



Prifysgol Cymru
Y Drindod Dewi Sant
University of Wales
Trinity Saint David

Component 2

Program: MSc in Data and Artificial Intelligence

Student Id: 2424033

Student Name: Dev Shaileshbhai Mistri

Module: Data Security, Governance and Compliance

Module Code: ACCA7028

Lecturer: Dr Mohamed Ben Farah

1. Research on Security Frameworks and Models

In today's hyper-connected and digital-first environment, organizations face mounting challenges in managing confidentiality, integrity, and availability of data. These challenges are compounded by the increasing complexity of IT infrastructure, rise in remote work, growing reliance on cloud services, and stringent compliance requirements. In response, security frameworks and models have emerged as essential tools to guide organizations in designing, implementing, and maintaining secure information systems. This section explores key security frameworks and models—specifically ISO/IEC 27000 series, ITIL, NIST Cybersecurity Framework (CSF), COBIT, and the Zero Trust Security Model—offering a comparative analysis with the aid of diagrams, tables, and examples.

1.1 ISO/IEC 27000 Series – Information Security Management System (ISMS)

The **ISO/IEC 27000 series**, particularly **ISO/IEC 27001**, is the most widely recognized international standard for establishing an Information Security Management System (ISMS). The core of ISO/IEC 27001 is to enable organizations to establish, implement, monitor, and continually improve their information security processes. It provides a risk-based and process-oriented approach that is applicable across all sectors.

Key Components of ISO/IEC 27001:

- Understanding the organizational context
- Leadership commitment and policy development
- Information security risk assessment and treatment
- Documentation and implementation of controls
- Internal audits and management review
- Continuous improvement (Plan-Do-Check-Act)

The standard includes **Annex A**, which outlines **114 security controls** across 14 domains, including access control, physical security, cryptography, communications security, and more (ISO/IEC, 2022).

PDCA Model Diagram:

The **Plan–Do–Check–Act (PDCA)** cycle is central to ISO/IEC 27001, promoting a continuous improvement process:

- *Plan*: Define the ISMS, assess risks, and set objectives
- *Do*: Implement the necessary controls and policies
- *Check*: Monitor and evaluate the ISMS through audits and KPIs
- *Act*: Make improvements based on the results of audits and evaluations

This cycle ensures that security management remains dynamic and adaptable over time. ISO/IEC 27001 is especially suitable for **NatureGarden (NG)**, whose international operations and heavy reliance on cloud-based systems demand a standardized and scalable security approach.

1.2 ITIL – Information Technology Infrastructure Library

The **Information Technology Infrastructure Library (ITIL)** is a globally adopted framework for **IT service management (ITSM)**. Though not primarily a security framework, ITIL includes essential processes that support information security governance and compliance.

Relevant ITIL Processes and Security Functions:

ITIL Process	Security Relevance
Information Security Mgmt.	Aligns IT security with business goals
Access Management	Controls access rights to systems and data
Change Control	Assesses and manages risk during IT changes
Incident Management	Ensures prompt detection and response to security incidents

ITIL operates across five lifecycle stages: **Service Strategy, Service Design, Service Transition, Service Operation, and Continual Service Improvement**. Within each phase, information security is embedded to ensure that IT services are delivered and managed securely.

Diagram Description:

A typical ITIL lifecycle diagram shows security practices integrated across all five stages of service delivery. For instance, change management ensures security risks are considered before deploying new features, while incident management ensures threats are handled efficiently.

For a company like NatureGarden that heavily depends on wireless IT infrastructure and cloud-based applications, integrating ITIL with other security frameworks enhances operational resilience and governance.

1.3 NIST Cybersecurity Framework (NIST CSF)

Developed by the **National Institute of Standards and Technology (NIST)**, the NIST CSF offers a structured and adaptable approach to managing cybersecurity risks. It was originally designed for critical infrastructure but has since been adopted across various industries globally.

The framework consists of five **core functions**:

1. **Identify:** Understand assets, risks, and governance requirements
2. **Protect:** Implement controls to safeguard assets and services
3. **Detect:** Monitor to identify cybersecurity incidents
4. **Respond:** Take action to contain and mitigate threats
5. **Recover:** Restore affected systems and services

1.4 COBIT – Control Objectives for Information and Related Technologies

COBIT, developed by ISACA, is a business framework for the governance and management of enterprise IT. COBIT enables organizations to create value through effective governance of IT processes, ensuring alignment between business goals, regulatory compliance, and risk management.

COBIT Core Domains:

- **Governance Objectives:** Evaluate, Direct, Monitor
- **Management Objectives:** Align, Plan, Build, Run, Monitor

Diagram Description:

The COBIT process model is often depicted as a layered structure, with Governance feeding into Management domains. These domains translate business needs into actionable IT processes.

For NatureGarden, implementing COBIT would ensure IT systems are not only secure but also aligned with strategic business priorities and international standards. It supports decision-making and resource allocation in a secure, efficient manner.

1.5 Zero Trust Security Model

The **Zero Trust Model** is a modern cybersecurity architecture that challenges the traditional notion of perimeter-based security. In Zero Trust, no user or device is trusted by default—even those inside the corporate network.

Core Principles of Zero Trust:

- **Verify explicitly:** Always authenticate based on all available data
- **Use least privilege access:** Limit user permissions to the minimum necessary
- **Assume breach:** Design systems as if they are already compromised

Diagram Description:

A Zero Trust diagram typically shows user devices connecting to corporate resources via a broker that verifies identity, location, device posture, and risk level before granting access. Each resource (e.g., HR system, cloud storage) has its own access policies.

This model is particularly relevant for **NatureGarden**, given its global workforce, BYOD culture, and wireless-based operations. Implementing Zero Trust ensures granular control over access and minimizes the attack surface.

1.6 Comparative Summary of Frameworks and Models

Framework/ Model	Focus Area	Strengths	Suitability for NG
ISO/IEC 27001	Risk management, ISMS	Globally recognized, audit-friendly, continuous improvement	Highly suitable
ITIL	IT service management	Operational integration, process optimization	Good support for operations
NIST CSF	Cybersecurity governance	Flexible, maturity-focused, adaptable	Very relevant
COBIT	IT governance	Aligns IT with business, strong risk and compliance oversight	Highly beneficial
Zero Trust	Identity & access control	Strongest access control model, cloud/BYOD readiness	Crucial

Conclusion

The implementation of an effective cybersecurity posture requires a strategic blend of security frameworks and models. Each framework reviewed in this section brings unique strengths:

- **ISO/IEC 27001** offers structured, risk-based ISMS management;
- **ITIL** embeds security into operational service delivery;
- **NIST CSF** enables adaptable and scalable risk management;
- **COBIT** bridges governance with IT strategy;
- **Zero Trust** provides a forward-thinking, identity-driven architecture.

For an organization like NatureGarden—operating globally with wireless-first, cloud-enabled infrastructure—a **hybrid security strategy** is recommended. Integrating ISO/IEC 27001 for ISMS, NIST CSF for risk alignment, and Zero Trust for access control offers comprehensive protection tailored to its needs.

References

- [ISO/IEC. \(2022\). ISO/IEC 27001: Information security management systems – Requirements. International Organization for Standardization.](#)
- [NIST. \(2024\). Framework for Improving Critical Infrastructure Cybersecurity, Version 2.0. National Institute of Standards and Technology.](#)
- [ISACA. \(2019\). COBIT 2019 Framework: Introduction and Methodology.](#)
- [Axelos. \(2019\). ITIL Foundation: ITIL 4 Edition. The Stationery Office.](#)
- [Rose, S., Borchert, O., Mitchell, S., & Connelly, S. \(2020\). Zero Trust Architecture \(NIST SP 800-207\). National Institute of Standards and Technology.](#)
- [AlHogail, A. \(2015\) Design and validation of information security culture framework. Computers in Human Behavior, 49, 567–575.](#)

Appendix

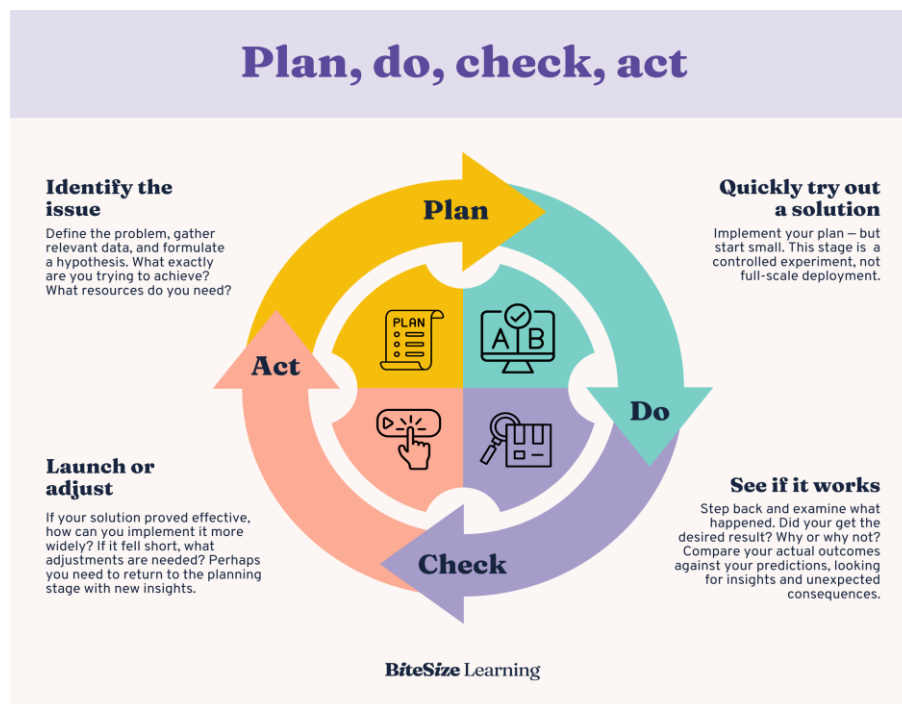


Figure 1: The **Plan–Do–Check–Act (PDCA)** cycle is central to ISO/IEC 27001, promoting a continuous improvement process:

NIST Cybersecurity Framework



Figure 2: Each function includes categories and subcategories, with references to controls in ISO/IEC 27001, COBIT, and other standards. The framework also defines **implementation tiers** (Partial to Adaptive), allowing organizations to assess their cybersecurity maturity.

NIST CSF is particularly useful for organizations like NatureGarden that need a **customizable** and **risk-driven** strategy to address cybersecurity threats while maintaining regulatory compliance.