

❖ FINAL Additional Files

[1] B. Bulgurcu, H. Cavusoglu, and I. Benbasat, "Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness," *MIS Quarterly*, vol. 34, no. 3, pp. 523–548, 2010.

https://www.researchgate.net/publication/220260207_Information_Security_Policy_Compliance_An_Empirical_Study_of_Rationality-Based_Beliefs_and_Information_Security_Awareness

[2] European Commission, *General Data Protection Regulation (GDPR)*, Brussels, Belgium, 2022.

<https://cacm.acm.org/research/an-overview-of-it-service-management/>

[3] Humphreys, E. (2017). *Implementing the ISO/IEC 27001 Information Security Management System Standard*. Artech House.

<https://dl.acm.org/doi/abs/10.5555/1543682>

[4] Pereira, R., & Silva, M. M. (2012). A literature review: Guidelines and contingency factors for IT governance. *Journal of Information Systems and Technology Management*, 9(1), 73–108.

https://www.researchgate.net/publication/255568537_A_Literature_Review_IT_Governance_Guidelines_and_Main_Areas

[5] Morrow, B. (2012). BYOD security challenges: Control and protect your most sensitive data. *Network Security*, 2012(12), 5–8.

<https://www.sciencedirect.com/science/article/abs/pii/S1353485812701113>

[6] Axelos. (2019). *ITIL Foundation: ITIL 4 Edition*. TSO.

<https://abim.go.ug/sites/files/%28ITIL%29%20Axelos%20-%20ITIL%20Foundation%204%20edition-Axelos%20%282019%29%5B1%5D.pdf>

[7] NIST. (2018). *Framework for Improving Critical Infrastructure Cybersecurity*

<https://nsarchive.gwu.edu/sites/default/files/documents/4446571/National-Institute-of-Standards-and-Technology.pdf>

[8] Marrone, M., & Kolbe, L. M. (2011). Uncovering ITIL claims: IT executives' perception on benefits and Business-IT alignment. *Information Systems and e-Business Management*, 9(3), 363–380.

<https://link.springer.com/article/10.1007/s10257-010-0131-7>

[9] ISO 27001 – Plan-Do-Check-Act

<https://pecb.com/article/the-plan-do-check-act-pdca-cycle-a-guide-to-continuous-improvement>

[10] ITIL Security Management

<https://www.collidu.com/presentation-til-security-management>

[11] NIST Framework

<https://www.forescout.com/blog/how-to-comply-with-the-5-functions-of-the-nist-cybersecurity-framework/>

Figure 1: ISO 27001 – Plan-Do-Check-Act (PDCA) Cycle

- This model ensures continuous improvement in information

security processes.

- It guides the implementation of security controls through four phases: Plan, Do, Check, and Act.
- Commonly used in ISO/IEC 27001 to manage and improve an Information Security Management System (ISMS).



Figure 2: ITIL Security Management Process

- ITIL outlines a structured approach to security through five domains: Policy, Risk Management, ISMS, Communication Strategy, and Controls.
- It ensures alignment between IT services and security goals, forming the operational arm of IT governance.
- Supports the daily integration of security tasks, rather than treating them as standalone audits.

ITIL SECURITY MANAGEMENT

The Process Includes

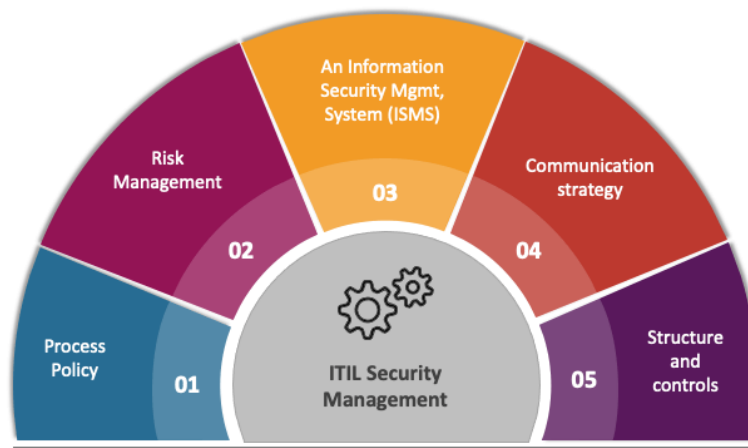


Figure 3: NIST Cybersecurity Framework

- The NIST CSF is divided into five essential functions: Identify, Protect, Detect, Respond, and Recover.
- It provides a flexible and risk-based approach to managing cybersecurity at an operational level.
- Highly adaptable for cloud-based and BYOD environments,

making it ideal for Nature Garden context.



Table 1: Key Roles for Governance & Compliance

Role	Responsibilities
Board of Directors	Approves security budgets, monitors governance, and aligns strategy with risk tolerance.
Chief Information Security Officer (CISO)	Leads the ISMS, defines policy, manages the security roadmap, and oversees incidents.

Data Protection Officer (DPO)	Ensures compliance with GDPR and privacy laws, handles data subject requests.
IT Security Team	Implements technical controls (e.g., firewalls, encryption, access management).
Legal & Compliance Team	Tracks regulatory changes, reviews contracts, and coordinates with third-party vendors.
HR Department	Provides employee security training, ensures policy awareness and adherence.

Implementation Plan – What NG Should Do

Based on ISO 27001 Annexe A, NG should implement key controls in the following areas:

Control Category	Recommended Controls for NG
Information Security Policies	Create and communicate a company-wide security policy
Organisation of Information Security	Define roles and establish security oversight (e.g. CISO or Data Protection Officer)
Access Control	Use RBAC (Role-Based Access Control), MFA, and network segmentation
Operations Security	Conduct regular vulnerability scans and security audits
Communications Security	Encrypt wireless transmissions (WPA3), implement secure VPNs
Incident Management	Develop and test an incident response plan

Table 2: High-Level Implementation Plan

Area	Action	Timeline	Owner
Security Policy	Draft and approve security policies	Month 1	IT Governance
BYOD Management	Implement MDM (Mobile Device Management)	Month 2–3	IT Operations
Access Control	Enforce RBAC and MFA	Month 3	Network Team
Risk Assessment	Identify and classify assets	Month 1	Risk Manager
Cloud Security	Review configurations, apply encryption	Month 2	Cloud Architect
Training & Awareness	Conduct user security awareness training	Monthly	HR & Security
Incident Response	Develop and test playbooks	Month 4	Security Lead