

**Designing an Integrated Information Security, Governance, and
Compliance Framework for NatureGreen**

BY: Omar Sufer 2420868@student.uwtsd.ac.uk

Abstract

This report examines the information security, governance, and compliance challenges faced by NatureGreen (NG) and evaluates how established frameworks can be applied to address these issues. NG is a global brand worth billions but lacks any structured governance and security frameworks, relies on wireless connectivity, and uses cloud services to deliver its IT services. The report reviews popular frameworks such as the ISO/IEC 27001, ISO/IEC 27002, ITIL, and the NIST Cybersecurity Framework, and analyses their relevance to NG's operational context. Based on the review, a suitable framework is proposed to match the challenges and risks that NG faces as an organisation. The report will then discuss why it is good practice to constantly have new or updated regulations and standards.

Contents Page

Abstract	2
1. Introduction	4
2. Case Scenario: NatureGreen (NG)	5
3. Assumptions	5
4. Review of Information Security Frameworks and Models	6
4.1 ISO/IEC 27001 and ISO/IEC 27002	6
4.2 Information Technology Infrastructure Library (ITIL)	6
4.3 NIST Cybersecurity Framework	7
4.4 Comparison of Frameworks	8
5. Proposed Information System Security, Governance and Compliance Framework for NatureGreen	9
5.1 Overview of the Proposed Approach	9
5.2 Governance and Strategic Planning for Security	9
5.3 Security Policies	10
5.4 Risk Management	10
5.5 Protection Mechanism	11
5.6 Compliance and Continuous Improvement	11
6. The Importance of Continually Updating Regulations and Standards	12
7. Conclusion	12
8. References	13

1 Introduction

Technology has been rapidly evolving and with it the reliance of organisations on using it to store, process and share information using technologies such as cloud computing and social media. While these changes have made it easier for organisations to become more accessible to their customers, they also increase their exposure to information security threats [1]. In order to combat this issue, modern organisations need to evolve their approaches to information security, governance, and compliance in order to protect their data, customers, and meet legal obligations where they trade.

NatureGreen (NG) is a globally recognised and sought-after company that provides customers with products for a healthier lifestyle. With their global presence, they rely on using cloud services to deliver their IT services to both staff and clients, relying mostly on a wireless network infrastructure, and maintaining a large only and social media presence to promote their brand. In addition, NG is currently under pressure by both staff and customers to allow them to use their personal devices to access the company network, known as Bring Your Own Device (BYOD) practices [2]. While implementing BYOD practices and relying mostly on a wireless network infrastructure will help increase NG's flexibility, productivity, and scalability, they will also introduce major security risks. Risks include unauthorised access to sensitive staff and customer data, threats to system integrity, and potential compromise of the company's intellectual property. The risks that NG faces are made even worse by the absence of an established information security policy framework and governance structure within the company.

This report will examine how already established information security, governance, and compliance frameworks can be applied to help NG's security risks. The report will begin by reviewing relevant security frameworks and models, including some from the ISO/IEC 27000 series, Information Technology Infrastructure Library (ITIL), and other related standards, showing how each one is relevant to what NG needs and lacks. Using all of this information, the report will then propose a tailored information security, governance, and compliance framework designed specifically to meet NG's needs and risk profile.

Finally, the report will discuss the importance of constantly updating regulations and standards in response to how technology evolves and the emerging threats that might come with it.

2 Case Scenario: Nature Green(NG)

NatureGreen (NG) is an organisation that operates globally using cloud-based services to deliver its IT services and resources to its staff and customers. It is estimated that 95% of the organisation's network infrastructure is wireless. Moreover, NG relies on its social media presence to promote its brand, further increasing the risk of being hacked and damaging its reputation. Furthermore, NG is facing a demand to support Bring Your Own Device (BYOD) practices by customers and employees. By increasingly allowing the use of personal devices to access the company's systems and resources, it enhances productivity and convenience, but it also introduces more security risks, such as unauthorised access, data leaks, and damage to the company's reputation [3]. This threat increases as NG's user base increases, where it becomes more likely that a compromised user tries accessing NG's network, which complicates the security management.

The protection of sensitive information is a major concern for NG. The organisation holds a large amount of personal data belonging to staff and customers, and since they work globally, they are subject to data protection legislation such as the General Data Protection Regulation (GDPR) [4]. In addition, NG's intellectual property is worth billions, making it a high-value target for hackers. The risk of a successful breach means that the company can result in major financial losses, legal penalties and a massive distrust by their staff and customers. Furthermore, while NG recognises the importance of information security, it currently lacks any form of information security policy and formal governance structure. Meaning that, NG cannot systematically assess security risks, enforce any security controls or demonstrate compliance to any regulatory body.

Finally, the reliance on wireless connectivity, cloud-based services, and BYOD practices, on top of not having a structured security governance framework, exposes NatureGreen to more information security risks. This highlights the importance of a structured, risk-based information security, governance, and compliance approach using recognised frameworks.

3 Assumptions

The following assumptions have been made in order to support the analysis and proposed security, governance, and compliance framework for NatureGreen(NG), based on the scenario given.

1. NG operates within multiple legal jurisdictions and is therefore subject to international data protection regulations such as the General Data Protection Regulation(GDPR), due to its global staff and customer base.
2. NG uses third-party cloud service providers for the hosting and processing of customer data, operating under a shared responsibility model for information security.
3. NG processes and stores sensitive information, including personal data and intellectual property, which requires protection against unauthorised access.

4 Review of Information Security Frameworks and Models

Information security frameworks and models are used for structured and standardised approaches for an organisation to manage security risks. Rather than relying on reactive measures, frameworks allow organisations to identify risks, implement appropriate controls, and apply compliant measures with the legal requirements they must follow. This section will review information security and service management frameworks that are relevant to how NatureGreen (NG) operates, focusing on their strength, weaknesses, and applicability to NG's security challenges.

4.1 ISO/IEC 27001 and ISO/IEC 27002

ISO/IEC 27001 is a popular standard that gives the requirements for managing and continuously improving a company's Information Security Management System (ISMS). Its main purpose is to provide a structured management framework for organisations to govern information security in a risk-based approach. Its main advantage is requiring organisations to identify and treat risks based on their potential business impact and how likely they might occur [5]. This makes ISO/IEC 27001 relevant for NG because of the lack of any security governance and large threat potential due to their popularity and worth.

ISO/IEC 27002 complements ISO/IEC 27001 by working as a practical guide for the information security objectives given with the ISMS. ISO/IEC 27002 is a standard that provides organisations with structured guidance on a wide range of security measures that can be used to address identified risks. These measures include both technical and organisational safeguards, allowing organisations to select and implement controls that are appropriate to how they operate [6]. This flexibility works well for NG since it allows for security controls to be tailored to its cloud-based operations and wireless infrastructure.

For NG, ISO/IEC 27001 and 27002 are a strong foundation for addressing threats to personal data, intellectual property worth billions, and cloud-stored data. On the other hand, they are limited to describing outcomes rather than providing detailed instructions on how the services should operate.

4.2 Information Technology Infrastructure Library (ITIL)

ITIL is a framework that provides organisations with guidance on how to design, transition, operate, and continually improve their IT services. Its main focus is how the organisation's IT services support their objectives and help deliver them in a consistently reliable way [7]. It's important to note that while ITIL is not a security framework, it tries to create an operational environment for the organisation so security requirements can be used effectively.

At its core, ITIL offers a flexible approach for managing day-to-day IT service delivery. This is relevant to information security because the framework promotes predictable and consistent deliverables using the lifecycle perspective in which the services will be designed, transitioned into operations, which will continuously be reviewed for improvement at every step, making security a consideration throughout the service lifecycle [8]. However, a major limitation of ITIL is that it does not define how the information security risks should be assessed or which controls should be implemented.

4.3 NIST Cybersecurity Framework

The National Institute of Standards and Technology (NIST) cybersecurity framework was created to help organisations manage cybersecurity risks in a structured manner. Rather than giving mandatory requirements, NIST provides a common structure for organising cybersecurity activities across a lifecycle of identification, protection, detection, response, and recovery. The lifecycle allows organisations to align their cybersecurity activities with their business objectives, risk level, and their available resources, allowing an ongoing assessment of cybersecurity that can improve and evolve with the company's wants and needs [9]. With recent updates to the framework, further emphasis was placed on governance by focusing on organisational accountability and integration with enterprise risk management throughout the cybersecurity lifecycle. The core strength of the NIST cybersecurity framework is its flexibility; it understands that organisations differ in their risk exposure, operational levels, and financial capacity [10]. The lifecycle allows for the organisation to use a suitable approach that can be continuous with incremental improvement. This is particularly valuable for an organisation such as NatureGreen, which is at risk of large cyber attacks. However, despite its recent updates focusing on governance, the NIST framework is still less prescriptive compared to formal governance standards



Figure 1: NIST 2.0 cybersecurity lifecycle [11]

4.4 Comparison of Frameworks

Each of the reviewed frameworks address a different aspect of information security, meaning that no single frameworks meets all criteria to help a massive organisation such as NG on their own.

Table 1: Comparison of Security Frameworks

Framework	Primary Focus	Strengths	Limitations
ISO/IEC 27001	Information security governance	Risk-based ISMS, compliance	Weak operational guidance
ISO/IEC 27002	Security controls	control guidance	No governance structure
ITIL	IT service management	Operational efficiency	Weak security guidance
NIST	Cybersecurity lifecycle	Incident response and resilience	Limited compliance focus

ISO/IEC 27001 is the most relevant framework for NG, since it provides a formal governance and risk-based approach to managing information security. However, it offers limited guidance on how security should be controlled in daily IT operations. ISO/IEC 27002 addresses this gap by providing guidance on the selection of security controls that can be used to stop the identified risks, although ISO/IEC 27002 itself does not provide any governance or compliance mechanism on its own. ITIL complements this approach by focusing on how the IT services are designed, delivered, and operated while continuously improving, allowing for a consistent service delivery and incident handling. On the other hand, its limitation is that it does not define security risks or controls, making it an unsuitable framework to manage security on its own. Finally, the NIST cybersecurity framework is valuable because of its lifecycle-based approach to managing cybersecurity incidents, especially detection, response, and recovery. Unfortunately, while it increasingly recognises governance considerations, it's less prescriptive than ISO/IEC 27001. Overall, while ISO/IEC 27001 is the most relevant framework for NatureGreen, the most effective approach is an integrated one, with ISO/IEC 27001 providing governance foundation, supported by ISO/IEC 27002 for control selection, ITIL for operational service management, and NIST for enhancing cybersecurity resilience.

5 Proposed Information System Security, Governance and Compliance Framework for NatureGreen

5.1 Overview of the Proposed Approach

NatureGreen (NG) relies heavily on digital technologies to support its business operations, such as its cloud-based services, wireless connectivity, and Bring Your Own Devices (BYOD) practices. On top of that, the absence of a security governance structure means there is an increased information security, potentially legal, and operational risks that NG faces.

In response to the risks, this section proposes a tailored information security, governance, and compliance framework designed specifically for NG. Utilising research done in previous sections, the approach uses best practice standards such as ISO/IEC 27001, ISO/IEC 27002, and will be supported by the IT service management principles drawn from the ITIL. As previously concluded, rather than applying a single framework in isolation, the proposed approach will integrate different approaches into one cohesive structure that fits NG's business objectives.

The framework is designed to be risk-based and scalable, enabling NG to protect its sensitive data and meet regulatory obligations and effectively respond to threats.

5.2 Governance and Strategic Planning for Security

Strong governance is the foundation of effective information security. NG is a global brand without any defined security leadership, allowing for decisions to be made without proper risk management and accountability. To address this issue, the proposed governance structure establishes a clear governance structure and hierarchy that aligns with ISO/IEC 27001 requirements for leadership and accountability. Defining operational responsibility clearly to ensure effective implementation and the show of accountability within the organisation.

Table 2: Proposed Security Governance Structure

Role	Responsibility
Board of Directors	Oversight of information security strategy and risk
Chief Information Security Officer (CISO)	Development and management of the ISMS
Data Protection Officer (DPO)	Data protection and GDPR compliance
IT Security Team	Implementation administrative controls
Employees and Contractors	Compliance with security policies

5.3 Security Policies

Security Policies allow governance decisions to become organisational rules. NG's lack of governance means there will be a lack of formal security documentation for people within the organisation to follow. The proposed framework prioritises policies that directly address NG's highest risk areas, focusing on BYOD practices. Access control within the organisation and data protection.

Table 3: Security Policies for NatureGreen

Policy	Purpose
Information Security Policy	Defines overall security objectives and responsibilities
BYOD Policy	Regulates use of personal devices
Access Control Policy	Enforces least-privilege access
Data Classification Policy	Protects sensitive and critical data

5.4 Risk Management

Risk management is the most important part of the framework. In accordance with ISO/IEC 27001 principles, NG should use a structured and continuous risk management process, by identifying risks, assessing them, creating a specific treatment, then reviewing and updating.

The key risks that NG faces come from wireless infrastructure, cloud dependency, and BYOD practices. These risks must be evaluated based on their business impact and their likelihood to ensure proportionate control measurement and priority.

Table 4: Example Risk Assessment

Risk	Likelihood	Impact	Risk Treatment
Data leakage via BYOD	High	High	Mobile device management, data encryption
Cloud data exposure	Medium	High	Data encryption, contractual controls
Insider threats	Medium	High	Access controls, logging

This risk based approach ensures that security resources are priorities effectively where the organisation needs them.

5.5 Protection Mechanism

After dealing with identified risks, NG should implement a layered set of security controls in accordance with ISO/IEC 27002 to decrease the chances of them showing up. The controls need to be categorised into technical, administrative, and physical measures.

Table 5: Security Controls

Control Type	Control	Purpose
Technical	Multi-Factor Authentication	Prevent unauthorised access
Technical	Encryption	Protect data confidentiality
Administrative	Security awareness training	Reduce human error
Physical	Secure access controls	Protect physical assets

5.6 Compliance and Continuous Improvement

NG is a global brand, meaning that compliance with legal and regulatory requirements is an important part of the proposed framework to ensure no legal trouble occurs. The framework aligns NG’s practices with relevant regulations, such as the GDPR, to allow the brand to operate globally legally. This approach is only effective if NG continuously evolves to work with updated regulations around the world.

6 The Importance of Continually Updating Regulations and Standards

As technology evolves, the information security regulations and standards need to rapidly evolve alongside it to deal with the cyber threat landscape. For example, as organisations use new technology such as cloud computing, wireless networking, AI chatbots, etc.... Old security assumptions become outdated [12]. Making static regulations and standards dangerous will put organisations that use them at a higher security risk.

For NG, evolving data protection laws reflect changes in societal expectations around privacy and ethical data use [13], so adapting to them maintains staff and customer trust. The purpose of these updates is to ensure that organisations are responsible guardians of personal and sensitive data that is shared with them. For NG, which has an international customer base and heavily relies on cloud services to process and store its data, updated regulations can provide clearer guidance on customer needs and expectations.

Finally, similarly to what was discussed in the proposed framework for NG, maintaining up-to-date regulations and standards is a good practice. This is because, as technology evolves, adapting to their new regulations and standards will place organisations such as NG in a better position to manage risk and maintain compliance.

7 Conclusion

This report analysed NatureGreen's information security challenges and reviewed how some established frameworks can be used to address its governance, compliance, and security requirements. The analysis showed that while ISO/IEC 27001 is the most relevant for NG, no single framework deals with the requirements needed, showing that an integrated approach would be best. Finally, the report analysed the importance of maintaining up-to-date information security regulations and standards in response to rapid technological changes. Talking about how, as organisations increasingly rely on new technology, older security assumptions become outdated and place the organisations at a higher risk of cyber threat if they haven't evolved with it. For NatureGreen, adapting to evolving data protection laws is particularly important as they are a global brand and must maintain customer trust by showing how they comply with new regulations and keep customer data safe.

8. References

- [1] J. Lewallen, "Emerging technologies and problem definition uncertainty: The case of cybersecurity," *Regulation & governance*, vol. 15, no. 4, pp. 1035–1052, 2021, doi: 10.1111/rego.12341.
- [2] M. Eslahi, M. V. Naseri, H. Hashim, N. M. Tahir, and E. H. M. Saad, "BYOD: Current state and security challenges," in *2014 IEEE Symposium on Computer Applications and Industrial Electronics (ISCAIE)*, IEEE, 2014, pp. 189–192. doi: 10.1109/ISCAIE.2014.7010235.
- [3] Mohammed Rahmat Ali and Pathan Ahmed Khan, "BYOD... A SYSTEMATIC APPROACH FOR ANALYZING AND VISUALIZING THE TYPE OF DATA AND INFORMATION BREACHES WITH CYBER SECURITY," *NeuroQuantology*, vol. 20, no. 15, p. 849, 2022, doi: 10.14704/NQ.2022.20.15.NQ88081.
- [4] S.-D. Axinte, G. Petrică, and I. Bacivarov, "GDPR Impact on Company Management and Processed Data," *Calitatea*, vol. 19, no. 165, pp. 150–153, 2018.
- [5] G. Culot, G. Nassimbeni, M. Podrecca, and M. Sartor, "The ISO/IEC 27001 information security management standard: literature review and theory-based research agenda," *TQM journal*, vol. 33, no. 7, pp. 76–105, 2021, doi: 10.1108/TQM-09-2020-0202.
- [6] I. Bashofi and M. Salman, "Cybersecurity Maturity Assessment Design Using NISTCSF, CIS CONTROLS v8 and ISO/IEC 27002," in *2022 IEEE International Conference on Cybernetics and Computational Intelligence (CyberneticsCom)*, IEEE, 2022, pp. 58–62. doi: 10.1109/CyberneticsCom55287.2022.9865640.
- [7] H. Gunawan, A. B. P. Irianto, and J. G. P. Negara, "Implementation of sustainable service improvement in organizations using framework information technology infrastructure library (ITIL)," *Procedia Computer Science*, vol. 234, pp. 748–755, 2024.
- [8] H. Gunawan, "Strategic Management for IT Services Using the Information Technology Infrastructure Library (ITIL) Framework," in *2019 International Conference on Information Management and Technology (ICIMTech)*, IEEE, 2019, pp. 362–366. doi: 10.1109/ICIMTech.2019.8843711.
- [9] L. A. Gordon, M. P. Loeb, and L. Zhou, "Integrating cost–benefit analysis into the NIST Cybersecurity Framework via the Gordon–Loeb Model," *Journal of cybersecurity (Oxford)*, vol. 6, no. 1, 2020, doi: 10.1093/cybsec/tyaa005.
- [10] P. P. Roy, "A High-Level Comparison between the NIST Cyber Security Framework and the ISO 27001 Information Security Standard," in *2020 National Conference on Emerging Trends on Sustainable Technology and Engineering Applications (NCETSTE)*, IEEE, 2020, pp. 1–3. doi: 10.1109/NCETSTE48365.2020.9119914.
- [11] NIST FIGURE REFERENCE: National Institute of Standards and Technology, *The NIST Cybersecurity Framework (CSF) 2.0*, NIST CSWP 29, Gaithersburg, MD, Feb. 26, 2024. Available: <https://doi.org/10.6028/NIST.CSWP.29>

[12] Ejiofor Oluomachi, Akinsola Ahmed, A. Wahab, and Edozie Samson, "Assessing The Effectiveness Of Current Cybersecurity Regulations And Policies In The US," *arXiv.org*, 2024, doi: 10.48550/arxiv.2404.11473.

[13] L. N. Berg, "Transformation of legal impact in the context of the modern information and technological structure (case study of the relations connected with genomic information)," *SHS web of conferences*, vol. 134, p. 117, 2022, doi: 10.1051/shsconf/202213400117.