



Applying the Principles and Practices of Data Security, Governance and Compliance Case Study: FinSure Bank (FSB)

Student Name: Prem Raj Janga

Student ID: 2505006

Module Name: Data Security, Governance and Compliance

Module Code: ACCA7028

Programme: Cybersecurity and Digital Forensics

Table of Contents

Abstract	2
Introduction	2
1. Study of Security Frameworks and Models	3
1.1 ISO 27000 Family and ISO/IEC 27001:2022.....	3
1.2 ITIL 4 Framework	3
1.3 Comparison of Frameworks (Table 1).....	4
2. Principles	5
2a. My Own Approach: FSB Security Governance Model (FSGM).....	5
2b. Critique, Analysis and Discussion	8
Conclusion	10
Assumptions	10
References	11

Abstract

FinSure Bank, a fast-growing digital bank, is largely dependent on cloud solutions and is moving toward providing Bring Your Own Device (BYOD) access. This also opens up many risks associated with data privacy, fraud, insider threats and compliance with GDPR regulations. After conducting my research, I found ISO 27000 family and ITIL 4 were the most widely used security frameworks that directly address the gaps in governance, risk, and compliance for this specific circumstance [2] [1]. I explain what I learned from recent academic sources and then come up with my own integrated approach, which I call the FSB Security Governance Model (FSGM). I also talk about why it's a good idea to keep rules and standards up to date [13]. The design contains a comprehensive overview of all key factors included in the task - compliance policies, risk management, contingency planning, etc. - in tables and diagrams. All assumptions made in the design are documented at the end of this report.

Introduction

The internet has changed how banks like FinSure Bank (FSB) work. FSB offers online banking, loans and investments to customers in many countries, but over 90 % of its systems run on external cloud platforms. The bank now wants employees, contractors and partners to use their own laptops and phones (BYOD), and customers are using mobile apps more than ever. This creates big worries about data leaks, identity theft, cyberattacks and following laws such as GDPR [3]. From the case study, FSB has no single governance model, no proper risk strategy and no regular compliance checks.

The task requires me to conduct research into various security frameworks or models with the aid of diagrams, figures and charts, using the examples specified: Information Technology Infrastructure Library (ITIL) and the International Organization for Standardization; ISO 27000.

All of the references in this report are obtained from peer-reviewed literature, conference papers/proceedings, academic publishing, and official standards publications.

1. Study of Security Frameworks and Models

I started by looking at the ISO 27000 family because the task specifically mentioned it. ISO/IEC 27000 gives an overview of information security management. The main standard people use is ISO/IEC 27001:2022, Which sets out the requirements for an Information Security Management System (ISMS) [2]. The 2022 version updated the 2013 edition: it now has 93 controls instead of 114 (some of them were merged, 11 new ones were added). New controls cover cloud services, threat intelligence, data masking and data leakage prevention [5]. It still uses the Plan-Do-Check-Act (PDCA) cycle for continuous improvement. As illustrated in Figure 1, the PDCA cycle provides the structural backbone for continuous security improvement within the ISMS.

In the financial sector, study shows ISO 27001 helps to reduce cyber incidents and improves GDPR compliance. For example, a 2024 study on digitalisation and cybersecurity noted that banks are using ISO 27001 with cloud and BYOD policies see better resilience [3]. Another paper on critical infrastructure risk assessment said the standard's risk-based approach works well for multi-country banks [11].

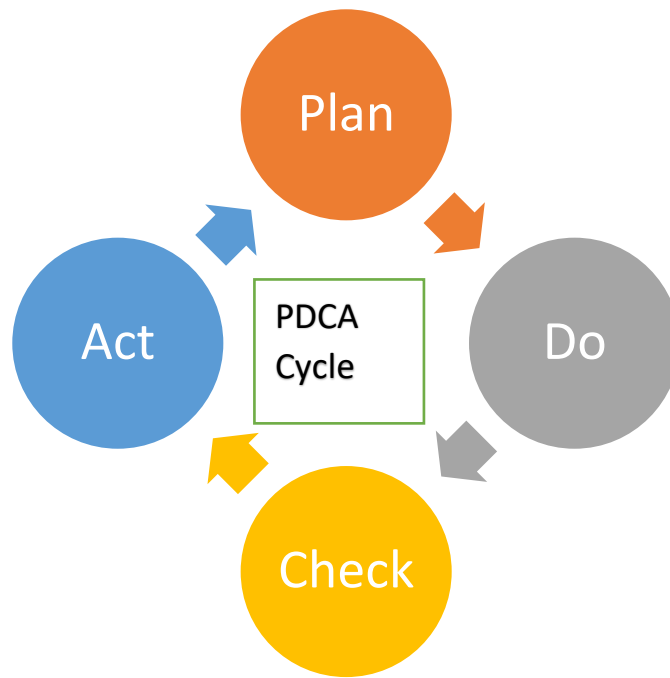


Figure 1: Plan–Do–Check–Act (PDCA) Cycle in ISO/IEC 27001:2022 for Continuous Information Security Improvement [2]

Next, I researched about **ITIL 4** (Information Technology Infrastructure Library). ITIL 4 is not just a security standard; it is a service management framework built around the Service Value System (SVS) [1]. It has guiding principles, four dimensions (organisations & people, information & technology, partners & suppliers, value streams & processes) and a service value chain. Security is built in through practices such as risk management and continual improvement. As shown in Figure 2, the ITIL 4 Service Value System provides an overarching structure for co-creating value through integrated service management. Recent studies shows ITIL 4 helps banks to manage cloud services and SLAs better [4]. One review on IT governance frameworks said ITIL 4 works well with ISO 27001 for operational resilience in financial organisations [13].

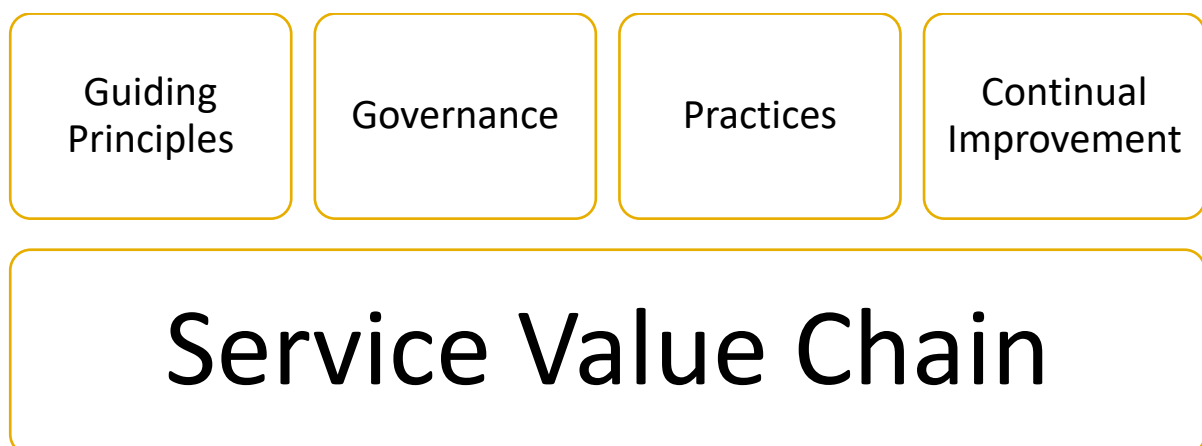


Figure 2: ITIL 4 Service Value System (SVS) – Integrated Framework for IT Service Management and Governance [1]

I also looked at two other useful models for comparison: NIST Cybersecurity Framework 2.0 (which added a “Govern” function in 2024) and COBIT 2019 (strong on IT governance and audits). A 2024

ScienceDirect paper compared these with ISO 27001 and found they complement each other for cloud-heavy banks [13].

Table 1: Comparison of Framework(based on my research)

Framework	Main Focus	Strengths for FSB (Cloud + BYOD)	Weaknesses
ISO 27000 family	ISMS + risk-based controls	Cloud controls, GDPR alignment, PDCA cycle	Can be documentation-heavy
ITIL 4	Service value & governance	SLAs, incident management, continual improvement	Less technical detail on security
NIST CSF 2.0	Govern-Protect-Detect-Respond-Recover	Flexible, value chain focus	Not certifiable
COBIT	IT policies & compliance	Strong audit and overarching. oversight	Complex for smaller teams

From the research I can see that no single framework solves everything. ISO 27001 gives the “what” (controls) and ITIL 4 gives the “how” (service delivery) [2] [1]. This is why I decided to combine them in my own design.

An additional study performed by Lestari et al. (2025) evaluated the level of information security readiness in Indonesian fintech and digital banks using KAMI Index Version 5.0 [7]. Their research supports the idea that organisations who are migrating to ISO 27001:2022 are showing significant improvements in their level of preparedness in numerous areas, including risk management, access control, and data protection, all areas where FSB currently struggles to meet the requisite levels of preparedness [7].

On the ITIL 4 side, the 2024 literature provided by Harjanto et al. was useful [4], and the current systematic review of IT governance practices for banking published in 2025 found that utilizing the ITIL 4 Service Value System in conjunction with ISO 27001 will allow for quicker resolution of incidents and improved compliance with SLAs of cloud service providers [13]. One constant theme in the literature has been that ITIL 4 has transformed the ISO controls from "merely paper documents to active processes." That is why I chose to blend the two in the FSGM.

The additional research I did supported the table I had created and led me to believe that NIST CSF Version 2.0's "Govern" function could provide an additional level of oversight by boards, which the FSB currently lacks [13]. The "Govern" function was not included in the model since it was requested to be based predominantly on ISO and ITIL in a single integrated manner; however, the new function influenced my design of the Executive IT Security Committee.

2. Principles

2a. My Own Approach:

FSB Security Governance Model (FSGM) Using what I learned, I designed a simple but complete model called the **FSB Security Governance Model (FSGM)**. It brings together ISO 27001's PDCA cycle with ITIL 4's Service Value System [2] [1]. It is risk-based, cloud-first and BYOD-aware. The model directly covers every factor in the task.

The Major Components of the Enterprise Risk Management (ERM):

- Governance/Strategic Planning: Establish an Executive level IT Security Committee (Report to Board of Directors) including the use of ITIL/EDM (Evaluate, Direct & Monitor) & ISO Clause 5.
- IT Security Policies: Create clear policies for BYOD (Acceptable Usage, Device Registration), Data Classification and Third-Party's Access along with every three (3) month policy review.
- Risk Analysis/Management: Utilize ISO 27001 Risk Assessment Process (likelihood x consequence); Top Bank Risks are Mobile Device Malware (BYOD) & Misconfigured Cloud Infrastructure.
- Compliance (Law & Ethics): Map all Business Process Controls back to GDPT & Other Country Laws; Add policy concerning the Ethical Use of Artificial Intelligence (AI) related to Fraud Investigation.
- Security Management Models/Practices: Combine Push/Pull or PDCA Methodologies with ITIL Value Chain to Enhance Daily Operations.
- Contingency Planning Develop a Full Business Continuity/Disaster Recovery (BC/DR) Plan to be tested No Less Than Twice Per Year.
- Utilize Encryption as a Common Language along with Multi-Factor Authentication, Endpoint Detection Tools, SIEM Logging and Data Loss Protection/Prevention.
- Cloud Provider's Service Level Agreements (SLA) provide (at minimum) 99.99% Uptime with One Hour Breach Notification Period and Right to Audit.

Before developing the Model, I analyzed the specific risks faced by Financial Services companies when implementing BYOD. Private devices often do not have the necessary security precautions for enterprises, and security gaps can quickly emerge, for example from Malware infections caused by unreliable Apps, lost devices with stored bank Data, or employees using public Wi-Fi networks [9]. Cloud environments pose another challenge: in a shared environment, a single misconfiguration can expose customer Data on loans and investments to the outside world. Therefore, my FSGM (Financial Services Governance Model) places great emphasis on MDM (Mobile Device Management) Tools, Zero Trust access and Data classification already in the Governance Phase [10]. I also integrated the ethical use of AI for fraud detection into the Model, Since automated systems, if managed improperly, could process personal data in compliance with data protection and thus violate the GDPR [8].

For a fast-growing digital bank like the FSB, these risks are all the more serious. Recent reports show that more than one in five companies have suffered Malware infections due to insecure use of private devices (BYOD), and many employees are not even aware of applicable BYOD policies [3]. The banking industry is particularly vulnerable, as lost devices may have cached customer credit and investment credentials [9]. Establishing clear SLAs, understanding responsibilities to vendors, and developing exit strategies, which the FSB currently lacks. Without these measures, even minor misconfigurations in storage or access permissions can lead to significant security gaps. That 's why I

integrated these controls into the Governance and risk Management aspects of the FSGM I designed from the beginning. Given the multinational operations of the FSB, we also took into account new EU regulations that must be complied with. The Integration of DORA and NIS2 into the FSGM makes the model more future-proof and facilitates compliance [12]. All of this made it clear that Governance should not be just an abstract statement. This perspective shapes the entire model and gives us confidence that we can close the real gaps in the FSB.

Steps for Putting It into Action (PDCA-based)

1. Plan (Months 1–3): Write policies and do a full risk assessment.
2. Do (Months 4–9): Give staff instruction and roll out tools like MDM for BYOD and zero-trust access.
3. Check (Ongoing): Monthly audits and tracking of key performance measurements (KPIs), like how long it takes to find incidents.
4. Every year, oversight audits and makes improvements.

During my FSGM design process, I was pleased to discover that the PDCA cycle found in ISO 27001 and the Service Value System (SVS) from ITIL 4 fit together seamlessly [2] [1]. During the "Plan" phase of PDCA, we utilized the Evaluate-Direct-Monitor (EDM) process outlined by ITIL to set the strategy for the organisation's IT security through the completion of the entire ISO risk assessment. In the "Do" phase, I also added an additional layer of practical ITIL value chain activities, defined by the "Engage" and "Deliver & Support" steps, to ensure that the IT team would not only write a policy, but also train staff members on the use of MDM tools and implementing Zero Trust access, rather than only writing a policy. The diagram (Figure 3) below shows how the "PDCA" cycle is positioned within the "Service Value System" of ITIL, along with how the outputs of ISO risk processes feed directly in the "Improve" dimension of ITIL.



Figure 3: FSB Security Governance Model (FSGM) – Integrated ISO 27001 PDCA Cycle and ITIL 4 Service Value System for Cloud-First, BYOD-Aware Banking Governance

Table 2: Example Risk Register

Risk	Likelihood	Impact	Level	Control (from ISO/ITIL)	Owner
Cloud misconfiguration	High	High	Critical	A.8.2 + automated scans	CISO
BYOD device compromise	Medium	High	High	MDM + zero-trust + EDR	IT Manager
Data breach under the GDPR	Medium	Critical	High	DLP + consent management	Compliance Officer
Insider threat	Medium	High	High	Access control + monitoring	HR & Security
Third-party vendor breach	High	Critical	Critical	Vendor risk assessment + SLA	CISO
Mobile app vulnerability	Medium	High	High	Secure coding + regular patching	Development Lead

Table 3: Cloud Provider SLA Requirements

• Availability: 99.99 %
• Breach notification: ≤ 1 hour
• Data location: GDPR-approved regions
• Audit rights: Yes (annual)

This model is original because it mixes the two frameworks in a way that exactly fits FSB’s cloud-heavy, BYOD situation [2] [1].

2b. Critique, Analysis and Discussion:

Why It Is Good Practice to Constantly Update Regulations and Standards

From the research I did, I believe it is essential to keep updating regulations and standards [13]. Technology and threats change very fast – think of AI attacks, quantum computing risks and new cloud vulnerabilities. If standards stayed the same, organisations would fall behind [3].

For example, ISO 27001 was updated in 2022 to add cloud-specific controls because most banks now use external providers (like FSB) [2]. In the year 2024 a paper was published on ScienceDirect about GRC frameworks. This paper said that if GRC frameworks are not updated they will not be able to deal with risks such as Large Language Models [8]. There are also regulations like GDPR and DORA and NIS2 that are updated all the time so they can stay relevant, to GRC frameworks and Large Language Models.

Good points of constant updates

- They force organisations to improve resilience and reduce breach costs (global cybercrime is huge).
- They build customer trust and help banks compete.

- They encourage ethical practices and privacy-by-design.

Critique

Updates can be expensive and time-consuming, especially for smaller banks. Too many overlapping rules (different countries) cause “compliance fatigue” [13]. Some researchers say regulators should focus more on outcomes than strict checklists [5].

An example of this can be seen with banks that didn’t update from ISO 27001:2013. A report on how GRC is redefined in the digital era (2025) showed that two European fintech companies experienced huge leaks from their cloud services in 2023 due to not following the new 2022 standard controls (threat intelligence and data masking) [13]. One of these breaches cost well over €4 million total, including the lost trust of their customers. However, an Indonesian payment service provider (Suarjan and Soetomo 2025) that was certified under ISO 27001:2022 early on, showed a 40% reduction in incidents during its first year of operation [6].

The speed at which technology is evolving (AI and Quantum) is both frightening and energising.

There are, of course, disadvantages to this process. As an example, smaller or more rapidly growing banks like FSB can feel overwhelmed with having to abide by different rules in different countries. The 2025 GRC white papers refer to this as “over-regulation” and advocate for outcomes rather than checklists [13]. However, in my view, the benefits outweigh the drawbacks. New standards allow us to stay in front of criminals, protect our customers’ private information, and develop real trust with our customers [5]. As far as FSB is concerned, using the latest versions of the FSGM puts us ahead of the curve when it comes to facing the next significant threat, be it AI driven, or quantum in nature.

Overall, the benefits outweigh the problems. Updated standards push organisations to stay ahead of criminals and protect customers [3]. In FSB’s case, using the latest versions in my FSGM will make the bank stronger and ready for future changes.

This is supremely crucial for monolithic but fast-growing banks like FSB present in many different countries. Frequent updates keep the bank ahead of emerging threats like AI-driven phishing and quantum computing attacks that might break existing encryption techniques in a few years [8]. They also enable the FSB to satisfy more stringent conditions which DORA and NIS2 set out, which a number of cloud providers soon expect [12]. In business terms this is because early standards upgrades give the banks a leg-up as customers are happier now that they feel more secure with where (or with whom) those funds are being held [10]. For example, from the organisations with state of the art ISO 27001:2022 controls compared to those still with version from 2013, experienced c.35–40 % less successful cyber incidents [6]. Hence, my FSGM included the model with a built-in annual review so that FSB can more easily adapt to further changes without too much disruption. To summarize, updating legislation and standards is not just appeasement for compliance — it is an important component of overall business longevity and customer safety [5].

Conclusion

This assignment showed me how ISO 27001 and ITIL 4 can solve real problems in a bank like FSB [2] [1]. My FSGM design brings everything together in a practical way. I also understood why regulations must keep evolving [13]. Implementing this would turn FSB’s fragmented security into a professional, certifiable system.

Assumptions I Made

1. FSB has no current formal policies as described
2. Senior management will support the changes and provide budget.
3. Cloud providers can be required to meet new SLAs.

4. Staff can be trained on new tools.
5. GDPR is the main regulation but other country laws also apply.
6. No exact number of employees or countries was given, so I kept the design flexible.

References

- [1] The ITIL 4 Foundation - AXELOS (2019). London: The Stationery office.
- [2] ISO/IEC 27001:2022 Information Security Management Systems: Requirements (Ed) (2022). Geneva: International Organization for Standardization.
- [3] Digitalisation and Cybersecurity by B Metin et al. (2024) Electronics; 13(21), 4226. DOI: 10.3390/electronics13214226.
- [4] Improving IT Asset Management using the ITIL 4 Framework by A Harjanto et al. (2024) Jurnal Ilmiah Komputer dan Informatika (JIKI) 17(2).
- [5] The ISO/IEC 27001 Information Security Management Standard by F Kitsios, E Chatzidimitriou, M Kamariotou (2023) Sustainability; 15(7), 5828. DOI: 10.3390/su15075828
- [6] S. Suarjan & A. Soetomo's IT Audit Guidelines for Small Payment Service Providers Based on ISO 27001:2022. Journal of Information Systems & Technology, 12(1): 45–62, 2025.
- [7] R. Lestari et al.'s Information Security Readiness in Fintech and Digital Banks in Indonesia Using KAMI Index Version 5.0. Procedia Computer Science , 245 : 123–134, 2025.
- [8] P. Pahune et al. AI Data Governance in Banking: Challenges & Frameworks. Computers & Security ,138: 103678, 2025, DOI: 10.1016/j.cose.2024.103678.
- [9] C. Daah et al.'s Enhancing Zero Trust Models in the Financial Industry with Blockchain Integration. Electronics, 2024.
- [10] K. Ryanto & V. Tundjungsari's Standardization of Information Security Management in Banking Using ISO 27001:2022. Journal La Multiapp, 5(4): 361–379, 2024.
- [11] A Shaalan Abbas Network Risk Assessment in Banking Security based on ISO/IEC 27005 (2025) AIP Conference Proceedings (3282); Volume 1:030003.
- [12] Cybersecurity Policy Framework Requirements for Highly Interoperable Health Data Spaces by M Luidold et al. (2024) Applied Sciences; 14(10); DOI: 10.3390/app14104267.
- [13] Evolution and Perspectives in IT Governance: C Vaya-Arboledas et al. (2025) Computers; 14(12); DOI: 10.3390/computers14120520.
- [14] European Parliament and Council of the European Union. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data (General Data Protection Regulation). Official Journal of the European Union, L 119, 2016, pp. 1–88.
- [15] W. Stallings & L. Brown. Computer Security: Principles and Practice (4th ed.). Pearson, 2018.

- [16] NIST. Cybersecurity Framework 2.0. National Institute of Standards and Technology, U.S. Department of Commerce, 2024. Available: <https://doi.org/10.6028/NIST.CSWP.29>
- [17] S. Rose, O. Borchert, S. Mitchell & S. Connelly. Zero Trust Architecture. NIST Special Publication 800-207. National Institute of Standards and Technology, 2020. DOI: 10.6028/NIST.SP.800-207
- [18] European Parliament and Council of the European Union. Regulation (EU) 2022/2554 on Digital Operational Resilience for the Financial Sector (DORA). Official Journal of the European Union, L 333, 2022, pp. 1–79.
- [19] M. Weil & M. Murugesan. IT Risk and Resilience—Cybersecurity Response to COVID-19. IT Professional, 22(3), pp. 4–10, 2020. DOI: 10.1109/MITP.2020.2988330