



Prifysgol Cymru
Y Drindod Dewi Sant
University of Wales
Trinity Saint David

Name: Patel Vinay Bhikhabhai

Student ID: 2519364

Course Name: MSc Cybersecurity and Digital Forensics

Module: Data Security, Governance and Compliance

Module Code: ACCA7028_LON

University: University of Wales, Trinity Saint David

1. Abstract

2. Introduction

3. Critical Evaluation of Security, Governance, and Compliance Frameworks

- 3.1 ISO 27001 – Information Security Management System (ISMS)
- 3.2 ITIL 4 – IT Service Management
- 3.3 COBIT – IT Governance Framework
- 3.4 NIST Cybersecurity Framework (CSF)
- 3.5 GDPR – General Data Protection Regulation
- 3.6 Comparative Analysis of Frameworks

4. Proposed Governance, Security, and Compliance Model for FinSure Bank (FSB)

- 4.1 Governance Structure
- 4.2 Security Policy Framework
- 4.3 Risk Management Framework
- 4.4 Monitoring and Reporting
- 4.5 Business Continuity

5. Benefits of Security, Governance, and Compliance for FSB

- 5.1 Improved Risk Visibility
- 5.2 Regulatory Readiness
- 5.3 Cost Reduction
- 5.4 Improved Decision-Making
- 5.5 Enhanced Operational Efficiency

5.6 Increased Stakeholder Confidence

6. Advanced Security Enhancements for FinSure Bank (FSB)

6.1 Zero Trust Security Model

6.2 Cloud Security Enhancement

6.3 Artificial Intelligence in Cybersecurity

6.4 Cybersecurity Awareness and Training

6.5 Third-Party Risk Management

6.6 Summary of Advanced Security Measures

7. Conclusion

8. References

1. ABSTRACT

=> In today's world, security, governance, and compliance have become integral elements of all organizations that use data. In this context, this report analyzes how FSB (FinSure Bank) can benefit from the implementation of such a governance and compliance model in terms of data security. As a company providing cloud-based financial services for its customers, FSB needs to face the growing number of cyberattacks aimed at compromising its financial data and breaching its internal controls.

=> First, this paper discusses the significance of data governance and compliance within digital businesses based on the analysis of five industry-specific frameworks – ISO 27001, ITIL 4, COBIT, the NIST CSF, and the GDPR. Then, the research proposes to implement an integrated model of governance, security, and compliance at FSB to meet its needs concerning risk management, access control, policy development, and compliance.

2. INTRODUCTION

=> The evolution of digital technologies, such as cloud computing and mobile applications, has had a profound impact on how companies conduct their operations. Although technology enables increased efficiency, scalability, and availability for customers, it exposes firms to various cybersecurity threats, such as data breaches, cybercrime, and malicious attacks. Consequently, organisations need to establish an adequate data security, governance, and compliance framework to address the emerging challenges.

=> FinSure Bank (FSB) is one of the fast-growing financial service providers that utilise cloud computing infrastructure for the delivery of financial services to its customers. The company provides online banking, loan facilities, and investment opportunities to its clients residing in several different geographical areas. Moreover, the use of BYOD policies and mobile banking further adds to the existing concerns about data security and potential insider threats at FSB.

=> Although it manages sensitive customer data, FSB does not have an established security governance framework. Thus, the lack of data management processes and strategies poses several risks for the company in terms of cyberattacks and regulatory requirements, such as GDPR.

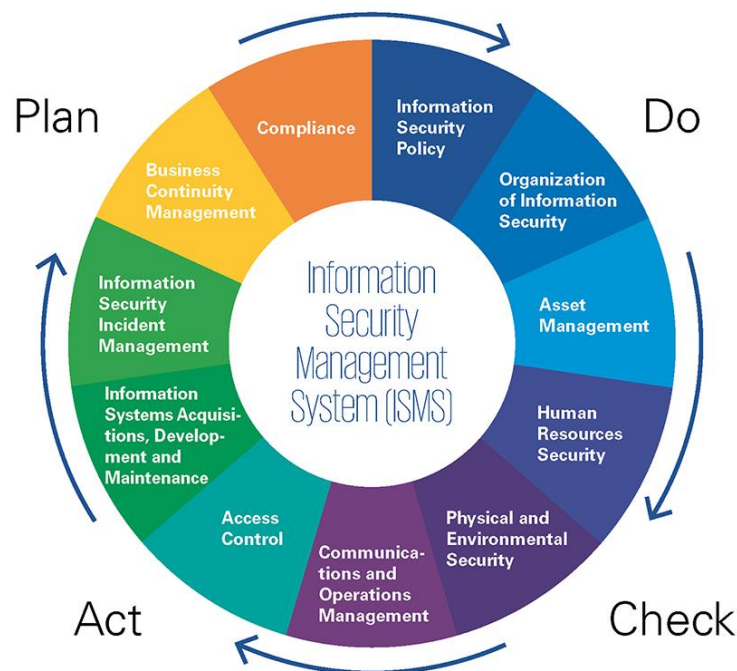
=> The purpose of this report is to critically assess the major models of information security management, including ISO 27001, ITIL 4, COBIT, and the NIST Cybersecurity Framework, and suggest an effective combination that will strengthen security, governance, and compliance at FSB. This report also stresses the need for ongoing improvement and the integration of IT and business goals.

3. Critique of Frameworks

3.1 ISO 27001 - Information Security Management System (ISMS)

=> This is one of the globally accepted frameworks that can be used to manage information security in a systematic way. This framework can help FinSure Bank (FSB) and other organisations to detect vulnerabilities and risks then use relevant controls to protect financial information. ISMS framework applies PDCA (Plan-Do-Check-Act), which is aimed at enhancing the performance of security control activities.

=> As far as the importance of ISO 27001 is concerned, this framework plays a critical role in helping FSB to develop information security policies, access controls and risk assessment processes among others. However, this framework is focused on security controls only and does not include governance or service management of information technology.



=>Explanation of the Diagram:

=> The diagram shows the ISMS (Information Security Management System) according to ISO 27001 using the Plan-Do-Check-Act cycle. The plan stage will focus on identifying risks, developing policies, and setting security objectives.

=> During the do stage, implementation of the security control processes will be done. In the check stage, monitoring and auditing of the security control process will be carried out. During the act stage, improvements will be made by performing necessary actions from audit findings and review process performances.

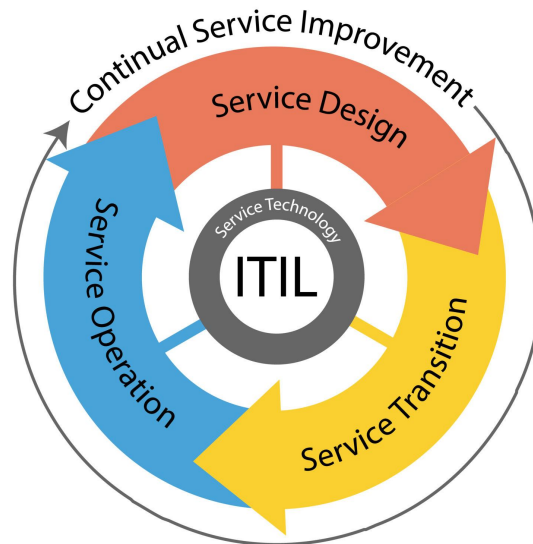
=> For FinSure Bank (FSB), the PDCA cycle allows for proactive management of cybersecurity threats, improving security control, and remaining compliant with the regulation.

3.2 ITIL 4 – IT Service Management

=> ITIL 4 offers guidance on delivering efficient and reliable IT services that meet business requirements. ITIL 4 emphasizes important processes such as incident management, change management,

and service delivery.

=> From an FSB perspective, ITIL 4 guarantees that cybersecurity practices are integrated into everyday IT operations. For instance, incident management enables quick reactions to cyber attacks, whereas change management safeguards systems from vulnerabilities when upgrading them. Nevertheless, ITIL lacks specific security measures; therefore, it should be used alongside other standards, including ISO 27001.



=>Explanation of the Diagram:

=> This diagram demonstrates the ITIL 4 Service Value System, where the value is achieved through the use of a circular continuous improvement model like PDCA cycle.

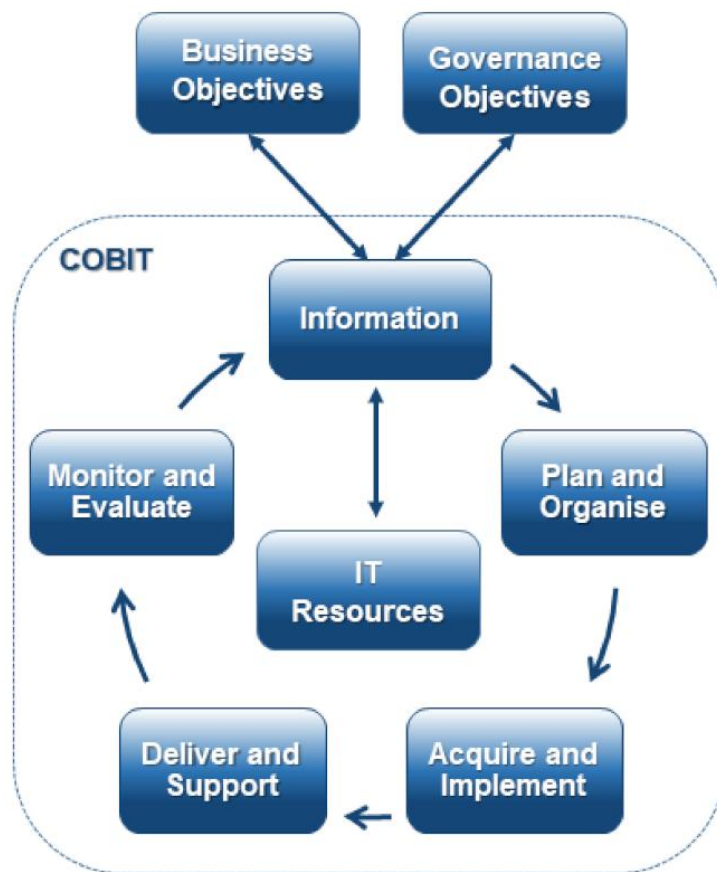
=> The diagram shows how the process of planning, designing, delivering, monitoring, and improving the IT services in FinSure Bank (FSB) is done. Each step indicates some important service management activities, which include stakeholder engagement, change management, incident management, and performance measurement.

3.3 COBIT – IT Governance Framework

=> The COBIT framework centers around aligning information technology practices with business objectives while ensuring proper governance and risk management. The framework offers performance measuring instruments and detailed accountabilities.

=> In regard to FSB, COBIT enables top management to assess the performance of information technology systems and ensure that security policies are aligned with business objectives. COBIT

works at a strategic level and needs to be integrated with technical standards to be implemented.



=>Explanation of the Diagram:

=> The following figure represents the COBIT IT Governance Framework, which depicts the relationship between governance and management process elements required to achieve strategic alignment between the IT systems and the business.

=> The COBIT framework is segmented into two components—governance (EDM) and management (APO, BAI, DSS, MEA)—that represent core organizational functions.

=> In the case of FinSure Bank (FSB), such a framework allows senior managers to measure and control IT activities, assess potential risks, and develop IT security strategies in line with the business requirements.

3.4 NIST Cybersecurity Framework (CSF)

=> NIST CSF is a risk-based and flexible approach to managing cyber-security risks. It encompasses five major functions: Identify, Protect, Detect, Respond, and Recover.

=> Regarding FSB, the framework can help with detecting threats proactively and responding to incidents effectively. Being flexible, it allows for adjusting to different conditions. Nonetheless, the framework is not a certification program and should be complemented by ISO 27001.



=>Explanation of the Diagram:

=> The following diagram is the representation of the NIST Cyber Security Framework (CSF), which gives an organizational structure for cyber security risk management.

=> The core elements, which include Identify, Protect, Detect, Respond, and Recover, are all part of the cyber security risk management life cycle.

=>This framework allows FinSure Bank (FSB) to identify cyber security risks proactively, secure itself from such risks, detect any risks that may have occurred, respond to them, and recover quickly from those incidents.

3.5 GDPR – Data Protection Regulation

=> This ensures that any organisation processes personal data in a lawful, transparent, and secure way. This regulation is very important to FSB because it involves sensitive data of customers.

=> Non-compliance leads to substantial financial sanctions and reputation loss. This means that GDPR should also be included in the technological frameworks to ensure compliance.



>Explanation of the Diagram:

=> This diagram presents the key principles of the GDPR framework in a circular format, adapted to a landscape layout for better visual clarity. It highlights core principles such as data minimisation, purpose limitation, security, and accountability.

=>For FinSure Bank (FSB), these principles ensure that customer data is processed securely, lawfully, and transparently. The outer layer represents regulatory enforcement and data subject rights, emphasising continuous compliance and protection.

3.6 Comparison

=> All the mentioned approaches have their distinct role in securing different areas related to organizational security and governance. For instance, ISO 27001 has an aim to create an effective ISMS by introducing controls and reducing possible threats related to information security. ITIL facilitates the delivery of quality services within the scope of IT service management. Meanwhile, COBIT is a governance framework where processes of IT and business strategy align to make the best decisions.

A).ISO 27001 – Information Security:

=> This standard provides the guidelines for establishing and maintaining effective information security controls within an organization. The ISMS in ISO 27001 can help FinSure Bank (FSB) in protecting their financial information and customer data against any cyber threat or attacks.

B).ITIL – Service Management:

=> This framework aims at improving the quality of IT service management through aligning the IT services to the business requirements. This involves managing services including incident management, change management, and service delivery among others. This will help ensure that IT services provided at FSB are reliable and efficient while also being able to react faster in case of any security incident.

C).COBIT – Governance:

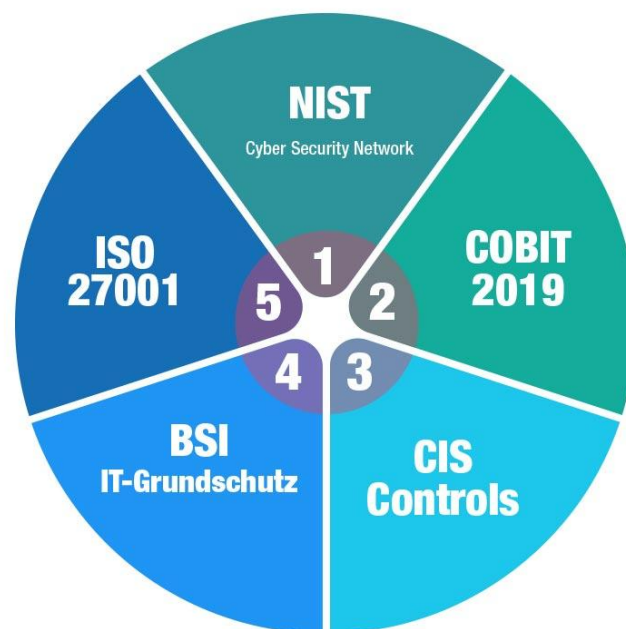
=> It is a governance framework aimed at ensuring that IT systems are aligned with organizational goals and objectives. It also helps in defining roles and responsibilities and measuring performance. At FSB, COBIT will help in making strategic decisions regarding IT resources and management of associated risks.

D).NIST – Cybersecurity Risk Management:

=> This cybersecurity risk management framework comprises five core functions that help organizations manage cybersecurity risks effectively. These include identifying, protecting, detecting, responding, and recovering from cybersecurity threats. This framework will help FSB identify the cybersecurity risks and respond effectively to any cyber incidents.

E).GDPR – Legal Compliance:

=> GDPR guarantees that data handling practices are conducted legally, fairly, and safely. Data protection practices are required under GDPR, as are measures of accountability. GDPR compliance is important for FSB in ensuring that no fines result from a breach in confidentiality.



=>Explanation of the Diagram:

=> This diagram illustrates the integration of key frameworks used by FinSure Bank (FSB) to manage security, governance, and compliance. Each framework addresses a specific organisational need: ISO 27001 ensures information security, ITIL enhances IT service management, COBIT supports governance and strategic alignment, NIST manages cybersecurity risks, and GDPR ensures legal compliance. The circular structure highlights how these frameworks work together to provide a comprehensive and continuous approach to organisational security and performance.

4. Proposed Model for FSB

4.1 Governance Structure

=> It is necessary to develop a clear governance structure at FinSure Bank (FSB) to ensure that all processes related to information security and compliance are coordinated and well-managed. With an adequate governance structure, FSB will be able to align its cybersecurity approach with its busi-

ness goals while assigning responsibilities at each level.

=> The highest level of governance comprises the Board of Directors. They provide strategic direction and ensure that all cybersecurity initiatives are aligned with organisational objectives. The board of directors oversees the budget, sets risk appetite levels, and monitors the overall performance of governance.

=> The Chief Information Security Officer (CISO) is a critical position at FSB. The CISO manages the overall cybersecurity strategy for the organisation and identifies emerging cybersecurity risks. The CISO is responsible for implementing cybersecurity policies and strategies in different departments.

=> The Data Protection Officer (DPO) is another key position at FSB. The DPO ensures that FSB complies with data protection laws, especially GDPR. It entails carrying out regular data protection impact assessments and ensuring adherence to data protection principles.

=> It is the responsibility of the IT Security Team to deploy the necessary technical controls such as hardening of systems, managing vulnerabilities, and monitoring network traffic in real time. These members are vital in identifying and addressing any security threats that arise.

=> Lastly, the Data Stewards are tasked with ensuring that the data is accurate, of high quality, and classified correctly.

=> In general, the above governance model allows FSB to adopt an integrated and strategic approach to security management and risk management for the purpose of achieving organisational objectives.

4.2 Security Policy Framework

=> There is a need for adopting a robust security policy framework within the FinSure Bank (FSB) for ensuring the consistency of protection of information resources in FinSure Bank. These policies will define appropriate behaviour within the organisational setup along with setting out various responsibilities that are necessary for ensuring the confidentiality of such information.

=> The Access Control Policy is adopted by FSB in order to implement role-based access control (RBAC). The concept of least privilege is used for restricting unnecessary access rights to the user.

=> The Authentication Policy enhances the system's security through multi-factor authentication and stringent password requirements. In effect, this protects user accounts from getting compromised and avoids any unauthorised entry into the system especially in the cloud environment.

=> The BYOD policy deals with the threats posed by allowing personal devices into the organisation. This policy mandates device registration, mobile device management (MDM), and encryption for any corporate data accessible through these devices.

=> The Data Classification Policy helps classify information into various categories which include but are not limited to Public, Internal, Confidential and Restricted. As a result, FSB can implement security measures that will help in avoiding data leakage depending on the level of confidentiality.

=> The Incident Response Policy outlines how to manage security threats that may affect the organisation. It clearly stipulates what should be done upon discovering security threats including reporting the same and how the problem can be solved in a timely manner.

=> The Vendor Management Policy helps in assessing third-party vendors against their ability to adhere to set security measures. This includes checking their compliance with the required security policies and frameworks such as ISO 27001 and GDPR among others.

=> Lastly, the training and awareness strategy fosters a security-aware culture at FSB through provision of cybersecurity trainings, phishing drills, and regulations updates. Employees are thus able to identify and appropriately react to possible threats.

=> Overall, this framework of security policies gives an adequate foundation for risk management, compliance, and governance within FSB.

4.3 Risk Management Process (FSB)

=> Risk management is crucial to the protection of vital information resources and the continuity of operations in a digitally oriented enterprise like FinSure Bank (FSB). Considering that FSB deals with personal and financial data of high value, there must be an organised risk management process within the company to ensure security.

=> In the risk management process applied by the FSB, risks are classified according to their probability and level of impact so that the company can focus on those that pose a significant threat to FSB. There are high risks in the areas of BYOD abuse, cloud data breaches, insider attacks, and GDPR non-compliance, among others.

=> Risk Management Table(FSB)

Risk	Likelihood	Impact	Level	Mitigation
BYOD misuse	High	High	Critical	MFA + MDM
Cloud breach	Medium	High	High	Encryption
Insider threat	Medium	High	High	Monitoring
System failure	Low	High	Medium	Backup
GDPR breach	Medium	High	High	DPO

4.4 Monitoring and Reporting

=> Monitoring and reporting are key elements in sustaining a good security stance in FinSure Bank (FSB). Through these two processes, the organization is able to identify any threats early and be able to act on them appropriately. The process also helps the firm meet various compliance requirements.

=> The 24/7 Security Information and Event Management (SIEM) monitoring system helps the firm analyze and monitor all security related information on a regular basis. As a result, the organization can identify any abnormality within its systems and take necessary action accordingly.

=> Vulnerability scans should be conducted at least once in a month. Through these scans, the organization identifies vulnerabilities within its systems.

=> Governance reports on a quarterly basis help the top management understand how well the organisation is performing in terms of its security posture, compliance, and risk indicators. Such governance reports make it easier for the top management to make decisions and keep the security policies consistent with the organisational strategy.

=> On the other hand, annual security audits are essential in assessing the efficiency of the Information Security Management System (ISMS) adopted by an organisation. The audits help determine whether the ISMS adheres to standard frameworks like the ISO 27001 as well as the General Data Protection Regulation (GDPR).

=> In summary, a systematic approach towards monitoring and reporting plays a significant role in helping FSB monitor the state of its security environment.

4.5 Business Continuity

=> It is vital that FSB creates a business continuity plan that will ensure that their activities could proceed regardless of various disruptive events, including but not limited to cyberattacks, system crashes, or natural disasters. Since the bank is heavily dependent on cloud computing solutions and other IT resources, having a well-developed plan becomes crucial.

=> Among the elements of a business continuity plan there are daily backups that ensure proper storage of critical data and make it possible to retrieve it in case of a data breach. In order to ensure protection of such information, the backups must be both secure and encrypted.

=> Another part of creating an effective business continuity plan is the formulation of a Disaster Recovery Plan (DRP). It is important that the document include recovery objectives. An RTO of four hours and RPO of daily backups would be sufficient in this case.

=> Furthermore, redundant systems must be implemented in order to avoid single points of failure and guarantee high levels of availability and stability of FSB's computer networks.

=> Lastly, it is vital to have a reliable system for remote access, especially when there are remote workers and partners. This can be done by having Virtual Private Networks (VPNs), along with Multi-Factor Authentication (MFA).

=> In conclusion, a good continuity plan ensures that FSB will be able to recover from any disruption to the normal operations of the company.

5. Further Benefits for FinSure Bank (FSB)

=> The application of an integrated information security, governance, and compliance regime offers other benefits apart from ensuring the safety of information assets. Such benefits will be advantageous to the organisation in terms of organisational efficiency, better decisions, and sustainability.

=> For example, the application of the information regime will enhance risk visibility for FSB, enabling it to have a deeper insight into possible risk sources within its system. This is achieved by continuously assessing risks and ensuring that risk assessments are always updated.

5.1 Better Risk Awareness

=> Allows FinSure Bank (FSB) to be able to spot and comprehend security risks and weaknesses in its infrastructure

=> Assists in ongoing risk assessment and monitoring within the cloud, network, and end-user operations

=> Helps prioritize those aspects of the organization that have more likelihood and impact in terms of risk

=> Makes risk management more proactive by addressing the problems while they remain minor

=> Increases awareness about insider threats, cyber attacks, and operational inefficiencies

5.2 Compliance

=> Helps in adhering to statutory and regulatory obligations like GDPR and Data Protection Act

=> Aids FSB in being prepared for both internal and external audits

=> Fosters proper documentation of processes and information handling

=> Avoids legal and regulatory non-compliance penalties and other forms of sanctions

5.3 Cost Saving

- => Helps save money that might be lost because of cyber attacks, data leaks, and system breakdowns
- => Helps save costs related to responses, recoveries, and legal proceedings
- => Avoids being fined by staying in line with regulations, e.g., GDPR
- => Promotes proper distribution of resources by focusing on risky spots
- => Ensures minimum downtime for business and continuous functioning of services

5.4 Better Decision Making

- => Supplies current and up-to-date information about security risks and system performance
- => Facilitates making decisions on the basis of real data by upper management
- => Implements strategic thinking and IT security strategy
- => Prioritizes the investment into security measures and new technologies
- => Increases the quality of governance via visibility and reporting

5.5 Greater Efficiency

- => Increases operational efficiency by adopting frameworks like ITIL
- => Improves cooperation between various departments and helps avoid mistakes
- => Improves incident detection and reaction due to the introduction of tools for monitoring and responding to events
- => Optimizes usage of available IT resources and cloud computing services
- => Saves time and energy by automating monitoring and reporting processes

5.6 Stakeholder Confidence

- => Earns customer trust thanks to the protection of their personal data
- => Gains regulatory authorities' confidence because of effective governance
- => Helps improve the organization's reputation and its brand
- => Earns trust of partners and third parties
- => Improves customer satisfaction

6.6. Enhanced Security Measures for FinSure Bank (FSB)

- => In addition to the existing security practices and governance framework, FinSure Bank (FSB) must implement more advanced security strategies to cope with contemporary cyber challenges and increase the resilience of the banking institution.

6.1 Zero Trust Security Approach

- => FinSure Bank should employ a Zero Trust security strategy in which there are no trusted users or devices in the corporate environment. All access attempts must be authenticated and authorised to ensure that the requests do not come from malicious insiders.

6.2 Enhanced Cloud Security

- => Considering the importance of the cloud environment for FSB operations, enhanced cloud security measures are necessary to protect the financial information against any security risks.

6.3 Use of AI in Cybersecurity

- => Use of AI and machine learning technologies can be helpful to improve the threat identification and response measures. These techniques can help process large amounts of data and identify suspicious activities with more precision than traditional methods of threat identification and response.

6.4 Importance of Cybersecurity Awareness and Training

=> Human error continues to be a significant concern related to cybersecurity. Therefore, FSB needs to spend resources on employee training and awareness programmes for effective cybersecurity management.

6.5 Third-Party Risk Management

=> It is imperative for FSB to manage the risk posed by its third-party relationships. For this purpose, FSB should ensure strict adherence to data and security compliance by third parties.

6.6 Summary Table for Enhanced Security Strategies

Domain of Security	Description	Benefits to FSB
Zero Trust Approach	Constant user and device verification	Limits unauthorised access attempts
Cloud Security Strategy	Encryption and secure cloud configuration	Protects sensitive data
AI in Security	Automated threat detection and response	Faster incident response
Training & Awareness	Employee education and phishing tests	Reduces human errors
Third-Party Risk	Vendor security assessments	Ensures compliance and security

7. Conclusion

=> This report has discussed the importance of data security, governance, and compliance in safeguarding modern digital organizations like FinSure Bank (FSB). The analysis of various frameworks, such as ISO 27001, ITIL 4, COBIT, the NIST Cybersecurity Framework, and GDPR, has shown that each framework possesses its own merits in terms of securing organizational information assets, enhancing governance capabilities, and ensuring compliance with regulatory requirements.

=> The integration framework designed in this report has provided a systematic solution for resolving security issues faced by FSB, such as establishing effective security policies, implementing efficient risk management techniques, conducting regular monitoring activities, and having robust compliance procedures in place. The alignment of all these frameworks will enable FSB to strengthen its security position and mitigate potential risks in cloud computing and BYOD environments.

=> Moreover, the report has noted that cybersecurity is a dynamic process that needs regular review and improvement to counter new security threats. Therefore, through this integration model, FSB can protect its core information assets, build customer confidence, and sustain long-term growth.

8. IEEE References

- [1] International Organization for Standardization (ISO), "ISO/IEC 27001 Information Security Management," ISO, 2022. [Online]. Available: <https://www.iso.org/isoiec-27001-information-security.html>. [Accessed: 22 April 2026].
- [2] AXELOS, "ITIL 4 Framework Overview," AXELOS, 2019. [Online]. Available: <https://www.axelos.com>. [Accessed: 22 April 2026].
- [3] ISACA, "COBIT 2019 Framework," ISACA, 2019. [Online]. Available: <https://www.isaca.org/resources/cobit>. [Accessed: 22 April 2026].
- [4] National Institute of Standards and Technology (NIST), "Cybersecurity Framework (CSF)," NIST, 2018. [Online]. Available: <https://www.nist.gov/cyberframework>. [Accessed: 22 April 2026].
- [5] European Commission, "General Data Protection Regulation (GDPR)," European Union, 2016.

- [Online]. Available: <https://ec.europa.eu/info/law/law-topic/data-protection>. [Accessed: 22 April 2026].
- [6] National Cyber Security Centre (NCSC), “Cyber Security Guidance,” NCSC, 2023. [Online]. Available: <https://www.ncsc.gov.uk>. [Accessed: 22 April 2026].
- [7] European Union Agency for Cybersecurity (ENISA), “ENISA Threat Landscape,” ENISA, 2023. [Online]. Available: <https://www.enisa.europa.eu>. [Accessed: 22 April 2026].
- [8] SANS Institute, “Incident Handler’s Handbook,” SANS, 2022. [Online]. Available: <https://www.sans.org>. [Accessed: 22 April 2026].
- [9] Microsoft, “Azure Security Documentation,” Microsoft Learn, 2023. [Online]. Available: <https://learn.microsoft.com>. [Accessed: 22 April 2026].
- [10] Cloud Security Alliance (CSA), “Security Guidance for Cloud Computing,” CSA, 2023. [Online]. Available: <https://cloudsecurityalliance.org>. [Accessed: 22 April 2026].

⇒Other References

1. Cloud Security Alliance (CSA), “Top Threats to Cloud Computing,” 2023. Available: <https://cloudsecurityalliance.org/research/top-threats> (Accessed: 22 April 2026).
2. Palo Alto Networks, “What is Zero Trust Security?,” 2023. Available: <https://www.paloaltonetworks.com/cyberpedia/what-is-zero-trust> (Accessed: 22 April 2026).
3. Fortinet, “What is Data Security?,” 2023. Available: <https://www.fortinet.com/resources/cyber-glossary/data-security> (Accessed: 22 April 2026).
4. Kaspersky, “What is Cybersecurity?,” 2023. Available: <https://www.kaspersky.com/resource-center/definitions/what-is-cyber-security> (Accessed: 22 April 2026).
5. Check Point Software, “Cyber Security Best Practices,” 2023. Available: <https://www.checkpoint.com/cyber-hub> (Accessed: 22 April 2026).