



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

Module Title:

Data Security, Governance and Compliance

Module Code:

ACCA7028

Assignment Title:

**Apply the Principles and Practices of Data security, Governance and Compliance
Based on a Given Scenario.**

Student Name:

MD Mahadi Hasan

Student ID:

2505591

Programme:

MSc in Software Engineering and Artificial Intelligence

University Name:

University of Wales Trinity Saint David (Swansea Campus)

Lecturer:

Assoc. Prof. Carlene Campbell

Submission Date:

08 January 2026

Table of Contents

Abstract.....	3
1. Introduction.....	4
2. Literature Review.....	4
2.1 Introduction to Security Frameworks and Standards.....	4
2.2 ISO/IEC 27001.....	5
2.3 Information Technology Infrastructure Library (ITIL).....	6
2.4 NIST Cybersecurity Framework.....	7
2.5 Comparative Discussion.....	7
3. Proposed Security, Governance and Compliance Framework for NatureGreen (NG).....	8
3.1 Design Principles and Assumptions.....	8
3.2 Security Governance Structure.....	8
3.3 Risk Management Approach.....	9
3.4 Security Policies Framework.....	9
3.5 Technical and Organisational Controls.....	9
3.6 Compliance and Standards Alignment.....	10
3.7 Incident Response and Contingency Planning.....	10
3.8 Service Level Agreements (SLAs).....	10
4. Why Regulations and Standards Must Be Continuously Updated.....	11
4.1 Evolution of Cyber Threats.....	11
4.2 Technological Advancements and Changing Risk Profiles.....	11
4.3 Regulatory Compliance and Legal Obligations.....	11
4.4 Organisational Resilience and Governance.....	11
4.5 Ethical Considerations and Stakeholder Trust.....	12
5. Conclusion.....	12
References.....	13

Abstract

This report looks at how data security, governance, and compliance are used in a multinational company that mainly operates in a cloud and wireless setup. The study is based on NatureGreen (NG), a well-known company that offers many online services and lets both employees and customers use their personal devices to access the company's resources.

Because there are no clear rules or management systems for security, NG is more likely to face problems with protecting data, keeping intellectual property safe, and following regulations. To deal with these issues, the report looks closely at well-known security frameworks and service management approaches, such as ISO/IEC 27001 and the Information Technology Infrastructure Library (ITIL).

The lessons learned from this review help create a custom security, governance, and compliance plan that fits the way NG operates. This plan includes structures for managing security, ways to handle risks, making policies, and using technology to protect against threats, all in line with the rules and regulations that apply.

In addition, the report talks about the need to keep security rules and standards up to date as new cyber threats appear, technology improves, and legal requirements change. It shows that having a security system that is organized but can also change is important for companies to stay strong, trustworthy, and in line with laws in today's connected digital world.

1.INTRODUCTION

The fast growth of digital technologies has greatly changed how companies work and provide services. Tools like cloud computing, wireless networks, and mobile devices have made it easier for businesses to be flexible, grow quickly, and connect with people around the world. But these new technologies have also made companies more vulnerable to cyberattacks, data leaks, and failing to follow important rules [4], [6]. As businesses increasingly depend on digital systems to operate, the need to protect sensitive information and important business ideas has become a top priority, not just a technical concern [6].

Ensuring data security, proper governance, and compliance with regulations is crucial for safeguarding information, managing it effectively, and adhering to legal and ethical standards. Governance plays a vital role in helping companies make clear and structured decisions, while compliance ensures they follow relevant laws, such as data protection regulations and industry-specific guidelines [5], [8]. Without strong security measures and a solid governance framework, companies can suffer from various issues, including operational disruptions, financial losses, and harm to their reputation [6].

NatureGreen (NG) is a well-known group that works in the healthy living area and has a big presence around the world. They have a strong online presence and are active on social media. The company uses a lot of cloud services and wireless networks, and about 95% of their setup runs without cables. NG is also under more pressure to allow people to use their own devices, like phones or tablets, to connect to the company's systems and resources. Even though this can be helpful for business, there isn't a clear security policy in place, which has led to a mixed and uneven level of security [6].

The purpose of this report is to carefully look at existing data security and governance systems and to create a thorough plan for security, governance, and compliance that fits NatureGreen's way of doing business. The report also wants to explore why it's important to keep updating security rules and standards to deal with new cyber dangers and changes in technology and laws [1], [2].

2.LITERATURE REVIEW

2.1 Introduction to Security Frameworks and Standards

As information systems in organizations become more complicated, there has been a growing need for structured security frameworks and standards [6], [8]. These frameworks are created to assist in handling risks, making sure that organizations follow the necessary rules, and making their operations more effective. They provide clear steps for identifying potential threats, putting in place protective actions, and maintaining a safe and secure environment for business activities.

In this section, we will explore three widely recognized frameworks—ISO/IEC 27001, the Information Technology Infrastructure Library (ITIL), and the NIST Cybersecurity Framework—to understand their usefulness and how practical they are for companies that rely on cloud and wireless technologies [1], [2], [3].

2.2 ISO/IEC 27001

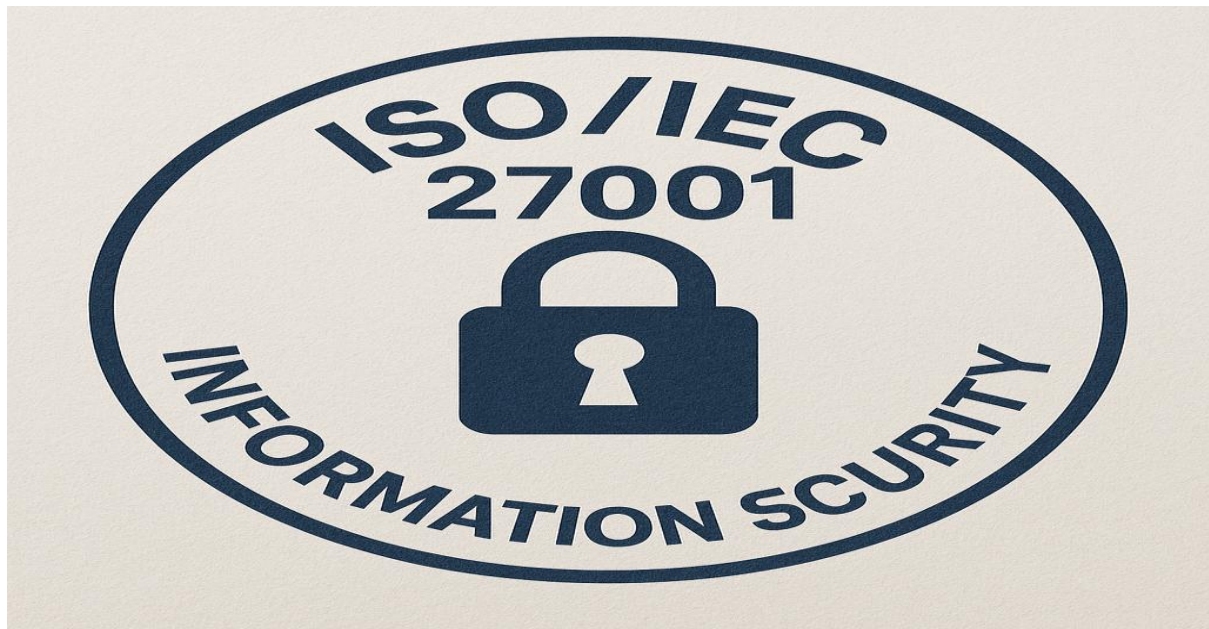


Figure 1: ISO/IEC 27001

ISO/IEC 27001 is a globally accepted standard that sets out the requirements for setting up, running, keeping, and improving an Information Security Management System (ISMS) [1]. The standard uses a risk-focused approach, which means organizations must find out about possible security risks and use the right controls based on their business needs and the level of danger they face [9]. This clear and organized way of handling security makes ISO/IEC 27001 a good choice for companies that deal with a lot of sensitive information in different systems.

A major advantage of ISO/IEC 27001 is its focus on always improving security using the Plan-Do-Check-Act (PDCA) cycle. This helps organizations keep checking and making their security better over time, especially as new threats and rules come up [1], [7]. The standard also helps meet legal and regulation needs by asking for clear policies, set roles, and ways to check and review processes [1], [5].

Even though ISO/IEC 27001 has many advantages, some research shows that putting it into practice can take up a lot of resources, especially for companies that don't have strong management systems in place. The cost of getting certified, regular checks, and the need for experts can be tough to handle [7]. Also, while ISO/IEC 27001 tells you what you need to do, it doesn't give much help on how to actually set up certain security

measures. This means companies have to figure out on their own how to apply these rules in their own work environment [6].

2.3 Information Technology Infrastructure Library (ITIL)

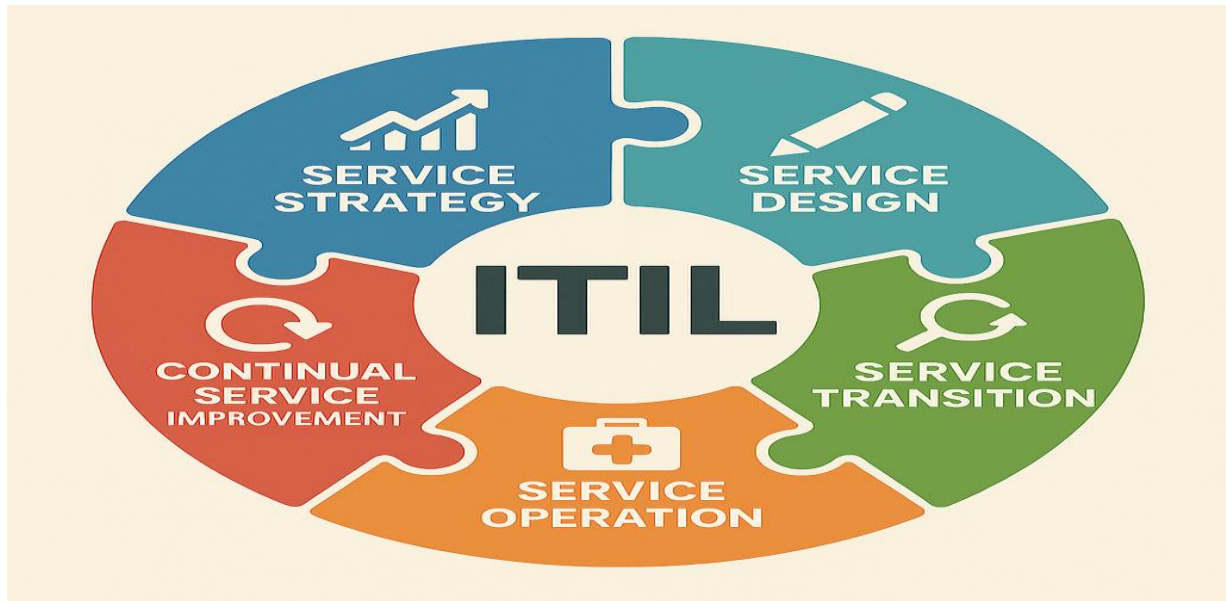


Figure 2 : Information Technology Infrastructure Library (ITIL)

The Information Technology Infrastructure Library, or ITIL, is a popular set of guidelines used to manage IT services. It helps make sure that IT services work well with the goals of the business [3]. ITIL isn't specifically designed with security in mind, but it still plays a helpful role in managing risks, ensuring that things operate smoothly, and keeping IT services running effectively. It provides clear guidance on how to plan, deliver, and improve IT services, which is crucial for maintaining reliable and secure operations [6].

In the field of information security, ITIL complements other standards such as ISO/IEC 27001 by offering real-world strategies for service delivery and incident management [3]. By implementing practices like change management, incident response, and service level agreement setting, organizations can gain better control over the security and availability of their systems. For companies that use cloud services, ITIL helps in managing external providers and setting clear service agreements [4].

However, one main issue with ITIL is that it doesn't include specific security rules. Because of this, ITIL needs to be used together with other security standards to handle the needs for keeping information private, accurate, and available [6].

2.4 NIST Cybersecurity Framework



Figure 3 : NIST Cybersecurity Framework (CSF)

The NIST Cybersecurity Framework (CSF) offers a flexible and risk-focused way to handle cybersecurity risks [2]. It is organized into five main areas: Identify, Protect, Detect, Respond, and Recover. This structure helps organizations evaluate their current security situation and focus on improvements based on their risk tolerance and business goals [2]. The framework is appreciated for being adaptable and offering useful, real-world advice, which makes it work well for businesses of different sizes and levels of experience.

One significant advantage of the NIST Cybersecurity Framework is that it helps businesses become more resilient and better equipped to deal with security challenges. It emphasizes the importance of identifying potential issues at an early stage and having the capability to recover swiftly, which in turn helps organizations minimize the impact of security incidents [2]. In addition, the NIST CSF is compatible with other widely recognized standards such as ISO/IEC 27001, enabling companies to integrate various security frameworks into a single, comprehensive, and efficient strategy [1], [2]. This integration allows for a more unified and effective approach to managing cybersecurity risks across different parts of an organization.

2.5 Comparative Discussion

When looked at together, ISO/IEC 27001, ITIL, and the NIST Cybersecurity Framework each bring useful strengths. ISO/IEC 27001 helps with strong governance and meeting regulations, ITIL helps manage services and operations well, and the NIST CSF helps with managing security risks and building resilience [1], [2], [3]. But none of these frameworks on their own can fully cover all the security needs of today's cloud-based companies [6], [8].

Because of this, many studies suggest using a combined method that brings together governance, how organizations run their operations, and security measures. This method helps companies deal with both big-picture and day-to-day security issues, while making sure they follow rules and can change quickly as new threats appear [1], [2], [6].

3.PROPOSED SECURITY, GOVERNANCE & COMPLIANCE FRAMEWORK

For NatureGreen (NG)

3.1 Design Principles and Assumptions

The security, governance, and compliance framework for NatureGreen is built using a method that focuses on risks, follows international standards, and meets business needs [1], [9]. Since NatureGreen uses a lot of cloud services, wireless networks, and personal devices, the framework is made to be flexible, scalable, and always improving [2], [6]. It matches global standards but can also change to fit the company's specific operations and rules.

3.2 Security Governance Structure

Good security governance is important to make sure that information security efforts match the goals of the company and follow the rules and regulations [6], [8]. For NatureGreen, a centralized governance approach is suggested, with a Chief Information Security Officer (CISO) in charge. This CISO will report to top management and will handle creating the security plan, making sure policies are followed, and managing risks.

A group of people from different areas like IT, legal, compliance, human resources, and top management should come together to form an Information Security Governance Committee [1], [6]. This group will help approve security rules, check risk reports, and make sure everyone in the company takes responsibility. This setup helps leaders make smart decisions and keeps the whole organization on track with security goals.

Level	Role/Group	Key Responsibilities / Members
1	Senior Management / Board	Sets strategic direction, approves budgets, defines risk appetite
2	Chief Information Security Officer (CISO)	Leads security strategy, reports to board, oversees enterprise-wide security posture
3	Information Security Governance Committee	Cross-functional team: IT, Legal, Compliance, HR, Senior Management — ensures alignment and oversight
4	Operational Security Teams	Executes security operations: IT Ops, Cloud Security, Network Security, Incident Response, Risk & Compliance

Table 1: Security Governance Structure

3.3 Risk Management Approach

A clear plan for managing risks is suggested to find, check, and deal with security risks in NatureGreen's environment. This plan follows the risk assessment methods from ISO/IEC 27001 and includes ongoing checks [1], [9]. Risks linked to wireless networks, cloud service providers, and personal devices are found through regular risk checks and reviews of possible weaknesses [9].

Each risk that is found is looked at based on how likely it is to happen and how much it could affect keeping information secret, making sure information is accurate, and making sure services are available. The right way to handle each risk—like reducing the risk, passing it to someone else, accepting it, or avoiding it—is chosen depending on how much risk the organization is willing to take.

3.4 Security Policies Framework

To deal with the lack of official security measures, a complete set of security policies has been suggested. These policies are the base of NatureGreen's security and give clear directions to workers and others involved [6]. Important policies that are in place include a Bring Your Own Device (BYOD) policy, a data classification policy, an access control policy, and an acceptable use policy.

The BYOD policy outlines the security guidelines that employees must follow when using their personal devices to connect to company systems and access work-related resources. This policy requires the use of strong authentication methods, such as complex passwords or multi-factor authentication, and ensures that personal devices meet certain security requirements before they can be used for work purposes. The data classification policy helps in organizing information based on its level of sensitivity, so that appropriate security measures can be applied to protect the data effectively. These policies help keep security consistent throughout NG's spread out and wireless network setup [6], [8].

3.5 Technical and Organisational Controls

A layered defense method is suggested to keep NatureGreen's information safe. This involves implementing multi-factor authentication to make it harder for unauthorized users to access systems, ensuring that data is encrypted both when it is stored and when it is being transmitted across networks, dividing the network into separate sections to limit access and contain potential breaches, and continuously monitoring security systems to detect and respond to threats in real time s [2], [6]. These measures work together to reduce the risk of unauthorized access and data breaches, which is especially important in environments with many wireless connections where security vulnerabilities can be more common.

Organisational controls like security awareness training and role-based access control work together with technical solutions to deal with risks connected to people. Ongoing training helps employees know what security duties they have, and access controls make sure only approved users can use system features [6], [8].

3.6 Compliance and Standards Alignment

Following the law and rules is very important in the new plan. NatureGreen's work is expected to happen in areas that have rules about protecting data, like the GDPR. The new plan makes sure security steps match what the rules require by including things like data protection ideas, ways to check things are done right, and ways to make sure everyone is responsible [5].

ISO/IEC 27001 offers the main framework for meeting compliance requirements. ITIL helps with managing services and running operations smoothly. The NIST Cybersecurity Framework helps build stronger resilience by emphasizing the process of identifying problems, dealing with them effectively, and bouncing back after incidents [3]. When NatureGreen uses this framework, it demonstrates its commitment to being responsible and complying with necessary standards, all while maintaining the ability to adapt and function smoothly in different situations [2].

3.7 Incident Response and Contingency Planning

Having a good incident response plan is important for reducing the harm caused by security issues. The framework provides a straightforward plan that clearly defines who is in charge of what and how communication should happen during an incident. This plan enables the organization to quickly identify, halt, and resolve issues that impact its systems or data, ensuring minimal disruption [2].

It's also wise to have plans ready for unexpected situations, such as disaster recovery and business continuity strategies. These plans help maintain service operations even during major disruptions [3], [6].

3.8 Service Level Agreements (SLAs)

Because NatureGreen relies on external cloud service providers, it is essential to establish clear Service Level Agreements (SLAs) [3], [4]. These agreements should clearly define the responsibilities of each party regarding security measures, set out the expected performance standards, specify the response times for addressing any incidents, and outline the compliance requirements that must be followed [6]. Having such agreements in place ensures that all parties understand their roles and obligations, and that the external services provided meet NatureGreen's requirements for security and legal compliance.

4. WHY REGULATIONS & STANDARDS MUST BE CONTINUOUSLY UPDATED

4.1 Evolution of Cyber Threats

Cyber threats are becoming more serious and complicated, which means the old ways of keeping things safe are no longer enough [2], [6]. Previously, security rules were designed to protect against threats that came from outside the network, but now, the risks are different. Modern attacks often come from things like improperly configured cloud services, weak Wi-Fi networks, and compromised personal devices. Hackers are also using more advanced strategies, such as automated scanning techniques and targeted attacks, which means companies need to update their security rules and standards to reflect the actual risks they face today, rather than relying on outdated methods.

4.2 Technological Advancements and Changing Risk Profiles

The fast adoption of cloud computing, mobile technologies, and Bring Your Own Device (BYOD) policies has significantly transformed the way organizations manage risks [4], [6]. While these tools make everyday operations more efficient, they also introduce new security challenges. For example, it becomes harder to determine who is responsible for data, who has access to it, and how to handle risks from external partners or third-party services.

Companies like NatureGreen, which rely heavily on wireless and cloud-based systems, might find that traditional standards are no longer sufficient. These outdated rules may not account for risks related to shared infrastructure or unmanaged personal devices.

4.3 Regulatory Compliance and Legal Obligations

From a compliance point of view, it's important to keep regulations up to date to deal with changing legal and social standards about protecting data and ensuring privacy. Laws like the General Data Protection Regulation (GDPR) show a stronger focus on holding organizations accountable, being open and honest, and respecting people's rights [5], [6]. As how data is handled continues to change, the rules that govern this must also change to make sure companies stay legally compliant and act in an ethical way.

4.4 Organisational Resilience and Governance

Keeping regulations and standards current allows organizations to remain strong and flexible by promoting a culture of continuous improvement. Security frameworks such as ISO/IEC 27001 emphasize the importance of regular reviews and updates, as security is not something that can be set up once and left untouched [1]. It requires ongoing maintenance and enhancement to stay effective over time. NatureGreen consistently updates its standards, which helps the organization effectively respond to emerging threats, changing regulations, and evolving business requirements.

4.5 Ethical Considerations and Stakeholder Trust

Beyond the technical and legal considerations, regularly updating rules reflects an organization's commitment to safeguarding personal and sensitive information. Today, more customers and employees are expecting businesses to act responsibly and with care when it comes to protecting their data. If a company's security measures are outdated or insufficient, it could appear as though they are not fulfilling their responsibilities, which can damage trust and weaken long-term relationships with both customers and partners [6], [8].

In summary, the ever-changing nature of cybersecurity threats, technological advancements, and regulatory requirements means that static, one-size-fits-all rules are no longer sufficient to protect data effectively. As a result, companies must adopt adaptable standards and strong management practices to ensure they remain secure, compliant, and capable of maintaining confidence from customers and partners in a continuously evolving environment.

5.CONCLUSION

This report aimed to look at how data security, governance, and compliance are used in a big company that works across many countries and relies heavily on wireless and cloud technologies. The report used NatureGreen as an example to closely examine existing security frameworks and standards, and to check how well they work for today's cybersecurity issues.

The report looked at different standards like ISO/IEC 27001, ITIL, and the NIST Cybersecurity Framework [6]. It found that none of these alone can fully cover all the security needs of today's businesses. The report showed that combining these approaches works better to balance how organizations are run, manage their operations, and protect their security.

Based on this analysis, a tailored security, governance, and compliance strategy was recommended to effectively address NatureGreen's unique risk factors, such as its extensive reliance on cloud services, wireless network infrastructure, and bring-your-own-device (BYOD) policies [1], [2], [3]. The proposed plan emphasizes strong governance structures, decision-making that is informed by risk assessments, clearly established security policies, and a multi-layered approach that includes both technical and organizational protective measures to ensure comprehensive protection [1], [2], [5].

Overall, the results show that having a security system that is both forward-thinking and flexible is important for companies like NatureGreen. This helps protect important information, keep valuable ideas safe, and ensure the company runs smoothly and effectively over the long term, especially in a constantly changing digital world.

Reference:

- [1] ISO/IEC, "ISO/IEC 27001:2022 – Information Security Management Systems," ISO, 2022.
- [2] NIST, "Framework for Improving Critical Infrastructure Cybersecurity," National Institute of Standards and Technology, 2023.
- [3] AXELOS, ITIL® Foundation: ITIL 4 Edition, London, UK, 2019.
- [4] P. Mell and T. Grance, "The NIST Definition of Cloud Computing," NIST SP 800-145, 2011.
- [5] European Union, "General Data Protection Regulation (GDPR)," 2018.
- [6] M. Whitman and H. Mattord, Principles of Information Security, 7th ed., Cengage, 2021.
- [7] S. Calder, Implementing ISO/IEC 27001, IT Governance Publishing, 2018.
- [8] R. Steinberg et al., Information Security Management Principles, 2nd ed., Wiley, 2016.
- [9] ISO/IEC, "ISO/IEC 27005: Information Security Risk Management," ISO, 2022.