



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

Assignment Title: Apply the principles and practices of Data security,

Governance and Compliance based on a given scenario.

Program: MSc in Data and Artificial Intelligence

Student ID: 2426433

Student Name: Mohammad Anas Abdul

Salam Ansari

Module: Data Security, Governance and

Compliance

Code: ACCA7028

Lecturer: Dr Mohamed Ben Farah

ABSTRACT

As businesses rapidly digitalise, it is becoming increasingly apparent that information security is a major issue, particularly for companies that operate globally and widely use cloud-based infrastructure. Nature Garden (NG) is a widely known health and wellness business that faces several significant security challenges because of its reliance on a wireless network, pressure from its Bring Your Own Device (BYOD) policy, and lack of any formally documented information security policies. This paper aims to explore international frameworks such as ISO/IEC 27001 and ITIL to provide recommendations that could support the design of an information system that is comprehensive, secure, and compliant for NG. This report proposes a hybrid approach that integrates ISO's Information Security Management System (ISMS) with ITIL's service management capabilities. Security policies, compliance and contractual obligations, information protection, governance and risk management, and contingency planning, developed with the use of activity diagrams and tables, are discussed or illustrated. The report also discusses and critiques the need for current regulations and standards to be continuously updated and amended to better respond to emerging cyber threats and new legal requirements in information security. The recommendations aim to support NG in becoming a security-aware and compliant enterprise.

1. INTRODUCTION

In the digital era, organisations are more reliant on wireless networks, cloud networks, and mobile devices to deliver services and remain competitive. Unfortunately, the more dependent an organisation becomes on these technologies, the more vulnerabilities are created in its information systems. Nature Garden (NG), a global leader in the health and wellness industry, is no different. NG is a multinational organisation that has a global presence. They offer services worldwide and have a substantial online and social media presence. NG lacks a documented, cohesive information security framework. NG also has pressure to develop and allow staff and customers to access their services on personal devices (BYOD) [5].

NG currently faces a variety of cyber threats, including, but not limited to, unauthorised access, data breaches, loss of intellectual property, and security compliance failures. NG's lack of security controls and processes places its digital assets, sensitive client information, and corporate brand under threat. The multinational organisation must also adhere to various data protection laws and regulatory requirements arising from protecting the personal data of customers,

e.g., the General Data Protection Regulation (GDPR) [4].

The purpose of this report is to design a tailored security, governance, and compliance framework for NG by utilising two internationally recognised frameworks as a guide for the process, ISO/IEC 27001 and ITIL. As an Information Security Management System, the ISO/IEC 27001 standard provides a risk-based process framework for implementing security controls. ITIL is globally recognised as the most widely used IT service management framework, and its processes also encapsulate notable elements of governance and compliance [1].

2. Literature Review

The increasing complexity of cyber threats and regulatory frameworks has pushed organisations to adopt methodological approaches towards information security and compliance management. The two best-known systems here include the ISO/IEC 27000 series of standards and the Information Technology Infrastructure Library (ITIL). Both systems provide methodical approaches to protect information assets, manage risk, and integrate IT services with business strategy [3].

2.1 ISO/IEC 27000 Family – ISO/IEC 27001 Focus

The International Organisation for Standardisation (ISO) and the International Electrotechnical Commission (IEC) created the ISO/IEC 27000 series as information security management system (ISMS) standards. ISO/IEC 27001 is used most often in this series, providing a comprehensive method of safe handling of sensitive information [3].

ISO/IEC 27001 embraces the Plan-Do-Check-Act (PDCA) cycle in promoting ongoing improvement of information security processes (ISO, 2022). The standard deals with 114 controls across spheres from physical security to access control, cryptography, and communications security (Humphreys, 2017). Taking a risk-based approach, ISO/IEC 27001 enables organisations to systematically identify, evaluate, and handle security risks [2].

According to Siponen et al. (2020), ISO/IEC 27001 is especially beneficial to multinational corporations because it is harmonisable and adaptable to jurisdictions such as GDPR. The system also enforces responsibility and documentation, which makes it easier to be transparent and auditable.

Its detractors think that ISO 27001 certification can be costly and bureaucratic

unless wisely cut down to fit an organisation's needs (Bulgurcu et al., 2010). However, it is still the de facto standard for achieving a minimum security posture as well as adherence to the regulations.

2.2 ITIL Security Management

ITIL, supported by Axelos, is a globally renowned framework for IT service management (ITSM). ITIL is different from ISO/IEC 27001 in that it's not specifically focused on information security but, more broadly, the alignment of IT services with business goals. ITIL delves into processes such as incident management, change management, and service continuity, all of which are instrumental to an IT environment that is safe and robust (Axelos, 2019) [6].

The ITIL Security Management process matches IT security with business security through a systematic set of procedures and policies. Its main goal is to protect information assets and ensure usability and availability. ITIL, as noted by Galup et al. (2009), encourages interdepartmental coordination, reducing silos and introducing security considerations across service lifecycles .

ITIL adoption has been linked with improved organisational efficiency, improved incident resolution time, and improved customer satisfaction (Marrone & Kolbe, 2011). For companies such as Natures Garden, whose service delivery is based on cloud and wireless infrastructure, ITIL's practicality against security measures is particularly relevant.

2.3 NIST Cybersecurity Framework (CSF)

The American National Institute of Standards and Technology (NIST) designed the Cybersecurity Framework (CSF) as a flexible, voluntary framework to help organisations address and respond to cyber threats. NIST CSF is structured into five functions, Identify, Protect, Detect, Respond, and Recover, that together form an end-to-end approach for managing the cybersecurity activities lifecycle (NIST, 2018) [7].

As compared to ISO/IEC 27001 or ITIL, NIST CSF is an implementation-centric framework that provides realistic controls and tools that may be shaped based on an organisation's threat landscape and maturity. It is specifically tailored for the Nature Garden dynamic environment, where threats will always shift and security practices should be modified accordingly [3].

For Nature Garden, NIST CSF implementation will enhance threat detection and response via facilitating continuous monitoring and feedback processes.

The framework also facilitates regulatory compliance with norms like GDPR and CCPA via processed risk analysis and documentation processes [4].

3. Case Scenario Analysis: Nature Garden Security Challenges

Nature Garden (NG), which is a top global brand in the healthcare and wellness industry, has caught up with digital technologies at a very rapid pace to continue its global operations, employee relationships, and customer relationships. NG, which has nearly 95% of its network infrastructure dependent on wireless technology, and with the introduction of cloud services for internal and customer applications hosting, is largely dependent on digital platforms. But this revolution of the internet has also come with a multi-faceted array of security, governance, and regulatory issues that need to be tackled in a systematic way.

3.1 Lack of Formal Security Policies

The biggest threat to NG is that it doesn't have a formalised information security policy structure. Without formalised policies, there are no access control procedures, information handling procedures, incident response procedures, or user procedures. Bulgurcu et al. (2010) argue that organisations with poor security policies are more vulnerable to insider attack and operational compromise, particularly in such high-risk industries as health and well-being, where customer trust is critical [1].

3.2 BYOD (Bring Your Own Device) Pressures

NG is under internal and external pressures to implement BYOD, under which employees and customers use their own devices within the company networks. While BYOD brings flexibility and productivity into the business, it brings top threats, including:

- **Uncontrolled endpoints** that may not adhere to security standards
- **Data leakage** risks if sensitive information is stored on personal devices
- **Lack of visibility** for IT teams to monitor access and usage

As noted by Morrow (2012), organisations that adopt BYOD without proper security controls may inadvertently open doors to malware, phishing, and shadow IT [5].

3.3 Cloud and Wireless Network Vulnerabilities

NG depends on a cloud infrastructure that, though cost-effective and scalable, has introduced additional data privacy, regulatory, and vendor management challenges. Weakly architected cloud parameters or the absence of encryption expose sensitive customer or intellectual property information.

- Rogue access points
- Weak encryption protocols (e.g., WPA2 vulnerabilities)
- Eavesdropping and man-in-the-middle attacks

According to ENISA (2020), organisations using wireless networks without adequate segmentation, authentication, and encryption mechanisms face elevated exposure to network breaches.

3.4 Intellectual Property Protection

NG's intellectual property, such as probable product recipes, proprietary health studies, and ad copy, is a multibillion-dollar resource. The firm has no procedures in effect, however, to isolate and protect such sensitive data.

Without digital rights management and data classification, IP can be accidentally shared, leaked, or stolen. According to a Ponemon Institute study in 2021, 63% of organisations have lost IP due to poor access controls and unsecured endpoint security (Ponemon, 2021) [4].

3.5 Legal and Compliance Exposure

Being a multinational corporation, NG is exposed to numerous data protection laws and regulations, including

- **GDPR** (Europe)
- **HIPAA** (in case the business is doing business in U.S. healthcare facilities)
- **CCPA** (California)

In the absence of a compliance monitoring system, NG is at risk of facing legal and monetary penalties. Non-compliance can result in:

- Fines

- Lawsuits
- Loss of reputation

For example, British Airways was in 2018 fined £20 million for not protecting personal data under GDPR (ICO, 2020). NG faces the same if its data handling is not examined and improved to international standards.

3.6 Strategic Gap

Besides technical vulnerabilities, NG's IT governance deficiency also includes the ability to allocate resources, make decisions, and assign security budgets. There is no accountability established and no incident response plan written, nor an ongoing monitoring process. In their opinion, Weill & Ross (2004) also think that IT governance is necessary to guide security expenditures against business goals and risk acceptance.

3.7 Summary of Key Security Gaps at NG:

Area	Current Status	Risk Level	Urgency	Area
Security Policies	Absent	High	Immediate	Security Policies
BYOD Access Control	Unstructured	High	High	BYOD Access Control
Cloud Configuration	No formal assessment	Medium–High	High	Cloud Configuration
Wireless Network Security	Lacking segmentation/encryption	High	Immediate	Wireless Network Security
Intellectual Property (IP)	No classification or controls	High	Immediate	Intellectual Property (IP)
Regulatory Compliance	No monitoring in place	Very High	Immediate	Regulatory Compliance

4. Proposed Security Framework for Nature Garden

This section advises a step-by-step solution to implementing Nature Garden (NG) security, governance, and compliance. The solution is to integrate two of the most widely used standards, ISO/IEC 27001 and ITIL. The integration will help NG protect its data, reduce risks, and comply with legal requirements (e.g.,

GDPR). Tables and diagrams are included to ensure the plan is clear.

4.1 ISO/IEC 27001 – Security Laws and Risk Management

What is ISO/IEC 27001?

It is a global standard that enables firms to manage information security through established rules and risk management [3].

How NG can use it:

- Set formal security policies (documented rules on how to keep data secure).
- Count and classify vital data like customer data and intellectual property.
- Assess the risk of identifying potential attacks, like hacking or loss of data.
- Use security controls such as
 - Confident password and multi-factor authentication.
 - Encrypting data (so it cannot be accessed in case it is stolen).
 - Limiting access to and use of sensitive papers.

Key Point: ISO 27001 uses a Plan-Do-Check-Act (PDCA) cycle of continuous improvement [3].

Diagram 1: ISO 27001 – Plan-Do-Check-Act



4.2 ITIL Security Management Approach

What is ITIL?

ITIL helps organisations improve the way they manage IT services. ITIL includes guidance for responding to incidents and offers ways to mitigate IT service interruptions [6].

How NG will utilise it:

- Use Incident Management to quickly identify and address security incidents.
- Use Access Management to restrict access to data.
- Use Change Management to review updates to cloud and wireless applications.
- Use service continuity to ensure correct planning and restoration processes for backups.

ITIL will assist you in helping secure the incorporation of security as part of the day-to-day process, not just an audit response [4].

Diagram 2: ITIL Security Management

ITIL SECURITY MANAGEMENT

The Process Includes



4.3 NIST Cybersecurity Framework (CSF)

What is NIST CSF?

The U.S. National Institute of Standards and Technology developed the NIST Cybersecurity Framework (CSF) to help organisations manage and reduce cybersecurity risks. The NIST CSF is widely used across sectors and provides a flexible framework built around five concurrent and continuous key functions: Identify, Protect, Detect, Respond, and Recover. The NIST CSF translates technical actions to business activities and objectives, making it useful for organisations of any size or complexity [7].

How NG will utilise it:

- Identify and establish, and continue to outline, critical digital assets and risk priorities.
- Protect to configure technical controls such as encryption, secure authentication, and firewall settings.
- Detect to identify anomalies or unauthorised actions by implementing real-time logging and alerting systems.
- Respond to create and exercise a security incident response plan (for example, for ransomware or data leaks).
- Recover to develop and exercise a backup system and business continuity plans to return quickly to base operations.

The NIST CSF will enable NG to establish an intentional and ongoing cybersecurity program that focuses on prevention and incident recovery simultaneously [2].

Diagram 3: NIST Framework



4.4 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 1: 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

5. Governance and Compliance Planning

5.1 Risk Management

Risk management is a foundational element of any information security strategy. For NG, which relies heavily on cloud services, BYOD, and wireless networks, a structured risk management framework is essential to identify, evaluate, treat, and monitor both internal and external threats [1].

Using ISO/IEC 27005 and NIST CSF as guides, NG can implement a **cyber risk management cycle** that includes:

- **Asset identification:** Determine critical assets such as customer data, intellectual property, and cloud systems.
- **Threat assessment:** Identify potential threats like unauthorised access, data breaches, malware, and insider threats.
- **Vulnerability analysis:** Examine weaknesses in the current infrastructure, including a lack of endpoint protection or weak access

controls.

- **Risk evaluation:** Assign risk levels based on impact and likelihood.
- **Risk treatment:** Implement mitigation strategies, such as encryption, multifactor authentication (MFA), and employee training.

5.2 Legal and Ethical Considerations (e.g., GDPR)

As NG operates internationally, it must comply with several data protection and privacy regulations. Among the most significant is the General Data Protection Regulation (GDPR), which applies to any organisation processing personal data of EU residents [2].

Key GDPR obligations include:

- **Data minimisation:** Only collect data necessary for a specific purpose.
- **User consent:** Ensure explicit, informed consent for data processing.
- **Right to erasure:** Allow users to request deletion of their data.
- **Breach notification:** Notify regulators and affected individuals within 72 hours of a data breach.
- **Data protection by design and by default:** Embed privacy into systems and processes.

In addition to legal compliance, ethical considerations must guide NG's practices. This includes:

- **Transparency** in how customer and employee data is collected and used.
- **Fairness** in profiling, analytics, and marketing.
- **Accountability** through auditing and clear documentation.

Ethical behaviour reinforces brand reputation, builds trust, and supports long-term sustainability.

5.3 Roles and Responsibilities

Defining and assigning clear roles is essential to enforce governance, accountability, and continuous security. NG should adopt an RACI matrix (Responsible, Accountable, Consulted, Informed) for managing security initiatives [4].

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.

6. Conclusion

The report has provided a thorough assessment of Nature Garden ongoing information security issues and recommended a strategic security governance and compliance framework that was reviewed in the context of Nature Garden operational context. Given the company's cloud-based, wireless, and BYOD based architectures, the lack of formalised policies, assigned roles and responsibilities, and integrated security solutions exposes the organisation to significant cyber risk and regulatory infringements.

Drawing on internationally recognised frameworks such as ISO/IEC 27001, ITIL, and the NIST Cybersecurity Framework (CSF), the report has suggested a layered approach to information security, which incorporates both high-level governance and operational activity. ISO/IEC 27001 provides the skeleton for a risk-based Information Security Management System (ISMS), whilst ITIL ensures security activity will take its place as part of the organisation's day-to-day IT operations. Adding the agility and responsive approach of the NIST CSF in its approach to cyber risk, with the oversight and governance, ensures security activity will become business as usual.

More widely, the report referenced the additional role of regulatory compliance, particularly with GDPR, as part of the critical role of maintaining stakeholder data and business integrity. The report underscored the importance of

continuous improvement, transparency, and formalised roles across departments.

6.1 Strategic Recommendations:

- **Implement ISO/IEC 27001 ISMS**
 - Establish security policies, perform risk assessments, and apply Annex A controls to secure all information assets [4].
- **Adopt ITIL Security Processes**
 - Integrate incident management, change control, access management, and service continuity into daily IT operations.
- **Apply the NIST Cybersecurity Framework**
 - Use the Identify-Protect-Detect-Respond-Recover model to build cyber resilience and real-time response capabilities [6].
- **Ensure Regulatory Compliance (e.g., GDPR)**
 - Embed data protection principles by design and conduct routine audits to maintain compliance [1].

6.2 Practical Recommendations:

- **Develop and roll out BYOD and MDM policies** to control device access and mitigate data leakage risks [5].
- **Classify and protect intellectual property** with encryption, access control, and digital rights management (DRM).
- **Set up an IT Governance Board** chaired by a CISO to provide leadership and monitor security initiatives.
- **Provide mandatory training programs** for staff and executives to improve security awareness and compliance culture.

- **Draft strong service-level agreements (SLAs)** with cloud vendors to ensure accountability in data handling and breach response.
- **Conduct quarterly risk reviews** and update the security roadmap based on emerging threats and lessons learned.

7. References

[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/](#)

8. Appendix

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.

