



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

200
1822 - 2022

Student name: Shimranbanu L. Shaikh (2419481)

Course: MSc. Data and Artificial intelligence (Level 7)

Module: Data Security, Governance and Compliance (ACCA7028)

Component 2.

Title: Implementing Data Security, Governance, and Compliance
Principles and Practices for NatureGarden (NG)

Lecturer: Dr Mohamed Ben Farah

No.	Title	Page no.
1	Abstract	3
2	Introduction	
3	Literature review	
4	Design Approach for NG	
5	Analysis and Discussion	
6	Importance of Regulatory updates	
7	Conclusion	
8	References	
9		
10		

1.Abstract

NatureGarden (NG) is one of the world's top wellness brands. NG relies heavily upon cloud-based software and a wireless framework. There is an increasing demand for a Bring-Your-Own-Device (BYOD) approach to this cloud-based consumption. NG is under increasing scrutiny regarding their data and its security, compliance, and governance. This report is focused on analysing NG's current situation, and providing a complete security framework incorporating ISO/IEC 27001, NIST, ITIL, and COBIT frameworks. It provides a unique governance structure, risk strategy and compliance measures for NG to undertake concerning its intellectual property protection and data privacy measures, including its virtual global consumption. The recommendations conclude with an argument for the need for evolving security regulations, and the need to keep enhancing security policy.

2.Introduction

3.Literature review

4.Design Approach for NG

5.Analysis and Discussion

6. Importance of Regulatory Updates

7.conclusion

8.References

Security Frameworks for Data Security, Governance, and Compliance

Executive Summary

As organizations navigate the current digital world, there are rising threats and pressures from regulators concerning cyber risks and governance. Organizations must implement principled frameworks that minimize risk and protect sensitive information, provide a governance framework, and comply with various standards and regulations, such as GDPR, HIPAA, and PCI DSS. The focus of this report is critical security frameworks and models. The report outlines ITIL, ISO 27000 series, the NIST Cybersecurity Framework (CSF), and COBIT. These frameworks model the process for protecting sensitive data, improving IT governance and alignment with business, and regulatory and legislative compliance. Following diagrams and charts, the report presents the components of these frameworks, how organizations have implemented these frameworks, and approaches for integration into their existing infrastructures. The report should provide organizations interested in bettering their security posture more possibilities for achieving that objective.

1. Introduction

Data security, governance and compliance play an essential role in an organization's resilience to changing circumstances. Security frameworks provide a repeatable and standardized method of risk management, data governance, and ensuring compliance with local and federal laws as well as legal obligations and industry standards. The following report focuses on ITIL, ISO 27000 family, NIST Cybersecurity

Framework, and COBIT and their purposes stemming from data security, governance and compliance perspective. Diagrams and charts show the structure of testing and a comparative analysis highlights the pros and cons of each and their intended workflow.

2. Information Technology Infrastructure Library (ITIL)

2.1 Overview

ITIL is an internationally recognized framework for IT service management, focusing on aligning IT services to the needs of a business and its stakeholders. The latest version of ITIL, version 4 looks at service value systems and embraces security activities throughout the service lifecycle, and organizations consider the appropriate security approaches to support data security and compliance.

2.2 Key Components

- Service Asset and Configuration Management (SACM): Keeps track of IT assets to make sure data-related resources are securely managed.
- Incident Management: Aims to respond to security incidents, such as data breaches, to minimize the impact of the incident.
- Change Management: Provides a process to control changes to systems to avoid vulnerabilities.
- Information Security Management: Incorporates security policies governing IT services to promote confidentiality, integrity, and availability of data.

2.3 Application in Data Security, Governance, and Compliance

ITIL Improving data security through controls integrated into service management processes such as securing assets with SACM. ITIL accountability through defined roles and processes support governance, and compliance with incident management and change management practices are aligned with regulations for timely reporting of breaches and controlled IT changes.

2.4 Diagram: ITIL Service Value System



Figure 1: ITIL Service Value System with Security Integration

This diagram illustrates how ITIL embeds security across its lifecycle, from strategy to continual improvement.

3. ISO/IEC 27000 Series

3.1 Overview

The ISO/IEC 27000 series is a comprehensive and widely accepted standard on information security management systems (ISMS). ISO/IEC 27001 specifies requirements for establishing an ISMS, while ISO/IEC

27002 provides guidance on implementation, ISO/IEC 27005 offers guidance on risk management and ISO/IEC 27014 discusses governance.

3.2 Key Components

- **ISO/IEC 27001:** Provides the requirements for an ISMS including risk assessment and security controls.
- **ISO/IEC 27002:** Provides a list of 93 controls, divided into four categories (organizational, people, physical and technological).
- **ISO/IEC 27005:** Provides guidance on the risk assessment and treatment of security for data.
- **ISO/IEC 27014:** Provides guidance on the governance of information security.

3.3 Application in Data Security, Governance, and Compliance

ISO 27001 secures data through risk management on information assets. It identifies threats to information assets and provides controls to mitigate these threats. The governance is established through a parent structure that provides policies, adopts roles and responsibilities to provide accountability for the governance. Secondly, ISO 27001 certification shows compliance with other regulations like GDPR and HIPAA, but also adds clarity and credibility to organizations.

3.4 Chart: ISO 27001 Control Domains

Domain	Number of Controls	Examples
Organizational	37	Security policies, risk assessment

Domain	Number of Controls	Examples
People	8	Training, access control
Physical	14	Secure areas, equipment protection
Technological	34	Cryptography, malware protection

Table 1: ISO 27001:2022 Annex A Control Domains

This chart summarizes the control distribution in ISO 27001:2022, highlighting their focus areas.

4. NIST Cybersecurity Framework (CSF)

4.1 Overview

Created by the National Institute of Standards and Technology, the NIST CSF is a flexible framework for managing cybersecurity risks, especially for critical infrastructure. Its core functions—Identify, Protect, Detect, Respond, Recover and Govern—provide an ideal overall structure to think about data security.

4.2 Key Components

- **Identify:** Understands assets and risks.
- **Protect:** Implements safeguards like access controls.
- **Detect:** Monitors for security events.
- **Respond:** Manages incidents effectively.
- **Recover:** Restores systems post-incident.

- **Govern:** Establishes oversight and policies.

4.3 Application in Data Security, Governance, and Compliance

The NIST Cybersecurity Framework facilitates data security by understanding risk and taking safeguards to mitigate those risks. The concept of governance in the NIST CSF aligns data security with the organizations' mission and goals, while also allowing organizations flexibility in adhering to regulations, including FISMA and GDPR compliance.

4.4 Diagram: NIST CSF Core Functions



Figure 2: NIST CSF Core Functions

This diagram shows the cyclical nature of NIST CSF, emphasizing continuous security improvement.

5. Control Objectives for Information and Related Technologies (COBIT)

5.1 Introduction

COBIT 2019 is a governance and management framework for Information and Technology (IT) that aligns IT with business objectives.

COBIT includes security controls to protect data and support compliance.

5.2 Key Elements

- Governance Objectives: Align IT with the business's high-level plans and strategies.
- Management Objective: Effectively manage IT resources and risks associated with the need to implement a risk management within applicable governance requirements.
- Security Controls: Protecting data using policies and processes.

5.3 Role in Data Security, Governance, and Compliance

COBIT helps with data security by generating a risk management and control framework. Lastly, its governance component helps with accountably and managing risks. Organizations are usually required to comply with data standards like Sarbanes-Oxley Act, COBIT aligns with compliance standards.

6. Comparative Analysis

Framework	Focus Area	Key Strength	Compliance Alignment
ITIL	IT Service Management	Aligns IT with business needs	GDPR, HIPAA
ISO 27001	Information Security	Comprehensive ISMS with certification	GDPR, HIPAA, PCI DSS

Framework	Focus Area	Key Strength	Compliance Alignment
NIST CSF	Cybersecurity	Flexible, risk-based approach	FISMA, GDPR
COBIT	IT Governance	Aligns IT with business goals	SOX, ISO 27001

Table 2: Comparison of Security Frameworks

7. Integration Strategies

Organizations can integrate frameworks for enhanced outcomes:

- **ITIL and ISO 27001:** ITIL operationalizes ISO 27001's controls within service management processes.
- **ISO 27001 and NIST CSF:** Combines ISO's structured ISMS with NIST's risk-based functions.
- **COBIT and ISO 27001:** COBIT's governance complements ISO's security focus for robust compliance.

8. Conclusion

Security frameworks such as ITIL, ISO 27000, NIST CSF, and COBIT provide essential guidance for implementing and managing data security, governance and compliance. ITIL is where to align IT services with security needs, ISO 27001 offers a certifiable ISMS and supporting documents, NIST CSF brings flexibility for organizations and businesses, and COBIT for governance alignment. Integrating ISO 27001 an

organization to safeguard their data and improve governance structure while meeting compliance requirements. The addition of diagrams and flow charts clarify their structures and support implementation.