



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

Apply the principles and practices of Data security, Governance and Compliance based on the given scenario.

Submitted by:

MD Azizul Khan

Student ID: 2514708

Course Code: ACCA7028

Programme: MSc in Software Engineering and Artificial Intelligence

Submitted To:

Assoc. Prof. Carlene Campbell

Lecturer, Data Security, Governance and Compliance

Submission Date: 08 January 2026

Table of Contents

Abstract

1. Introduction
2. Literature Review of Security Frameworks
 - 2.1 ISO/IEC 27001 and ISO/IEC 27002
 - 2.2 NIST Cybersecurity Framework
 - 2.3 ITIL v4
 - 2.4 COBIT 2019
 - 2.5 Zero Trust Architecture
 - 2.6 Comparative Table
3. Designed Security Governance and Compliance Approach for NG
 - 3.1 Governance Structure
 - 3.2 Security Policies
 - 3.3 Risk Management Approach
 - 3.4 BYOD Security Strategy
 - 3.5 Cloud Security Strategy
 - 3.6 Wireless Security Strategy
 - 3.7 Incident Response and Business Continuity
4. Critical Discussion: Why Regulations Must Evolve
5. Assumptions
6. Conclusion
7. References

Abstract

This report evaluates NatureGreen's (NG) current security posture and proposes a comprehensive governance and compliance approach tailored to its cloud-centric and wireless-dependent environment. Drawing on established frameworks—including ISO/IEC 27001, the NIST Cybersecurity Framework, ITIL v4, COBIT 2019, and Zero Trust Architecture—the report identifies significant gaps in NG's governance, policies, and technical controls. It outlines a structured governance model, essential security policies, a formal risk management methodology, and targeted strategies for BYOD, cloud, and wireless security. The analysis is based on several assumptions regarding NG's operational maturity, technological landscape, and regulatory obligations. A critical discussion highlights why existing regulations are can no longer keep up with rapid technological change and increasingly sophisticated cyber threats. The report ends by stressing the importance of proactive, adaptive security practices to ensure NG's long-term resilience.

1. Introduction

Digital transformation has become a defining characteristic of modern organisational operations, reshaping how businesses communicate, deliver services, and manage information. The widespread adoption of cloud computing, mobile technologies, and wireless networks has enabled organisations to achieve unprecedented levels of efficiency, scalability, and global reach. However, these advancements have also introduced new layers of complexity in managing information security. As organisations become increasingly interconnected, their exposure to cyber threats grows proportionally. Attackers now exploit vulnerabilities across distributed systems, cloud environments, and personal devices, making traditional perimeter-based security models insufficient.

NatureGreen (NG), a multinational organisation with a diverse global presence, exemplifies the challenges associated with modern digital ecosystems. With approximately 95% of its network infrastructure operating wirelessly and its core services delivered through cloud-based platforms, NG relies heavily on technologies that inherently increase its exposure to cyber risks. The organisation's intention to support Bring Your Own Device (BYOD) access for both staff and customers further expands its attack surface, introducing risks related to device security, data leakage, and unauthorised access. These risks are exacerbated by NG's lack of formal security policies, governance structures, and risk management processes, leaving the organisation vulnerable to operational disruptions, regulatory penalties, and reputational damage.

This report reviews key security frameworks—including ISO/IEC 27001, the NIST Cybersecurity Framework, ITIL v4, COBIT 2019, and Zero Trust Architecture—to identify

best practices that can strengthen NG's security governance. It proposes a tailored governance and compliance model designed to strengthen NG's security posture and ensure alignment with international standards. The report also critically evaluates the limitations of existing regulations in addressing emerging technologies and evolving cyber threats. The analysis concludes with recommendations aimed at enhancing NG's long-term resilience and security maturity.

2. Literature Review of Security Frameworks

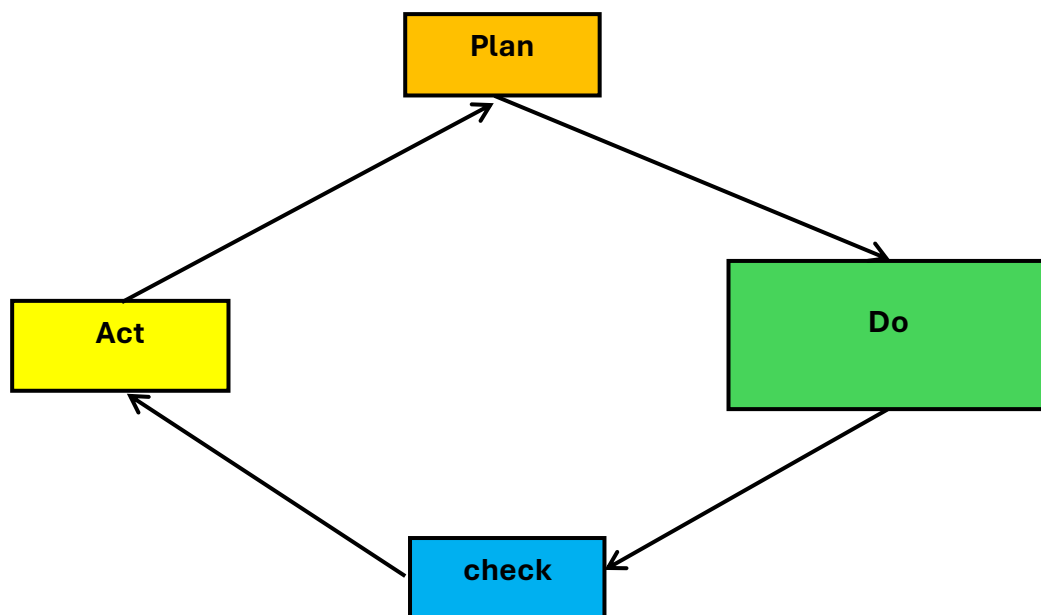


Figure 1

PDCA Cycle

Insert a circular diagram showing Plan → Do → Check → Act.

2.1 ISO/IEC 27001 and ISO/IEC 27002

ISO/IEC 27001 and ISO/IEC 27002 are internationally recognised standards that offer a structured framework for managing information security. ISO/IEC 27001 defines the requirements for implementing an Information Security Management System (ISMS), using a risk-based approach that ensures organisations consistently identify, assess, and treat information security risks. The standard promotes a culture of continuous improvement through the Plan–Do–Check–Act (PDCA) cycle, which encourages organisations to regularly evaluate the effectiveness of their controls and adapt to evolving threats.

ISO/IEC 27002 complements ISO/IEC 27001 by providing detailed guidance on the implementation of security controls. The standard includes 93 Annex A controls covering organisational, people, physical, and technological domains. These controls span critical domains such as asset management, access control, cryptographic protection, and supplier security. For organisations like NG, which rely heavily on cloud services and wireless networks, ISO/IEC 27002 offers practical guidance on implementing controls that mitigate risks associated with distributed environments and third-party dependencies.

The relevance of ISO/IEC 27001 and 27002 to NG is significant. The standards provide a comprehensive framework for establishing governance structures, defining security policies, and implementing technical controls that align with international best practice. By adopting these standards, NG can enhance its security maturity, improve regulatory compliance, and reduce its exposure to cyber threats.



Figure 2

NIST Cybersecurity Framework Core Functions.

A horizontal diagram with five labelled blocks: Identify, Protect, Detect, Respond, Recover.

2.2 NIST Cybersecurity Framework

The NIST Cybersecurity Framework (CSF) is a widely used model that offers a flexible, risk-based method for managing cybersecurity. Its five core functions—Identify, Protect, Detect, Respond, and Recover—provide a comprehensive view of an organisation's security posture and guide controls across the entire cyber risk lifecycle. The Identify function focuses on understanding assets, business context, and risks, enabling effective prioritisation. Protect includes safeguards such as access control, training, and data security. Detect emphasises continuous monitoring and anomaly identification, while Respond outlines processes to contain and mitigate incidents. Recover focuses on restoring operations and improving resilience. For NG, the CSF is highly suitable for its cloud-based, wireless-dependent environment, particularly due to its strong emphasis on detection and response in distributed infrastructures.

2.3 ITIL v4

ITIL v4 is an IT service management framework centred on delivering value through effective service design, delivery, and continual improvement. While ITIL is not specifically a security framework, it provides essential governance processes that support the stability and reliability of IT services. Key components of ITIL v4 include Change Management, Incident Management, Problem Management, and Service Level Agreement (SLA) Management.

For NG, ITIL v4 offers valuable guidance on managing the operational aspects of its cloud services and wireless infrastructure. The framework's emphasis on structured processes and continuous improvement aligns with NG's need to maintain service quality and minimise disruptions. However, ITIL must be complemented by technical security frameworks to address the specific risks associated with information security.

2.4 COBIT 2019

COBIT 2019 is a governance and management framework that provides guidance on aligning IT processes with organisational objectives. The framework emphasises value delivery, risk optimisation, and resource optimisation, making it particularly relevant for organisations seeking to establish robust governance structures.

COBIT 2019 includes a comprehensive set of governance and management objectives that cover areas such as strategic alignment, performance management, and risk management. For NG, COBIT provides a strong foundation for defining roles, responsibilities, and decision-making processes. The framework's emphasis on

governance is particularly valuable given NG's current lack of formal structures and policies.

2.5 Zero Trust Architecture

Zero Trust Architecture (ZTA) is a modern security model that operates on the principle of "never trust, always verify." Unlike traditional perimeter-based security models, Zero Trust assumes that no user or device is inherently trustworthy, regardless of their location. Key components of ZTA include identity-based access control, microsegmentation, continuous authentication, and least-privilege access.

For NG, Zero Trust is highly relevant due to its reliance on BYOD, cloud services, and wireless networks. These technologies increase the risk of unauthorised access and lateral movement. Adopting a Zero Trust model helps NG minimise these risks and strengthen its security posture.

2.6 Comparative Table

Framework	Purpose	Strengths	Limitations	Relevance to NG
ISO 27001	Establish an ISMS and provide a risk-based security model.	Globally recognised; comprehensive controls; strong governance; supports compliance.	Resource-intensive; requires ongoing audits; slower to adapt to emerging threats.	Highly relevant due to need for governance, policies, and structured risk management.
NIST CSF	Provide a flexible cybersecurity risk management framework.	Practical; strong detection/response focus; adaptable to cloud and hybrid environments.	Less prescriptive; requires interpretation; not a certification standard.	Very relevant for cloud and wireless environments and incident response.
ITIL v4	Improve IT service management and operational stability.	Strong governance; improves service quality; supports change and incident processes.	Not security-specific; must be paired with technical frameworks.	Useful for managing cloud services and operational processes.
COBIT 2019	Align IT governance with business objectives.	Strong governance model; clear accountability and decision-making structures.	Limited technical depth; requires integration with other frameworks.	Highly relevant for establishing governance and strategic oversight.
Zero Trust Architecture	Eliminate implicit trust; verify every user/device.	Strong for BYOD, cloud, and wireless; reduces lateral movement; modern approach.	Requires cultural change; can be complex to implement across legacy systems.	Extremely relevant due to NG's BYOD, cloud, and wireless-heavy environment.

Table 1

Comparative Summary of Frameworks.

A table comparing ISO 27001, NIST CSF, ITIL v4, COBIT 2019, and Zero Trust across: Purpose, Strengths, Limitations, Relevance to NG.

3. Designed Security Governance and Compliance Approach for NG

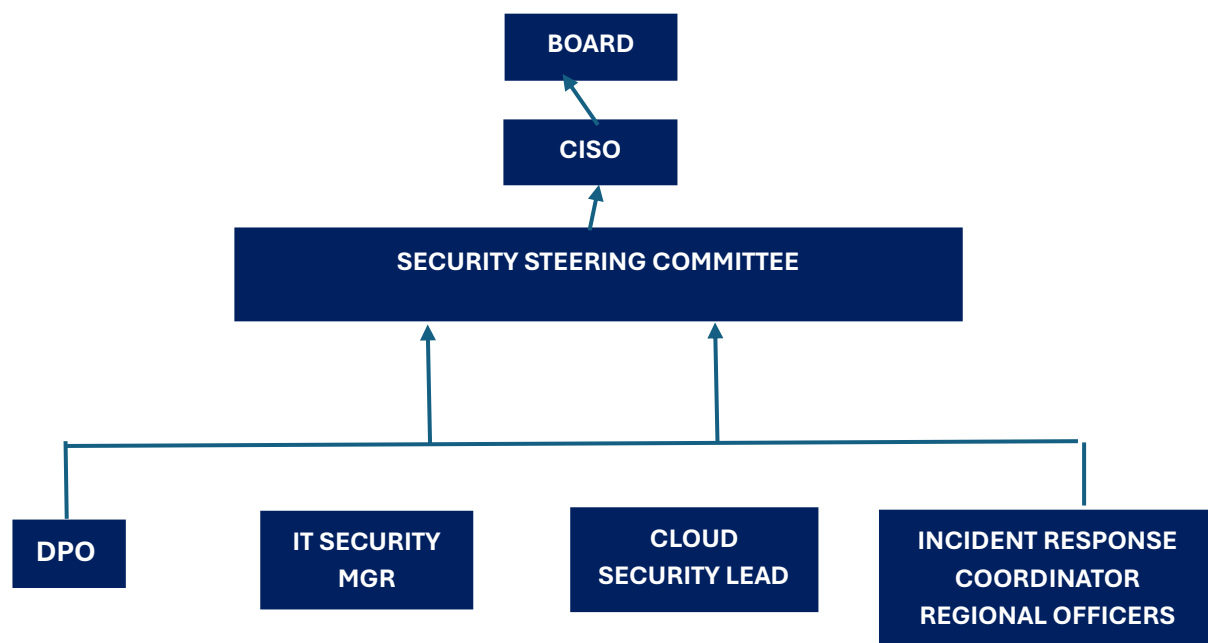


Figure 3

Proposed Security Governance Structure.

An organisational chart showing Board → CISO → Security Steering Committee → DPO, IT Security Manager, Cloud Security Lead, Incident Response Coordinator, Regional Officers.

3.1 Governance Structure

NG's lack of a formal security governance structure presents significant risks, particularly given its reliance on cloud services and wireless networks. A well-defined governance model is vital for establishing accountability, ensuring compliance, and aligning security initiatives with organisational objectives. The proposed structure begins with appointing a Chief Information Security Officer (CISO), reporting directly to the Board and overseeing NG's security strategy. This ensures security considerations are embedded in high-level decision making and that risk-based decisions are applied consistently. Supporting the CISO, a Security Steering Committee should provide cross-functional oversight, including representatives from IT, legal, compliance, operations, and regional teams. Its responsibilities include reviewing risks, approving initiatives, and monitoring compliance. To operationalise the model, specialised roles are required: a Data Protection Officer for regulatory compliance, an IT Security Manager for daily operations, a Cloud Security Lead for cloud-related risks, and an

Incident Response Coordinator for rapid containment. Regional Security Officers ensure consistent implementation across NG's global footprint.

3.2 Security Policies

NG requires a comprehensive set of security policies to ensure that security practices are applied consistently and can be effectively enforced across the organisation. These policies form the backbone of risk management, support regulatory compliance, and shape expected employee behaviour. Central to this framework is the Information Security Policy, which articulates NG's commitment to safeguarding its information assets and clearly defines the security roles and responsibilities assigned to employees. A BYOD Policy is essential for managing the risks associated with personal devices, while an Access Control Policy defines the principles and procedures for controlling who can access systems and data, and when that access is removed.

A Cloud Security Policy outlines the controls required to secure cloud services, including identity and access management, encryption, and monitoring. A Wireless Network Security Policy defines the controls required to secure NG's wireless infrastructure, while a Data Classification and Handling Policy provides guidance on how to classify, store, and transmit sensitive information. An Incident Response Policy explains how the organisation detects, deals with, and recovers from security incidents, while a Supplier Security Policy ensures that third-party providers meet NG's security requirements.

3.3 Risk Management Approach

NG must adopt a structured risk management methodology aligned with ISO 27005 and NIST SP 800-30. This methodology involves identifying assets, threats, vulnerabilities, and impacts; analysing likelihood and severity; evaluating risks against NG's risk appetite; selecting appropriate treatments; and continuously monitoring risks. A risk register should document each risk and track its status over time. This ensures that NG maintains visibility over its risk landscape and can prioritise resources effectively.

Risk management is particularly important for NG given its reliance on cloud services and wireless networks. These technologies introduce unique risks, including data breaches, unauthorised access, and service disruptions. By using a clear and structured approach to managing risk, NG can identify and mitigate these risks before they result in significant harm.

3.4 BYOD Security Strategy

NG's BYOD environment significantly expands its attack surface. Personal devices often lack the security controls found on corporate devices, increasing the risk of malware infections, data leakage, and unauthorised access. A strong BYOD strategy should

include Mobile Device Management (MDM) to enforce encryption, remote wipe, and application controls. Zero Trust identity measures—such as multi-factor authentication and conditional access—ensure that only verified users and devices can access corporate resources.

Network segmentation limits the impact of compromised devices by isolating them from critical systems. User training is also essential for reducing risks caused by user behaviour, such as phishing and careless browsing. These measures collectively support secure flexible working practices while maintaining a robust security posture.

3.5 Cloud Security Strategy

As a cloud-based organisation, NG must adopt a cloud security strategy grounded in the Shared Responsibility Model, which clarifies the division of security duties between NG and its cloud providers. A well-defined Responsibility Model, which delineates how security duties are distributed between all involved parties, is fundamental to maintaining effective control over cloud resources. Robust encryption—both at rest and in transit—safeguards sensitive information from interception or misuse. Clearly articulated Service Level Agreements (SLAs) establish the minimum security expectations that providers must meet, while continuous monitoring ensures that cloud environments remain resilient and aligned with these standards over time. These controls address the unique risks of NG's cloud-centric operations and help maintain visibility and control over organisational data.

3.6 Wireless Security Strategy

With 95% of NG's infrastructure operating wirelessly, a dedicated wireless security strategy is essential. Wireless networks are naturally easier for attackers to attack such as eavesdropping, rogue access points, and unauthorised access. WPA3 encryption provides strong protection for wireless communications, while 802.1X authentication ensures that only authorised devices can connect to the network.

Rogue access point detection helps identify unauthorised devices that may be used to intercept traffic or launch attacks. Continuous monitoring offers insight into network activity, supporting the early identification of suspicious behaviour, enabling NG to detect and respond to potential threats. MAC filtering and network segmentation further enhance security by limiting access to critical systems.

3.7 Incident Response and Business Continuity

NG should adopt the NIST Incident Response Lifecycle, which includes preparation, detection and analysis, containment, eradication, recovery, and lessons learned. Preparation means putting incident response plans in place, training staff, making sure teams can respond effectively, and setting up monitoring tools. Detection and analysis

involve identifying potential incidents and assessing their impact. Containment involves cutting off impacted systems to stop the problem from getting worse, further damage, while eradication involves removing the cause of the incident.

Recovery involves restoring normal operations and verifying that systems are functioning correctly. Lessons learned involve reviewing the incident to identify areas for improvement. Business continuity requires a backup strategy, disaster recovery planning, communication procedures, and regular testing. These measures are critical in NG's cloud-based and wireless-dependent environment, where incidents can escalate rapidly and have widespread operational impact.

4. Critical Discussion: Why Regulations Must Evolve

Existing regulations such as GDPR, ISO 27001, and NIST provide strong foundations but were not designed for today's fast-moving digital ecosystems. Cloud computing, IoT, AI, and 5G introduce risks that older regulations struggle to address. Cyber threats are becoming more advanced, with attackers exploiting automation, AI, and weaknesses in the supply chain. Compliance by itself does not ensure security, and many regulations unintentionally encourage a checklist-driven approach.

Globalisation complicates compliance due to conflicting regional laws and cross-border data flows. Existing frameworks also evolve slowly and do not fully address modern concepts such as Zero Trust or cloud-native architectures. Regulatory enforcement is inconsistent, encouraging superficial compliance. Future regulations must be adaptive, collaborative, and technology-neutral.

For NG, these limitations are significant due to its cloud-based, wireless-heavy environment and global operations. NG must go beyond compliance and adopt proactive, modern security practices.

5. Assumptions

The recommendations and analysis in this report emphasise the importance based on several key assumptions about NatureGreen's operational environment and organisational context. It is assumed that NG intends to maintain its cloud-first strategy and wireless-dominant infrastructure, with no immediate plans to revert to on-premise systems. The report also assumes that NG operates across multiple jurisdictions and is therefore subject to a combination of international data protection regulations, including GDPR and regional equivalents. Additionally, it is assumed that NG has the organisational capacity to implement the proposed governance structure, including the appointment of specialised security roles such as a CISO, DPO, and Cloud Security Lead. Finally, the analysis assumes that NG is committed to adopting industry-recognised frameworks and is willing to invest in the cultural and technical changes required to achieve long-term security maturity. These assumptions set the

stage for how the security model is designed the proposed governance and compliance approach.

6. Conclusion

This report has identified significant gaps in NG's governance, policies, and technical controls. A multi-layered approach—drawing on ISO/IEC 27001, NIST CSF, ITIL v4, COBIT 2019, and Zero Trust—is essential for strengthening NG's security posture. The proposed governance model, policies, risk management processes, and targeted strategies for BYOD, cloud, and wireless environments provide a strong foundation for resilience. However, compliance alone is insufficient. NG must adopt adaptive, forward-looking security practices to remain secure in an evolving threat landscape.

7. References

- American Society for Quality. (2023). *Plan-Do-Check-Act cycle*. ASQ. <https://asq.org>
- Amazon Web Services. (2023). *AWS shared responsibility model*. AWS. <https://aws.amazon.com/compliance/shared-responsibility-model/> (aws.amazon.com in Bing)
- Axelos. (2019). *ITIL Foundation: ITIL 4 edition*. TSO (The Stationery Office).
- European Union. (2016). *Regulation (EU) 2016/679 of the European Parliament and of the Council (General Data Protection Regulation)*. *Official Journal of the European Union*.
- IEEE Standards Association. (2020). *IEEE 802.1X-2020: Port-based network access control*. IEEE.
- International Organization for Standardization. (2018). *ISO/IEC 27005:2018 Information technology — Security techniques — Information security risk management*. ISO.
- International Organization for Standardization. (2022). *ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection — Information security management systems — Requirements*. ISO.
- International Organization for Standardization. (2022). *ISO/IEC 27002:2022 Information security, cybersecurity and privacy protection — Information security controls*. ISO.
- ISACA. (2018). *COBIT 2019 framework: Introduction and methodology*. ISACA.
- ISACA. (2019). *COBIT 2019 framework: Governance and management objectives*. ISACA.

Kindervag, J. (2010). Build security into your network's DNA: The Zero Trust Network Architecture. Forrester Research.

*Microsoft. (2023). Shared responsibility in the cloud. Microsoft Azure.
<https://learn.microsoft.com/azure/security/fundamentals/shared-responsibility>
(learn.microsoft.com in Bing)*

National Institute of Standards and Technology. (2012). NIST SP 800-30 Revision 1: Guide for conducting risk assessments. U.S. Department of Commerce.

National Institute of Standards and Technology. (2012). NIST SP 800-61 Revision 2: Computer security incident handling guide. U.S. Department of Commerce.

National Institute of Standards and Technology. (2018). Framework for improving critical infrastructure cybersecurity (Version 1.1). U.S. Department of Commerce.

National Institute of Standards and Technology. (2020). NIST SP 800-207: Zero Trust Architecture. U.S. Department of Commerce.

Wi-Fi Alliance. (2018). Wi-Fi CERTIFIED WPA3™: Advanced security for personal and enterprise networks. Wi-Fi Alliance.