

Data Security, Governance and Compliance



Assignment Report

Student Name: Abdullah Al Maruf

Student ID: 2526089

Module Code: ACCA7028

Programme: MSc Cybersecurity and Digital Forensics

Lecturer: Dr. Ayman Al Hajjar

Submission Date: 29th April 2026

Table of content

Abstract	3
1. Introduction	3
2. Recommended Security Frameworks and Models	3
2.1 ISO/IEC 27000 Series and ISO/IEC 27001	3
2.2 ITIL 4 Framework	4
2.3 NIST Cybersecurity Framework 2.0	5
2.4 COBIT Governance Framework	6
3. Key Security Areas for FSB	7
3.1 Compliance: Laws and Ethics	7
3.2 Governance and Strategic Planning for Security	8
3.3 Security Policies	9
3.4 Risk Management	9
3.5 Security Management Models and Practices	10
3.6 Contingency Planning	10
3.7 Protection Mechanisms	11
3.8 Service Level Agreements	11
4. Designed Security Approach and Critical Analysis	11
4.1 Designed Security Approach for FSB	11
4.2 Critical Analysis: Updated Regulations & Standards ..	12
5. Conclusion	13
References	14

Abstract

FinSure Bank (FSB) works in a very digital and cloud-based environment, which makes it hard to keep data safe, follow the rules, and stay compliant. This research looks at important information security frameworks like ISO/IEC 27001, ITIL 4, NIST Cybersecurity Framework 2.0, and COBIT to help the organization fix its broken security system and lack of formal risk management. It also looks at important areas including following the rules, governance structures, security policies, risk management processes, contingency planning, protection measures, and service level agreements. This report suggests a layered and integrated security approach to strengthen the FSB's overall security posture, safeguard sensitive financial data more effectively, and make operations more resilient. The research also looks at how important it is to keep rules and standards up to date as cyber threats and technology develop. In general, the results show that the digital financial sector needs to have an organized, proactive, and constantly evolving security policy in order to keep confidence, make sure compliance, and promote long-term company success.

1. Introduction

FinSure Bank (FSB) is a digital-first financial company that is growing quickly. It depends a lot on cloud-based infrastructure, mobile banking services, and third-party interfaces. This digital revolution makes things run more smoothly and makes customers happier, but it also opens up big security holes, such as data breaches, cyberattacks, insider threats, and not following the rules. The organization is much more open to these dangers because it doesn't have a single governance model, systematic risk management, or formal security measures.

This research looks at important security frameworks and models, such as ISO/IEC 27001, ITIL 4, NIST Cybersecurity Framework 2.0, and COBIT, to help FSB with its problems with security, governance, and compliance. It also looks at important security areas like compliance, regulations, risk management, protection measures, and service level agreements. This investigation led to the creation of a layered and integrated security methodology that will make FSB's overall security stronger. Lastly, the paper critically looks at how important it is to keep rules and standards up to date so that organizations can stay strong and follow the rules in a world where threats are always changing.[1]

2. Recommended Security Frameworks and Models

2.1 ISO/IEC 27000 Series and ISO/IEC 27001

The ISO/IEC 27000 family sets standards for managing information security that are recognized around the world. ISO/IEC 27001 is the most significant standard for FSB since it helps the organization set up, run, keep up, and keep improving an Information Security Management System (ISMS). ISO/IEC 27001 should be used by FSB to set up a formal security management system.

covering:

- Information security policies
- Risk assessment and treatment
- Access control
- Asset management
- Supplier security
- Incident response
- Business continuity
- Compliance monitoring

This is highly suitable for FSB because the bank currently lacks unified governance, formal risk management and structured compliance audits.



1: ISO 27001 ISMS Continuous Improvement Cycle

The PDCA cycle (Plan–Do–Check–Act) is a way to manage and improve processes by making them better all the time. It starts with setting goals and controls, then putting them into action, keeping an eye on performance, and making changes as needed. This cycle helps businesses work more efficiently, lower risks, and keep their security management up to par [2].

Application to FSB

FSB should embrace ISO/IEC 27001 to create a single ISMS that includes BYOD, cloud services, third-party suppliers, and client data. This would make it possible to have a managed and auditable security framework. Regular risk assessments, effective access controls including role-based access and multi-factor authentication, and ongoing monitoring and internal audits will keep sensitive financial data safe and make sure that the company follows GDPR and financial rules. Also, training and awareness programs for employees will lower dangers that come from people and make security more mature and consistent overall [2].

2.2 ITIL 4 Framework

ITIL 4 is a framework for managing IT services that helps businesses do a good job of it. This is very important for FSB because it relies on digital services like mobile banking, cloud infrastructure, client portals, and internal finance systems. It gives organized advice on how to provide secure and dependable services while keeping important corporate data safe (PeopleCert). FSB can handle incidents better, control system changes better, and make sure services continue by using ITIL best practices. In general, ITIL will make operations more efficient, make services more reliable, and make sure that IT services are in line with business goals [3]. FSB should use ITIL for:

- Incident management
- Change management
- Service continuity
- Supplier management
- Service level agreements
- Access request handling
- Problem management

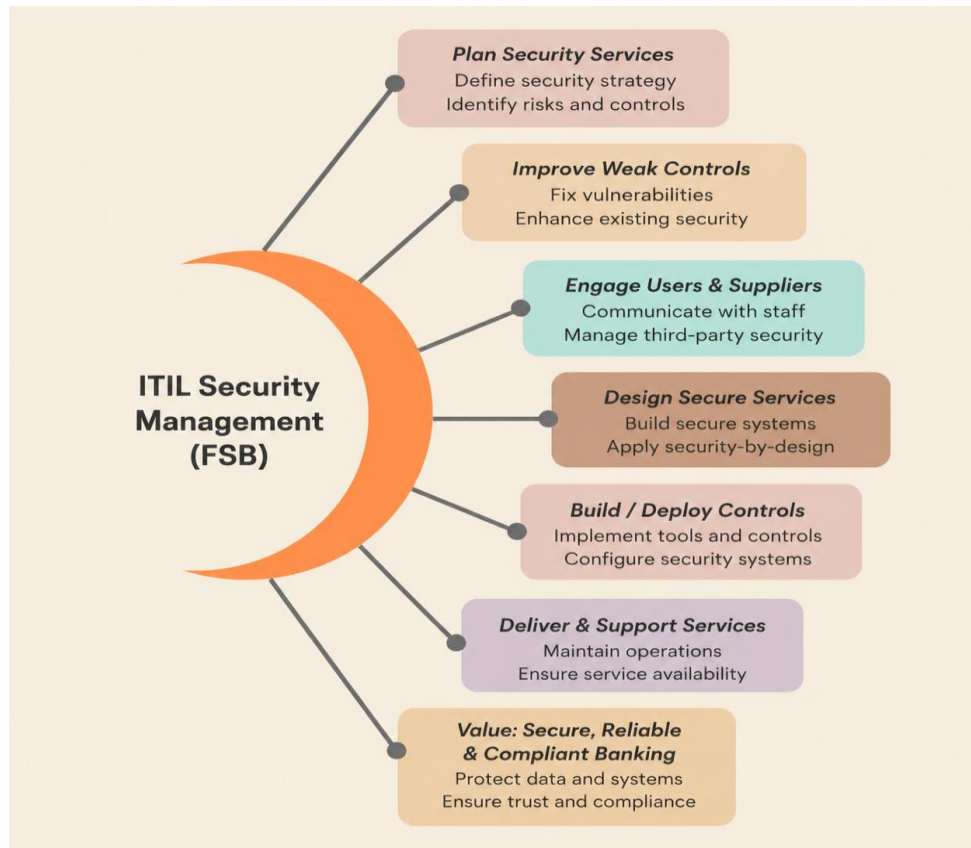


Diagram 2: ITIL Service Value Chain for FSB

The illustration below shows how the ITIL-based security management process works for FinSure Bank. It shows how the different steps are linked to make sure that services are delivered in an organized way. It shows a path from planning and enhancing controls to providing banking services that are safe, dependable, and legal.

Application to FSB

FSB should use ITIL to run its daily security operations and make sure that all of its digital banking platforms provide the same level of service. This includes organized incident handling, escalation, recovery, and continuous improvement. It also helps with defining SLAs, managing changes and problems, increasing responsibility, operating resilience, service reliability, and keeping the banking environment safe and under control [3].

2.3 NIST Cybersecurity Framework 2.0

The NIST Cybersecurity Framework 2.0 has six main functions Govern, Identify, Protect, Detect, Respond, and Recover—that cover the entire security lifecycle and make leadership more accountable and responsible. These functions assist manage cybersecurity risks and make systems more resilient. It is adaptable for cloud-based companies like FSB and helps with risk-based decision-making, constant monitoring, and compliance with industry and regulatory standards [4].

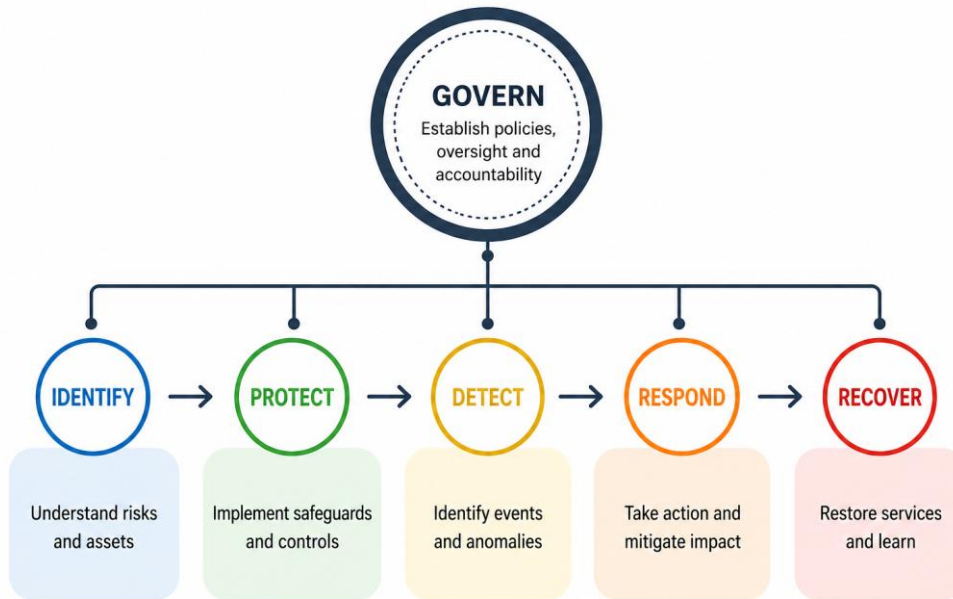


Diagram 3: NIST CSF 2.0 Model

This figure shows the NIST Cybersecurity Framework, with the governance function displaying the flow from Identify to Recover. It shows how companies safeguard their systems and make them more secure by following a set of processes that keep them strong all the time.

Application to FSB

NIST Function	Application to FSB
Govern	Create security leadership, policies and accountability
Identify	Identify cloud assets, customer data, BYOD devices and supplier risks
Protect	Apply MFA, encryption, access control and endpoint protection
Detect	Monitor fraud, unusual logins and insider activity
Respond	Create incident response plans and escalation procedures
Recover	Restore systems using backups and disaster recovery plans

NIST CSF is suitable because FSB needs a simple but complete cybersecurity model that connects governance, technical controls and incident response [5].

2.4 COBIT Governance Framework

COBIT is a framework for IT governance that makes sure that technology is in line with business goals and that IT resources are managed well. COBIT lets FSB's top management see cybersecurity as more than just a technical issue; it also sees it as an important issue for corporate governance. It makes it easy for everyone in the company to be accountable, take risks, and monitor performance. COBIT also helps in following the rules, making internal controls stronger, and making better decisions through ongoing monitoring and auditing [6].

FSB should use COBIT to define:

- Board-level security accountability
- Risk ownership
- Security performance indicators
- Audit responsibilities
- Governance reporting
- Compliance oversight



Diagram 4: COBIT Governance View

Application to FSB

COBIT would help FSB make sure that senior management, IT teams, compliance teams, and business units all know what their security duties are and take responsibility for them. It sets up robust governance structures, makes sure everyone is responsible, and makes sure that cybersecurity is in line with company goals and rules. COBIT also provides ongoing monitoring, performance assessment, and auditing, which makes risk management better and makes sure that IT activities are well controlled [7].

3. Key Security Areas for FSB

3.1 Compliance: Laws and Ethics

Because it handles very sensitive personal and financial information, FSB has to follow data protection and financial rules. The UK GDPR and the Data Protection Act 2018 set severe rules for how you handle and protect personal data in the UK. The UK GDPR has important rules like legality, fairness, openness, purpose limitation, data minimization, accuracy, storage limitation, integrity, privacy, and responsibility. Not following the rules can lead to big fines, legal problems, and damage to your reputation. So, FSB needs to put in place strong data governance, regular audits, and explicit privacy measures to make sure that they are always following the rules and keeping customers' trust[7]. This means for FSB:

- Customer data must be collected lawfully.
- Data should only be used for clear banking purposes.
- Sensitive data must be encrypted and protected.
- Customers should understand how their data is used.
- Data breaches must be reported through proper procedures.
- Access to financial records must be logged and audited.

Ethically, FSB must protect customers from fraud, identity theft and misuse of personal information.

3.2 Governance and Strategic Planning for Security

FSB requires a clear way to run things. Different teams shouldn't work on security without coordinating with each other. There should be a dedicated board to oversee security.



Diagram 5 :Recommended Governance Structure

This graphic shows a clear chain of command within FSB, with duties moving from the Board of Directors to operational staff and other parties. It shows how important the Chief Information Security Officer and the Security Governance Committee are in controlling and keeping an eye on security practices. The structure makes sure that everyone is responsible, that communication is clear, and that business goals and security controls are in line with each other. In general, it helps the whole organization have good governance, manage risks, and follow the rules.

The governance model should clearly define security roles and responsibilities to ensure accountability and align cybersecurity strategy with business goals. Regular risk reporting, compliance audits and supplier security assessments are essential to identify vulnerabilities, ensure GDPR compliance and manage third-party risks. A structured BYOD approval process and continuous cloud security monitoring are required to control device access and protect externally hosted systems, ensuring a secure and resilient digital environment [8].

3.3 Security Policies

FSB should create formal security policies to guide staff, contractors and third-party partners.

Important policies include:

Policy	Purpose
Information Security Policy	Defines overall security rules
BYOD Policy	Controls personal laptops and mobile devices
Access Control Policy	Defines user permissions and MFA
Cloud Security Policy	Controls external cloud-hosted systems
Data Protection Policy	Supports GDPR compliance
Incident Response Policy	Explains how to report and handle incidents
Acceptable Use Policy	Defines safe use of company systems
Third-Party Security Policy	Controls partner and supplier access

FSB should put in place a full set of security rules to make sure that its data and information systems are always safe. These guidelines for access control, cloud use, data protection, incident response, and

third-party security help the organization manage risks well. robust enforcement of regulations like BYOD, which entails registering devices, encrypting data, robust authentication, and managing mobile devices, is important for lowering risks. In general, clear policies help with following the rules, raise security awareness, and make sure that the operating environment is safe and managed [9].

3.4 Risk Management

FSB should put in place a structured and ongoing risk management procedure to find, evaluate, and reduce security vulnerabilities across all of its systems. The first step in this process is to find risks including cyberattacks, insider threats, and cloud vulnerabilities. Then, the risks are looked at to see how likely they are to happen and how they might affect corporate operations. Based on how serious they are, the risks that have been looked at are then put in order of importance. This lets the FSB use the right treatments, such mitigation, transfer, acceptance, or avoidance. Regular reviews and constant monitoring make sure that new and growing dangers are found early and that controls stay effective. This organized strategy helps FSB cut down on possible losses, make better decisions, and keep the financial environment safe and strong [8].

Example FSB Risk Matrix

Risk	Likelihood	Impact	Risk Level	Treatment
BYOD malware infection	High	High	Critical	MDM, antivirus, device compliance
Cloud misconfiguration	Medium	High	High	Cloud audits, least privilege
Insider data theft	Medium	High	High	Monitoring, access control, logging
Mobile banking fraud	High	High	Critical	MFA, fraud detection
Third-party breach	Medium	High	High	Supplier audits and SLA controls

Risk can be calculated as:

$$\text{Risk} = \text{Likelihood} \times \text{Impact}$$

3.5 Security Management Models and Practices

FSB should not just use one model; it should use multiple. This table shows the main security frameworks and models that FSB uses to support its information security policy. Each one helps with governance, risk management, and operational control. They work together to make a complete approach by combining formal security management, best practices, service operations, and basic security principles. This combined usage of frameworks makes sure that sensitive data is well protected, that rules are followed, and that the security environment is strong [7].

Model / Framework	Main Use for FSB
ISO/IEC 27001	Formal ISMS and security controls
ISO/IEC 27002	Best-practice control guidance
NIST CSF 2.0	Cybersecurity lifecycle and risk communication
ITIL 4	IT service and incident management
COBIT	Governance, accountability and audit control
CIA Triad	Basic security principle for data protection

For FSB:

- **Confidentiality** protects customer banking records.
- **Integrity** ensures financial transactions are accurate.
- **Availability** ensures online and mobile banking remain accessible.

3.6 Contingency Planning

FSB needs contingency plans to continue operations during cyber incidents, outages or disasters. Key plans include:

- Business Continuity Plan
- Disaster Recovery Plan

- Incident Response Plan
- Backup and Restoration Plan
- Cloud Outage Plan
- Fraud Response Plan
- Communication Plan

The contingency planning approach shows FSB how to respond to cyber disasters or system breakdowns in an organized way. The first step is to put an incident response strategy into action. Then, the problem needs to be contained and investigated to limit the damage. To make sure that business can continue, the organization then uses disaster recovery and backup solutions to restore systems. Finally, a review of the occurrence is done to figure out what went wrong and how to do better next time. To stay ready and operationally strong, backups, recovery goals, and reaction methods must be tested on a regular basis [9].

3.7 Protection Mechanisms

FSB should apply technical, administrative and physical controls.

Technical Controls

- Multi-factor authentication
- Encryption for data at rest and in transit
- Endpoint detection and response
- Firewalls and web application firewalls
- Security information and event management
- Data loss prevention
- Mobile device management
- Vulnerability scanning
- Zero Trust access control

Administrative Controls

- Security policies
- Staff awareness training
- Supplier contracts
- Access reviews
- Compliance audits
- Risk assessments

Physical Controls

- Secure offices
- CCTV
- Access cards
- Server room protection
- Visitor logs

The Defence-in-Depth strategy for FSB uses several levels of security measures to keep systems and data safe from a range of attacks. It starts with governance and policies to set rules and goals. Then, there is training for users to make them more aware of hazards that come from people. Identity and access control makes sure that only those who are allowed to use systems can do so, and network security keeps data safe while it is being sent. Endpoint and BYOD security keep devices safe, while application and cloud security keep hosted services safe. Finally, encrypting and backing up data is a great way to safeguard critical information and make sure it can be recovered in case of an event. This makes a complete and powerful security architecture[10].

3.8 Service Level Agreements

FSB hosts more than 90% of its infrastructure outside of its own buildings, therefore rigorous Service Level Agreements (SLAs) are necessary to make sure that everything is safe, reliable, and accountable. A good SLA should clearly spell out uptime assurances, who is responsible for security monitoring,

how long it takes to respond to incidents, and how often data should be backed up. It must also include goals for disaster recovery, rules for following the GDPR, and the right to audit to keep up with government standards. Also, having clear rules on who owns the data, where it resides, and what happens if someone doesn't follow the rules helps FSB avoid legal and operational problems [9].

Example SLA Table

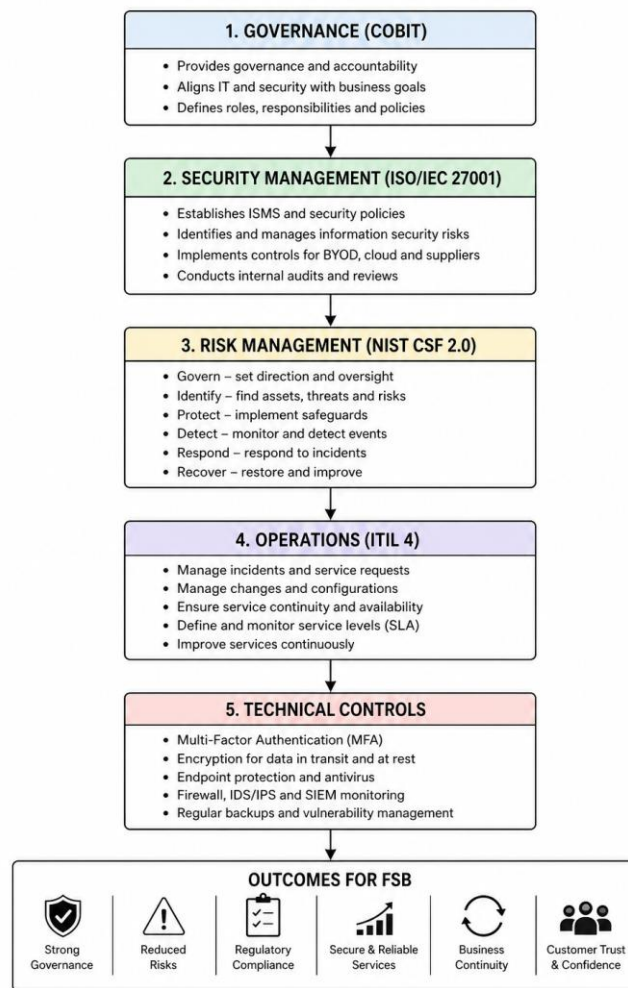
SLA Area	Requirement for FSB
Availability	99.9% uptime for banking services
Incident Notification	Supplier must notify FSB within agreed time
Backup	Daily encrypted backups
Recovery	Defined recovery time and recovery point objectives
Compliance	Must support UK GDPR and financial regulations
Audit	FSB must have audit rights over supplier controls

4. Integrated Security Architecture and Governance Model for FSB

4.1 Designed Security Approach for FSB

FSB's security problems can be handled better with a tiered and integrated security architecture that includes governance, risk management, operational processes, and advanced technical controls. The approach starts with COBIT, which makes sure that IT strategy and business goals are in line with each other, that there is strong governance and accountability, and that executives can oversee cybersecurity and make educated decisions. ISO/IEC 27001 sets up a formal ISMS at its heart. This makes sure that policies, risk assessments, and controls are applied the same way across BYOD, cloud infrastructure, and third-party services. It also supports ongoing compliance through audits and monitoring. The NIST Cybersecurity Framework 2.0 uses a lifecycle strategy (Govern, Identify, Protect, Detect, Respond, and Recover) that lets FSB find problems before they happen, put controls in place, spot suspicious behavior, and respond in a way that keeps business going. By managing incidents, service delivery, and system changes, ITIL 4 helps operations run more smoothly and makes sure that financial services are safe, reliable, and of high quality. It also helps IT teams and business departments work together better, which makes services more available and cuts down on interruptions. The method also uses current security measures including Zero Trust architecture, continuous monitoring (SIEM), endpoint protection, cloud security posture management, and rigorous access control methods. These technologies make the whole defense system stronger and keep sensitive financial data safe from new cyber attacks [11].

Simple Security Approach for FinSure Bank (FSB)



(Diagram 6: Integrated Security Approach for FinSure Bank (FSB))

This diagram shows a simple, organized security plan for FSB. It shows how governance, risk management, operations, and technical controls all work together in a clear way. It shows how each layer helps make banking services safe, legal, and dependable.

Layer	Framework Used	Key Function	Application to FSB
Governance	COBIT	Strategic control & accountability	Defines roles, ensures leadership oversight and aligns IT with business goals
Security Management	ISO/IEC 27001	ISMS & policies	Implements risk-based security controls across BYOD, cloud and data systems
Risk Management	NIST CSF 2.0	Cybersecurity lifecycle	Identifies, protects, detects, responds and recovers from threats
Operations	ITIL 4	Service management	Manages incidents, service delivery and system changes
Technical Controls	Security Tools	Protection mechanisms	MFA, encryption, SIEM, endpoint security, Zero Trust
Compliance	GDPR / DPA 2018	Legal & regulatory	Ensures data protection, audits and legal compliance

This integrated approach ensures:

- Strong governance and accountability
- Continuous and proactive risk management
- Secure and efficient service delivery
- Full regulatory and legal compliance
- Enhanced visibility and monitoring of threats
- Improved resilience against cyberattacks and system failures

4.2 Critical Analysis: Importance of Updated Regulations and Standards

Due to cyber dangers are always changing, groups like the FSB need to keep updating their security rules and standards. Ransomware, phishing, insider threats, and AI-driven cyberattacks are all examples of modern attacks that are always changing, which makes old measures useless.

New rules, like the GDPR, make sure that companies keep up good data protection policies and follow the law. In the banking industry, failing to follow new rules can lead to fines, legal problems, and losing customers' trust, which is very important.

Also, new frameworks push businesses to use new technologies like Zero Trust architecture, enhanced threat detection, and cloud security controls. This makes it easier for the organization to stop, find, and deal with dangers. From a governance point of view, changing norms make it easier to hold people accountable, be open, and manage risk. They also help with ongoing improvement, which is important for keeping a solid security posture. So, periodically updating rules and standards is not only a good idea, but also necessary to make sure that an organization stays safe, strong, and compliant in the long run.

Also, continually changing rules might make things harder, such making implementation more expensive, making operations more complicated, and requiring staff to be trained all the time. If not handled well, frequent changes can also make it hard for organizations to stay compliant. Even with these problems, the benefits of updating standards far exceed the drawbacks. This is because they help organizations stay safe, competitive, and in line with changing technology and threats [11].

5. Conclusion

In conclusion, FinSure Bank works in a digital world that is very fast-paced and full of risks, thus good information security, governance, and compliance are very important. The analysis shows that using well-known frameworks like ISO/IEC 27001, ITIL 4, NIST Cybersecurity Framework 2.0, and COBIT is an organized and complete way to handle security threats and make an organization more resilient. All of these frameworks operate together to promote governance, risk management, operational efficiency, and compliance with rules.

The suggested integrated security approach makes sure that security is built into every part of the organization, from making strategic decisions to putting technical controls in place. FSB can protect sensitive financial data and keep service delivery reliable by putting in place solid policies, risk management processes, contingency plans, and protection mechanisms. Also, by constantly updating rules and standards, the organization can stay in line with the law, improve security processes, and deal with new risks.

FSB needs a proactive, layered, and always-changing security approach to secure its assets, keep customers' trust, and be successful in the digital financial industry for a long time.

References:

- [1] International Organization for Standardization, ISO/IEC 27001:2022 Information Security Management Systems – Requirements, ISO, 2022. Available: <https://www.iso.org/standard/27001>
Accessed: Aug. 2026
- [2] International Organization for Standardization, ISO/IEC 27002:2022 Information Security Controls, ISO, 2022. Available: <https://www.iso.org/standard/75652>
Accessed: Aug. 2026
- [3] National Institute of Standards and Technology, The NIST Cybersecurity Framework (CSF) 2.0, NIST, 2024. Available: <https://www.nist.gov/cyberframework>
Accessed: Aug. 2026
- [4] ISACA, COBIT 2019 Framework: Governance and Management Objectives, ISACA, 2019.
- [5] AXELOS, ITIL Foundation: ITIL 4 Edition, TSO (The Stationery Office), 2019.
- [6] PeopleCert, ITIL 4 Practitioner: Information Security Management, PeopleCert. Available: <https://www.peoplecert.org>
Accessed: Aug. 2026
- [7] Information Commissioner’s Office (ICO), Guide to the UK GDPR – Data Protection Principles, 2023. Available: <https://ico.org.uk>
Accessed: Aug. 2026
- [8] UK Government, Data Protection Act 2018 and UK GDPR Overview, GOV.UK. Available: <https://www.gov.uk/data-protection>
Accessed: Aug. 2026
- [9] National Cyber Security Centre (NCSC), Cyber Security Guidance for Organisations, UK. Available: <https://www.ncsc.gov.uk>
Accessed: Aug. 2026
- [10] ENISA, Cybersecurity and Resilience Guidelines, European Union Agency for Cybersecurity, 2023. Available: <https://www.enisa.europa.eu>
Accessed: Aug. 2026
- [11] W. Stallings, Network Security Essentials: Applications and Standards, 6th ed. Pearson, 2017.