

Case Study: Scenario 5

Public Booking System (GovBook Services)

University of Wales Trinity Saint David
MSc in Cybersecurity and Digital Forensics

Group Members

Dharmikkumar Dabgar : 2536691

Janvi Poshia : 2543705

Sneha bhesaniya : 2544720

Jinal Ahir : 2535262

Karina Jiwani : 2536600

1. Security Governance vs. Security Management

Security Governance (The "Steering Wheel")

Governance is about the big picture, strategy, and oversight. It is handled by senior leadership or a government board.

- **Focus:** Setting strategy, ensuring compliance with laws (like data protection), and deciding what risks are acceptable.
- **GovBook Example:** The board decides that avoiding passport data leaks is the top priority and secures a large budget for cybersecurity. They are ultimately accountable to the public if a breach happens.

Security Management (The "Engine Room")

Management is the day-to-day implementation of the governance strategy. It is handled by IT and Security teams.

- **Focus:** Putting the tools, processes, and people in place to actually protect the system.
- **GovBook Example:** The IT team takes the board's budget and installs firewalls, sets up database encryption, and configures multi-factor authentication for citizens.

2. Key Governance Processes (ISO/IEC 27014:2013)

ISO 27014 outlines core processes that directors must use to govern security:

- **Evaluate:** Leadership must constantly look at what could go wrong. *Example: Assessing the impact if a ransomware attack takes the driving license system offline.*
- **Direct:** Based on the evaluation, leadership gives orders and budget. *Example: Mandating a backup system for passport bookings and approving a £500,000 budget for it.*
- **Monitor:** Governance checks if the system is actually secure. *Example: Reviewing monthly reports on how many hacking attempts were blocked or checking audit results.*
- **Communicate:** Keeping everyone in the loop to build trust. *Example: Publishing clear privacy notices on the GovBook website so citizens know their health data is safe.*

3. Role of Policies, Standards, and Guidelines

These documents create the rulebook for keeping GovBook secure, going from broad rules to specific instructions.

Policies (The "Law")

- **Role:** Mandatory, high-level rules set by management.
- **GovBook Example:** *Data Privacy Policy*: "Only government employees with a verified business need are allowed to access citizen medical records. Sharing passwords is forbidden."

Standards (The "Speed Limit")

- **Role:** Specific, measurable technical requirements that must be followed to satisfy the policy.
- **GovBook Example:** *Password Standard*: "All employee passwords must be exactly 14 characters long and changed every 90 days."

Guidelines (The "Safe Driving Tips")

- **Role:** Recommended advice and best practices to help staff make good decisions (not strictly mandatory).
- **GovBook Example:** *Phishing Awareness Guidelines*: A helpful guide for GovBook support staff on how to spot suspicious emails containing fake links.