

ACCA7028 – DATA SECURITY, GOVERNANCE AND COMPLIANCE

FinSure Bank (FSB): Information Security, Governance and Compliance Framework

[Submitted in partial fulfilment of the requirements for ACCA7028]

Module Code: ACCA7028

Academic Year: 2026–2027

Student Name : Diyaben Pradipbhai Patel

Student ID : 2523935

Abstract

This report examines the information security, governance, and compliance challenges facing FinSure Bank (FSB), a cloud-based digital financial services provider. It evaluates ITIL 4, ISO/IEC 27001, NIST CSF 2.0, COBIT 2019, and PCI-DSS v4.0 to design a tailored security architecture addressing FSB's cloud-first and BYOD risks. The report proposes an integrated, eight-domain approach combining governance, Zero Trust principles, and compliance mechanisms. Finally, it critically analyses why continuously updating regulations is essential in a fast-evolving threat landscape, arguing that compliance should drive sustainable growth and customer trust.

1. INTRODUCTION

As global use of the Internet continues to grow, the demand for and reliance on Internet-based information creates an increasing expectation of access. FinSure Bank (FSB) has experienced rapid international expansion and cloud adoption, but this growth has outpaced its security capabilities, creating a critical gap in risk management and governance. This report evaluates key frameworks (ITIL 4, ISO/IEC 27001, NIST CSF 2.0, COBIT 2019, PCI-DSS v4.0) to design an integrated security, governance, and compliance approach tailored to FSB's infrastructure. It also critically discusses the necessity of evolving regulations. Section 2 outlines assumptions, Section 3 reviews frameworks, Section 4 presents the proposed approach, and Section 5 provides critical analysis.

2. Assumptions

Before presenting the proposed security architecture, it is important to state the assumptions that underpin the design. These assumptions are based on the case scenario and help define the scope of the proposed solution.

Table 1: Assumptions for the Proposed FSB Security Framework

No.	Assumption	Justification
1	FSB operates across UK and EU jurisdictions.	The case states that FSB serves clients across multiple countries, meaning GDPR and financial regulations are likely to apply [8].

2	Over 90% of FSB's infrastructure is hosted externally in cloud environments.	This is directly stated in the case scenario and makes cloud security a priority. As noted by Kumar and Goyal (2019), financial institutions operating in the cloud face distinct data residency, shared-responsibility, and multi-tenancy risks that require tailored governance approaches [20].
3	Employees, contractors, and third-party partners use personal devices for work access.	The case specifically identifies pressure to support BYOD access.
4	FSB processes sensitive personal, financial, and payment-related data.	The bank offers online banking, savings, loans, and investment services.
5	FSB currently lacks a formal security governance framework.	The case states that security policies, governance frameworks, and compliance controls are fragmented.
6	FSB does not yet have a mature SOC or formal continuous monitoring capability.	The case describes the organisation's approach as fragmented, with no unified governance model.
7	Third-party vendors are critical to FSB's operations.	Since most infrastructure is externally hosted, vendor risk management is essential.
8	Customer-facing systems such as mobile banking are mission-critical.	Customers increasingly use mobile banking apps, making availability and trust central to business continuity.

9	FSB requires formal incident response and contingency planning.	The case highlights cyberattacks, fraud, insider threats, and regulatory risk.
10	FSB must align security with business growth.	The organisation is rapidly expanding and needs controls that support rather than block growth.

3. Research on Security Frameworks and Models

Before building a custom solution for FSB, it is important to understand the specific strengths of existing global frameworks. A common mistake in security design is to select one familiar standard, such as ISO/IEC 27001, and assume that it can solve every security, governance, and compliance problem. In reality, different frameworks serve different purposes.

For this reason, FSB should not simply “pick one” framework. Instead, it should use a combined approach, drawing the strongest elements from different models. This section evaluates ITIL 4, ISO/IEC 27001, NIST CSF 2.0, COBIT 2019, and PCI-DSS v4.0, and explains how each one can support FSB’s security needs.

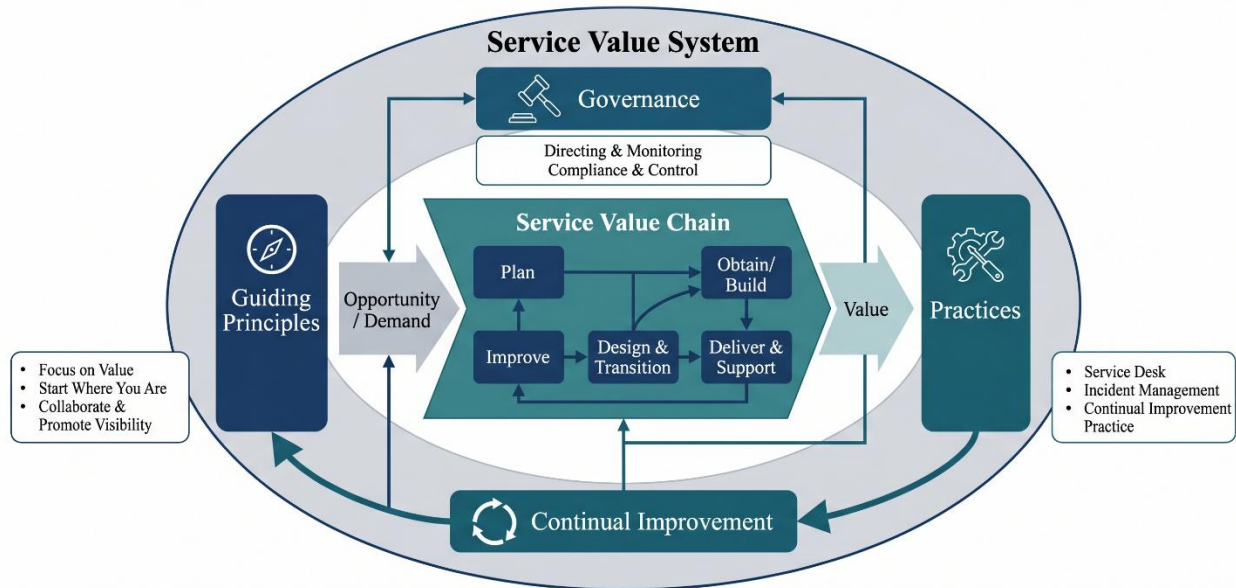
3.1 Information Technology Infrastructure Library (ITIL)

ITIL 4 is a widely adopted framework for IT Service Management (ITSM) that focuses on value creation and aligning IT services with business needs [1]. Unlike prescriptive checklists, ITIL provides a structured way to manage IT services. This is highly useful for FSB because the bank’s security challenges go beyond technical controls. They actively involve service reliability, supplier management, incident handling, and change control for customer-facing digital services.

As shown in Figure 1, the ITIL 4 Service Value System integrates governance, guiding principles, service value chain activities, practices, and continual improvement to support effective service delivery [1].

Figure 1: ITIL 4 Service Value System (SVS) [1]

ITIL 4 Service Value System (SVS)



For FSB, the real strength of ITIL is the operational structure it provides. Incident Management gives the bank a clear process for responding to service disruptions and cyber incidents instead of reacting in an unstructured way. Supplier Management is also highly relevant because more than 90% of FSB's infrastructure is hosted externally. This means that the security and reliability of third-party cloud providers directly affect FSB's own operational resilience.

Service Level Management is another important ITIL practice for FSB. It allows the bank to turn general security expectations into measurable commitments, such as uptime targets, incident notification timelines, and patching deadlines. This is especially important for a digital bank where service downtime can quickly affect customer trust and regulatory confidence.

(See Appendix A for Table 2)

For FSB, ITIL is especially useful because it helps security become part of daily operations. Security should not be treated as a separate activity that happens only during audits or after incidents. Instead, it should be integrated into service design, service transition, service operation, and continuous improvement.

3.2 ISO/IEC 27000 Series

While ITIL provides operational discipline, ISO/IEC 27001 provides the main foundation for information security governance. ISO/IEC 27001 is widely recognised as the international standard for establishing, implementing, maintaining, and continually improving an Information Security Management System (ISMS) [2].

For a financial institution such as FSB, ISO/IEC 27001 is highly valuable because it provides a structured and auditable way to manage information security risks. Certification against ISO/IEC 27001 can also help FSB demonstrate security maturity to regulators, partners, investors, and customers.

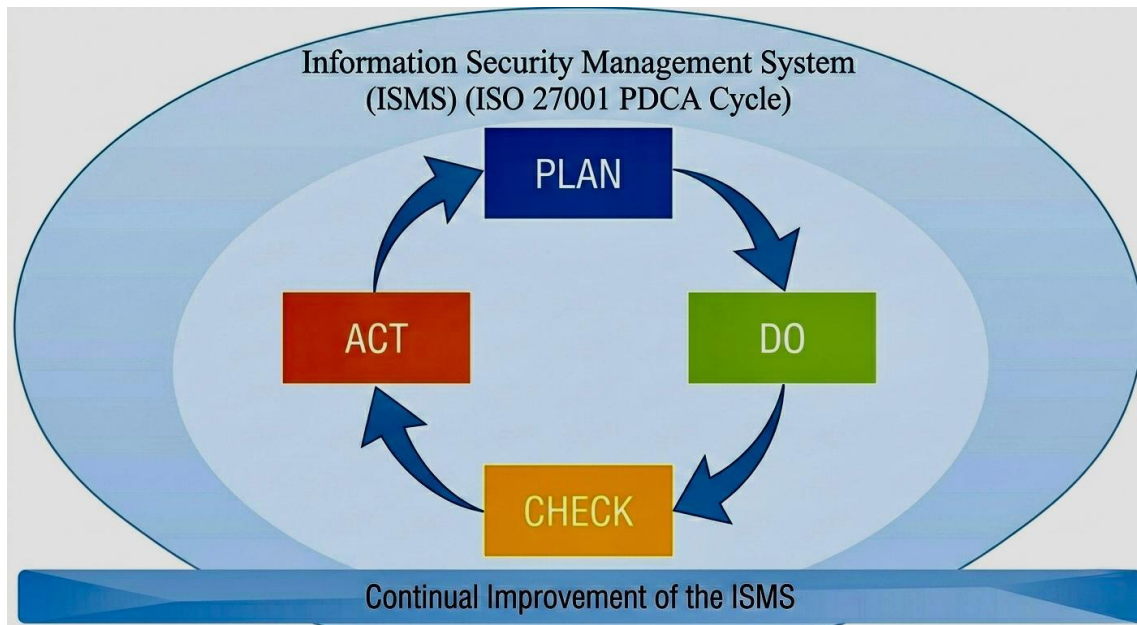
The 2022 version of ISO/IEC 27001 updated and streamlined its control structure. The previous 114 controls were reduced to 93 controls, grouped into four themes: organisational, people, physical, and technological controls [2]. This update reflects the modern threat environment more closely, including cloud security, threat intelligence, data masking, and secure configuration.

Beyond ISO/IEC 27001 itself, other standards in the ISO/IEC 27000 family are also relevant to FSB:

ISO Standard	Relevance to FSB
ISO/IEC 27001	Provides the core ISMS structure and certification pathway.
ISO/IEC 27005	Supports structured information security risk management [3].
ISO/IEC 27017	Provides guidance for cloud security controls.
ISO/IEC 27018	Supports protection of personally identifiable information in cloud environments.
ISO/IEC 27701	Extends ISO 27001 towards privacy information management and GDPR alignment.
ISO 22301	Supports business continuity and resilience planning [4].

As illustrated in Figure 2, ISO/IEC 27001 is based on the Plan-Do-Check-Act cycle, which supports continuous improvement in information security management [2].

Figure 2: ISO/IEC 27001 Plan-Do-Check-Act (PDCA) Cycle [2]



(See Appendix A for Table 3)

For FSB, the ISO/IEC 27001 model is particularly important because security cannot remain static. The bank's cloud environment, mobile banking services, third-party dependencies, and BYOD risks will continue to change. The PDCA cycle ensures that controls are reviewed and improved over time rather than implemented once and forgotten.

3.3 NIST Cybersecurity Framework 2.0

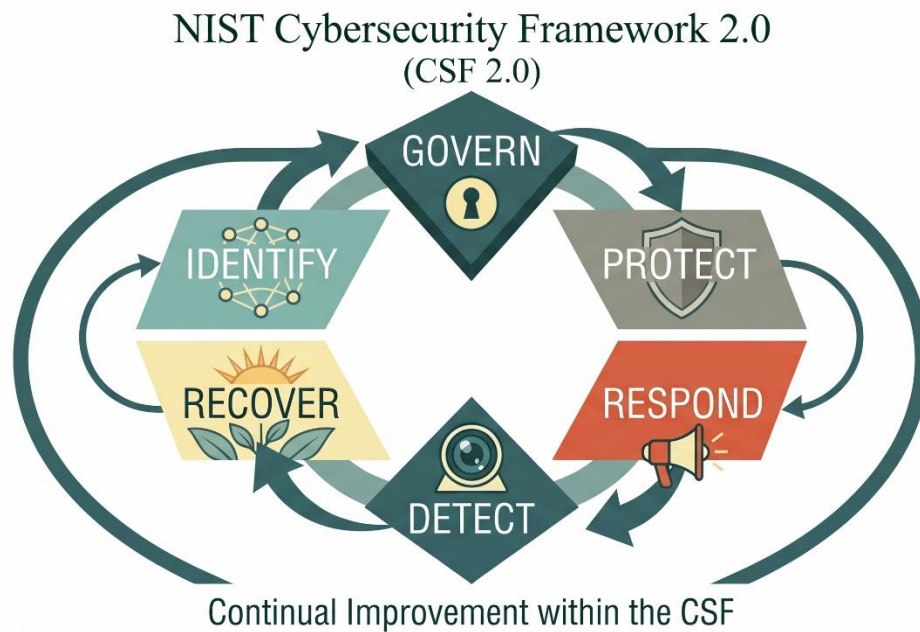
The NIST Cybersecurity Framework was originally developed for critical infrastructure in the United States, but it is now widely used internationally because of its practical and flexible structure. Rather than acting as a strict checklist, it provides a clear way to organise cybersecurity capabilities and communicate risk [5].

NIST CSF 2.0 is especially relevant to FSB because the 2024 update added a sixth core function: Govern. Earlier versions focused on Identify, Protect, Detect, Respond, and Recover. The addition

of Government is important because it makes clear that cybersecurity is not only a technical issue. It is also a leadership, accountability, and strategic risk issue [5].

As shown in Figure 3, the NIST CSF 2.0 consists of six core functions: Govern, Identify, Protect, Detect, Respond, and Recover [5].

Figure 3: NIST Cybersecurity Framework 2.0 Core Functions [5]



For FSB, NIST CSF 2.0 is also a useful communication tool. It allows technical security issues to be explained clearly to senior management and the board. This matters because FSB currently lacks a unified governance model and formal risk management strategy. NIST helps translate complex security concerns into a structure that leadership can understand and act upon.

Table 4: NIST CSF 2.0 Functions Applied to FSB

Function	Primary Objective	FSB Action Plan
Govern	Define strategy, oversight, and accountability.	Appoint CISO, create Board Risk Committee, define risk appetite, and approve security strategy.

Identify	Understand assets, risks, suppliers, and data flows.	Build cloud asset inventory, map customer data flows, and maintain third-party risk register.
Protect	Reduce likelihood and impact of cyber incidents.	Implement Zero Trust, MFA, MDM, encryption, RBAC, and secure configuration.
Detect	Identify cybersecurity events quickly.	Deploy SIEM, SOC monitoring, UEBA, endpoint detection, and cloud monitoring.
Respond	Act effectively when incidents occur.	Develop incident response plan, escalation process, legal notification process, and communication templates.
Recover	Restore services and improve resilience.	Define RTO/RPO targets, test backups, conduct post-incident reviews, and improve recovery plans.

3.4 COBIT 2019

COBIT 2019, published by ISACA, focuses on the governance and management of enterprise IT. While ISO/IEC 27001 is concerned with information security management and NIST CSF helps organise cybersecurity functions, COBIT is particularly strong in governance, accountability, auditability, and control ownership [6].

For FSB, COBIT is valuable because the organisation operates in a regulated financial environment. Regulators do not only expect banks to have security controls. They also expect clear accountability, documented decision-making, evidence of oversight, and separation of duties. COBIT helps address these needs by linking business objectives to IT governance objectives.

COBIT 2019 is based on governance and management objectives. It helps organisations ensure that technology supports enterprise goals, creates value, manages risk, and uses resources responsibly [6]. This is important for FSB because the bank's security risks are directly linked to its business strategy. Its expansion, cloud dependency, mobile services, and BYOD adoption all create risks that must be governed at board level.

(See Appendix A for Table 5)

For FSB, COBIT helps bridge the gap between technical controls and leadership accountability. This is important because security cannot remain only within the IT department. A digital bank must treat cybersecurity as a business risk, not just a technical problem.

3.5 Payment Card Industry Data Security Standard (PCI-DSS)

PCI-DSS is a mandatory security standard for organisations that store, process, or transmit payment card data. Since FSB provides banking and financial services, it is highly likely that the organisation processes cardholder data or interacts with payment systems. Therefore, PCI-DSS compliance is not optional [7].

PCI-DSS v4.0 includes 12 core requirements covering areas such as secure networks, access control, encryption, vulnerability management, monitoring, and security testing [7]. These requirements are especially relevant to FSB because financial data is one of its most sensitive assets.

One important feature of PCI-DSS v4.0 is the customised implementation approach. This allows organisations to meet security objectives using modern technologies, including cloud-native controls, as long as the intended security outcome is achieved. This is useful for FSB because its infrastructure is mostly cloud-hosted rather than traditional on-premise infrastructure.

(See Appendix A for Table 6)

For FSB, PCI-DSS is particularly important because failure to comply can result in fines, reputational damage, increased transaction fees, or even loss of card processing rights. This makes PCI-DSS both a compliance requirement and a business continuity concern.

3.6 Comparative Framework Summary

The frameworks discussed above do not compete with each other. Instead, they address different aspects of FSB's security and governance needs. ITIL supports service management, ISO/IEC

27001 provides an ISMS foundation, NIST CSF supports risk and cybersecurity communication, COBIT strengthens governance and accountability, and PCI-DSS addresses payment card security.

Figure 4: Integrated Model of Cybersecurity Frameworks for Governance, Risk, Operations, and Compliance

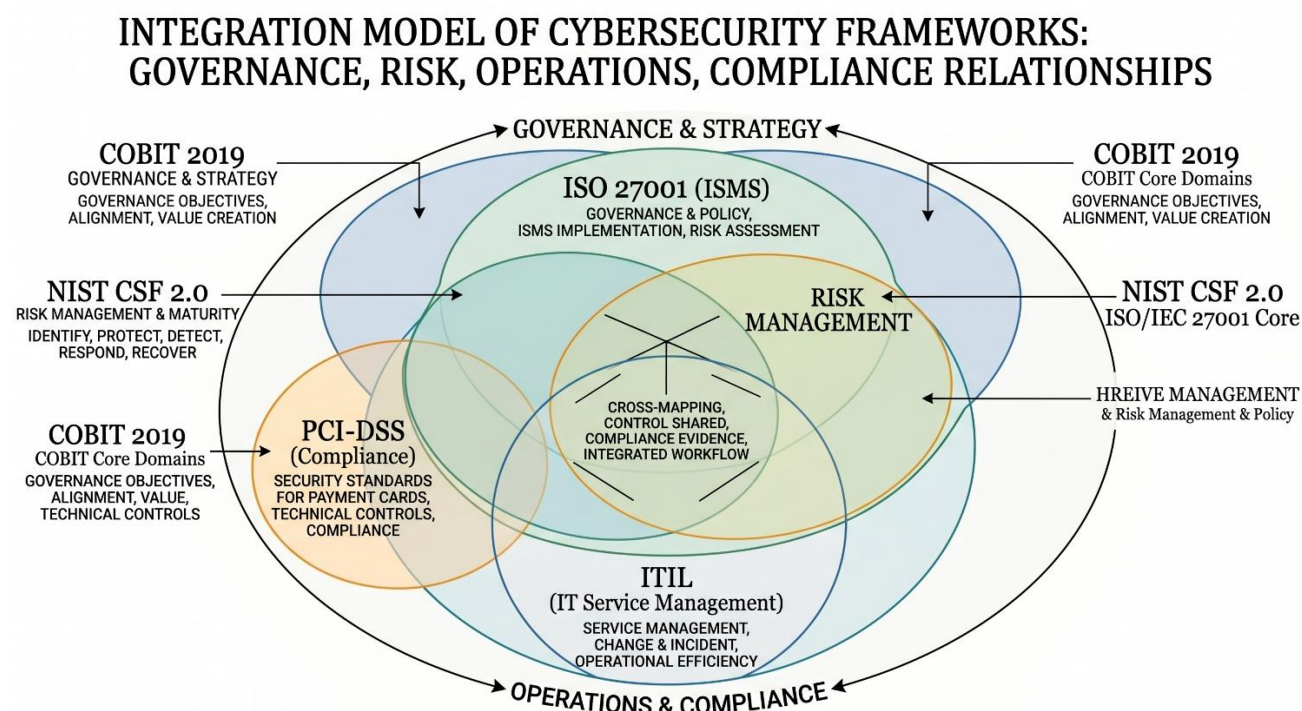


Figure 4 illustrates how different cybersecurity frameworks integrate to support governance, risk management, operational efficiency, and regulatory compliance within FinSure Bank. While ISO/IEC 27001 provides the foundation for information security management, NIST CSF 2.0 supports risk identification and response. ITIL contributes to operational service management, COBIT strengthens governance and strategic alignment, and PCI-DSS ensures compliance with financial data protection requirements.

A multi-framework approach is the most suitable option for FSB. No single framework covers all of the bank's needs. ISO/IEC 27001 provides the security management structure, NIST CSF 2.0 provides the cybersecurity risk language, ITIL supports operational service management, COBIT strengthens governance, and PCI-DSS ensures payment security. This combined approach allows FSB to create a security programme that is not only compliant on paper but practical and resilient in daily operation.

4. Proposed Security Approach for FinSure Bank

Having analysed the strengths and limitations of the key security frameworks, the next step is to apply these concepts in designing a tailored solution for FSB. The strategy outlined below is not a collection of separate recommendations. Instead, it is a layered security architecture where each domain supports the others.

FSB cannot have strong governance without clear policies. Policies cannot work without risk management. Risk management cannot be effective without technical controls, monitoring, and accountability. For this reason, the proposed solution is structured as an integrated security, governance, and compliance model.

Figure 5: Integrated Layered Security Architecture for FinSure Bank

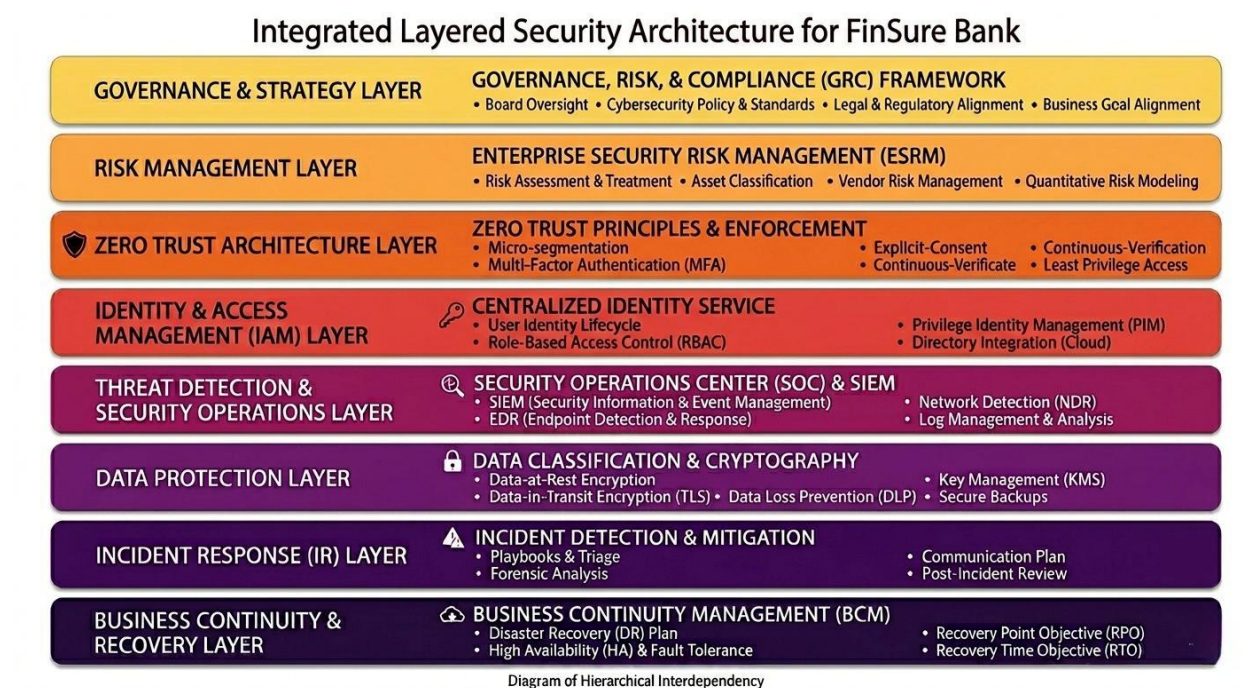


Figure 5 presents a layered cybersecurity architecture designed specifically for FinSure Bank's cloud-based and BYOD-driven environment. The model follows a top-down approach, beginning with governance, risk, and compliance to ensure alignment with business objectives and regulatory requirements.

The architecture incorporates Zero Trust principles and Identity and Access Management to control access and minimise potential attack surfaces. Threat detection is handled through a Security Operations Centre, supported by SIEM and EDR technologies, enabling continuous monitoring and rapid response to security incidents.

Data protection mechanisms, including encryption, data classification, and data loss prevention, are used to safeguard sensitive financial information. The incident response layer ensures structured handling of security breaches, while the business continuity layer supports resilience through disaster recovery planning and defined recovery objectives.

This layered approach ensures that all security controls are interconnected and continuously reinforced, providing a comprehensive and scalable security solution tailored to FSB's operational needs.

4.1 Governance and Strategic Planning for Security

The first priority for FSB is to establish clear ownership of security at the top of the organisation. At present, security decisions appear to be fragmented across different teams, with no unified view of risk and no clear accountability to the board. This creates a serious weakness because security decisions may be made inconsistently or delayed when urgent action is required.

The proposed governance structure draws on COBIT 2019 and the Govern function of NIST CSF 2.0 [5], [6]. It creates a clear hierarchy of accountability without creating unnecessary bureaucracy.

Two executive appointments are essential for this structure to work.

First, FSB should appoint a Chief Information Security Officer. The CISO should report directly to the CEO or board risk committee. Placing the CISO under the CTO can create a conflict of interest because technology delivery pressures may compete with security requirements.

Second, FSB should appoint a Data Protection Officer. Given the volume of personal data processed by FSB, this role is important for GDPR compliance and privacy governance [8], [13]. Strong governance will allow FSB to make security decisions consistently, assign responsibility clearly, and provide evidence of accountability to regulators and auditors.

4.2 Compliance – Laws and Ethics

Compliance is not optional for FSB. As a financial institution handling sensitive customer and financial data, the bank must meet legal, regulatory, and ethical obligations. The cost of compliance may seem high, but the cost of non-compliance can be far greater. Regulatory penalties, customer loss, legal action, and reputational damage can all seriously affect the bank's future.

Compliance and ethics are connected, but they are not the same thing. Regulations set the minimum legal baseline. Ethics should guide FSB to go beyond the minimum where customer trust and responsible data use are at stake.

FSB should adopt the following ethical principles:

Ethical Principle	Application to FSB
Data Minimisation	Collect and retain only the personal data needed for legitimate banking purposes.
Transparency	Clearly explain how customer data is used, stored, shared, and protected.
Privacy by Design	Build privacy controls into systems from the beginning rather than adding them later.
Whistleblower Protection	Allow employees and contractors to report security or data misuse concerns safely.
Fair Use of Data	Ensure analytics, fraud detection, and AI systems do not unfairly disadvantage customers.

In a digital-first banking environment, trust is central to business success. Customers are not simply buying a banking product; they are trusting FSB with their savings, identity information, and financial future. Therefore, compliance and ethics should be treated as strategic priorities.

4.3 Security Policies

Policies connect high-level governance decisions with daily security behaviour. Without clear policies, employees, contractors, and third parties may rely on personal judgment, leading to inconsistent and risky behaviour.

FSB currently lacks a centralised security policy framework. To address this, the bank should implement a Minimum Viable Policy Suite. These policies should be approved by the Information Security Steering Committee and reviewed regularly.

Policies only work when people understand them. Every employee, contractor, and third-party user should acknowledge the relevant policies annually. However, acknowledgement alone is not enough. FSB should also include policy training in onboarding and provide annual refresher training using short, scenario-based modules.

4.4 Risk Management Strategy

Risk management is currently one of FSB's main weaknesses. The proposed approach is based on ISO/IEC 27005, which provides a structured method for identifying, analysing, evaluating, treating, and monitoring information security risks [3]. This also aligns with the Identify function of NIST CSF 2.0 [5].

Risk owners must be named individuals, not vague teams or departments. If nobody owns a risk directly, it is unlikely to be managed properly. Any risk above FSB's agreed tolerance level should require formal approval from the CISO or the Board Risk Committee.

4.5 Security Management Models and Practices

The central technical principle for FSB should be Zero Trust. Traditional security models assume that systems inside the network perimeter can be trusted. This assumption no longer works for FSB because most infrastructure is cloud-hosted and users may connect from personal devices and remote locations.

Zero Trust assumes that no user, device, application, or network should be trusted automatically. Every request must be verified before access is granted [17]. This model is particularly relevant for FSB because traditional perimeter-based security is ineffective in cloud and BYOD environments, a reality increasingly supported by recent academic evaluations of Zero Trust

efficacy in modern banking infrastructures (Almashhadani et al., 2021) [21]. Identity and Access Management is one of the most important parts of Zero Trust. If identity controls fail, attackers can access sensitive banking systems using legitimate-looking accounts.

FSB should also implement a Security Information and Event Management platform to collect logs from cloud platforms, endpoints, applications, and network systems. This should be supported by a Security Operations Centre. Initially, FSB may use a managed SOC provider to gain 24/7 monitoring quickly, with a longer-term plan to build internal capability.

User and Entity Behaviour Analytics should also be used to detect unusual behaviour, such as impossible travel, abnormal data downloads, or access outside normal working patterns. This is especially useful for detecting insider threats and compromised accounts.

4.6 Contingency Planning

A bank that goes offline, even for a few hours, can lose customer trust very quickly. Outages may also lead to regulatory attention, financial loss, and reputational damage. Therefore, contingency planning must be treated as a business continuity discipline, not simply as an IT exercise.

The proposed contingency planning approach aligns with ISO 22301 and FCA operational resilience expectations [4], [12].

(See Appendix A for Table 7)

4.7 Protection Mechanisms

Technical controls turn governance and policy decisions into practical protection. The following protection mechanisms are prioritised based on FSB's highest risks, including cloud compromise, BYOD exposure, fraud, ransomware, insider threats, and data breaches.

4.8 Service Level Agreements

Since over 90% of FSB's infrastructure is hosted externally, supplier security is directly linked to FSB's own security. A weak supplier can create a serious risk even if FSB's internal controls are strong.

Service Level Agreements should not only cover availability. They must also include security, incident reporting, audit rights, data residency, encryption, and exit requirements.

SLAs should then be reviewed annually and whenever FSB's risk profile changes. Suppliers who repeatedly fail to meet security commitments should face service credits, remediation requirements, or contract termination.

5. Critical Analysis – Why Evolving Regulations and Standards Are Essential Good Practice

It is understandable that organisations sometimes view regulatory change as inconvenient. New standards often require gap assessments, updated policies, training, audits, and investment. However, this view misunderstands the purpose of regulation. Regulations and standards exist because the threat environment, technology landscape, and public expectations are constantly changing.

For FSB, changing regulations should not be seen as an administrative burden. They should be seen as an early warning system that helps the bank adapt before risks become unmanageable.

5.1 The Threat Landscape Moves Faster Than Static Rules

Regulations and standards exist because the threat environment, technology landscape, and public expectations are constantly changing. For FSB, changing regulations should act as an early warning system. Cyber threats evolve rapidly through Ransomware-as-a-Service and AI-driven phishing, meaning static rules quickly become outdated. This is why standards like ISO/IEC 27001 must be updated to address cloud security and data masking [2]. Simultaneously, technology adoption often outpaces regulation. FSB now relies on cloud platforms, mobile apps, and AI-supported fraud detection. Regulations like DORA and the EU AI Act [9], [11] are direct responses to these modern ICT and AI risks. Furthermore, regulatory change forces organisations to improve. Companies often treat certification as a finish line, allowing controls to stagnate. Updated standards force FSB to conduct gap analyses and expose hidden weaknesses. Evolving regulations also enforce accountability. Mandatory breach reporting under GDPR [8] prevents organisations from hiding incidents and helps maintain the consumer trust essential for digital banking. Finally, international harmonisation reduces complexity. Using shared frameworks like NIST and ISO makes it easier for FSB to manage compliance across multiple jurisdictions [2], [5], [6].

5.2 Critical Evaluation

Although updated regulations are necessary, a valid critique is the risk of "compliance fatigue." Rapidly scaling organisations can struggle with the administrative burden of continuous audits. For FSB, this balance must be actively managed. The bank must balance the cost of continuous compliance against the need for agile product delivery. However, because FSB handles sensitive cross-border data and relies heavily on third-party cloud vendors, weak or outdated standards would create far greater risk. The key is for FSB to treat compliance as part of business strategy rather than a separate administrative task, mapping regulations directly to business risks and board accountability.

6. Conclusion

FinSure Bank is at a significant point in its growth. Its digital-first strategy and cloud-based operating model create strong business opportunities, but they also introduce serious security, governance, and compliance risks. The current fragmented approach is not suitable for a financial institution handling sensitive customer and financial data across multiple jurisdictions.

This report has shown that no single framework is enough to address FSB's needs. ITIL 4 supports service management and incident handling. ISO/IEC 27001 provides the foundation for an auditable Information Security Management System. NIST CSF 2.0 supports structured cybersecurity risk management and board-level communication. COBIT 2019 strengthens governance, accountability, and auditability. PCI-DSS v4.0 ensures specific protection for payment card data [1], [2], [5], [6], [7].

The proposed eight-domain approach gives FSB a practical and integrated path forward. Governance, compliance, policies, risk management, Zero Trust security, contingency planning, protection mechanisms, and service level agreements all reinforce each other. This is important because security cannot succeed if it is treated as a collection of disconnected technical controls.

The report also highlights why evolving regulations and standards are essential. Cyber threats, technology, customer expectations, and international compliance requirements are constantly

changing. FSB must therefore treat security and compliance as continuous activities rather than one-time projects.

Overall, FSB should adopt a layered, standards-driven, and risk-based security architecture. This will help the bank protect sensitive data, meet regulatory expectations, manage third-party risk, support business continuity, and maintain customer trust. Information security should not be viewed as overhead. For FSB, it is a core part of sustainable growth and long-term success.

Appendix A: Supporting Framework Tables

Table 2: ITIL 4 Service Value System and Relevance to FSB

SVS Component	Security Impact and Application to FSB
Guiding Principles	Ensures that security controls are practical, proportionate, and aligned with business value.
Governance	Supports board-level oversight and aligns IT security with FSB’s risk appetite.
Service Value Chain	Embeds security checkpoints into planning, design, delivery, and support activities.
Practices	Supports Information Security Management, Incident Management, Risk Management, and Supplier Management.
Continual Improvement	Encourages regular audits, incident reviews, policy updates, and vulnerability remediation.

Table 3: ISO/IEC 27001 PDCA Cycle Applied to FSB

PDCA Phase	Core ISO 27001 Activities	FSB-Specific Implementation
Plan	Define scope, conduct risk assessment, select controls.	Develop asset register, define ISMS scope, approve security policies, and document risk appetite.
Do	Implement controls and awareness activities.	Enforce MFA, encrypt data at rest and in transit, implement BYOD controls, and train staff.

Check	Monitor, audit, and review security performance.	Use CISO dashboard, internal audits, SIEM reporting, and compliance reviews.
Act	Correct weaknesses and improve controls.	Maintain corrective action logs, update policies, and improve controls after incidents.

Table 5: COBIT 2019 Relevance to FSB

COBIT Area	Relevance to FSB
Governance Objectives	Supports board oversight, strategic alignment, and risk ownership.
Management Objectives	Helps define operational responsibilities for IT and security teams.
Auditability	Provides evidence for regulators, auditors, and internal assurance reviews.
Control Ownership	Ensures that security actions are assigned to named owners.
Alignment with Business Goals	Ensures security supports customer trust, growth, and resilience.

Table 6: PCI-DSS v4.0 Relevance to FSB

PCI-DSS Requirement Area	FSB Application
Network Security	Use firewalls, segmentation, WAF, and secure cloud network design.
Cardholder Data Protection	Encrypt cardholder data and restrict access to payment systems.

Vulnerability Management	Run regular scans, patch systems, and conduct penetration testing.
Access Control	Enforce MFA, least privilege, RBAC, and privileged access management.
Monitoring and Testing	Maintain logs, SIEM monitoring, and regular security testing.
Security Policy	Maintain formal policies and assign responsibility for cardholder data protection.

Table 7: Contingency Planning Targets for FSB

Contingency Element	FSB Target	Accountable Owner
Recovery Time Objective – Online Banking	Maximum 4 hours	CTO / Cloud Architect
Recovery Point Objective – Customer and Transaction Data	Maximum 1 hour	Database Lead / Cloud Architect
Recovery Time Objective – Internal Systems	Maximum 24 hours	IT Operations Lead
BCP Testing	Full test twice per year; tabletop exercises quarterly	CISO / BCM Lead
Backup Strategy	3-2-1 backup rule with separate cloud region storage	Cloud Architect
Crisis Communication	Pre-approved templates for customers, regulators, and media	Legal / DPO
Crisis Management Team	CEO, CISO, CFO, Legal Counsel, Communications Lead	CEO

References

- [1] AXELOS (2019) *ITIL Foundation: ITIL 4 Edition*. London: TSO. https://www.servicenow.com/uk/products/itsm/what-is-itsm.html?campid=268142&cid=p:itsm:dg:nb:prsp:phr:goog_en_edu:emea:uki&s_kwcid=AL!11692!3!793495506883!p!!g!!it%20infrastructure%20library%20framework&ds_c=GOOG_EMEA_ALL_EN_DEMANDGEN_ITSM_PRSP_NonBrand_PHR_UKI-EDU&cmcid=23343519792&ds_ag=Framework+-+ITIL_PHR&cmpid=195572165728&ds_kids=2477814419674&gclsrc=aw.ds&gad_source=1&gad_campaignid=23343519792&gbraid=0AAAAA-8OK3JoeGmulh6Rx82P9oVK7x52i&gclid=CjwKCAjwctHPBhADEiwAWo3sJn8PUrD9ArBGTEXjuc2XK7cthfGIAAnDVT7UGywdB0xNTTHo0ZhrzXBoCsZ0QAvD_BwE
- [2] International Organization for Standardization (2022) *ISO/IEC 27001:2022 – Information Security, Cybersecurity and Privacy Protection*. Geneva: ISO. <https://www.iso.org/standard/27001>
- [3] International Organization for Standardization (2022) *ISO/IEC 27005:2022 – Guidance on Managing Information Security Risks*. Geneva: ISO. <https://blog.ansi.org/ansi/iec-27005-2022-security-risk-management/#:~:text=ISO/IEC%2027005:2022%20%E2%80%93%20Information%20Security%20Risk%20Management,as%20the%20catalyst%20for%20this%20rapid%20progression.>
- [4] International Organization for Standardization (2019) *ISO 22301:2019 – Security and Resilience: Business Continuity Management Systems*. Geneva: ISO. <https://www.iso.org/standard/75106.html#:~:text=What%20is%20ISO%2022301?,Increases%20trust%20among%20stakeholders>
- [5] National Institute of Standards and Technology (2024) *Cybersecurity Framework 2.0*. Gaithersburg, MD: NIST. <https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf>

- [6] ISACA (2019) *COBIT 2019 Framework: Governance and Management Objectives*. Schaumburg, IL: ISACA. <https://www.isaca.org/resources/news-and-trends/industry-news/2019/using-cobit-2019-performance-management-model-to-assess-governance-and-management-objectives>
- [7] PCI Security Standards Council (2022) *PCI DSS v4.0*. Wakefield, MA: PCI SSC. <https://www.pcisecuritystandards.org/standards/pci-dss/>
- [8] European Parliament and Council (2016) *Regulation (EU) 2016/679: General Data Protection Regulation*. Official Journal of the European Union. <https://eur-lex.europa.eu/eli/reg/2016/679/oj>
- [9] European Parliament and Council (2022) *Regulation (EU) 2022/2554: Digital Operational Resilience Act*. Official Journal of the European Union. <https://eur-lex.europa.eu/eli/reg/2022/2554/oj/eng>
- [10] European Parliament and Council (2022) *Directive (EU) 2022/2555: NIS2 Directive*. Official Journal of the European Union. <https://eur-lex.europa.eu/eli/reg/2022/2554/oj/eng>
- [11] European Parliament and Council (2024) *Regulation (EU) 2024/1689: Artificial Intelligence Act*. Official Journal of the European Union. <https://eur-lex.europa.eu/eli/reg/2022/2554/oj/eng>
- [12] Financial Conduct Authority (2021) *PS21/3: Building Operational Resilience*. London: FCA. <https://www.fca.org.uk/publications/policy-statements/ps21-3-building-operational-resilience>
- [13] UK Information Commissioner's Office (2023) *UK GDPR Guidance and Resources*. Available at: <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/>
- [14] National Cyber Security Centre (2024) *Annual Review 2024*. London: NCSC. <https://www.ncsc.gov.uk/>
- [15] Anderson, R. (2020) *Security Engineering: A Guide to Building Dependable Distributed Systems*. 3rd edn. Hoboken, NJ: Wiley. <https://www.cl.cam.ac.uk/archive/rja14/book.html>
- [16] Whitman, M.E. and Mattord, H.J. (2021) *Principles of Information Security*. 6th edn. Boston, MA: Cengage Learning. <https://dl.acm.org/doi/book/10.5555/3153651>

- [17] Rose, S., Borchert, O., Mitchell, S. and Connelly, S. (2020) *Zero Trust Architecture*. NIST Special Publication 800-207. Gaithersburg, MD: NIST.
<https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf>
- [18] Von Solms, R. and Van Niekerk, J. (2013) 'From information security to cyber security', *Computers & Security*, 38, pp. 97–102.
<https://www.sciencedirect.com/science/article/abs/pii/S0167404813000801?via%3Dihub>
- [19] Siponen, M. and Willison, R. (2009) 'Information security management standards: Problems and solutions', *Information & Management*, 46(5), pp. 267–270.
<https://www.sciencedirect.com/science/article/abs/pii/S0167404813000801?via%3Dihub>
- [20] Kumar, R. and Goyal, R. (2019) 'A systematic literature review of cloud computing security in the financial sector', *Journal of King Saud University – Computer and Information Sciences*, 34(8), pp. 5405–5419.
- [21] Almashhadani, A.O., et al. (2021) 'A critical analysis of Zero Trust Architecture: Concepts, challenges, and solutions', *IEEE Access*, 9, pp. 131803–131820.