

UNIVERSITY OF WALES TRINITY SAINT DAVID(UWTSD)

**Assignment Title: Apply the principles and practices of Data security,
Governance and Compliance based on a given scenario.**

Md.Nabil Rahman

ID: 2504501

Course Code: ACCA7028

Course Name: Data Security, Governance and Compliance

Lecturer: Assoc. Prof. Carlene Campbell

MSc Software Engineering and Artificial Intelligence

January 8th 2026

Abstract

NatureGreen (NG) is a fast-growing company with strong online presence and heavy dependence on information systems. Rapid expansion without structured security governance has exposed NG to serious risks such as data breaches, intellectual property theft, and regulatory non-compliance. This assignment analyzes recognized information security frameworks and models, and proposes a comprehensive, customized security governance approach for NG. The discussion emphasizes why continuously updated regulations, standards, and policies are essential for sustaining security in a dynamic threat landscape.

Contents

Abstract	i
List of Figures	iii
1 Introduction	1
2 Information Security Frameworks and Models	1
2.1 IT Infrastructure Library (ITIL)	1
2.2 ISO/IEC 27001	2
2.3 Security Models	3
2.3.1 CIA Triad	3
2.3.2 Defense-in-Depth Model	3
3 Customized Security Approach for NatureGreen	4
3.1 Security Governance and Strategy	4
3.1.1 Information Security Governance Roles and Responsibilities (RACI Matrix)	
Table:	4
3.2 Security Policies	6
3.3 Risk Management:	6
3.4 Compliance (Laws and Ethics)	7
3.5 Security Management Practices	7
3.6 Contingency and Business Continuity Planning	7
3.7 Protection Mechanisms	8
3.8 Service Level Agreements (SLAs)	8
4 Importance of Continuous Updates to Regulations and Standards	8
5 Extended Critical Analysis of Security Framework Adoption	9
6 Human Factors and Security Awareness	10
7 Integration of Security with Business Strategy	10
8 Future Security Considerations for NatureGreen	10
9 Conclusion	11
10 REFERENCES	12

List of Figures

2.1 ITIL Service Lifecycle 2

2.2 ISO/IEC 27001 ISMS (PDCA Cycle) 3

2.3 Defense-in-Depth Security Model 4

3.4 Information Security Governance Roles and Responsibilities (RACI Matrix) 5

3.5 Table:Sample Risk Assessment 7

1 Introduction

NatureGreen operates in the healthy living products sector and relies extensively on digital infrastructure, including e-commerce platforms, customer databases, social media systems, and cloud-based services. The absence of established security policies, combined with increasing cyber threats, places customer data, employee information, and intellectual property at significant risk. This assignment evaluates established security frameworks and applies them to NG's context to design an effective information security management approach.

2 Information Security Frameworks and Models

2.1 IT Infrastructure Library (ITIL)

ITIL is a best-practice framework focused on aligning IT services with business needs. From a security perspective, ITIL emphasizes Information Security Management (ISM) as part of service management [2].

Key Components Relevant to NG:

- Confidentiality, Integrity, and Availability (CIA Triad)
- Incident management and problem management
- Continuous service improvement

Benefits to NG: ITIL helps NG integrate security into daily IT operations, ensuring that security supports business objectives rather than acting as a barrier.

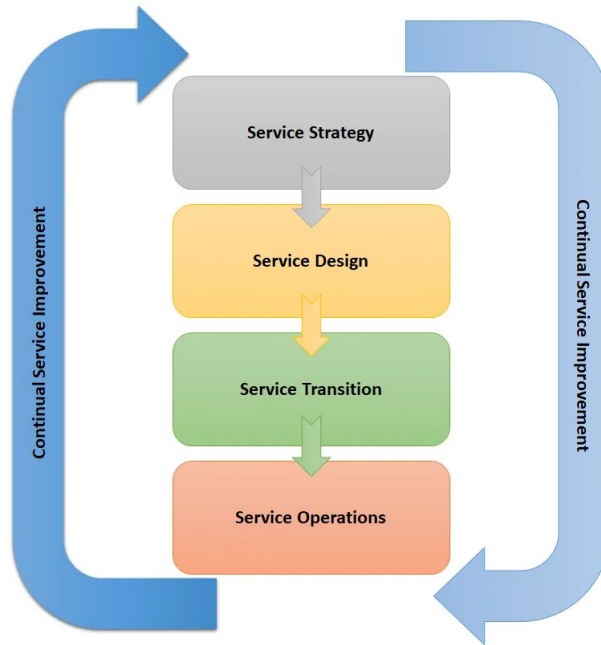


Figure 2.1: ITIL Service Lifecycle

2.2 ISO/IEC 27001

ISO/IEC 27001 is an international standard for establishing an Information Security Management System (ISMS) [1].

Core Elements:

- Risk assessment and risk treatment
- Security policies and objectives
- Management commitment and continual improvement

Benefits to NG: ISO/IEC 27001 provides NG with a structured and auditable approach to managing information security risks, increasing customer trust and regulatory compliance.

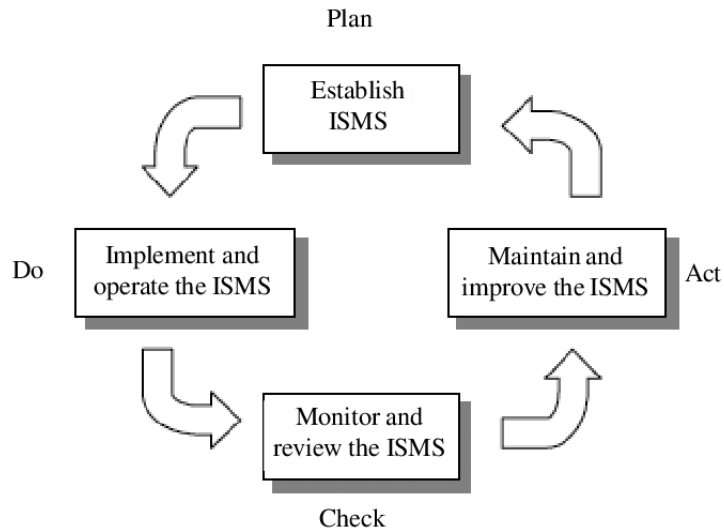


Figure 2.2: ISO/IEC 27001 ISMS (PDCA Cycle)

2.3 Security Models

2.3.1 CIA Triad

The CIA Triad forms the foundation of information security [4]:

- Confidentiality: Protecting customer and employee data
- Integrity: Ensuring data accuracy and consistency
- Availability: Ensuring systems remain accessible

2.3.2 Defense-in-Depth Model

This model applies multiple layers of security controls [5]:

- Physical security
- Network security (firewalls, IDS/IPS)
- Application security
- User awareness and training

Defense in Depth/ Layered Defense Model

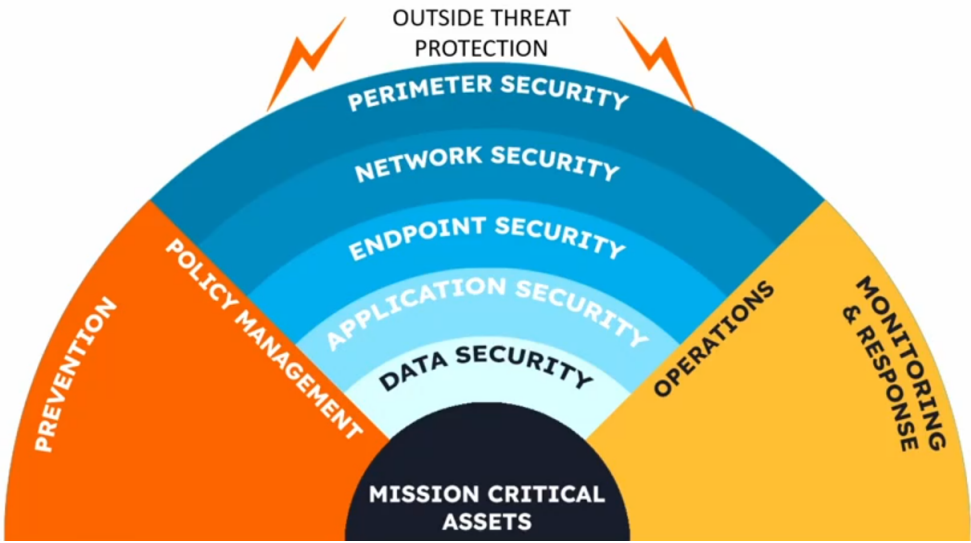


Figure 2.3: Defense-in-Depth Security Model

3 Customized Security Approach for NatureGreen

3.1 Security Governance and Strategy

NG should establish a Security Governance Committee responsible for:

- Aligning security with business goals
- Approving security policies
- Ensuring compliance with laws and standards

3.1.1 Information Security Governance Roles and Responsibilities (RACI Matrix)

Table:

Level	Role	Key Governance Responsibilities	Accountability (RACI)
Strategic	Board of Directors / CEO	Define "Risk Appetite" for IP; approve the Information Security Strategy; provide funding for security infrastructure.	A
Strategic	Chief Information Security Officer (CISO)	Develop the ISMS (ISO 27001); establish security benchmarks for cloud providers; lead the Incident Response Team (IRT).	R / A
Tactical	Information Security Manager	Oversee daily compliance with the BYOD policy; manage vulnerability assessments; coordinate security audits.	R
Tactical	Cloud Service Manager	Manage SLAs with cloud providers; ensure "Security by Design" in cloud architecture; oversee data sovereignty/residency.	R / C
Operational	Network Engineer	Configure and monitor WPA3 Enterprise wireless protocols; manage VLAN segmentation; detect rogue Access Points (APs).	R / I
Operational	Human Resources (HR)	Conduct security awareness training; enforce disciplinary actions for policy violations; manage employee offboarding (revoking cloud access).	C / I
Operational	Staff / Employees	Adhere to the Acceptable Use Policy (AUP); maintain the security hygiene of personal devices (BYOD); report phishing/suspicious activity.	I

Figure 3.4: Information Security Governance Roles and Responsibilities (RACI Matrix)

3.2 Security Policies

NG must implement formal security policies, including:

- Acceptable Use Policy
- Data Protection and Privacy Policy
- Access Control Policy
- Incident Response Policy These policies provide clear guidance and accountability across the organization.

3.3 Risk Management:

A structured risk management process should be adopted, in accordance with global best practices like NIST standards and ISO/IEC 27001 [1], [3]:

- Identify assets (customer data, IP, systems)
- Identify threats and vulnerabilities
- Assess likelihood and impact
- Implement controls
- Monitor and review

Asset	Threat	Impact	Control
Customer Database	Data breach	High	Encryption, access control
IP Designs	Theft	High	Network segmentation

Figure 3.5: Table:Sample Risk Assessment

3.4 Compliance (Laws and Ethics)

NG must comply with data protection laws and ethical standards, such as international data protection regulations and industry best practices [1], [3]:

- Data privacy regulations
- Consumer protection laws
- Industry best practices

Compliance ensures legal protection and strengthens customer trust.

3.5 Security Management Practices

Security practices should include controls recommended by recognized security standards and frameworks [3], [4]:

- Regular vulnerability assessments and penetration testing
- Security awareness training
- Incident response drills
- Logging and monitoring

3.6 Contingency and Business Continuity Planning

- NG should implement:
- Disaster Recovery Plan (DRP)
- Business Continuity Plan (BCP)
- Regular backups and recovery testing

3.7 Protection Mechanisms

Key technical controls include:

- Firewalls and intrusion detection systems
- Multi-factor authentication
- Data encryption (at rest and in transit)
- Endpoint protection

3.8 Service Level Agreements (SLAs)

SLAs with third-party vendors should define:

- Security responsibilities
- Incident response time
- Data protection requirements

4 Importance of Continuous Updates to Regulations and Standards

Cyber threats evolve rapidly, making static security measures ineffective [3]. Frequent revisions to security standards and regulations:

- Address emerging threats
- Ensure legal compliance
- Improve resilience and adaptability

Failure to update standards exposes organizations like NG to increased risk and potential regulatory penalties.

Information security is a constant process that must change in tandem with increasing cyberthreats and technical advancements. Ransomware, phishing, supply-chain attacks, and insider threats are just a few of the new tactics that threat actors are continuously developing in the dynamic digital environment in which organizations like NatureGreen operate. Static or outdated security measures soon lose their efficacy and may even give people a false sense of security [3].

Organizations are kept safe from emerging attack vectors through regular upgrades to security standards, legislation, and internal policies. Organizations must regularly review risk assessments, audit controls, and update documentation as part of the Plan-Do-Check-Act (PDCA) cycle, which is emphasized by international standards like ISO/IEC 27001 [1]. Organizations run the risk of losing compliance and exposing vital assets if this cycle is not followed.

Data protection laws are often updated to handle new types of data processing and international data transfers from a legal and ethical standpoint. If regulations are not followed, there may be severe financial penalties, harm to one's reputation, and a decline in customer confidence. Regulatory non-compliance might have long-term detrimental effects on NatureGreen, a company that greatly depends on consumer trust in its brand.

Additionally, ongoing improvements promote company flexibility. NatureGreen's risk profile shifts when it enters new markets and uses new technology like social media marketing tools and cloud computing. Security measures should not lag behind business expansion, but rather scale effectively with it thanks to updated standards and regulations.

5 Extended Critical Analysis of Security Framework Adoption

Although they offer solid direction, frameworks like ITIL and ISO/IEC 27001 have certain drawbacks. The expense and resources needed for formal security framework implementation and upkeep are a problem for NatureGreen. Organizations that are smaller or expanding quickly frequently face financial constraints and a shortage of qualified security experts.

Another limitation is that frameworks are often high-level and require customization to suit organizational context. Blindly adopting controls without understanding business processes may lead to inefficiencies or resistance from employees. Therefore, NatureGreen must adopt a risk-based approach, prioritizing controls that protect its most valuable assets, such as customer data and intellectual property.

Despite these challenges, the benefits outweigh the limitations. Framework-based security implementation promotes consistency, accountability, and transparency. It also facilitates communication with external stakeholders such as auditors, regulators, and business partners, who often expect alignment with internationally recognized standards [2].

6 Human Factors and Security Awareness

Technology cannot protect an enterprise on its own. Globally, human mistake continues to be one of the main causes of security events. Employees who use weak passwords, participate in phishing scams, or handle data improperly may unintentionally compromise systems. NatureGreen must thus fund ongoing security awareness and training initiatives.

Security awareness initiatives should include:

- Regular training sessions on phishing and social engineering
- Clear guidance on acceptable use of company systems
- Simulated attack exercises to test employee readiness

By fostering a security-aware culture, NatureGreen can significantly reduce the likelihood of successful attacks and improve incident response effectiveness [4].

7 Integration of Security with Business Strategy

Information security should not operate in isolation but must be integrated into NatureGreen's overall business strategy. Strategic alignment ensures that security investments support business objectives rather than hinder innovation. For example, secure e-commerce platforms enable customer trust, while strong intellectual property protection supports long-term competitiveness.

Senior management involvement is critical to this integration. Executive leadership must demonstrate commitment by allocating resources, approving policies, and actively participating in governance structures. This top-down approach reinforces the importance of security across the organization and encourages compliance at all levels.

8 Future Security Considerations for NatureGreen

Looking forward, NatureGreen must prepare for emerging technologies and associated risks. Increased use of cloud services, mobile platforms, and third-party vendors introduces new dependencies and attack surfaces. Supply-chain security and third-party risk management should therefore become strategic priorities.

In addition, NatureGreen should consider adopting advanced security capabilities such as:

- Security Information and Event Management (SIEM)
- Zero Trust security models

- Automated incident response tools

These technologies enhance visibility, detection, and response capabilities, allowing NatureGreen to remain resilient in an increasingly complex threat environment [3], [5].

9 Conclusion

Information security has evolved from a technical problem to a fundamental business requirement because to NatureGreen’s quick growth and robust digital presence. The current lack of formalized policies and governance structures leaves the organization vulnerable to data breaches, loss of intellectual property, and potential regulatory non-compliance, underscoring the need for immediate and strategic action.

This assignment has demonstrated how internationally recognized frameworks such as ITIL and ISO/IEC 27001, supported by foundational security models like the CIA Triad and Defense-in-Depth, can be applied to address NatureGreen’s security challenges. By implementing strong governance, comprehensive policies, effective risk management, and continuous improvement processes, NatureGreen can significantly enhance its security posture.

Ultimately, information security is an ongoing journey. Continuous updates to standards, policies, and controls are essential to maintaining resilience, ensuring compliance, and supporting sustainable business growth in an evolving digital landscape.

10 REFERENCES

- [1] ISO/IEC, ISO/IEC 27001: Information Security Management Systems, International Organization for Standardization, Geneva, Switzerland, 2022.
- [2] AXELOS, ITIL Foundation: ITIL 4 Edition, London, UK: The Stationery Office (TSO), 2019.
- [3] National Institute of Standards and Technology (NIST), Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1, Gaithersburg, MD, USA, 2018.
- [4] W. Stallings, Network Security Essentials: Applications and Standards, 6th ed. Boston, MA, USA: Pearson, 2017.
- [5] M. E. Whitman and H. J. Mattord, Principles of Information Security, 7th ed. Boston, MA, USA: Cengage Learning, 2021.