



University of Wales Trinity Saint David

Data Security, Governance and Compliance

Assignment Title

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

Name: Khushi Sangani

Student ID: 2520615

Course: MSc Cybersecurity and Digital Forensics

Module: Data Security, Governance and Compliance

Lecturer: Dr. Ayman Al Hajjar

Date: 24th April 2026

Abstract

This report looks at cybersecurity and governance frameworks like ISO/IEC 27001, NIST Cybersecurity Framework, COBIT 2019 and ITIL 4. It checks how well these frameworks help manage security risks in organisations. These frameworks give us a way to govern manage risks and keep our operations secure. They are the basis for cybersecurity practices.

This report proposes a custom cybersecurity and governance model for FinSure Bank. FinSure Bank is an organisation that works in a cloud-based and high-risk digital environment. Everything is centralized in the suggested methodology, including decision-making, risk management, work, and utilization of key systems. Additionally, it contains a strategy for ensuring safety as well as a method for determining which risks are crucial for the design. This helps address challenges, like using personal devices at work, cloud vulnerabilities and following regulations. The report shows that using established frameworks in a way can really improve an organisation's security. This is necessary to ensure FinSure Bank can withstand challenges and last long in the financial sector.

Contents

1	Introduction	5
1.1	ISO/IEC 27001	5
1.2	NIST Cybersecurity Framework 2.0	6
1.3	COBIT 2019	7
1.4	ITIL v4	8
1.5	GDPR and Data Protection Act 2018	9
2	Proposed Integrated Cybersecurity and Governance Model for FinSure Bank (FSB)	10
2.1	Strategic Security Architecture for FSB	10
2.2	Governance and Compliance Implementation Plan	11
2.3	Risk and Security Management Plan	11
2.4	Operational and Service Management Plan	12
2.5	Core Infrastructure and Asset Layer	12
2.6	Security Policy Architecture for FinSure Bank (FSB)	12
2.6.1	Security Policies and Hierarchy	12
2.6.2	Core Security Policies for FSB	13
2.7	Risk Prioritisation and Control Measures	13
2.8	Implementation Roadmap	13
2.9	Impact and Benefits of the proposed method	14
3	Conclusion	15
	References	16

List of Figures

1	ISO/IEC 27001 with Annex A Control Categories	6
2	NIST CSF Implementation Tiers	7
3	COBIT 2019 domains	8
4	ITIL 4 Service Value System (SVS)	8
5	Proposed Integrated Cybersecurity and Governance Model for FinSure Bank (FSB) . . .	11

List of Tables

1	Risk Assessment and Control Measures for FinSure Bank	13
---	---	----

List of Abbreviations

ISO	International Organization for Standardization
IEC	International Electrotechnical Commission
ISMS	Information Security Management System
NIST	National Institute of Standards and Technology
CSF	Cybersecurity Framework
COBIT	Control Objectives for Information and Related Technologies
ITIL	Information Technology Infrastructure Library
GDPR	General Data Protection Regulation
CISO	Chief Information Security Officer
DPO	Data Protection Officer
BYOD	Bring Your Own Device
MFA	Multi-Factor Authentication
MDM	Mobile Device Management
DPIA	Data Protection Impact Assessment
RBAC	Role-Based Access Control

1 Introduction

Cloud computing, mobile applications, and interconnected systems are vital to many organisations' data storage and service delivery in the modern age. While these technologies provide greater efficiency, they also pose serious risks to organisations through cyberattacks, including unauthorised access and data breaches [1, 2].

In the UK there are rules about how to protect data like the UK General Data Protection Regulation and the Data Protection Act 2018. These rules say that organisations have to handle data in a fair and transparent way. Non-compliance can result in significant financial penalties and/or lose the public's confidence in the organisation [3, 4].

In order to address these risk factors, organisations will implement structured security and governance frameworks. This report evaluates four key frameworks that an organisation can adopt ISO/IEC 27001, NIST Cybersecurity Framework 2.0, COBIT 2019, and ITIL 4 and whether they strengthen the organisation's overall data security, governance, and compliance. Further, this report will present a customised integrated cybersecurity and governance model for FinSure Bank (FSB), a cloud-based financial service provider, that faces risks related to data protection; BYOD practices; a unified governance framework; and complying with regulations.

1.1 ISO/IEC 27001

It is a system designed to manage an organization's security needs. The Plan-Do-Check-Act (PDCA) cycle is used for continuous improvement and risk based approach of ensuring confidentiality of information post-risk analysis & controls put forth. It provides a credible model demonstrating a company's dedication towards data privacy management system. It is known all over the world, irrespective of its scale and type. [5–7]

Annex A

Annex A lists 93 controls across four categories [5, 6]:

- Organisational controls
- People controls
- Physical controls
- Technological controls

Application to FinSure Bank (FSB)

FSB does not have a system to manage everything and a plan to deal with risks. If the FSB uses the ISO/IEC 27001 standard it can find risks see how bad they are and make them less of a problem. The FSB has to deal with risks from using cloud infrastructure keeping data safe and letting people use their own devices for work [8, 9].

The rules in Annex A can help the FSB make rules for who can access what how to protect data and how to work with suppliers. This will help the FSB follow the rules, for protecting data in the United Kingdom and make customers trust the FSB. The FSB really needs to follow these rules to keep customer data safe and build trust with them.

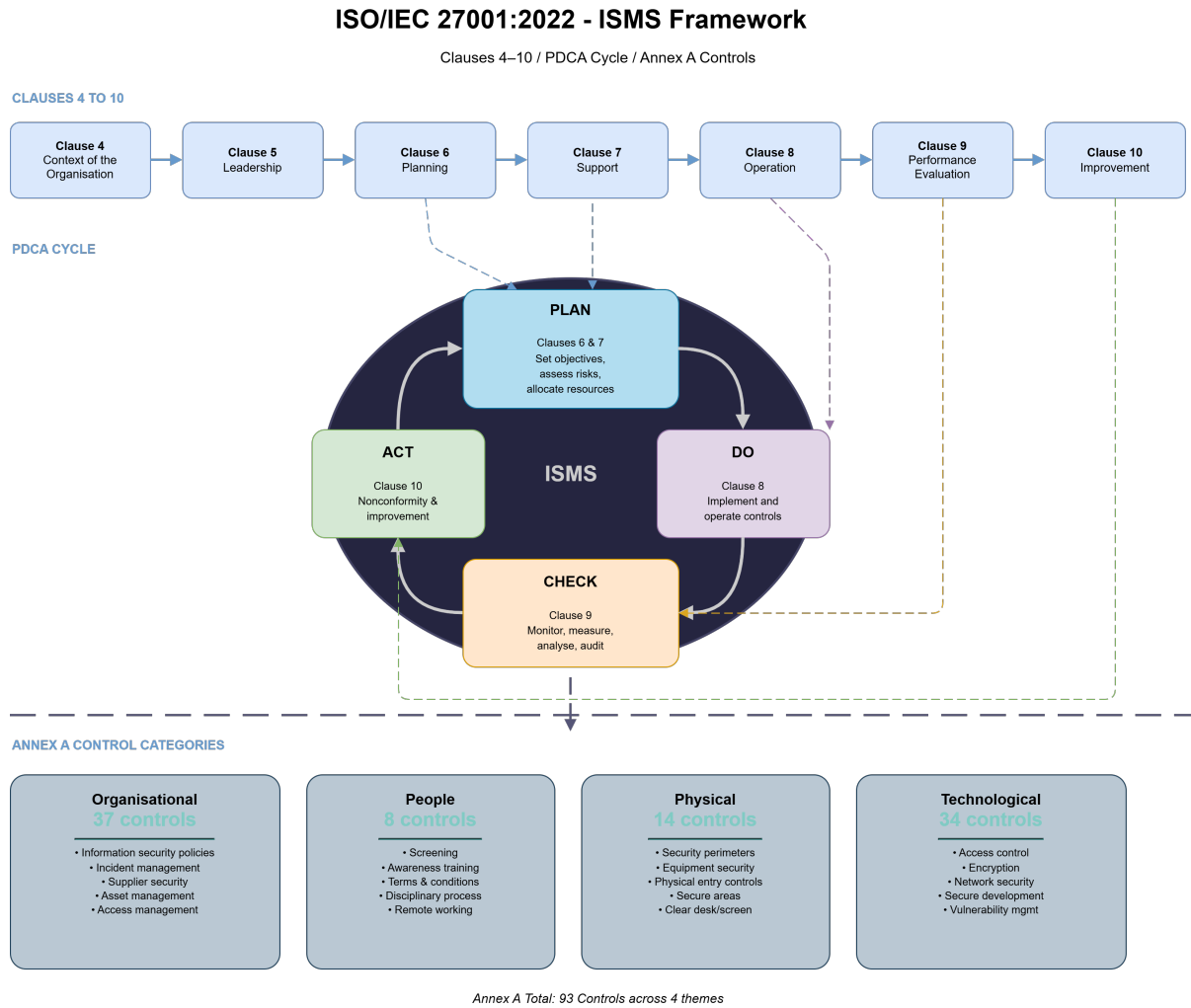


Figure 1: ISO/IEC 27001 with Annex A Control Categories

1.2 NIST Cybersecurity Framework 2.0

NIST Cybersecurity Framework 2.0 is developed by the U.S. National Institute of Standards and Technology in partnership with industry, academia and government. This framework helps organizations manage and reduce their cybersecurity risk in a way. It is based on six areas: Govern, Identify, Protect, Detect, Respond and Recover and profiles for comparing current versus target states. These areas have levels of maturity from Partial, to Adaptive, which help organizations see how well they are doing. [5,10]

Implementation Tiers

These tiers make it easier for organisations to see exactly where they stand right now and give them a clear path to level up their cybersecurity maturity [5].

- Tier 1 (Partial): Ad-hoc and reactive processes with limited risk awareness.
- Tier 2 (Risk-Informed): Some risk understanding exists, but implementation remains inconsistent.
- Tier 3 (Repeatable): Procedures have been developed and consistently followed.
- Tier 4 (Adaptive): Proactive, dynamic, and continually improving methods.

Application to FinSure Bank (FSB)

The FSB's security practices seem to be ad-hoc and reactive in nature (e.g., likely they are at the Tier 1 level). The framework gives a thorough plan for attaining Tier 3 (Repeatable) or Tier 4 (Adaptive)

NIST CSF 2.0 - Six Core Functions

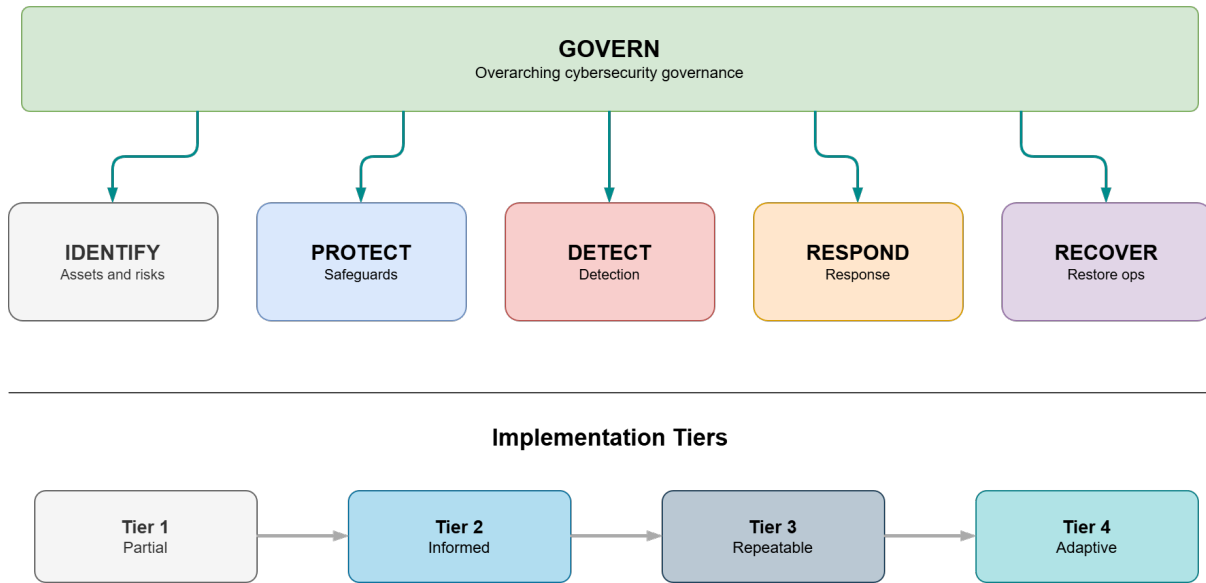


Figure 2: NIST CSF Implementation Tiers

stages of development. The Govern and Identify functions will provide a governance structure and create awareness of risk, while Profiles will show the relevant areas where there are gaps in data protection, third-party risks, or incident response and thus assist with ongoing improvement and making strategic decisions.

1.3 COBIT 2019

COBIT which stands for Control Objectives for Information and Related Technologies, was created in 2019 by the Information Systems Audit and Control Association also known as ISACA. This framework is really useful for managing the information technology of an organization. It helps organizations make sure their information technology is working well with their business goals. COBIT provides guidance on managing risk. Following laws, regulations, rules and policies when it comes to information technology [11, 12].

The COBIT framework is made up of 40 objectives for governing and managing information technology. These objectives are divided into five groups: EDM, APO, BAI, DSS and MEA. These five groups help organizations govern and manage their information technology, which's really important for COBIT [13–15].

Application to FinSure Bank (FSB)

FSB does not have a unified governance framework in place; adopting COBIT 2019 as a model for defining clear roles, responsibilities, and accountability for all staff members across the company will improve those areas at FSB. Using COBIT's five domains as a guide, FSB would be able to build out a security strategy, improve how IT assets are managed, and provide for ongoing assessment of governance controls and regulatory compliance.

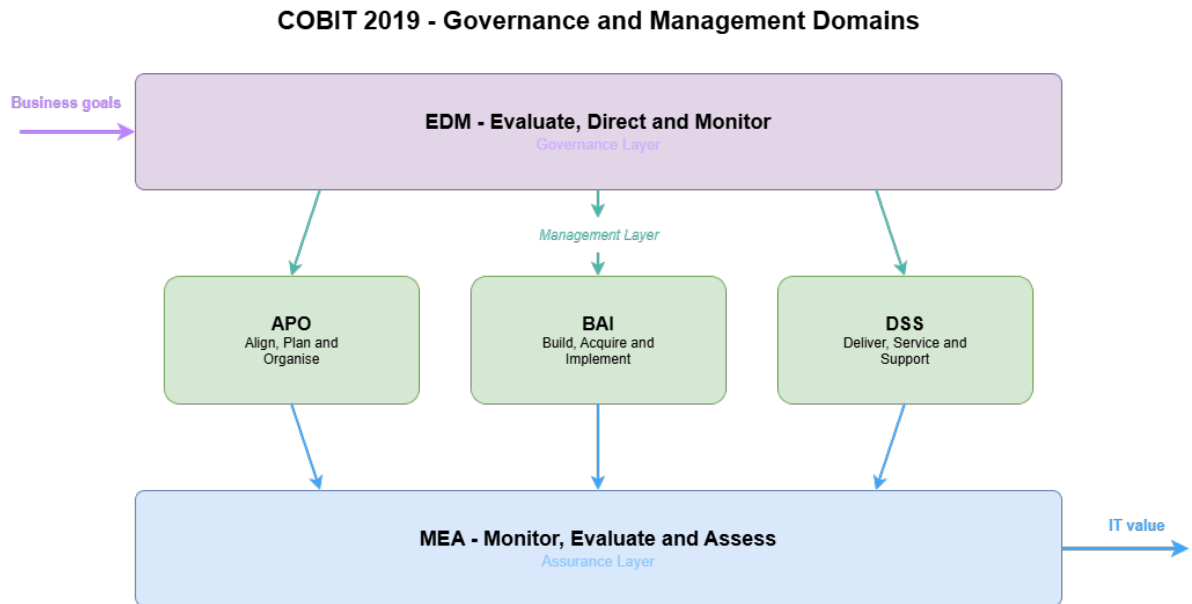


Figure 3: COBIT 2019 domains

1.4 ITIL v4

The ITIL 4 Framework is a worldwide standard for managing IT services. The framework provides best practice methods to help organizations with the design, delivery, and continued improvement of IT services, which ultimately provide genuine value to customers and other stakeholders. The most important component of the framework is the Service Value System (SVS), where the governance, the service value chain, the management techniques (including information security management) and the continuous improvement are synchronized in order to deliver services in tune with the strategic needs of the organization in a flexible and agile way. [16].

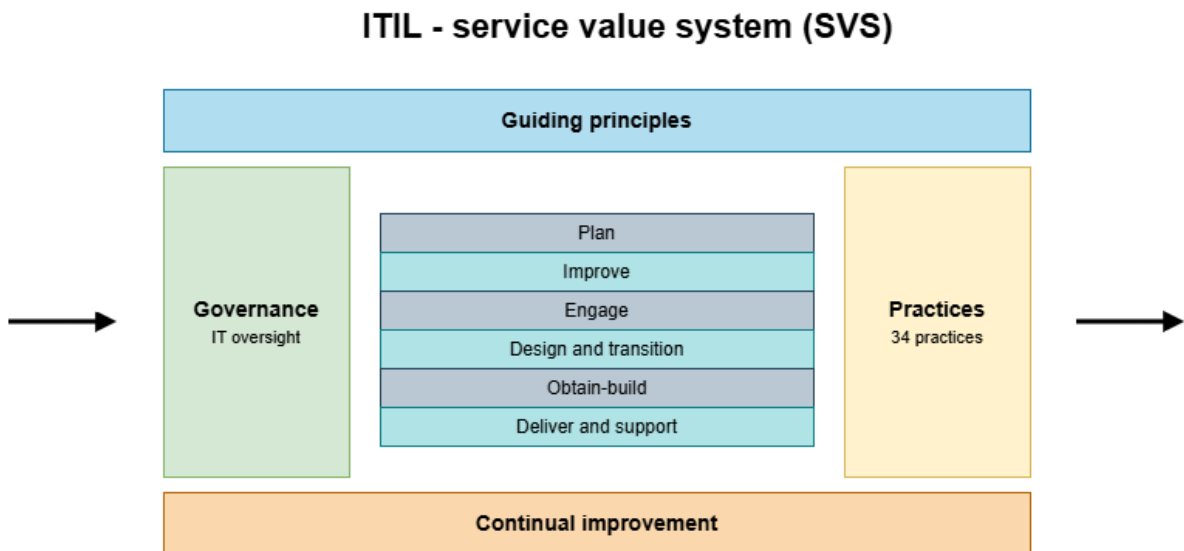


Figure 4: ITIL 4 Service Value System (SVS)

Application to FinSure Bank (FSB)

FSB is a highly reliant company on cloud and digital services. ITIL 4 would help to incorporate security into routine service delivery and operations. The guiding principles and information security management

practice deal with the risks posed by BYOD, cloud providers and third parties since it increased the quality of services and resilience of operations.

1.5 GDPR and Data Protection Act 2018

These privacy regulations are: they protect people's personal data. Companies can't be sloppy with that data. They must do it in a transparent and fair way when they gather, use or store it. [3]

The regulation is founded on principles, including data minimization, purpose limitation, accuracy, accountability, and security. Organisations are required to implement appropriate technical and organizational measures that are in compliance with these principles. [3]

Failure to comply with GDPR can result in severe penalties. GDPR penalties can be severe both financially and reputationally, and for a sector such as financial services, loss of trust can be more costly than money. When taken seriously, GDPR is an important part of how an organization builds and sustains trust with its customers, regulators and suppliers and becomes an integral part of data management. [3]

Relevance to FinSure Bank (FSB)

FSB works with large volumes of personal and financial information every day, which automatically exposes them to GDPR in the limelight. Proper adherence to GDPR requires FSB to establish real protections. That includes encryption, access controls and data classification, but also the accountability component of things, with a specific Data Protection Officer, maintaining transparent records of what data is handled, and why, and prior to committing to anything with a high privacy risk, run impact assessments. [4].

2 Proposed Integrated Cybersecurity and Governance Model for FinSure Bank (FSB)

FSB operates in a fast-moving, heavily digital environment and that comes with a lot of exposure. Between its dependence on cloud infrastructure, the widespread use of personal devices for work, and a governance structure that currently lacks a unified governance structure, the organization faces a genuine mix of cybersecurity, regulatory, and operational risks. Data breaches, unauthorised access, and falling foul of UK data protection law aren't distant possibilities; they're live concerns that need a proper, joined-up response.

That's the starting point for what this report sets out. Rather than recommending a patchwork of separate fixes, the proposed model pulls together the most relevant elements of ISO/IEC 27001, the NIST Cybersecurity Framework 2.0, COBIT 2019, ITIL 4, and UK GDPR [1–3, 16] into something cohesive and workable. The idea isn't to layer five frameworks on top of each other; it's to take what each one does well and combine them into a single, practical approach that FSB can actually combine them into a layered and operational model over time.

2.1 Strategic Security Architecture for FSB

The model identified for FSB is a four-layer architecture approach for alignment between governance, risk management, operational processes, and supporting infrastructure:

- **Governance and Compliance Layer** - Provides the policy framework for the organization to establish accountability within a regulatory framework.
- **Risk and Security Management Layer** - Provides a structured framework for the identification and mitigation of risk to the organization.
- **Operational and Service Management Layer** - Provides efficient and keeps day-to-day IT operations running securely and efficiently, without sacrificing one for the other.
- **Core Infrastructure Layer** - Represents the underlying IT environment, including cloud systems, financial platforms, BYOD devices, and third-party services.

The four layers of the architecture allow an organisation to implement security throughout the organisation and ensure a coordinated and proactive manner in managing cybersecurity risks, instead of isolating or responding to cybersecurity controls after the fact. The diagram shows how the governance, risk management, operational and infrastructure functions all interoperate to create a cohesive cybersecurity architecture for FinSure Bank and how the governance function provides control to the operational function in a top-down manner, as well as a continuous feedback loop for monitoring and evaluating security practices and making improvements.

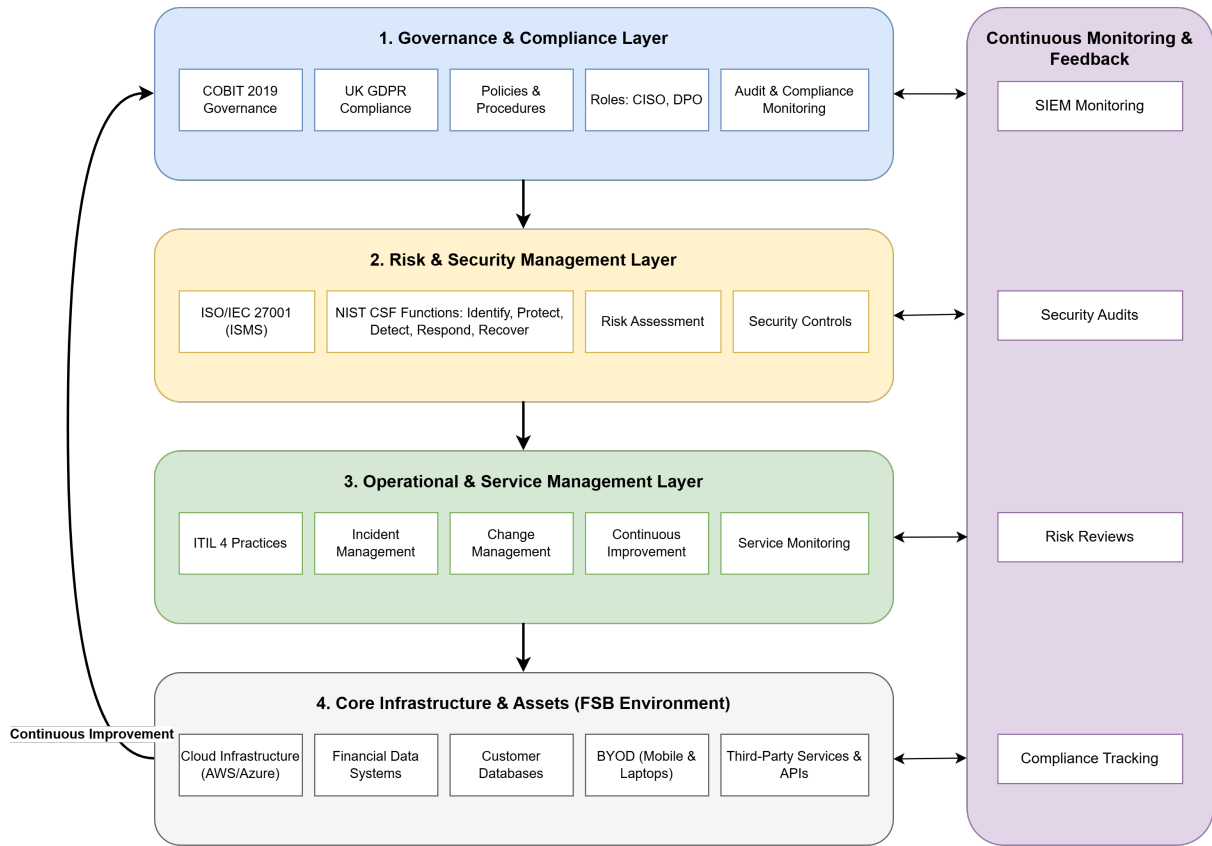


Figure 5: Proposed Integrated Cybersecurity and Governance Model for FinSure Bank (FSB)

2.2 Governance and Compliance Implementation Plan

None of the other pieces fall into place if governance is weak. FSB needs to sort out who is actually responsible for security decisions and that means putting real people in real roles, not just listing job titles in a document. Having a Chief Information Security Officer (CISO) and a Data Protection Officer (DPO) in place gives the organization a clear chain of accountability, which is something COBIT 2019 is pretty firm on [12].

Additionally, formal policies must be created with regards to access control, protecting data, and acceptable use of the data and periodically updated to ensure the organization continues to be protected against dynamic and emerging threats. Other compliance-related activities can be included within the workflow of the organization by incorporating such activities as maintaining records of processing activities, conducting Data Protection Impact Assessments (DPIA); conducting internal audits against ISO/IEC 27001 standards.

This will assure that the governance procedure is continuously observed, evaluated, and enhanced. As the governance structure is needed for accountability to be clearly determined and for decision-making to take place in a consistent manner across the entire organization, otherwise, security controls will not be applied in a consistent manner and will ultimately result in an increased likelihood of compliance failures as well as not effectively managing risk [17].

2.3 Risk and Security Management Plan

Good governance sets the direction, but risk management is where FSB has to get its hands dirty. That means actually knowing what assets matter most, what could realistically go wrong, and what needs to be done about it. ISO/IEC 27001 gives a solid structure for working through that process without cutting corners.

The NIST Cybersecurity Framework adds another useful lens here. Its five functions—Identify, Protect, Detect, Respond, and Recover aren't complicated in theory, but working through them properly forces

the organization to think about risk in a complete way rather than just focusing on prevention and hoping for the best [5, 10].

The threats FSB needs to keep a close eye on are pretty specific cloud vulnerabilities, the risk that comes from inside the organization, and the headaches that BYOD inevitably brings [18]. None of these are one-and-done problems. They shift, and the way FSB manages them has to shift too.

The real danger of skipping proper risk assessment isn't just leaving gaps it's spending time and money on the wrong things. Without a clear picture of where the biggest risks actually sit, it's easy to end up patching minor issues while something far more serious goes unnoticed.

2.4 Operational and Service Management Plan

To ensure that risk controls are effectively implemented, FSB must integrate security into its daily operations using ITIL 4 practices [16]. This includes structured processes for incident management, change management, and service monitoring.

Incident management ensures rapid response to security events, while change management prevents the introduction of new vulnerabilities. Continuous improvement practices enable FSB to refine its processes based on performance monitoring and incident analysis.

By embedding security within operational workflows, FSB can maintain both service efficiency and system resilience. To ensure that controls are enforced consistently in real-world situations, security must be integrated into operations. Without this integration, even well-designed security strategies may fail during implementation, leading to operational and security gaps.

2.5 Core Infrastructure and Asset Layer

Everything FSB does, every decision, every policy, every risk control ultimately depends on the technology underneath it all holding up. Cloud systems, financial platforms, customer databases, personal devices, third-party connections, this is the real world the organisation lives in, and it needs to be secured properly [19].

When something goes wrong at this level, the damage is immediate. Data gets exposed, systems go down, customer trust takes a hit. So the fundamentals have to be solid encryption, proper configurations, strict access controls, and eyes on the environment around the clock.

If the infrastructure is shaky, nothing built on top of it will save FSB. But when it's locked down properly, everything else, governance, risk management, operations, actually has something solid to stand on.

2.6 Security Policy Architecture for FinSure Bank (FSB)

A comprehensive cybersecurity framework requires a clearly articulated set of security policy architectures and the core policies upon which all governance, risk management, and operational controls are conducted within FSB.

A formalized policy framework will assist in mitigating risks, such as unauthorised access and data breaches, associated with FSB's cloud-based infrastructure and BYOD practices and will assist in adhering to UK GDPR requirements.

2.6.1 Security Policies and Hierarchy

To support the proposed cybersecurity model, FSB should implement a structured policy architecture aligned with ISO/IEC 27001 [7]. This ensures that security requirements are clearly defined and consistently applied across the organisation.

- **Level 1 - Policies**

High-level, board-approved documents defining overall security objectives and governance direction.

- **Level 2 - Standards**

Some mandatory technical requirements such as encryption, access control, and system configurations.

- **Level 3 - Procedures**

Step-by-step processes for implementing security controls in daily operations.

- **Level 4 - Guidelines**

Recommended best practices that support secure behaviour across the organisation.

This hierarchy ensures that governance decisions are translated into enforceable and operational security practices across all layers of FSB [11, 15, 20].

2.6.2 Core Security Policies for FSB

The following fundamental policies should be given top priority by FSB in order to address major risks:

- **BYOD Policy** - Ensures management of devices, separation of data, and secure use of personal devices [8].
- **Access Control Policy** - Implements role-based access and least privilege with strong authentication [6, 10].
- **Data Classification Policy** - Defines data sensitivity levels and appropriate protection measures [3].
- **Cloud Security Policy** - Ensures secure configuration, encryption, and monitoring of cloud services [19].
- **Incident Response Policy** - Sets up methods for identifying and responding to security [1].

2.7 Risk Prioritisation and Control Measures

After the creation of governance and policy frameworks, FSB should focus on major risks to guarantee efficient resource distribution. [1, 6, 10, 18]

Risk	Likelihood	Impact	Priority	Control Measure
Cloud data breach	High	High	Critical	Encryption, cloud audits
BYOD vulnerabilities	High	Medium	High	MDM, MFA
Insider threats	Medium	High	High	Access control, monitoring
Regulatory non-compliance	Medium	High	High	GDPR audits, DPO oversight
Third-party vendor risk	Medium	High	High	Vendor assessment, contracts

Table 1: Risk Assessment and Control Measures for FinSure Bank

The table finds the threats to FSB, which are the largest, and the risks of cloud-based account compromise and BYOD as high-priority threats. The vulnerabilities associated with the reliance of FSB is cloud-based data breaches and BYOD on cloud computing and remote working. By appreciating risks in the sense of the probability of occurrence and the effect that would be caused in case it occurred, FSB is able to determine where to concentrate its assets regarding adopting more efficient and organized ways of dealing with cybersecurity risks.

2.8 Implementation Roadmap

To successfully implement the proposed cybersecurity model, FSB should follow a phased approach:

- **Phase 1 - Assessment**
Do a gap analysis to assess existing security measures and pinpoint vulnerabilities.
- **Phase 2 - Governance and Policy Development**
Establish governance structures and implement the security policy framework.
- **Phase 3 - Technical Implementation**
Use encryption, multi-factor authentication, and surveillance.
- **Phase 4 - Training and Awareness**
Teach staff about cybersecurity rules, risks, and legal duties.

- **Phase 5 - Monitoring and Continuous Improvement**

Regularly check systems, run audits, and update security based on feedback and new threats.

2.9 Impact and Benefits of the proposed method

FSB's integration of governance frameworks, security policies and risk management processes represents a holistic solution to its existing challenges.

This model not only enhances data protection, reduces the risk of cyber attacks and ensures compliance with the UK GDPR, but also enhances operational efficiency by embedding security into all operational processes and allowing for improved decision-making.

Moreover, implementing this model increases the level of customer trust in FSB, which in turn helps to create a robust long-term organisational resiliency strategy. In moving from a reactive to a more mature, properly-governed approach to cybersecurity, FSB is establishing a foundation for a successful long-term strategy for establishing its trustworthiness with customers.

3 Conclusion

As discussed within this report, a variety of established cybersecurity frameworks were identified, including ISO/IEC 27001, NIST CSF 2.0, COBIT 2019 and ITIL 4 as used to assist organisations on effectively managing their risks associated with cybersecurity. Each of these frameworks has its own viewpoint on cybersecurity through such means as governance, risk management and operational practices, thus reinforcing the importance of a holistic approach to cybersecurity.

Utilising these results a customised model has been developed specifically for FinSure Bank (FSB), focusing upon its dependency on cloud services, BYOD policies and adherence to regulations. The layered methodology outlined within this report illustrates the means whereby FSB's governance, risk management, operational processes and technological infrastructure will work together as one to achieve enhanced security control.

The results of the analysis indicate that there must be a fully integrated and structured approach to cybersecurity within all modern financial organizations. The adoption of the development model outlined in detail within this report will bolster FSB's cybersecurity posture, assist with compliance to the UK General Data Protection Regulations (GDPR), and further establish its preparedness for new evolving threats from cyber attackers; thereby ensuring the organisation is capable of maintaining its long-term security and continuing earning trust from stakeholders.

References

- [1] S. Romanosky, “Examining the costs and causes of cyber incidents,” *Journal of Cybersecurity*, vol. 2, no. 2, pp. 121–135, 2016.
- [2] R. Anderson, C. Barton, R. Böhme, R. Clayton, M. J. Van Eeten, M. Levi, T. Moore, and S. Savage, “Measuring the cost of cybercrime,” in *The economics of information security and privacy*, pp. 265–300, Springer, 2013.
- [3] European Parliament and Council of the European Union, “Regulation (EU) 2016/679 (General Data Protection Regulation),” 2016. Official Journal of the European Union.
- [4] M. Mourby, H. Gowans, S. Aidinlis, H. Smith, and J. Kaye, “Governance of academic research data under the gdpr—lessons from the uk,” *International Data Privacy Law*, vol. 9, no. 3, pp. 192–206, 2019.
- [5] B. Reuben-Owoh and E. Haig, “A systematic review of voluntary cybersecurity standards and frameworks: B. reuben-owoh, e. haig,” *International Journal of Information Security*, vol. 24, no. 5, p. 206, 2025.
- [6] G. Culot, G. Nassimbeni, M. Podrecca, and M. Sartor, “The iso/iec 27001 information security management standard: literature review and theory-based research agenda,” *The TQM Journal*, vol. 33, no. 7, pp. 76–105, 2021.
- [7] K. Ryanto and V. Tundjungsari, “Standardization of information security management in the banking sector using the iso 27001: 2022 framework,” *Journal La Multiapp*, vol. 5, no. 4, pp. 361–379, 2024.
- [8] R. Palanisamy, A. A. Norman, and M. L. M. Kiah, “Byod policy compliance: Risks and strategies in organizations,” *Journal of Computer Information Systems*, vol. 62, no. 1, pp. 61–72, 2022.
- [9] J. Chigada and N. Daniels, “Exploring information systems security implications posed by byod for a financial services firm,” *Business Information Review*, vol. 38, no. 3, pp. 115–126, 2021.
- [10] C. Pascoe, S. Quinn, and K. Scarfone, “The nist cybersecurity framework (csf) 2.0,” 2024.
- [11] ISACA, *COBIT 2019 Framework: Governance and Management Objectives*. ISACA, 2019.
- [12] T. R. McIntosh, T. Susnjak, T. Liu, P. Watters, D. Xu, D. Liu, R. Nowrozy, and M. N. Halgamage, “From cobit to iso 42001: Evaluating cybersecurity frameworks for opportunities, risks, and regulatory compliance in commercializing large language models,” *Computers & Security*, vol. 144, p. 103964, 2024.
- [13] C. Anoruo, “Employing cobit 2019 for enterprise governance strategy,” *ISACA Journal*, 2019.
- [14] A. Amry, Y. Wirani, and Y. G. Sucahyo, “Assessment of it governance capability level using the cobit 2019 framework: A case study of xyz institution,” *JEPIN (Jurnal Edukasi dan Penelitian Informatika)*, vol. 11, no. 2, pp. 277–286, 2025.
- [15] S. De Haes and W. Van Grembergen, “Enterprise governance of information technology: Achieving alignment and value with cobit,” *Information Systems Management*, 2020.
- [16] M. A. Adegbite, “Data privacy and data security challenges in digital finance,” *Journal of Digital Security and Forensics*, vol. 2, no. 1, pp. 6–19, 2025.
- [17] L. Magnusson, S. Iqbal, P. Elm, and F. Dalipi, “Information security governance in the public sector: investigations, approaches, measures, and trends,” *International Journal of Information Security*, vol. 24, no. 4, p. 177, 2025.
- [18] S. Subashini and V. Kavitha, “A survey on security issues in service delivery models of cloud computing,” *Journal of network and computer applications*, vol. 34, no. 1, pp. 1–11, 2011.
- [19] Y. Alghofaili, A. Albattah, N. Alrajeh, M. A. Rassam, and B. A. S. Al-Rimy, “Secure cloud infrastructure: A survey on issues, current solutions, and open challenges,” *Applied Sciences*, vol. 11, no. 19, p. 9005, 2021.
- [20] B. Von Solms, “Information security governance: Cobit or iso 17799 or both?,” *Computers & Security*, vol. 24, no. 2, pp. 99–104, 2005.