

Data Security, Governance and Compliance Report for FinSure Bank

ACCA7028 Data Security, Governance and Compliance

Student Name	Md Shiblu Hossain
Student ID	2517990

Table of Contents

Contents

Data Security, Governance and Compliance Report for FinSure Bank	1
Abstract	4
1. Introduction	5
2. Assumptions	5
3. Security Frameworks and Models	6
4. Proposed Layered Governance Model for FSB	8
Layer 1 Governance and Accountability (COBIT + NIST CSF Govern) :	8
Layer 2 ISMS Foundation (ISO 27001:2022) :	8
Layer 3 Access and Technical Controls (Zero Trust + CIS Controls v8) :	8
Layer 4 Regulatory and Service Compliance (GDPR + PCI DSS + ITIL 4) :	8
Reasoning	9
5. Security Policies, Protection Mechanisms, and Contingency Planning	10
6. Why Regulations and Standards Must Be Continuously Updated	11
7. Recommendations	13
8. Conclusion	14
References	15

Abstract

FinSure Bank (FSB) is a multi-jurisdictional, cloud-based financial services company. Its rapid growth has led to key security vulnerabilities, such as unregulated BYOD access, poor governance and a lack of risk strategy. This report critically reviews the leading security frameworks - ISO/IEC 27001:2022, NIST CSF 2.0, COBIT 2019, ITIL 4, Zero Trust Architecture, CIS Controls v8, GDPR and PCI DSS v4.0.1 - and concludes that none of these frameworks is adequate for FSB's multiple threat scenarios. It advocates a multi-faceted governance approach integrating technical controls with governance and regulatory requirements. The report also suggests an ongoing regulatory upgrade is essential in the face of threats like AI-enhanced fraud and global data risk.

1. Introduction

Von Solms and Van Niekerk [1] assert that cyber security is no longer just a technical issue - it needs governance, culture and strategy, as well as compliance. This is the case for FSB. As more than 90% of its infrastructure is outsourced, it has an uncontrolled bring your own device (BYOD) environment and customers are transacting via mobile apps, the bank is exposed to threats of a technical, legal, operational and human nature. This report critically assesses various frameworks, proposes a governance design for FSB and explains, with reference to the academic and regulatory literature, why regulatory evolution is not necessarily onerous.

2. Assumptions

1. FSB handles personal data in GDPR jurisdictions, and manages payment card data, and is subject to GDPR and PCI DSS.
2. FSB uses third-party managed cloud infrastructure, but is ultimately responsible for the data.
3. BYODs are in use but there is no mobile device management policy.
4. There is currently no security risk register, security operations centre or security awareness training for staff.
5. Cybersecurity is not formally recognised as a governance position.

It is also assumed that FSB's business continuity and incident response is untested, and has no formal recovery time objectives nor crisis communication plans.

3. Security Frameworks and Models

ISO/IEC 27001:2022 offers a risk-based Information Security Management System (ISMS) that involves identifying assets and threats, implementing Annex A controls and continuous improvement [2]. The 2022 version includes controls for cloud services and threat intelligence, which will be pertinent for FSB. But Disterer [3] notes that ISO 27001 is often seen as a compliance rather than risk management standard, leading to a "paper" ISMS that isn't reflective of real-world operations, something FSB needs to take care to avoid.

NIST CSF 2.0 expands the five core functions (Identify, Protect, Detect, Respond and Recover) to include a sixth, Govern [4]. This is important for FSB as it requires cybersecurity to be board-owned. Its flexible, outcome-based, and voluntary nature lacks technical detail, so FSB needs to integrate it with CIS Controls for implementation.

Zero Trust Architecture (NIST SP 800-207) is based on the idea of "never trust, always verify and least privilege" [5]. Mandal, Khan and Jain [6] have shown ZTA greatly limits malicious movement within cloud-hosted IT systems, which translates to FSB's BYOD and third-party access concerns. The research also highlights that ZTA is costly in terms of identity and access management and training, hence the need for a staggered introduction.

COBIT 2019 links IT risk with business goals and promotes a senior management focus on security [7]. Cheng [8] states that cybersecurity issues in digital financial institutions stem from board-level governance issues - an insight COBIT speaks to. ITIL 4 supports COBIT by offering incident, change and supplier management processes [9], while CIS Controls v8 offers 18 prioritised and scalable technical security controls [10].

GDPR requires legitimate processing, privacy by design and 72-hour data breach notification [11]. PCI DSS v4.0.1 mandates safeguards to protect cardholder data via network segmentation, encryption and testing [12].

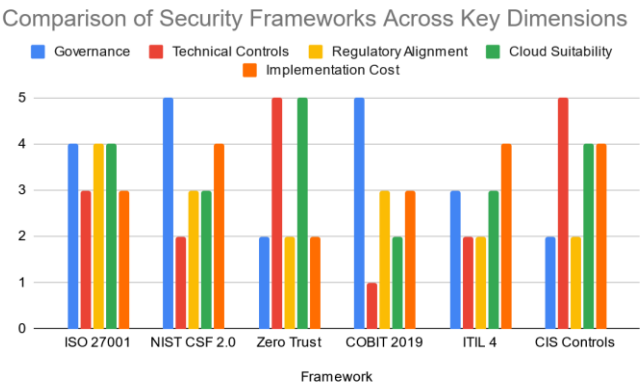


Figure 1: Comparison chart of major security frameworks relevant to FinSure Bank. (Designed by Author)

The scores are a judgement by the author based on framework documentation and literature [2-10]; 1-5 with 1 being the highest in this category

Table 1 : Security Framework Application to FSB

<i>Framework</i>	<i>Purpose</i>	<i>Contribution to FSB</i>	<i>Key Limitation</i>
ISO/IEC 27001:2022	ISMS	Risk assessment, controls, audit trail	Risk of compliance-only implementation [3]
NIST CSF 2.0	Security lifecycle	Board governance mandate; maturity tracking	No prescriptive technical controls [4]
Zero Trust	Secure access	Addresses BYOD, contractor, cloud access	High IAM cost and complexity [5], [6]
COBIT 2019	IT governance	Links security to business goals	Insufficient technical depth for cloud or mobile [7]
ITIL 4	Service management	Incident, change, supplier management	Not a security framework; must be combined with others [9]
CIS Controls v8	Technical controls	Practical prioritised safeguards	Does not address governance or regulatory compliance [10]
GDPR	Data protection	Customer privacy and breach obligations	Not clear on jurisdiction; not enforced consistently across jurisdictions [11]
PCI DSS v4.0.1	Payment security	Cardholder data protection	Reducing the scope of an organisation through segmentation can give an illusion of compliance [12]

The key point to take from this is that each governance framework is addressing a different aspect of the problem in FSB. They should not be combined - they must be to address the governance, technical, regulatory, and cloud security challenges in an organisation.

4. Proposed Layered Governance Model for FSB

FSB should implement a four-layer governance architecture :

Layer 1 Governance and Accountability (COBIT + NIST CSF Govern) :

An information security steering committee, including the IT, risk, compliance, legal and senior management should be formed. It's responsible for the risk register, policies and to the board. Cheng [8] shows that digital banks lacking board ownership of security experience greater costs and fines from breaches.

Layer 2 ISMS Foundation (ISO 27001:2022) :

FSB needs to formally identify and classify information assets - customer data, payment services, cloud data centres, mobile apps - threats and vulnerabilities, then select suitable Annex A controls. FSB should conduct annual internal audits and management reviews to drive continuous improvement. Layer 2 also demands FSB to produce a Statement of Applicability (SoA), listing which of ISO 27001 Annex A controls are selected, excluded and justified. This is critical for governance and audit, and to ensure that controls are selected based on risks identified

Layer 3 Access and Technical Controls (Zero Trust + CIS Controls v8) :

Multifactor authentication, device health checks and role-based access should be enforced for all internal access. Bring your own devices should be mobile device managed. Asset management, secure configurations, vulnerability management and audit and logs should be managed by CIS Controls Implementation Group 2.

Layer 4 Regulatory and Service Compliance (GDPR + PCI DSS + ITIL 4) :

GDPR compliance is integrated into data processing activities via privacy impact assessments, data minimisation and incident response plans. PCI DSS measures involve segmentation of networks hosting payment systems, encryption of credit card data and quarterly vulnerability assessments. ITIL 4 service management covers service level agreements with the cloud provider, incident escalation and change management.

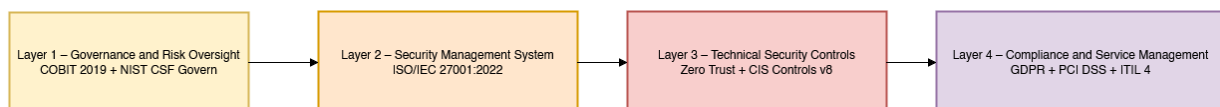


Figure 2: Proposed layered security governance model for FinSure Bank. (Designed by Author)

Table 2: Risk Register for FinSure Bank

<i>Risk</i>	<i>Likelihood</i>	<i>Impact</i>	<i>Control</i>
BYOD device compromise	High	High	ZTA, MFA, MDM, endpoint detection
Cloud provider outage or breach	Low	High	SLA audit rights, encryption, recovery testing
GDPR data breach	Medium	High	Privacy by design, DPIAs, 72-hour reporting
Insider threat	Low	High	Least privilege, PAM, behaviour monitoring
Payment card fraud	High	High	PCI DSS controls, network segmentation
Third-party supply chain attack	Medium	High	Supplier security assessments, contract controls

Reasoning

BYOD and payment card fraud are High likelihood because they are present, ongoing threats for digital banks. Cloud provider outage and insider threat are Low likelihood because reputable cloud providers have low likelihood of outages (99.999% uptime) and insider attacks - while severe - are still rare. GDPR breach and supply chain attacks are Medium - they could but don't always happen.

5. Security Policies, Protection Mechanisms, and Contingency Planning

FSB demands a range of policies for access control, bring your own device (BYOD), data classification, cloud computing, incident response and supply chain. Policies should have an owner, enforcement penalties and are reviewed annually. In the absence of policies, technical controls lack organisational backing to enforce effective security - something auditors and regulators will look for during assessments.

Technology controls require encryption of data in transit and at rest, access control, endpoint detection and response, penetration testing and back-up validation. Vendor agreements with cloud providers must include service uptime guarantees, geographic data location guarantees, incident reporting time frames and audit privileges. FSB cannot externalise its legal obligations for customer data protection just by outsourcing to a third party - as affirmed by GDPR Article 28 (processor liability) and PCI DSS which requires oversight of third-party service providers [11], [12].

The ENISA Threat Landscape 2024 [13] lists ransomware, social engineering and supply chain attack as the most significant threats to financial service organisations - all of which can be dealt with by the measures outlined above. For resilience, FSB needs to establish business continuity and disaster recovery processes, roles, communication plans and recovery time objectives. Incident management should adhere to the NIST CSF Respond and Recover functions: preparation, identification, containment, eradication, recovery and lessons learned [4]. Periodic testing with exercises such as phishing, ransomware and cloud outage simulation are required to practice these procedures prior to an incident.

6. Why Regulations and Standards Must Be Continuously Updated

The need for constantly evolving security standards and regulations is a strong proposition and not just a bureaucratic one. Cybersecurity risks outpace governance and if standards are not updated, they become irrelevant and organizations fall into a complacency trap, assuming that their existing controls are adequate. This is no abstract question; the 2013 edition of ISO 27001 did not include specific controls for cloud computing but, in the subsequent years, cloud computing grew rapidly in financial services leaving a governance gap for those organizations still using the older standard [2], [3]. Regulators and standards bodies must be proactive in closing such gaps, especially in industries such as banking that have links between organizations that affect the stability of the financial system.

There are three structural reasons why regulatory agility is needed. First, the changing nature of technology: cloud computing, mobile banking, artificial intelligence, Internet of Things, and so on, make potential cyber threats that previous standards did not contemplate. ISO 27001:2022 specifically includes cloud and threat intelligence controls that were not present in the 2013 edition in response to cloud computing that now typifies organizations like FSB [2]. Second, threat evolution: threat actors innovate. The ENISA Threat Landscape 2024 [13] shows that ransomware gangs now specifically target cloud backups to halt recovery efforts - something that requires new incident response and backup practices to mitigate. Third, regulatory harmonization: as financial firms such as FSB work across countries, national regulatory differences create loopholes. Kun [14] shows how EU financial regulation has failed to keep up with the speed of adoption of cloud services, introducing legal uncertainties about data location, audit rights and third-party liability that are addressed in the new regulations like DORA (Digital Operational Resilience Act).

The argument is that regulatory changes create costs, confusion and put smaller players at a disadvantage. It is a valid point. But the risk of doing nothing in a changing threat landscape poses a greater threat. The risk and cost of a serious breach, with associated fines, brand damage and loss of customers, is a multiple of the cost of compliance. In the case of FSB, failure to adopt new standards means that its mobile banking policies and procedures, cloud security and BYOD policies will be out of line with the evolving threat environment. In the case of FSB, failure to adopt new standards means that its mobile banking policies and procedures, cloud security and BYOD policies will be out of line with the evolving threat environment. DORA's ICT risk management and third-party governance will be mandated due to its multi-jurisdictional presence across EU countries, so proactively aligning is a strategic best practice, rather than a future regulatory burden.

Fourth, increasingly important for FSB is the integration of artificial intelligence with malicious cyber. Cyber criminals are using AI-powered deepfake audio and video to impersonate bank CEOs in social engineering scams, and large language model chatbots to generate highly sophisticated phishing messages. According to the ENISA Threat Landscape 2024 [13], AI-based attacks are a new priority threat for the financial sector. Standards written without regard to these AI-powered attacks quickly become obsolete, further emphasizing the need for ever-evolving standards. For FSB, its mobile first and cloud first business model means that its interfaces to customers and employees are the prime targets of

these types of AI-based social engineering attacks, and so standards alignment is an operational rather than optional practice.

7. Recommendations

FSB needs to roll out security improvements in three stages. Within 30 days: establish the security governance committee, implement multi-factor authentication (MFA) for all employees and third parties, approve interim BYOD and access control policies, and perform an emergency asset inventory to find what data FSB has and where it is located. Within 90 days: establish the approved risk register, review all cloud vendor contracts for security details, deploy mobile device management, develop an incident response plan and commence staff security awareness training. Within 180 days: complete ISO 27001 gap assessment and map controls to the NIST CSF, review for GDPR and PCI DSS compliance, and conduct the first full disaster recovery test. This incremental approach will prioritize the greatest risks and not overwhelm FSB's current small security team.

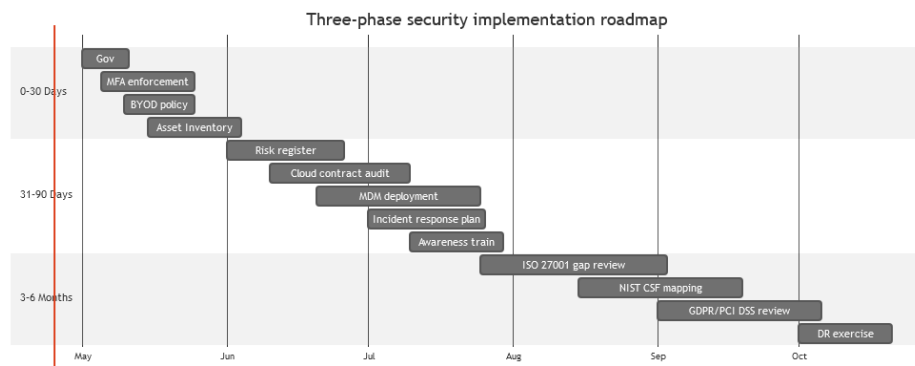


Figure 3: Roadmap visualizing the three-phase implementation plan. (Designed by Author)

8. Conclusion

The issue with FSB is not the absence of information security tools and technologies, but of integrated governance, risk and compliance. A multi-layered approach that combines ISO 27001, NIST CSF 2.0, Zero Trust, COBIT, ITIL 4, CIS Controls, GDPR, and PCI DSS offers an all-encompassing and easily actionable strategy to address FSB's risks. Crucially, security is considered a governance instead of an IT issue. Regulatory updates are not something to be avoided but the way governance frameworks evolve to address an adversarial threat environment that is not.

FSB should also understand security is a journey. As Disterer [3] observes, companies that consider framework implementation as a project rather than a programme are unlikely to see security improvements. The layered approach proposed here is therefore not a "set-and-forget" approach but an architecture that FSB can mature as its capacity, people and regulatory requirements grow and change. The layered approach proposed here is therefore not a "set-and-forget" approach but an architecture that FSB can mature as its capacity, people and regulatory requirements grow and change. In the end, the effectiveness of FSB's security will be a product of its culture and human capital, as well as its technical and governance controls. Von Solms and Van Niekerk [1] stress that cyber security requires a cultural transformation where all employees and not just the IT department are involved in information security. Training in security awareness, phishing simulations and the establishment of avenues to report suspicious events are therefore not "nice to haves" in the proposed governance framework, but rather prerequisites for its effective operation. A sophisticated technology and governance model which is subverted by inexperienced or careless staff will not provide the security FSB needs.

References

- [1] R. Von Solms and J. Van Niekerk, "From information security to cyber security," *Computers & Security*, vol. 38, pp. 97–102, 2013. [Online]. Available: <https://doi.org/10.1016/j.cose.2013.04.004>
- [2] International Organization for Standardization, "ISO/IEC 27001:2022 Information security management systems," ISO, 2022. [Online]. Available: <https://www.iso.org/standard/27001>
- [3] G. Disterer, "ISO/IEC 27000, 27001 and 27002 for information security management," *Journal of Information Security*, vol. 4, no. 2, pp. 92–100, 2013. [Online]. Available: <https://www.scirp.org/journal/paperinformation?paperid=30059>
- [4] 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>
- [5] 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>
- [6] S. Mandal, D. A. Khan, and S. Jain, "Cloud-based zero trust access control policy: An approach to support work-from-home driven by COVID-19 pandemic," *New Generation Computing*, vol. 39, pp. 599–622, 2021. [Online]. Available: <https://doi.org/10.1007/s00354-021-00130-6>
- [7] ISACA, "COBIT 2019 Framework: Introduction and Methodology," ISACA, 2019. [Online]. Available: <https://www.isaca.org/resources/cobit>
- [8] S. Cheng, "Cybersecurity governance and digital finance: Evidence from sovereign states," *Finance Research Letters*, vol. 65, 2024. [Online]. Available: <https://doi.org/10.1016/j.frl.2024.105533>
- [9] AXELOS, *ITIL Foundation: ITIL 4 Edition*. London, U.K.: The Stationery Office, 2019.
- [10] Center for Internet Security, "CIS Critical Security Controls Version 8," CIS, 2021. [Online]. Available: <https://www.cisecurity.org/controls/v8>
- [11] European Union, "Regulation (EU) 2016/679: General Data Protection Regulation," *Official Journal of the European Union*, 2016. [Online] Available: <https://gdpr-info.eu/>
- [12] PCI Security Standards Council, "PCI DSS v4.0.1," PCI SSC, Jun. 2024. [Online]. Available: https://www.pcisecuritystandards.org/document_library/
- [13] European Union Agency for Cybersecurity, *ENISA Threat Landscape 2024*, ENISA, 2024. [Online]. Available: <https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024>
- [14] E. Kun, "Challenges in regulating cloud service providers in EU financial regulation," *Computer Law & Security Review*, vol. 52, 2024. Available: <https://www.sciencedirect.com/science/article/abs/pii/S0267364923001413>