



MSc in Data & Artificial Intelligence

Data Security, Governance & Compliance

‘Component One’

“FinSure Bank Security Governance & Compliance Plan”

Submitted To

Dr Vijeyanthan Thayanathan

Mail: v.thayanathan@uwtsd.ac.uk

Submitted By

Tareque Hasnat Tuhin

Mail: 2513674@student.uwtsd.ac.uk

“Submission Date”

02 April, 2026

Abstract

I am writing this report for FinSure Bank. The bank is growing fast but has almost no security measures in place. Employees use their own laptops and phones to work. Customer data is not safe. I reviewed two well-known security guides: ITIL [11] and ISO 27001 [10]. Then I made my own simple four-layer plan. My plan includes: defining rules and who is in charge, identifying risks, implementing protections, and checking laws like GDPR [12]. I also explain why rules must keep changing—because hackers and technology never stay the same. I want to help the bank stop fraud, protect customers, and avoid big fines.

01. Introduction

I got a case about FinSure Bank. The bank is digital-first—almost everything is on the cloud. They let employees use personal devices (BYOD). Customers use mobile banking apps. That is nice for business, but very dangerous.

Right now, the bank has no single security policy. No one manages risks properly. No one checks whether they comply with GDPR [12] or other laws. I think this is a big problem.

In this report, I will do two main things:

- ➔ I will research two security frameworks—ITIL [11] and ISO 27001 [10]—and explain them with simple diagrams and tables.
- ➔ I will design my own complete approach for FinSure Bank. I will cover governance, security policies, risk management, protection tools, contingency planning, Service Level Agreements (SLAs), and compliance.

At the end, I will also explain why it is good to always have new or updated rules and standards.

I will state all my assumptions—like how big the bank is, how much money they have, etc. So you understand why I made my choices.

02. Researcher or security Frameworks & models

First, I read about ITIL [11] and ISO 27001 [10]. A security framework is like a recipe—it tells you step by step what to do to keep information safe. The NIST SP 800-53 framework [1] is another major standard that provides over 1000 security controls.

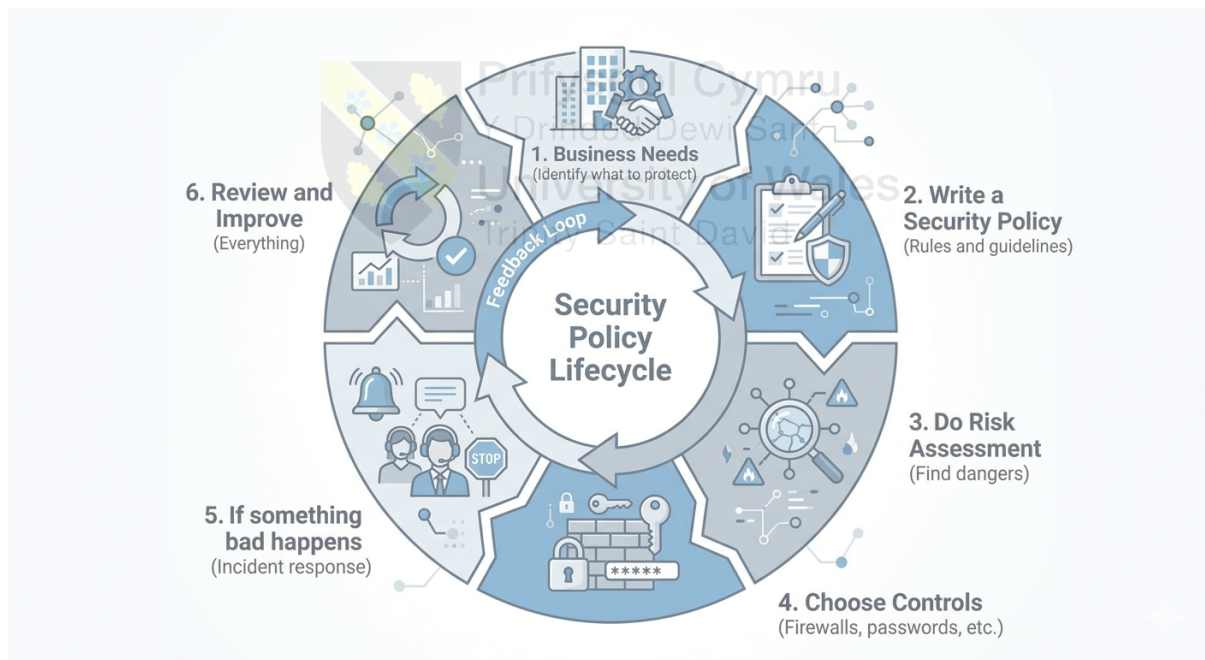
2.1 ITIL – Information Technology Infrastructure Library

ITIL is primarily for managing IT services, but it includes a section on ITIL Security Management [11]. I like it because it connects security with business goals.

What I like about ITIL for FinSure Bank [11]:

- ❖ It looks at people, processes, and technology—not just software.
- ❖ It has a clear process for handling incidents and problems.
- ❖ It helps write Service Level Agreements (SLAs) with cloud providers.

Simple diagram – how ITIL Security Management flows:



When would I use ITIL? I think ITIL is a good fit for banks that already use it for IT services. But for pure security, ISO 27001 [10] is more complete. So I will take the incident response and SLA ideas from ITIL.

2.2 ISO 27000 family (especially ISO 27001)

ISO 27001 is the most famous security standard in the world [10]. You can get a certificate to show you follow it. It lists 114 controls in 14 groups.

Key parts of ISO 27001 [10]:

- Top managers must be involved—not just IT people.
- You must do a proper risk assessment.
- You must choose controls like encryption, access control, and training.
- You must check and improve all the time—that is called continuous improvement.

Simple diagram—the Plan-Do-Check-Act cycle of ISO 27001 [10]:

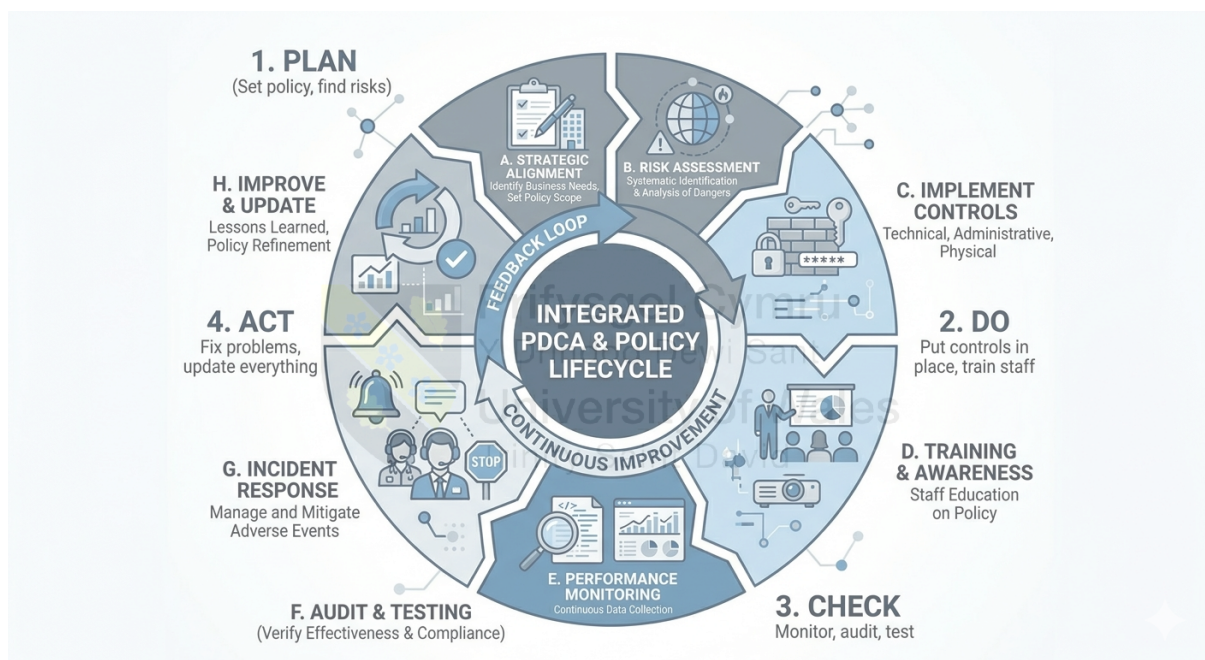


Table: Some important controls from ISO 27001 [10] that I will use

Control Group	Examples I will use for FinSure Bank
Access Control	Only give access to people who need it. Use MFA.
Cryptography	Encrypt all laptops and phones. Encrypt data in the cloud.
Physical Security	Lock server rooms. No one can enter

	without a badge.
Operations Security	Back up data every day. Test backups.
Compliance	Check GDPR rules [12] every 6 months.

Which one is better? I think both ITIL [11] and ISO 27001 [10] have good ideas. The NIST Cybersecurity Framework 2.0 [14] also provides useful guidance. For FinSure Bank, I will mix them.

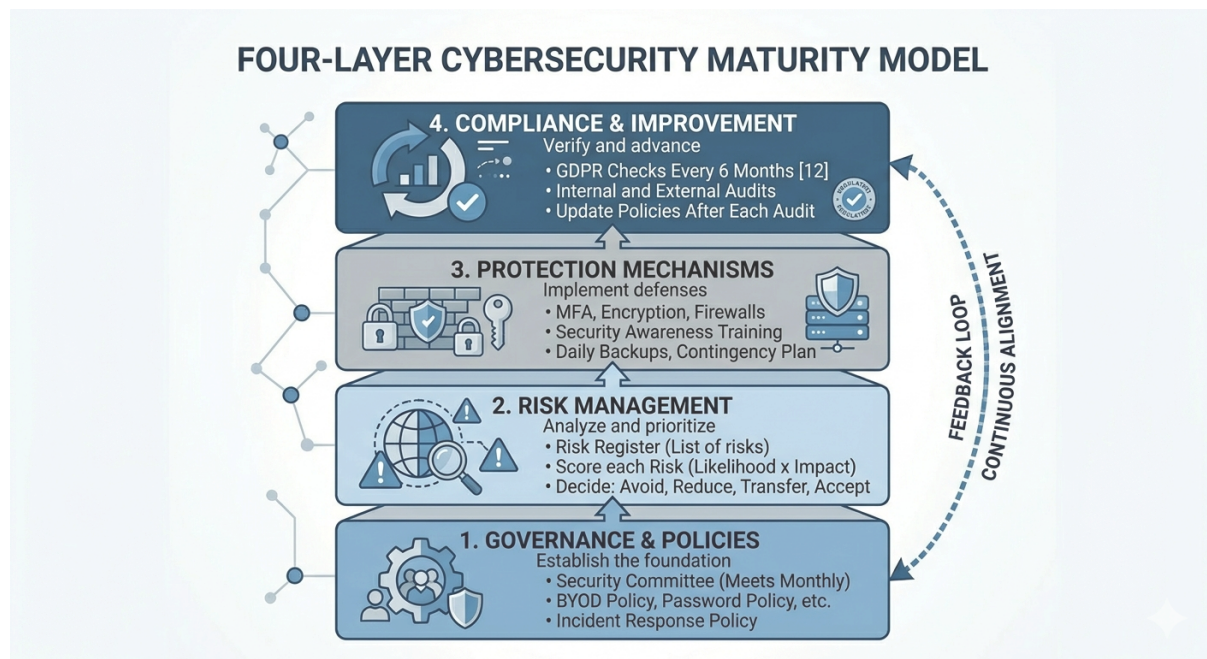
03. My own security, governance and compliance approach for FinSure Bank

Now I will design a plan that fits this bank. I will use ideas from ISO 27001 [10], ITIL [11], and NIST SP 800-53 [1]. I will call it the **Four-Layer Protection Plan**.

3.1 The four layers—a simple table

Layer	Names	What I will put in this layer
1	Governance & Policies	Who is in charge? What are the written rules?
2	Risk Management	Find dangers and decide which to fix first.
3	Protection Mechanisms	Tools, training, backups, contingency plans.
4	Compliance & Improvement	Check GDPR [12], audit, update, everything.

Diagram of my four layers:



3.2 Layer 1—Governance and policies

First, I will create a **Security Governance Committee**. Members: IT manager, legal person, HR, a senior manager, and a compliance officer. They meet once a month. According to ISO 27001 [10], leadership commitment is essential.

Policies I will write:

Policy Name	What it says in simple words
Acceptable use policy	Employees can only use bank systems for work
BYOD policy	Personal devices must have antivirus, screen lock
Data protection policy	Customer data must be encrypted
Incident response policy	If breach happens, call IT manager within 1 hour
Password policy	Minimum 12 characters, change every 90 days, use MFA

SLA with cloud provider	The cloud provider must respond in 2 hours [11]
-------------------------	---

3.3 Layer 2 – Risk management

I will use a simple risk matrix based on the NIST Risk Management Framework [15]. For each risk, I assign a Likelihood (1-5) and an Impact (1-5) score. Multiply to get a risk score.

Example risk table for FinSure Bank

Risk	Likelihood	Impact	Score	What I will do
Employee loses laptop with customer data	3	4	12	Encrypt all laptop [1]
A hacker breaks into cloud system	2	5	10	Strong firewalls. Patch monthly
Insider sells customer info	2	5	10	Monitor access logs [1]
BYOD device gets malware	4	3	12	Require antivirus [11]
GDPR fine for not reporting breach [12]	1	5	5	Report within 72 hours

3.4 Layer 3—Protection mechanisms

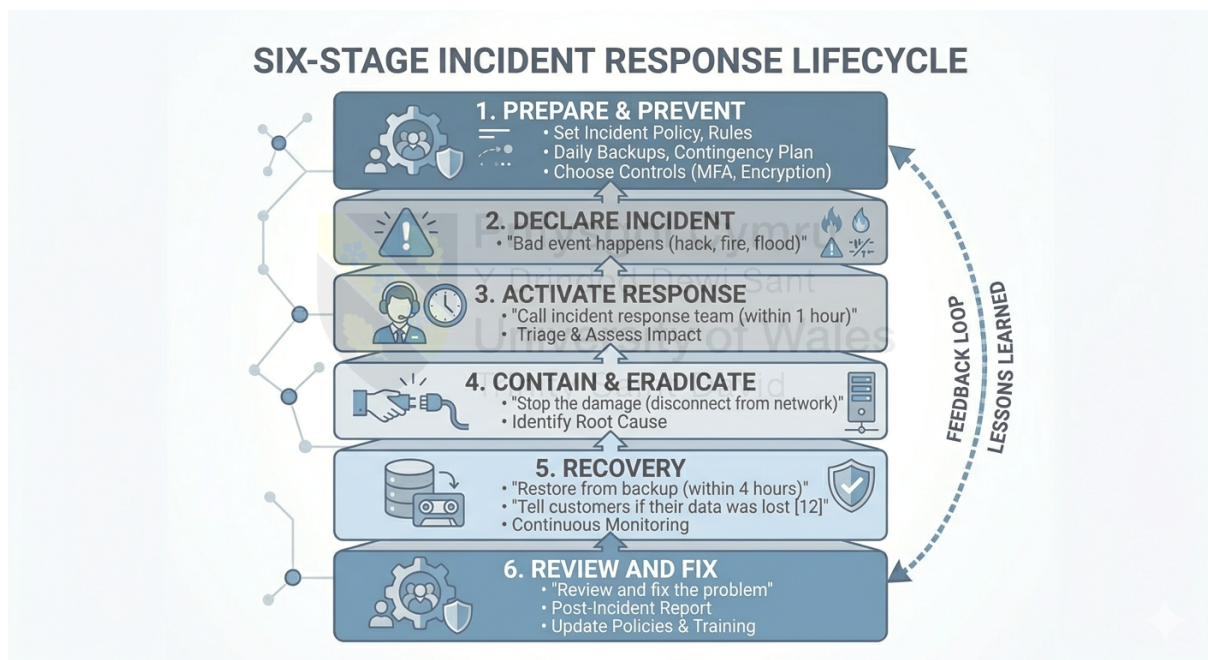
Table of protection tools I will use based on NIST SP 800-53 [1] and ISO 27001 [10]:

Total practice	How it helps
Multi-factor authentication (MFA)	Even if the password is stolen, hacker cannot log in
Ful disk encryption	If a laptop is stolen, data is scrambled [1]

Endpoint detection (EDR)	Finds viruses on BYOD devices
Firewall and network segmentation	Customer data is on separate network
Daily backups (tested weekly)	If ransomware hits, restore from backup
Security awareness training (every 6 months)	Teaches staff not click phishing links [16]
Phishing simulation (monthly)	I send fake phishing emails to test staff

Contingency planning [1]: I will write a Disaster Recovery Plan (DRP) and Business Continuity Plan (BCP).

Simple contingency flow:



3.5 Layer 4—Compliance and improvement

FinSure Bank must follow GDPR [12] because it has customers in Europe. Also, local banking laws. The UK ICO provides detailed guidance [13].

GDPR checklist table [12]:

GDPR requirement	How I will meet it
Article 32—Security of processing	Encryption, access, control, regular, testing

Article 33—Breach Notification	Tell authority within 72 hours
Article 35—Data protection impact assessment (DPIA)	Do DPIA before new app or service
Article 15—Right to access	Give customer data within 30 days

How I will keep improving [10][14]:

- ❖ Internal audit every 6 months.
- ❖ External audit every year.
- ❖ After every audit, update policies.
- ❖ Watch security news from ENISA [16].

04. Why is it good to constantly have new or updated regulations and standards

Now I explain why rules must keep changing. The ENISA Threat Landscape 2024 [16] shows that cyber threats evolve rapidly.

Reason 1—Technology changes all the time

Five years ago, nobody worried about AI phishing. Old rules did not mention cloud or BYOD. New rules force everyone to keep up. For example, GDPR [12] came into effect in 2018 and required breach reporting within 72 hours—that was a good change.

Reason 2—Hackers also learn and improve

It is like a game: defenders and attackers both get better. After the WannaCry attack in 2017, many countries updated their cyber laws. The NIST CSF 2.0 [14] was updated in 2024 to address new threats.

Reason 3 – What customers want changes

People now care more about privacy. New laws like GDPR [12] came into being because customers demanded it. If a bank only follows old rules, customers will lose trust.

So in short, updating rules is not a burden. It is necessary protection for everyone.

05. All my assumptions

Assumption	What I assumed
Size of bank	About 500 employees, 2000000 customers
Budget for security	Around 5000,000 pound per year
Existing technology	Microsoft 365 and AWS cloud. Basic firewalls, no MFA
Regulatory environment	Must follow GDPR [12] and local financial rules
Security maturity	Very low—no formal policies before my report
Management support	CEO and board will approve my plan
No major breach yet	No big hack has happened—so we have time
BYOD devices	Windows laptops and Android or iPhones
Cloud SLA	Cloud provider agree to 2 hour response [11]

06. Conclusion

FinSure Bank is in a dangerous position. No unified governance, no risk management, no compliance checks. But I believe it can be fixed.

I researched ITIL [11], ISO 27001 [10], and NIST frameworks [1][14]. I took the best parts and designed my own four-layer protection plan with:

- ❖ A security committee and clear policies (Layer 1)
- ❖ A risk matrix (Layer 2) based on NIST RMF [15]
- ❖ Practical protections like MFA, encryption, training, backups (Layer 3)

- ❖ GDPR compliance [12] and regular audits (Layer 4)

I also explained why rules must keep changing – because technology, hackers, and customer needs never stand still [16].

What the bank should do first:

- ★ Set up the Security Governance Committee this month.
- ★ Write and approve a BYOD policy and incident response policy.
- ★ Enable MFA for all employees within 2 weeks.
- ★ Run security awareness training for everyone [16].
- ★ Do a first risk assessment using my risk table.

If the bank follows my plan, I am confident it can reduce fraud, protect customer data, avoid big fines, and build trust.

References

- [1] National Institute of Standards and Technology, “*Security and Privacy Controls for Information Systems and Organizations (NIST SP 800-53 Rev. 5)*,” Gaithersburg, MD, USA, Sep. 2020. [Online]. Available: <https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final>
- [2] Cisco Systems, “*Framework Foundations: NIST SP 800-53 Solution Brief*,” San Jose, CA, USA, Nov. 2025. [Online]. Available: <https://www.cisco.com/c/en/us/products/collateral/security/nist-sp-800-53-sb.html>
- [3] Encryption Consulting, “*Elevate Your Security with NIST 800-53*,” May 2024. [Online]. Available: <https://www.encryptionconsulting.com/elevate-your-security-with-nist-800-53/>
- [4] Filament Information Security, “*NIST Special Publication 800-53*,” Aug. 2024. [Online]. Available: <https://www.filamentsecurity.org/nist-800-53/>
- [5] 6clicks, “*NIST SP 800-53 Security Guide: Protect Your Data*,” 2025. [Online]. Available: <https://www.6clicks.com/resources/guides/nist-sp-800-53>
- [6] CyberArrow, “*NIST SP 800-53 Compliance Hub*,” Jul. 2025. [Online]. Available: <https://www.cyberarrow.io/nist-sp-800-53-compliance-hub/>

- [7] Blue INK Security, “NIST 800-53 Standard,” 2025. [Online]. Available: <https://www.blueinksecurity.com/standards/nist-800-53>
- [8] Pretorin, “Understanding FedRAMP Rev5 Controls and Documentation,” Feb. 2026. [Online]. Available: <https://pretorin.com/blog/fedramp-rev5-controls-documentation/>
- [9] RAMPQuest, “A Guide to NIST 800-53 Compliance,” Apr. 2024. [Online]. Available: <https://rampquest.com/blog/a-guide-to-nist-800-53-compliance>
- [10] International Organization for Standardization, “ISO/IEC 27001:2022 Information Security Management Systems,” Geneva, Switzerland, 2022. [Online]. Available: <https://www.iso.org/standard/27001>
- [11] AXELOS, “ITIL 4: Security Management Practice,” 2023. [Online]. Available: <https://www.axelos.com/best-practice-solutions/itil>
- [12] European Commission, “General Data Protection Regulation (GDPR) – Official Legal Text,” Brussels, Belgium, 2018. [Online]. Available: <https://gdpr-info.eu>
- [13] UK Information Commissioner’s Office, “Guide to the UK General Data Protection Regulation,” London, UK, 2024. [Online]. Available: <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/>
- [14] National Institute of Standards and Technology, “NIST Cybersecurity Framework (CSF) 2.0,” Gaithersburg, MD, USA, Feb. 2024. [Online]. Available: <https://www.nist.gov/cyberframework>
- [15] National Institute of Standards and Technology, “Risk Management Framework (RMF) Overview (NIST SP 800-37 Rev. 2),” Dec. 2018. [Online]. Available: <https://csrc.nist.gov/publications/detail/sp/800-37/rev-2/final>
- [16] European Union Agency for Cybersecurity (ENISA), “ENISA Threat Landscape 2024,” Heraklion, Greece, Nov. 2024. [Online]. Available: <https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024>
- [17] Experts Exchange, “Proper Cybersecurity Controls in Application Design,” Sep. 2023. [Online]. Available: <https://www.experts-exchange.com/questions/29264962/Proper-Cybersecurity-Controls-in-Application-Design.html>

- [18] National Institute of Standards and Technology, “*NIST Special Publication 800-53A: Assessing Security and Privacy Controls*,” Gaithersburg, MD, USA, 2022. [Online]. Available: <https://csrc.nist.gov/publications/detail/sp/800-53a/rev-5/final>
- [19] National Institute of Standards and Technology, “*Digital Identity Guidelines (NIST SP 800-63-3)*,” Gaithersburg, MD, USA, Jun. 2017. [Online]. Available: <https://pages.nist.gov/800-63-3/>
- [20] Cloud Security Alliance, “*Cloud Controls Matrix (CCM) v4*,” Seattle, WA, USA, 2023. [Online]. Available: <https://cloudsecurityalliance.org/research/cloud-controls-matrix>

