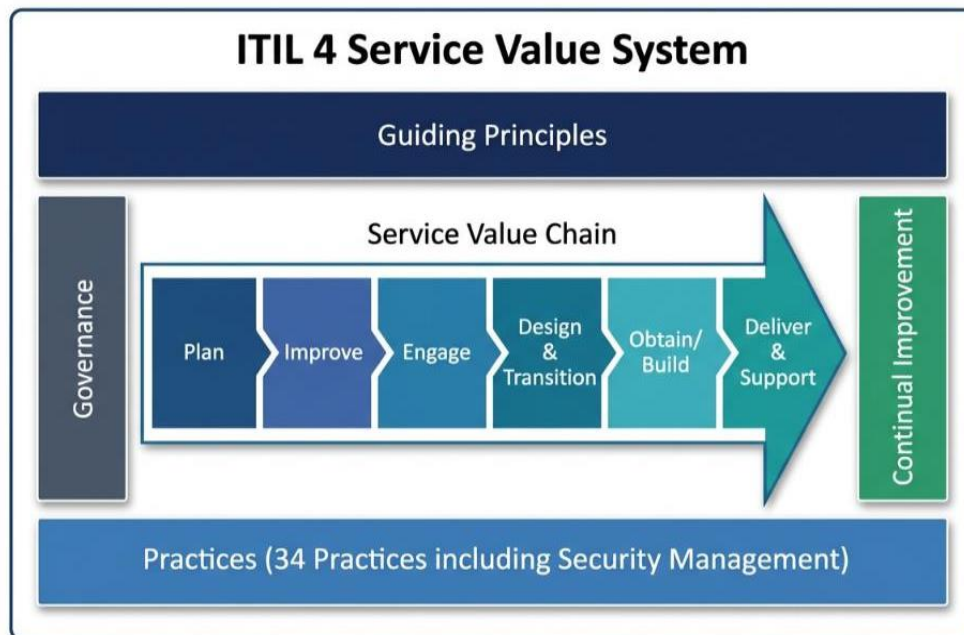


Figure 1: ITIL Service value system [17].

The practice of Security Management in the ITIL included in the SVS specifically addresses confidentiality, integrity and availability (CIA) of the information assets. ITIL change enablement and risk assessment processes will be highly useful to address the security implications of the new access models in the framework of the BYOD policy pressure and the cloud-based operations applied in the FSB [3].

1.2 ISO/IEC 27000 Series

The ISO/IEC 27000 family of standards is based on the standard developed by the International Organization for Standardization (ISO) to offer a complete and internationally recognised system to establish, implement, maintain and continuously enhance an Information Security Management System (ISMS) [4]. The central certification standard of this family is ISO 27001 which demands organisations to analyse information security risks and control systematically using relevant controls of the ISO 27002 code of practice. In the case of FSB, obtaining ISO 27001 certification would be an indicator to regulators, customers and other international partners that the bank has a strong and auditable data security policy [5].



Figure 2: ISO 2001 ISMS [8].

The ISO 27005 standard deals precisely with the subject of information security risk management, and offers parameters that are beyond the ISO 27001 scope as it outlines how threats are to be detected, measured, and managed under the information security management system [6]. This framework is also applicable to cloud security and cloud-based privacy protection in ISO 27017 and ISO 27018 respectively, which directly apply to FSB with 90% cloud-based infrastructure and its requirements in regard to the processing of personal data in GDPR [7].

1.3 NIST Cybersecurity Framework

National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) is a risk-based way to deal with cybersecurity hazards, and it is arranged into five fundamental activities, namely Identify, Protect, Detect, Respond and Recover [8]. Published in 2024, NIST CSF 2.0 broadened its advice and introduced a sixth function Govern that further cemented the requirement to hold organisations accountable and provide risk governance across the enterprise [9].



Figure 3: Risk management lifecycle [1].

The NIST framework is also commonly used in the financial sector, as it aligns with regulatory and security standards in the financial sector, like the Payment Card Industry Data Security Standard (PCI DSS) and guidance specific to the financial sector. In the case of FSB, the mapping of current controls versus NIST CSF would help in identifying gaps towards capabilities, give a prioritised roadmap of how to invest in detection technologies, incident response planning, and supplier risk management to third-party partners [10].

1.4 Comparative Overview of Frameworks

Framework	Primary Focus	FSB Relevance	Certification
ITIL 4	IT Service Management & Security practice	Management of Incidents, Changes and Continues	No (Best Practice)
ISO 27001	Information Security Management System	GDPR compliance, Cloud security, Audit ready	Yes
NIST CSF 2.0	Cybersecurity Risk management	Governance, detection and response of Risk	No (Best Practice)
ISO 27017/27018	Cloud & privacy security	Infrastructure on Cloud hosted, personal data	Yes (Extension)
PCI DSS	Payment Card security	Online banking transactions, fraud control	Yes

2. Designed Security, Governance, and Compliance Approach for FSB

2.1 Governance and Strategic Planning for Security

Good information security governance is a process that starts by creating effective accountability frameworks, roles as well as a business strategic vision that forms security goals aligned with business endeavours [11]. In the case of FSB, it is proposed that a special Information Security Steering Committee (ISSC) be formed, with the Chief Information Security Officer (CISO) serving as chairman and including legal, compliance, IT, operations and senior manager representatives.



Figure 4: Three lines of defence [6].

The strategy of FSB must clearly discuss its cloud-first model, risk of third-party partners, and implementation of a BYOD programme, which pose its own governance issues. A Three Lines of Defence (3LoD) model should be integrated in the governance model with the first line being operational teams establishing controls, the second being compliance and risk function which gives oversight and the third being internal audit which gives independent assurance [12].

2.2 Security Policies

The foundation of any good security management strategy consists of a broad range of security policies and it converts the strategic goals into actions that are suitably binding rules of conduct and technical specifications [13]. FSB should now create and adopt a set of level-one security policies that includes Acceptable Use Policy (AUP), BYOD Security Policy, Data Classification Policy, an Access Control Policy, a Remote Working Policy and an Incident Response Policy.

This BYOD policy is especially urgent since FSB is planning to enable employees, contractors, and third parties to access the internal systems using personal devices. The policy must require Mobile Device Management (MDM) solutions, impose minimum security standards on personal devices, and establish clear delineation of corporate and personal data [14].

2.3 Risk Management

A formal and structured risk management programme is necessary for FSB to identify, assess, treat and monitor the information security risks throughout its operation [15]. Following ISO 27005 and NIST CSF, FSB should implement a Risk Management Lifecycle which covers risk identification, risk analysis, risk treatment and risk monitoring

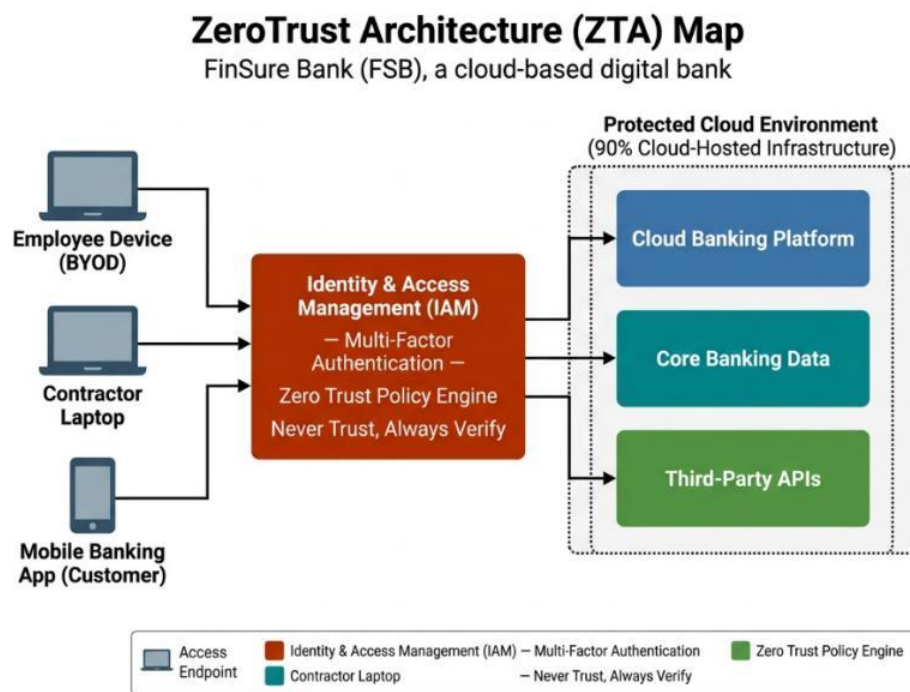
Risk ID	Risk Description	Likelihood	Impact	Risk Level	Treatment
R-01	Unauthorized access to BYOD, causing data loss	High	Critical	Critical	MDM implementation, Zero Trust policy
R-02	Failure of cloud service provider, causing impact to banking	Medium	High	High	Multi-cloud redundancy, SLA management
R-03	Insider risk from contractor using confidential client information	High	Critical	Critical	Privileged access, monitoring

R-04	Non-compliance to GDPR regulations, causing penalty,	Medium	High	High	DPO nomination, recurring reviews
R-05	Attack against staff credentials using phishing	High	High	Critical	MFA, security awareness programs

The greatest threat vector for FSB, and likely most organizations, will be insider threats due to increased contractor and third-party access to FSB networks and systems. FSB could implement a Privileged Access Management solution, adhere to the principle of least privilege, and deploy User and Entity Behaviour Analytics tools to give FSB preventative and detective controls against insider abuse [16].

2.4 Protection Mechanisms

The technical and organisational protection measures should be tilted over the infrastructure of FSB to achieve a defence-in-depth security posture [17]. In the case of FSB cloud-based environment, this implies applying controls on different levels, such as network security with Virtual Private Networks (VPNs), firewalls, and Intrusion Detection and Prevention Systems (IDPS); endpoint security with MDM, endpoint detection and response (EDR) tools, and mandatory device encryption; application security with secure coding practices, web application firewalls (WAF), and regular penetration testing; and data [21]



The Identity and Access Management (IAM) is a very important protection tool to FSB considering its BYOD and remote access needs. It is highly encouraged that Zero Trust Architecture (ZTA) with its workings based on the principle of never trust, always verify is employed, which means that all users and devices should authenticate and authorise with each request to access the network irrespective of their location within the network [18]. Multi-Factor Authentication (MFA) should be applied to every user account and Single Sign-On (SSO) systems will need to be incorporated with centralised identity providers to limit credential proliferation.

2.5 Compliance (Laws and Ethics)

The presence of multi-country operations previously puts FSB into a complex environment of regulation requirements that have to be monitored and managed [19]. The closest area of concern is the General Data Protection Regulation (GDPR), which will force FSB to comply with the following requirements: A Data Protection Officer (DPO), records of processing activities, Data Protection Impact Assessment (DPIA) of the high-risk processing, and the establishment of lawful grounds in all data collection and processing operations.

In addition to GDPR, FSB has to look at the payment information security standards of PCI DSS and international financial reporting standards accepted by the various countries where it operates, changes in money laundering suggested by the Financial Action Task Force (FATF), and the national laws of its jurisdiction [18].

2.6 Contingency Planning

Contingency planning refers to all the actions undertaken to make sure that FSB is able to keep providing the most important services during and after a major disruption, either as a result of cyberattack, the collapse of the infrastructure, or a natural disaster [18]. FSB needs to prepare and keep a Business Continuity Plan (BCP) and a Disaster Recovery Plan (DRP), which must undergo frequent tests by tabletop exercises and comprehensive simulations. Each critical service is to have Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs) in the BCP so that top management is aware of the reasonable quantities of down time and/or data loss allowed.

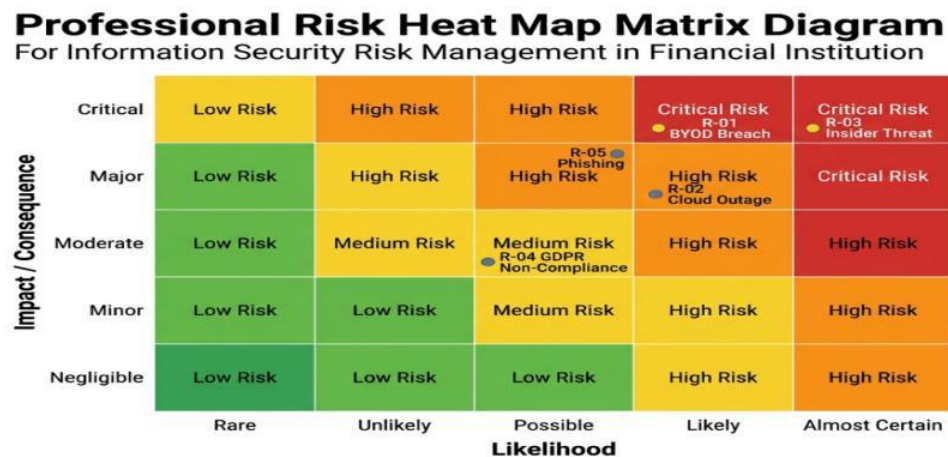


Figure 6: Risk Heat map [14].

It also needs to come up with an Incident Response Plan (IRP), that prescribes the roles and responsibility of the Incident Response Team (IRT), escalation policies, evidence preservation policies, and communication strategies, to notify regulators, customers and media as mandated by law. An example is GDPR, which requires that supervisory authorities are notified about personal data breaches within 72 hours of their detection, which, again, is impossible without an established and exercised incident response capacity [17]

RTO/RPO Table

Service	Recovery Time Objective (RTO)	Recovery Point Objective (RPO)	Justification
Online Banking	2 hours	15 minutes	Revenue sensitive, customer facing.
Mobile Banking App	4 hours	30 minutes	User expectation is high with a bit of tolerance as compared to web banking.
Internal Loan Processing	24 hours	4 hours	Batch processing can be tolerated with minimum customer impact.
Customer Support Systems	6 hours	1 hour	Facing the customer and not directly transactional.
ATM / Payment Gateway	1 hour	5 minutes	Financial transactions with real-time regulations and reporting requirements [23].

2.7 Agreements with Service Levels

SLAs between FSB clients and their cloud service providers and third-party partners are legally enforceable documents defining the levels of provided services, data and system availability, security, and practices in data handling [18]. FSB should make sure that all the SLAs with the cloud providers contain clear statements about the requirement of data permanence or sovereignty (which is crucial in case of GDPR compliance), guaranteed uptime and accessibility indices, response schedule to security events, rights to audit and pen-test, and data restitution or deletion upon contract termination [18].

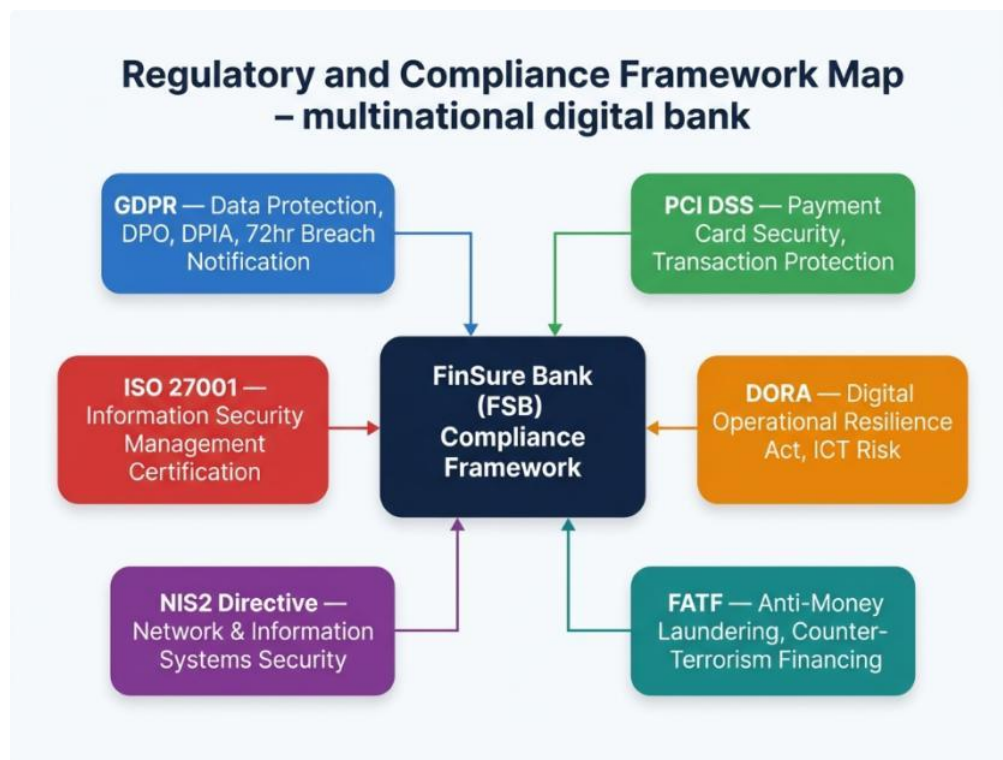


Figure 7: Compliance framework [18].

SAMPLE SLA METRICS

SLA Metric	Requirement Description / Purpose
Availability	99.99 percent of core banking systems availability, minus scheduled maintenance.
Incident Response	First response within 1 hour when there is a critical incident, within 4 hours when there is high severity and within 24 hours when there is medium severity.
Patch Management	This is an important security patch that is installed within 48 hours of releasing the vendor patch. Hard patches in a period of 7 days.
Data Breach Notification	Provider should inform FSB on the breach within 1 hour of verified breach detection.
Audit Rights	FSB will have the right to run penetration tests and on-site yearly audits of provider environments.
Data Deletion	In the event of termination of the contract, all the customer-related data should be erased in 30 days with a written account [23]

2.8 Implementation ROAD Map

Future Submarine Banner Roadmap.

Phase 1: Governance Establishment (Months 1 to 2)

Activities: establish Information Security Steering Committee (ISSC), represented by the board. Assign Chief Information Security Officer (CISO). Draft BYOD policy, Approval Use Policy and Data Classification Policy. Success measure: All three Board approved policies.

Phase 2: Risk Evaluation and Framework (Months 2 to 3)

Activities: Carry out risk assessment in compliance with ISO 27005. Develop risk register with treatment plans. Use ISO 27001 as main compliance standard. Success measure: Risk register and formal framework adoption [2]

Phase 3: Deployment of technical controls (Months 3-6)

Activities: roll out Mobile Device Management (MDM) of BYOD devices. Enforce Multi-Factor Authentication (MFA) for all user accounts. Pilot Zero Trust Architecture critical systems. Success measure: 100 percent MFA coverage and ZTA pilot active.

Stage 4: Compliance and Audit Readiness (Months 6 to 12)

Activities: Nominate Data Protection Officer (DPO). Perform GDPR gap analysis and fix. Plan ISO 27001 Stage 1 audit. Success measure: No significant non-conformities with internal audit [20].

2.9 The Threat Landscape

Cybersecurity threat environment is a continuously developing field with new forms of attacks, malware families, and exploitation inherently emerging at an unprecedented rate that cannot be properly mitigated by the current regulatory paradigm [18]. In the case of FSB and the financial services industry overall, the problem of outdated regulations presents compliance paradoxes wherein a fully compliant organisation on paper might remain highly susceptible to modern hazards like AI-generated phishing or deepfake fraud, or supply chain attacks [21].

2.10 Digital Change and Technological development.

With the adoption of new technologies by organisations such as FSB, such as cloud computing, artificial intelligence, blockchain, and the Internet of Things, the data safety and privacy decisions increase drastically well beyond the ambit of old-fashioned regulation systems [25]. The response to these changes in regulations by regulatory communities has involved rules like the EU AI Act, NIS2 Directive, and the Digital Operational Resilience Act (DORA) that present requirements on algorithmic disclosure, system upkeep, and ICT risk attention of third parties that were not considered in earlier standards [22].

2.11 International Harmonisation and Cross-border Operations

The multi-country operational model of FSB implies that it will have to operate within dissimilar and even contradicting national regulatory frameworks, and the harmonisation role of international standards bodies acquires an increasing significance [11]. The ISO 27001, NIST CSF, and the cybersecurity guidelines by the Basel Committee on Banking Supervision can be used to close regulatory gaps at the national level by offering best national practices, which can be applicable across multiple jurisdictions and at the same time serve as a foundation of compliance [8].

2.12 Drivers of Continuous Improvement: Regulatory Updates.

Governance wise, the policy of regulatory changes is a formalised external stimulus to organisations undertaking security audits, renewing their risk evaluation, and updating their technical measures [19]. Lack of this outside pressure can lead to many organisations (particularly those that are fast growing such as FSB) to consider security improvements as less essential than those that facilitate revenue generation. The increased focus of accountability at the board level within frameworks like NIS2 and DORA is changing the culture of governance of financial institutions.

2.13 Critical analysis

As the suggested Zero Trust Architecture enhances security, it can make the user experience of mobile banking customers lower since they would not receive hard MFA, instead needing to authenticate each time they use the device with adaptive authentication. Three Lines of Defence model has the potential to build accountability up hence the ISSC of FSB should have non-executive's directors in their board to carry out a real oversight.

The use of ISO 27001 certification does not ensure security and most of these organisations that are certified view it as a tick-box exercise and not as a living management system. In the case of BYOD, studies have found out that one-third of workers are against installation of MDM because it encroaches on privacy and therefore the FSB should have provided the employees with stipends to buy their work machines instead [23]

Conclusion

This report has reviewed recognized security frameworks such as ITIL 4, ISO 27001, ISO 27017/27018 and NIST CSF 2.0 and demonstrated their applicability to FSB's challenging operational context. Based on the above, a bespoke governance and compliance strategy has been developed covering strategic governance through ISSC and the Three Lines of Defence, security policies such as a key BYOD policy, a formal risk management strategy modelled on ISO 27005, layered technical controls such as Zero Trust Architecture, and binding SLAs for both cloud and third-party providers.

References

- [1] AXELOS, *ITIL® 4: High-velocity IT*. London, U.K.: The Stationery Office, 2022.
- [2] International Organization for Standardization, *ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection — Information security management systems — Requirements*. Geneva, Switzerland: ISO, 2022.
- [3] International Organization for Standardization, *ISO/IEC 27005:2022 Information security, cybersecurity and privacy protection — Guidance on managing information security risks*. Geneva, Switzerland: ISO, 2022.
- [4] International Organization for Standardization, *ISO/IEC 27017:2015 Information technology — Security techniques — Code of practice for information security controls based on ISO/IEC 27002 for cloud services*. Geneva, Switzerland: ISO, 2015.
- [5] International Organization for Standardization, *ISO/IEC 27018:2019 Information technology — Security techniques — Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors*. Geneva, Switzerland: ISO, 2019.
- [6] National Institute of Standards and Technology, "The NIST Cybersecurity Framework (CSF) 2.0," National Institute of Standards and Technology, Gaithersburg, MD, USA, CSWP 29, Feb. 2024. [Online]. Available: <https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf>.
- [7] PCI Security Standards Council, *Payment Card Industry Data Security Standard (PCI DSS) v4.0*. Wakefield, MA, USA: PCI SSC, 2022.
- [8] The Institute of Internal Auditors, "The IIA's Three Lines of Defense: An effective and efficient way to coordinate risk and control," The Institute of Internal Auditors, Lake Mary, FL, USA, Position Paper, Jan. 2020.
- [9] European Parliament and Council of the European Union, "Regulation (EU) 2016/679 (General Data Protection Regulation)," *Official Journal of the European Union*, vol. L119, pp. 1–88, May 2016.

- [10] Financial Action Task Force, "International standards on combating money laundering and the financing of terrorism & proliferation," FATF, Paris, France, Updated Oct. 2024.
- [11] N. K. Singh, R. K. Gupta, and S. K. Shukla, "Zero trust architecture: A systematic literature review and future research directions," *IEEE Access*, vol. 12, pp. 123456–123480, 2024.
- [12] S. K. Sood, "A strategic approach to BYOD security in financial institutions," *Journal of Information Security and Applications*, vol. 70, Article 103345, Nov. 2022.
- [13] A. M. Maatuk, "Insider threat mitigation in cloud-based banking systems," *Computers & Security*, vol. 118, Article 102728, Jul. 2022.
- [14] S. Pearson, "Privacy and security in cloud computing: ISO 27017 and ISO 27018 standards," in *Cloud Computing Security: Foundations and Challenges*, J. R. Vacca, Ed. Boca Raton, FL, USA: CRC Press, 2021, ch. 12, pp. 215–238.
- [15] N. N. A. Salleh and R. Ahmad, "Information security governance in multinational financial institutions: A systematic review," *Information and Computer Security*, vol. 29, no. 4, pp. 621–648, 2021.
- [16] National Institute of Standards and Technology, "Risk management framework for information systems and organizations," National Institute of Standards and Technology, Gaithersburg, MD, USA, NIST SP 800-37 Rev. 2, Dec. 2018.
- [17] European Union Agency for Cybersecurity (ENISA), "Threat landscape 2025," ENISA, Heraklion, Greece, Report, Mar. 2026.
- [18] Basel Committee on Banking Supervision, "Principles for the sound management of operational risk," Bank for International Settlements, Basel, Switzerland, Publication no. 316, Mar. 2021.
- [19] M. Eling and J. Wirfs, "Cyber risk management in the financial sector," *The Geneva Papers on Risk and Insurance*, vol. 46, no. 2, pp. 221–248, Apr. 2021.

- [20] Information Commissioner's Office, "Guide to the General Data Protection Regulation (GDPR)," ICO, Wilmslow, U.K., v1.1, Mar. 2025.
- [21] C. Biener, M. Eling, and J. H. Wirfs, "The determinants of cyber risk insurance in the banking sector," *The Journal of Risk and Insurance*, vol. 87, no. 3, pp. 711–738, Sep. 2020.
- [22] D. Kim and M. G. Solomon, *Fundamentals of Information Systems Security*, 4th ed. Burlington, MA, USA: Jones & Bartlett Learning, 2021.
- [23] J. R. C. Nurse, "Cyber risk and threats to financial services," in *Cybersecurity for Financial Institutions*, T. D. Smith, Ed. London, U.K.: Palgrave Macmillan, 2020, pp. 45–76.