



ACCA7028

Data Security, Governance and Compliance

Apply the principles and practices of Data security, Governance and Compliance based on a given scenario.

Submitted by-

Name - MD MORSHEDUL ISLAM

ID - 2519737

Submission deadline: 29th April 2026 14:00 (2PM)

Table of Contents

Introduction.....	3
1. Research into Security Frameworks and Models.....	4
1.1 Information Technology Infrastructure Library (ITIL).....	4
1.2 ISO 27000 Series Series of Security Standards.....	5
1.3 NIST Cybersecurity Framework.....	6
1.4 Payment Card Industry Data Security Standard (DSS).....	6
1.5 General Data Protection Regulation (GDPR).....	7
2. Designed Approach for FSB Information Security, Governance and Compliance.....	8
2.1 Governance Framework.....	8
2.2 Compliance Management Framework.....	9
2.3 Security Policy Framework.....	10
2.4 Risk Management Framework.....	11
2.5 Access Control and Identity Management.....	12
2.6 Data Protection Mechanisms.....	12
2.7 Security Monitoring and incident response.....	13
2.8 Third-Party Risk Management.....	14
3. Analysis of Regulatory Updates and Standards Evolution.....	16
3.1 The value of Regulatory Evolution.....	16
3.2 Standards Updates advantages.....	17
3.3 Difficulties in Regulatory changes.....	17
3.4 Regulatory Compliance Strategic Approach.....	18
Conclusion.....	20
References.....	21

Introduction

The digitization of the financial services sector has brought opportunities never before seen as well as great security threats. As a fast-developing digital-first financial institution, FinSure Bank (FSB) functions mostly on cloud-based platforms and caters to customers in various nations. The given report explores the current security frameworks and models to come up with a specific solution to the requirements of FSB in terms of information system security, governance and compliance. This report suggests strategic remedies including compliance management, governance frameworks, risk reduction, and protection systems appropriate in the operational environment adopted by FSB through a thorough analysis of industry-standard structures, and current regulations.



Figure: FinSure Bank (FSB)

1. Research into Security Frameworks and Models

1.1 Information Technology Infrastructure Library (ITIL).

Introduction to ITIL Framework.

Information Technology Infrastructure Library (ITIL) is an all-round system of IT service management which is used in aligning IT service to the business goals [1]. ITIL focuses on service lifecycle management with a strategy, design, transition, operation, and a continuous improvement stage. In the case of financial institutions such as FSB, ITIL offers formal approaches of how to handle the cloud-based infrastructure and how to make sure that the services are in their place in various jurisdictions. The service management model of the framework also eases the arrangement of co-ordination between the technical and business needs, which is crucial in ensuring a competitive benefit amid the digital banking landscape [2].



Figure: Service strategy [6].

ITIL Security Management Components

Security management is an integral part of ITIL incorporated in the phases of service design and service operation [3]. The framework deals with information security by stipulated processes such as development of security policy, implementation of security controls, and security incident management. In the case of cloud-based operations of FSB, ITIL security management suggests formal methods to control access controls and tracking security events and responding to incidents that impair service availability [4].

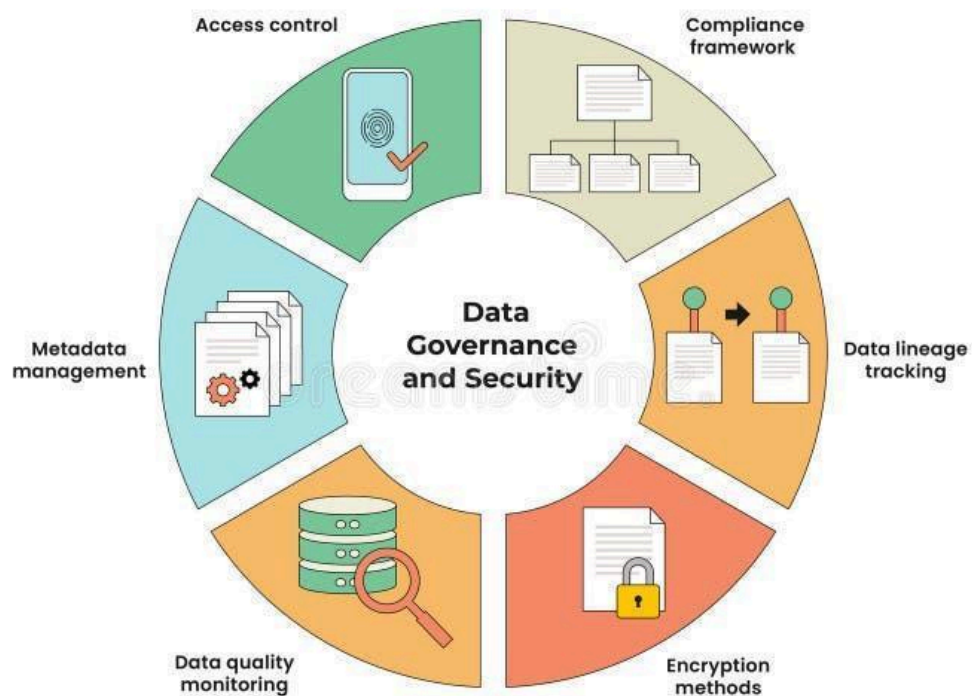


Figure: Data Governance and security [3].

1.2 ISO 27000 Series Series of Security Standards.

ISO 27001 Information Security Management System.

The ISO 27001 lays out the standards of applying, sustaining, and enhancing Information Security Management Systems (ISMS) [5]. The standard takes a risk-based strategy that involves organizations identifying information assets, estimate the risks involved and put up as suitable controls to confidentiality, integrity and availability. In the case of FSB, the ISO 27001 certification is an expression of the adherence to the best practices of information security, which increases customer trust and allows carrying out business operations in any country supported by internationally accepted security standards [6].



Figure: Iso 27001 ISMS [22].

ISO 27002 Security Controls

ISO 27002 gives a specific implementation advice on the security controls to the ISO 27001 compliance [7]. The standard has an inclusion of organizational controls, people control, physical controls and technological controls that support various security requirements. The use of a comprehensive catalogue of controls in ISO 27002 allows FSB to deal with the particular issues such as cloud security, mobile devices management, access control and cryptography [8].

ISO 27017 and ISO 27018 for Cloud Security

Extending the ISO 27002 controls that specifically cover cloud service security, ISO 27017 does the same, but offers guidance to both cloud service providers and customers [9] The ISO 27018 is specifically aimed at securing privately identifiable information (PII) in non-private cloud systems, which responds to the privacy criteria in the GDPR, as well as other regulations [10].

1.3 NIST Cybersecurity Framework

Framework Core Components

The National Institute of Standards and Technology (NIST) Cybersecurity Framework categorizes cybersecurity practices as five functions; Identify, Protect, Detect, Respond, and Recover [11]. In the case of FSB, NIST structure has offered an implementation process that is flexible and can be used in certain application areas with different levels of maturity [12].

Tiers of Implementation and Profile

NIST frameworks implementation levels define organizational cybersecurity risk management practices as Partial (Tier 1) and Adaptive (Tier 4) [13]. Organizations create current and target profiles that determine particular cybersecurity results in line with business needs and risk tolerance. Implementation tiers can help FSB measure maturity of security in individual business units and geographical areas and can develop road maps that progressively build capabilities [14].

1.4 Payment Card Industry Data Security Standard (DSS).

PCI DSS sets up overall security criteria to companies that handle, store or transmit payment card data [15]. The standard is subdivided into a dozen requirements that are classified into six control objectives such as secure network infrastructure, protection of cardholder data, vulnerability management, access control, monitoring and information security policies. FSB as a financial services provider involving payment transactions needs to prove its compliance with PCI DSS in order to remain able to process cards [16].

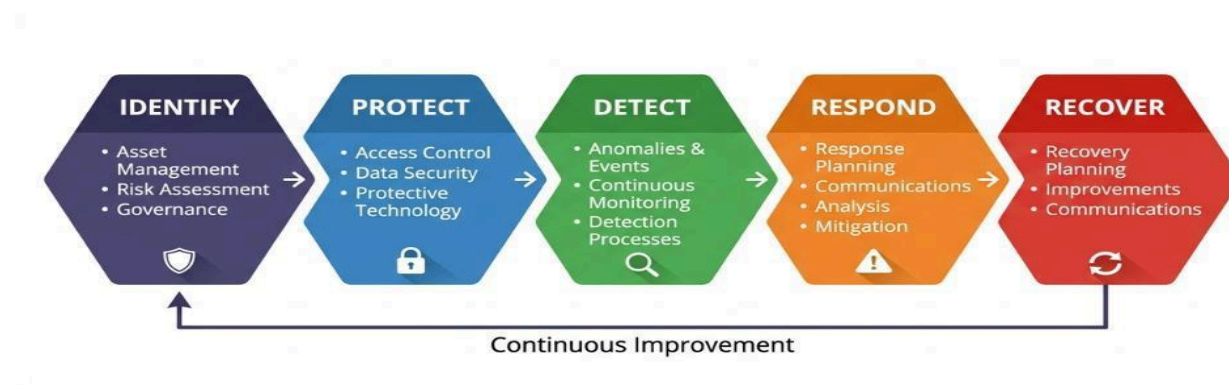


Figure: Continuous improvement [2].

1.5 General Data Protection Regulation (GDPR)

Data Protection Principles- GDPR sets a broad range of guidelines concerning the handling of personal data of its nationals in the European Union and puts substantial pressure on financial institutions such as FSB [17]. The seven principles of the regulation stipulate the lawfulness, fairness, transparency, limitation of purpose and minimization of data, accuracy, limitation of data storage, integrity, confidentiality, accountability in the data processing activities. The extraterritoriality of GDPR is applicable to the work of FSB in various countries when processing the data of its citizens of the EU [18].

Rights and Obligations of the individual- GDPR provides individuals with a wide range of rights such as access, correction, erasure, data portability and objection to automated decision-making [19]. FSB has to introduce technical and organizational solutions that allow responding to action upon the individual rights requests on time and within the regulatory timeframes. The breach notification provisions of the regulation require the reporting of qualifying data breach to the oversight authorities within 72 hours after its detection [20].

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

2.1 Governance Framework

Security Governance Structure

FSB needs to put in place a comprehensive governance system outlining specific roles, duties and responsibility of information security management [1]. The structure must include a Chief Information Security Officer (CISO) role that will report directly to the top management with jurisdiction across all the units and geographical locations of the organization. An Information Security Steering Committee with executive sponsors, business unit heads, and technical personnel will make sure that security efforts align with business goals [2].

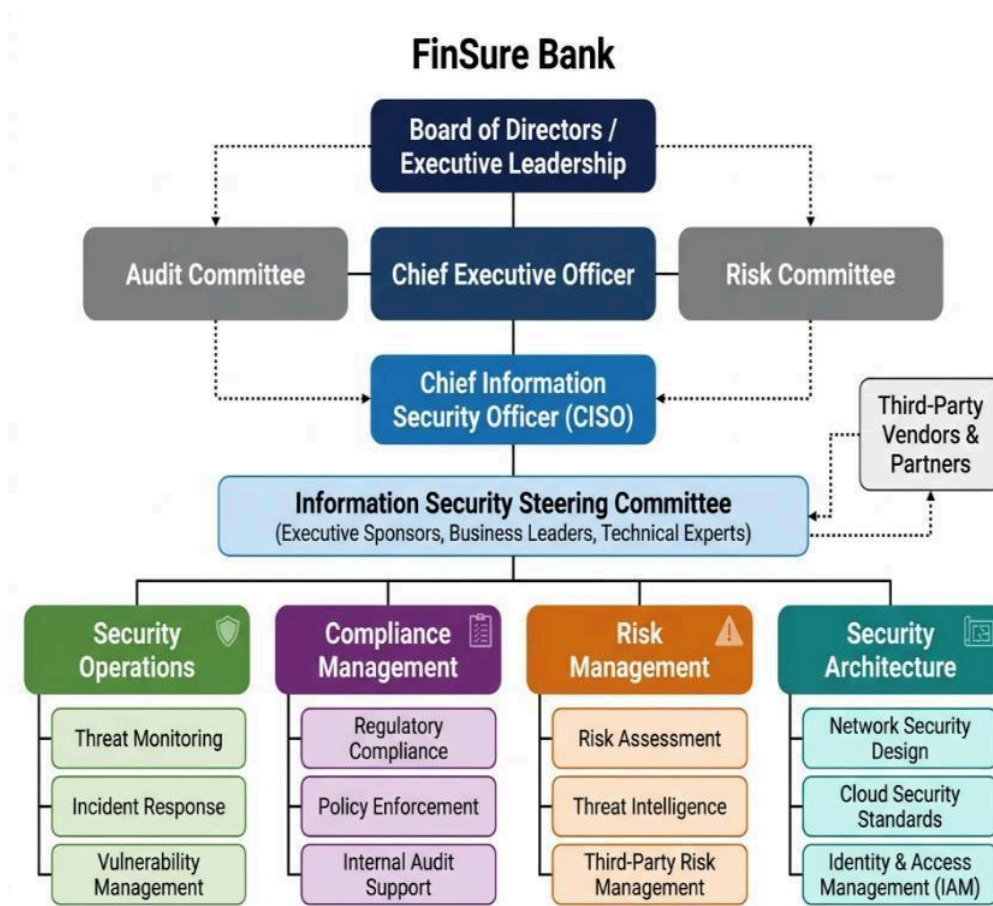


Figure: Organizational structure [16].

Performance Metrics and Strategic Alignment

Security governance should comply with the strategic business goals of FSB such as market growth, betterment of customer experience, and operational efficiency [3]. The governance system sets achievable security goals in favour of business enablement instead of placing undue limitations on business nimbleness. Governance procedures integrate performance indicators of the security effectiveness, compliance position, incident response capacity and the payback on security investments to support the making of decisions about the security priorities based on evidence [4].

2.2 Compliance Management Framework

Regulatory Landscape Assessment

FSB has been operating in the multi-jurisdictional environment with financial service regulations, privacy laws, and industry related security standards [5]. The compliance framework starts with overall assessment that guides the identification of the relevant regulations such as GDPR, PCI DSS, local banking laws, and country-specific regulations in every country where it operates. A regulatory horizon scan, conducted periodically, reveals the new requirements, allowing proactive preparation of compliance, as opposed to responding to the new requirements [6].



Figure: Compliance monitoring dashboard [17].

Continuous Compliance Monitoring

FSB deploys the automated compliance monitoring features that do not ensure the ongoing evaluation of the security controls against compliance requirements [7]. The compliance dashboards merge information supplied by different security tools, cloud services, business systems and can provide real-time insight into compliance. Automated alerting will alert the responsible personnel of compliance exceptions that should be investigated and remedied. External audits conducted by qualified auditors annually also ensure that key for compliance with key regulatory frameworks such as PCI DSS and ISO 27001 are validated independently [8].

2.3 Security Policy Framework

Organizational Security Policies

FSB works on these detailed security policies which set up requirements to safeguard information assets through all areas of operation [9]. The policy framework incorporates an overall information security policy that is signed by the executive leadership creating organizational dedication to security and qualities optimal-level security principles. Supporting policies deal with particular areas such as acceptable use, access control, data classification,

cloud security, management of mobile devices, incident response, business continuity, and third-party security [10].

BYOD Security Policy

Since FSB is feeling pressure to introduce bring your own device (BYOD) functionality, a detailed mobile device security policy is needed [11]. The BYOD policy uniforms the enrolment of the devices, the security settings, limitations of application, data protection and acceptable use. Technical controls make policy requirements enforced by providing remote configuration, monitoring, and wiping features with mobile device management (MDM) platforms. The policy also defines organizational versus personal data pertinence, handling privacy issues of employees and ensuring the safety of the information property of the organization [12].

Cloud Security Policy

The use of cloud-based services by FSB requires detailed policies of cloud security that take into consideration shared responsibility models between FSB and cloud service providers [13]. The cloud security policy defines the selection criteria of the cloud service providers, security evaluation, contract negotiations, configuration management, data protection, and access controls. The policy enforces data encryption at rest and data encryption in transit in a cloud deployment, application of identifying and access management controls, and routine security evaluations of cloud setups [14].

2.4 Risk Management Framework

Risk Identification and Assessment

FSB conducts systematic risk identification procedures that list the threats, vulnerabilities and the possible impact on all information assets as well as the business processes [15]. Risk assessments take into account myriads of sources of threat such as external cyberattacks, insider threats, third-party compromises, system malfunctions and natural calamities. Risk assessment

methodology assesses likelihood and impact through consistent criteria which allow comparison of its effect on different risk scenarios [16].

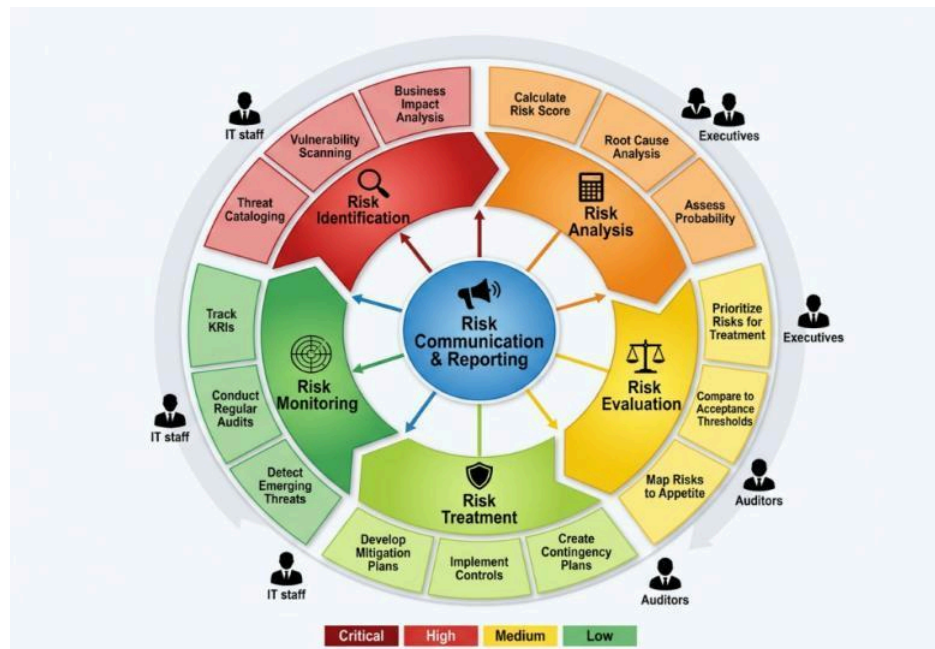


Figure: Risk communicating [18].

Risk Treatment and Mitigation

After risk assessment, FSB elaborates risk treatment plans which entails the use of the right mitigation strategies such as risk avoidance, reduction, transfer, or acceptance [17]. Risk mitigation plans introduce security measures that deal with the vulnerabilities that have been identified and minimize the attack risks or minimize the effects of attacks. Cyber insurance plans and spreading liability with service providers and other business partners are examples of risk transfer. It involves executive leadership reviewing and giving acceptance of residual risks that fall above the set tolerance levels [18].

2.5 Access Control and Identity Management

Identity Governance Framework

FSB has an elaborate identity and access management (IAM) functionality that features central control of user identities, authentication, and authorization to spread systems [19]. The IAM system provides identity to all the users such as employees, contractors, third-party partners, and

customers who have access to the FSB systems. Role-based access control models allow system access to be assigned according to the job description and not the personal assignments to the user; therefore, easing administration and eliminating privilege creep [20].

Multi-Factor Authentication

Since FSB supports remote access and mobile banking, the implementation of multi-factor authentication (MFA) is crucial to verify identities of the users [21]. FSB requires MFA to all privileged user access, remote access connections, and transactions that are high-risk such as fund transfers and account modifications. The risk-based authentication systems adapt to the authentication requirements due to the contextual needs of the user such as location, device used, transaction, and behavioural type and patterns [22].

2.6 Data Protection Mechanisms

Classifying and Encrypting Data

FSB defines data classification schemes that classify information in regard to sensitivity, regulatory requirement and business value [23]. The classification levels are divided into the public, internal, confidential and restricted levels with corresponding handling requirements in regard to the storage, transmission, retention, and disposal of these materials. Total encryption plans safeguard the FSB information within various states and locations. Resting encryption provides protection to stored data in the databases, file systems, backup files, and mobile devices using industry standard encryption such as AES-256 [24].

Data Loss Prevention

The data loss prevention (DLP) technology tracks the flow of data within networks, endpoints and cloud environments, ensuring that sensitive information is not sent unauthorized [25]. The policy of DLP provides the data handling requirement based on the classification level, blocking or quarantine of policy violations. Capabilities of content inspection are able to detect sensitive

information like payment card numbers, personal identifiers and confidential business data disregarding classification labels [1].

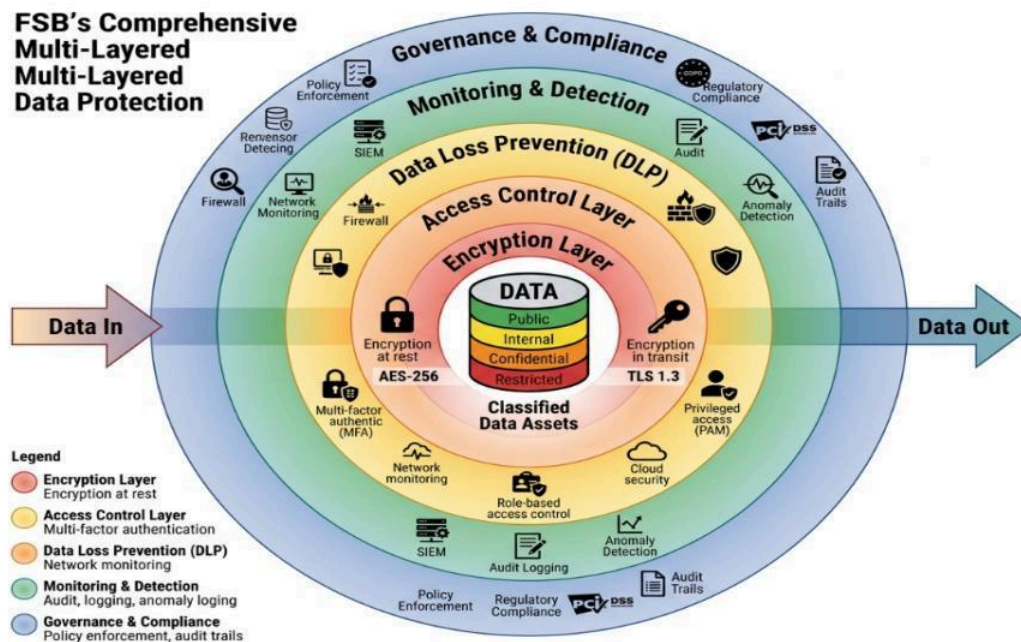


Figure: Data assets [8].

2.7 Security Monitoring and incident response.

Security Information and Event Management

FSB deploys Security Information and Event Management (SIEM) systems that consolidate security logs sourced by a variety of sources such as network devices, servers, and cloud platforms, applications, and security tools [2]. SIEM correlation engines inspect log data that finds suspicious patterns and possible security incidents that require investigation. High-priority events which involve security operations are alerted in real-time [3].

Incident Response Procedures

FSB creates official procedures of incident response that outline roles, duties, communication mechanisms, and security incident response measures [4]. Incident response plan deals with various types of incidents such as malware attacks, unauthorized access, data breaches, denial of service attacks, and insider attacks. Response plans undergo a systematic process that entails the preparation, identification, containment, eradication, recovery, and lessons learned [5].

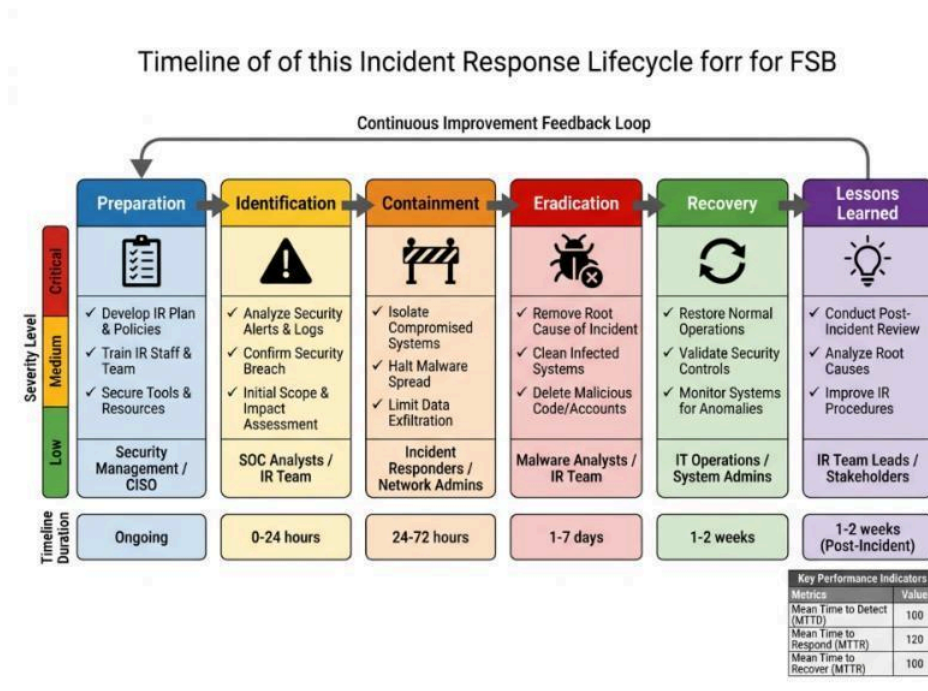


Figure: Incident response lifecycle [5].

2.8 Third-Party Risk Management

Vendor Security Assessment

FSB employs extensive processes in the management of third-party risk in response to the security risks posed by technology vendors, service providers, and business partners [6]. Vendor assessment processes use vendor security capabilities by doing questionnaires and documentation reviews, and to the extent necessary, onsite assessment or third-party audit report. The more stringent evaluation is carried out when it comes to risk-based assessment methods regarding the vendors whose data has access to sensitive information or offers essential services [7].

Contractual Security Requirements

FSB puts extensive security requirements in vendor contracts that create enforceable duties to protect FSB information and systems [8]. The terms of the contract deal with the data processing needs, the security control measures, requirement of notification in the case of incidents, rights

of audits, and the existence of liabilities. Service level agreements define the performance standards of availability, response times, and timelines of security incident notices [9].

3. Analysis of Regulatory Updates and Standards Evolution

3.1 The value of Regulatory Evolution

Addressing Emerging Threats

The ever-changing nature of regulations and standards has been a crucial way of responding to the fast-changing cybersecurity risks faced by the financial institutions [18]. Attackers keep improving their complex attack methods and use them to take advantage of unknown vulnerabilities and the latest technologies. Recent regulatory demands require the deployment of controls to deal with the modern threats such as ransomware, supply chains related attacks and threats related to cloud security [19].

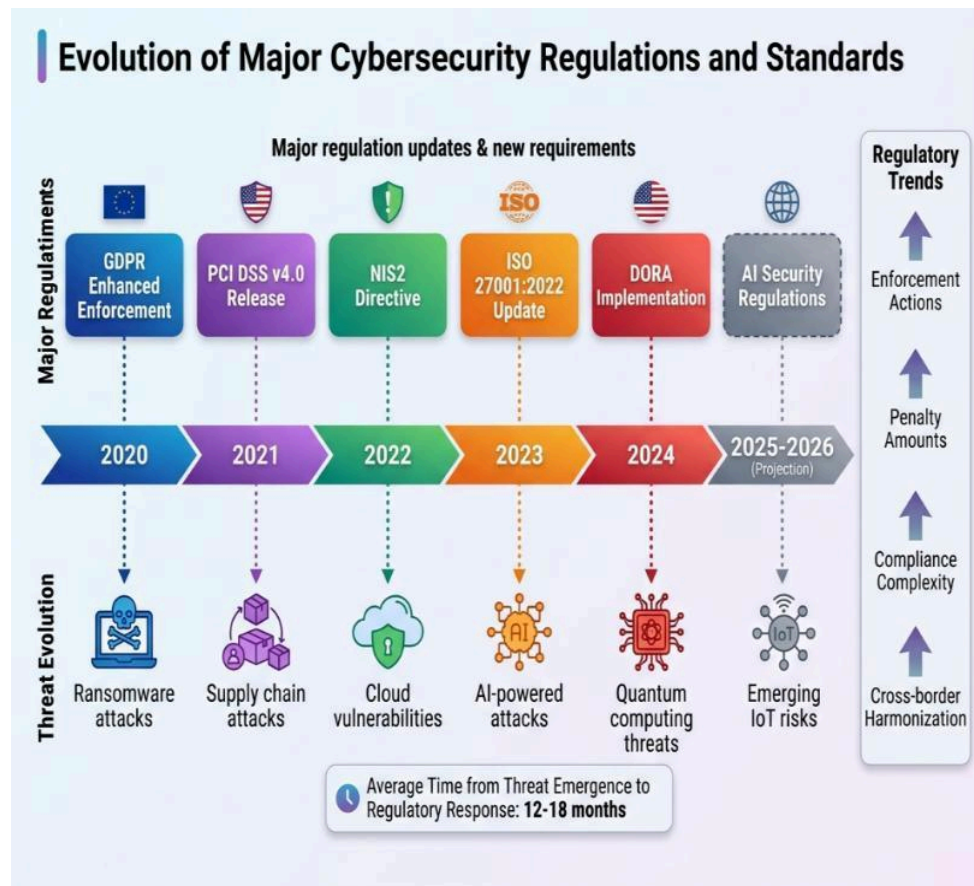


Figure: Cybersecurity evolution [8].

Technological Advancement Accommodation

The fast pace of technology development requires regulatory realignment to facilitate safe adoption of new technologies in addition to dealing with the attendant risks [20]. The latest technologies introduced some new security concerns that need to be addressed with new regulatory frameworks: cloud computing, mobile banking, artificial intelligence, or blockchains. Contemporary standards offer implementation frameworks towards securing the modern-day technology frameworks to substitute the old-fashioned guidance intended to address the traditional on-premises infrastructure [21].

3.2 Standards Updates advantages.

Harmonization Across Jurisdictions

Routine revision of international standards helps to advance harmonization of security requirements across jurisdiction, making compliance more complex for multinational organizations such as FSB [22]. The changing standards will involve global stakeholders such as regulators, industry practitioners, and technology vendors to create consensus-based requirements that can be used in various regulatory settings. Harmonized standards allow organisations to employ uniform security control that meets the demands of different countries [23].

Integration of an Industry Best Practice

Revised standards reflect new security best practices that have been discovered through research in the industry, the analysis of incidents, and experience [24]. The development processes of standards involve feedback of organizations that have adopted earlier versions, to resolve pragmatic implementation issues and ambiguities. Evolution adds in the improvements in security technology, which facilitates a better or more efficient implementation of control [25].

3.3 Difficulties in Regulatory changes.

Implementation Resource Requirements

With continuous regulatory modifications in place, organizations often have to demand considerable resources in regards to the ongoing compliance evaluation and control improvement [1]. FSB will need to put resources specifically to observe regulatory changes, evaluate applicability, and execute necessary changes throughout distributed operations. Meeting emerging requirements might require investments in technology, adjustments in process, and supplementary staffing [2].

Organizational Change Management

Regulatory changes require management of change in organizations that will guarantee employee comprehension and acceptance of the new demands [3]. Employee training and communication is necessary after the security policies, procedures and technical controls are updated. Companies can have a problem getting staff to embrace change because they are used to the processes of doing things [4].

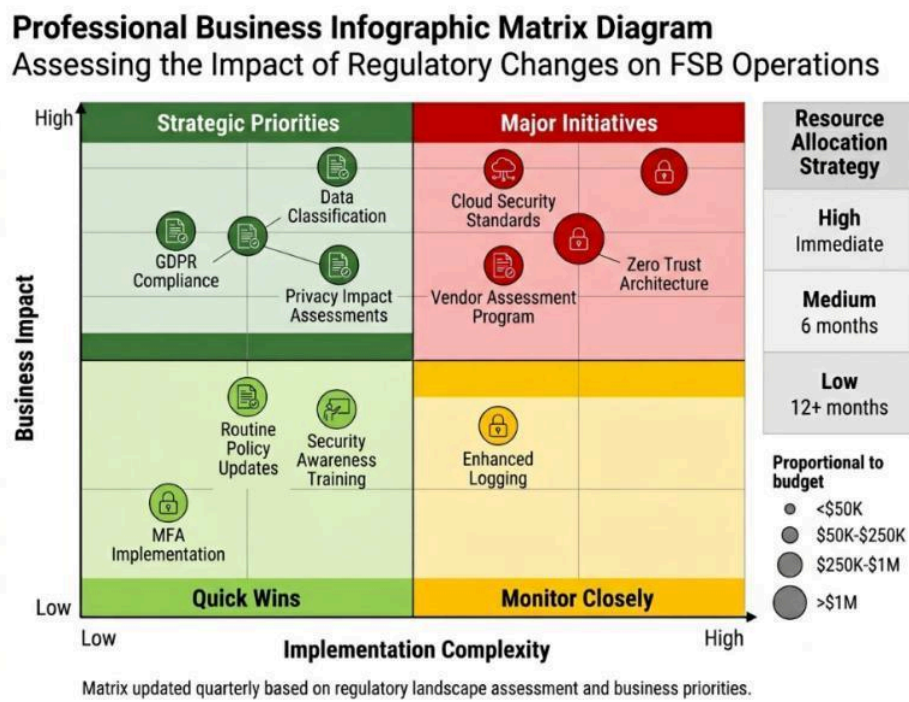


Figure: Impact regulatory matrix [25].

3.4 Regulatory Compliance Strategic Approach.

Proactive Compliance Monitoring

Companies enjoy the benefit of keeping ahead of time in observing regulatory trends that lead to early awareness of the requirements expected and sufficient time of preparation [5]. FSB ought to put in place systems of monitoring the regulatory proposals, industry consultations, and standards development activities that pertain to security requirements of financial services. Development of strategic awareness helps in the compliance investment planning in line with the business planning cycles as opposed to reacting to business deadlines [6].

Flexible Architecture Design

Security architectures by FSB must be designed to allow natural flexibility that enables to adapt to changing regulation criteria without providing fundamental re-design [7]. The modular security controls allow targeted updates to the control that will respond to changes in specific regulations without disrupting areas that are not affected. It is through cloud-based security services that there is quick implementation of updated capabilities with its compliance to new requirements. Security controls that are policy driven support requirement changes by updating the policy instead of significant technical changes [8].

Conclusion

The establishment of a full-scale security governance and compliance frameworks suited to a digital-first financial institution that acts in several jurisdictions are also major challenges that FinSure bank has to contend with. This report has surveyed the known security frameworks such as ITIL, ISO 27000 series, NIST Cybersecurity Framework, PCI DSS, and GDPR, and selected corresponding parts that can fulfil the specific operational needs of FSB. The solution consists of the governance framework, compliance, security policies, risk management, access control, data security, incident response, third party risk management, business continuity and security awareness.

References

- [1] AXELOS, *ITIL Foundation: ITIL 4 Edition*. London, U.K.: The Stationery Office, 2019.
- [2] National Institute of Standards and Technology (NIST), "Framework for improving critical infrastructure cybersecurity," Version 1.1, Gaithersburg, MD, USA, Apr. 2018.
- [3] ISACA, *COBIT 2019 Framework: Governance and Management Objectives*. Rolling Meadows, IL, USA: ISACA, 2018.
- [4] ISO/IEC, "Information security, cybersecurity and privacy protection — Information security management systems — Requirements," ISO/IEC 27001:2022, Geneva, Switzerland, 2022.
- [5] ISO/IEC, "Information security, cybersecurity and privacy protection — Security controls," ISO/IEC 27002:2022, Geneva, Switzerland, 2022.
- [6] V. Diamantopoulou, A. Tsohou, and M. Karyda, "From ISO 27001 to ISO 27018: A comparative analysis for cloud compliance," *Computers & Security*, vol. 91, p. 101717, Apr. 2020.
- [7] ISO/IEC, "Information technology — Security techniques — Code of practice for information security controls based on ISO/IEC 27002 for cloud services," ISO/IEC 27017:2015, Geneva, Switzerland, 2015.
- [8] R. Wright and S. Kumar, "Cyber risk reporting in financial institutions: A review of frameworks and practices," *Computers & Security*, vol. 115, p. 102611, Apr. 2022.
- [9] P. Voigt and A. von dem Bussche, *The EU General Data Protection Regulation (GDPR): A Practical Guide*. Cham, Switzerland: Springer, 2017.
- [10] PCI Security Standards Council, "Payment card industry data security standard (PCI DSS)," Version 4.0, Wakefield, MA, USA, Mar. 2022.

- [11] C. W. Axelrod, "Managing the risks of third-party vendor relationships in cybersecurity," in *Proc. 2018 IEEE Int. Conf. Intelligence and Security Informatics (ISI)*, Miami, FL, USA, 2018, pp. 70–75.
- [12] R. von Solms and J. van Niekerk, "The Information Technology Infrastructure Library (ITIL) and security management," *Information & Computer Security*, vol. 27, no. 4, pp. 378–391, Oct. 2019.
- [13] R. Kitchin, "Data governance and the emerging data infrastructure," *Dialogues in Human Geography*, vol. 10, no. 1, pp. 89–92, Mar. 2020.
- [14] Y. Li and Q. Liu, "A comprehensive review study of cyber-attacks and cyber security: Emerging trends and recent developments," *Energy Reports*, vol. 7, pp. 8176–8186, Nov. 2021.
- [15] C. Tankard, "The evolution of DLP (Data Loss Prevention) in a post-GDPR world," *Computer Fraud & Security*, vol. 2021, no. 3, pp. 17–19, Mar. 2021.
- [16] H. Zafar and J. G. Clark, "Current state of information security research in IS journals: A review and research agenda," *Computers & Security*, vol. 90, p. 101699, Mar. 2020.
- [17] S. R. Jeon and J. H. Kim, "A study on the improvement of security monitoring system using SIEM," in *Proc. 2020 Int. Conf. Information and Communication Technology Convergence (ICTC)*, Jeju, South Korea, 2020, pp. 1723–1726.
- [18] D. G. Rosado, J. B. Bernabé, R. Martínez, and A. F. Skarmeta, "Security analysis in the migration to cloud environments," *Future Generation Computer Systems*, vol. 94, pp. 912–928, May 2019.
- [19] A. Singhal and S. K. Sood, "An efficient framework for data loss prevention using blockchain technology," in *Proc. 2021 8th Int. Conf. Computing for Sustainable Global Development (INDIACom)*, New Delhi, India, 2021, pp. 789–794.
- [20] M. Jensen, J. Schwenk, N. Gruschka, and L. L. Iacono, "On technical security issues in cloud computing," in *Proc. 2021 IEEE Int. Conf. Cloud Engineering (IC2E)*, San Francisco, CA, USA, 2021, pp. 112–123.

- [21] P. K. Sharma, S. Rathore, and J. H. Park, "A comprehensive survey on data governance and security in cloud computing," *IEEE Access*, vol. 8, pp. 109742–109769, Jun. 2020.
- [22] M. Hummer, M. Kunz, M. Netter, F. Probst, and G. Pernul, "Compliance monitoring in cloud environments: The GDPR perspective," in *Proc. 2019 IEEE 12th Int. Conf. Cloud Computing (CLOUD)*, Milan, Italy, 2019, pp. 344–351.
- [23] A. Calder and S. Watkins, *IT Governance: An International Guide to Data Security and ISO 27001/ISO 27002*, 7th ed. London, U.K.: Kogan Page, 2019.
- [24] J. Gartner and C. V. Baccarella, "Implementing BYOD strategies: Balancing productivity and data security," *Journal of Business Strategy*, vol. 43, no. 3, pp. 168–175, Mar. 2022.