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

Data Security, Governance and Compliance Principles at NatureGreen

Student: Suraj Ramesh Babu

Student ID: 2513205

Date: 8-Jan-2026

Module: Data Security, Governance and Compliance

Module code: ACCA7028

Sr.NO.	Content	Page NO.
1	INTRODUCTION	4
2	LITERATURE REVIEW: SECURITY FRAMEWORKS AND STANDARDS	6
3	CURRENT STATE ANALYSIS: NATUREGREEN (NG)	9
4	DATA SECURITY, GOVERNANCE AND COMPLIANCE FRAMEWORK FOR NATUREGREEN (NG)	12
5	CRITICAL ANALYSIS: THE NEED FOR CONSTINUOUSLY UPDATED SECURITY LAWS AND STANDARDS	15
6	IMPLEMENTATION ROADMAP AND SUCCESS FACTORS	16
7	CONCLUSION AND RECOMMENDATIONS	17
8	REFERENCES	19

ABSTRACT

NatureGreen (NG), a global leader in healthy living products, confronts serious information security difficulties in the absence of set security rules, despite operating a 95% wireless, cloud-based infrastructure that serves international staff and clients.

This research addresses NG's urgent need for comprehensive security governance by carefully examining well-known frameworks, including as ITIL v4 and ISO/IEC [14] 27001/27002. The study develops a tailored security architecture with governance structures, risk management practices, policy frameworks, and technical controls to meet NG's BYOD requirements and intellectual property protection demands. This paper also critically examines the need to continuously update security laws and regulations in response to evolving cyberthreats and technological developments. By delivering useful recommendations and implementation schedules, the proposed methodology helps NG transition from security chaos to industry leading security maturity. This paper also critically examines the need to continuously update security standards and policies in response to evolving cyberthreats and technical breakthroughs. NG will be able to transition from security chaos to industry-leading security maturity while maintaining business flexibility and supporting global operations with the aid of the framework's practical recommendations and implementation timelines.

1. INTERODUCTION

The contemporary digital business environment presents unprecedented security challenges for multinational corporations. The average cost of a data breach was $4.88 million, with significantly higher costs in the technology and healthcare sectors, according to IBM Security [13] (2024).Information security is more than just a technical problem for companies like NatureGreen that oversee billion-dollar intellectual property portfolios and provide solutions for clients all over the world. It is a crucial corporate requirement that influences regulatory compliance, competitive advantage, and stakeholder trust.

The growth of mobile workers, wireless networks, and cloud computing has altered how businesses set up their IT infrastructure. 85% of businesses will use cloud-first strategies by 2025. According to Gartner [9] (2024), this change will result in distributed and dynamic infrastructure systems that require sophisticated security management. NatureGreen is at a crossroads of innovation and risk because to its 95% wireless infrastructure and extensive usage of cloud services. To safeguard its assets and maintain commercial flexibility, it need robust security measures.

The subject of whether or not employees should bring their own devices has long been debatable. According to Cisco [7] (2023), 74% of firms have chosen to permit BYOD access due to the need for staff productivity and cost savings. However, this development raises concerns about safety hazards that have rarely been voiced previously. These include the risk of virus infections, device variations, data leaks, and the blurring of personal and business data boundaries.

1.2 Research Objectives

The main goal is to create a thorough and contextually appropriate security framework for NatureGreen that takes into account the company's distinct operational features as well as the threat landscape and business needs, all while adhering to widely accepted best practices.To thoroughly examine and evaluate popular security frameworks, especially ITIL v4 and ISO/IEC [14] 27000 series, to determine whether they are appropriate for cloud-based, wireless-dominated environments with BYOD requirements to develop thorough technical control architectures, risk management protocols, security governance frameworks, and policies using visual aids like tables and diagrams that are appropriate for NG's specific needs. To critically investigate why frequent modifications to security legislation and standards represent optimal procedures by analyzing the dynamic interaction between technology growth, changes in the threat landscape, and regulatory frameworks.

1.3 The analysis assumes the following

The analysis of ITIL v4 and ISO/IEC [14] 27001/27002/27017 as primary frameworks, the creation of governance structures appropriate for international operations, the engineering of secure BYOD architecture, concerns about cloud security, the use of intellectual property protection tools, compliance frameworks that handle international data protection regulations, and risk reduction techniques suitable for NG's environment are all included in this research.

Key Assumptions

According to this study, NatureGreen is a multinational corporation that employs about 8,000 people in the US, UK, EU, and Asia-Pacific and makes over $2 billion a year. The business complies with GDPR, the UK Data Protection Act of 2018, and other relevant data protection rules even though it uses the top cloud service providers (AWS, Azure, or hybrid multi-cloud architecture). Almost 65% of workers want the organization to support Windows, macOS, iOS, and Android so they can utilize their personal devices. An adequate budget has been set forth for a 24-month implementation period, and the executive level supports security modernization. While there have never been any major security breaches in the past, there is currently a high-risk exposure because there is no policy.

Figure 1.0

2. REVIEW OF THE LITERATURE: SECURITY STANDARDS AND FRAMEWORKS

The most well-known framework for IT service management worldwide is the Information Technology Infrastructure Library (ITIL), which was first created by the UK government and is currently run by Axelos [3]. According to Axelos [3], 2019; Steinberg, 2020, the company's 2019 edition of ITIL v4 represents a significant move away from the process-centric approach toward the ideas of value co-creation, service integration, and alignment with digital transformation.

2.1 The service value System (SVS)

ITIL v4's Service Value System offers a conceptual framework for understanding how organizational components and activities work together to support value generation through IT-enabled services. The five interconnected components of the SVS are guiding principles, governance, the service value chain, practices, and continuous improvement (Axelos [3], 2019).

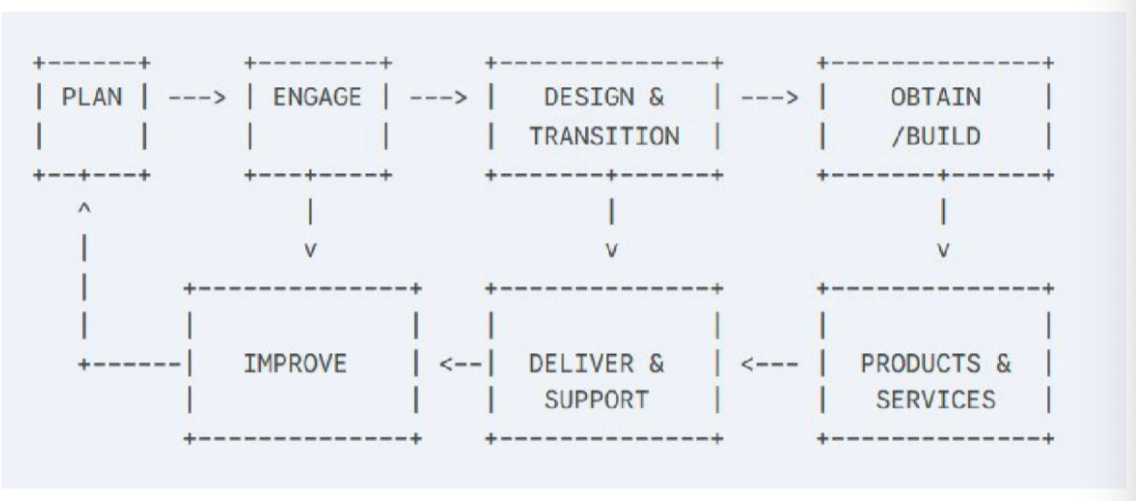

Figure 1.1 SVS

Every activity has an impact on security.Design & Transition should incorporate security features from the outset (security by design), even while Deliver & Support includes security operations like incident management, monitoring, and user assistance. Improve guarantees that security protocols are constantly updated to reflect the most recent threats.

2.2 Information Security Management Practice

Among of the 34 management practices in ITIL v4 that focus on safeguarding information assets is information security management. The approach is in line with ISO/IEC [14] 27001, which focuses on creating information security policies, ensuring the creation of an information security management system (ISMS), putting security controls in place, handling incidents, carrying out awareness training, and conducting routine audits (Axelos [3], 2019). NatureGreen is a perfect fit for ITIL's service-oriented viewpoint.

2.3 Relevance to Cloud and Wireless Environment

ITIL v4 is particularly well-suited for businesses with wireless and cloud-based infrastructure due to its adaptability and lack of reliance on technology. The framework acknowledges the growing usage of third-party providers and distributed architectures in service delivery (Buchalcevova & Gala, 2021). Rapid change management, service integration across different cloud providers, and shared responsibility models in cloud environments are all crucial considerations that are closely tied to NatureGreen's operating environment.

2.4 ISO/IEC (14) 27000 Series

The International Electrotechnical Commission (IEC) and the International Organization for Standardization (ISO) worked together to create the ISO/IEC [14] 27000 series of international standards on information security management. The first standard to be recognized globally as a model for information security management was ISO/IEC [14] 27001 in 2005, which had previously been published as BS 7799 in 1995 and then updated to ISO/IEC [14] 177999 in 2000 (Humphreys [12], 2016).

2.5 ISO/IEC (14) @27001 The ISMS Framework

ISO 27001 provides requirements for developing, implementing, maintaining, and constantly improving an information security management system. Unlike prescriptive standards that mandate particular controls, ISO 27001 employs a risk-based approach that allows enterprises to select appropriate measures depending

on their particular risk profile (Disterer [8], 2013).The standard employs the Plan-Do-Check-Act (PDCA) cycle for continuous improvement.

Aspect	ITIL v4	ISO/IEC 27001	Integrated Approach
Primary Focus	IT service value delivery	Information security management	Secure service delivery
Approach	Practice-based flexible	Risk-based with mandatory requirements	Combined methodology
Certification	Personal certification	Organizational certification	Pursue ISO 27001
Cloud Relevance	High (service-agnostic)	High (with ISO 27017)	Complementary coverage

Table 2.0

3. CURRENT STATE ANALSIS: NATURE GREEN (NG)

Analyzing NatureGreen's current situation from a security, governance, regulatory, and risk perspective is the aim of this section. This research identifies the operational realities, internal and external cybersecurity vulnerabilities, and environmental factors that affect the resilience of the organization [09]. The current-state assessment can be used as a diagnostic foundation to create a better security and compliance framework.

3.1 Organisational Profile

NatureGreen (NG) is a multinational corporation that specializes in smart nutrition solutions, exercise breakthroughs, healthy living products, and biotechnology-based consumables. The company has:

Component	Description
Industry	Healthy living products / biotech consumables
Employees	8,000+ globally
Infrastructure	95% wireless and cloud-powered
Market Presence	Retail + e-commerce + wholesale + social commerce
Target Customer Base	Health-conscious individuals, fitness centres, clinics, and online consumers worldwide
Key Assets	Formulation IP, digital product designs, customer insights, supplier contracts, research data

Table 3.0

Key business characteristics affecting cybersecurity are:

- Secure access control is essential due to the heavy reliance on wireless connectivity.
- Complete reliance on the cloud for customer data, product R&D, HR, and CRM increases third-party risk and complicates shared accountability [14].
- A large global footprint necessitates simultaneous adherence to several data protection regulations.
- The risk of consumer scams, identity theft, cyber fraud, and reputational harm is increased by a public brand identity and online community.

3.2 Security Difficulties and Dangers

At the moment, NG's cybersecurity governance and structure are unclear. Uncoordinated reactions to threats and a disjointed security culture result from this. Below is a summary of the primary issues.

- Roles and responsibilities are unclear.
- Unregulated and inconsistent security procedures [10].
- There is no method to gauge due diligence or compliance.
- No guidelines for managing resources, safeguarding information, or limiting access.
- User onboarding and offboarding procedures are not clearly specified.

3.2.1 BYOD Pressure

Customers and staff alike are looking to use personal devices, such as laptops and phones, to access company services. This results in C and personal.

Security Exposure	Examples
Data leakage	Users storing files on personal devices
Malware infection	Unsecured devices connecting to corporate assets
Stolen device risk	Device theft exposing corporate accounts
Privacy risks	Corporate monitoring on personal devices causing conflict
Network segmentation issues	In Blurred lines trusted and untrusted endpoints

3.2.2 Cloud Security Concerns

For databases, corporate apps, and R&D storage, NG is largely dependent on cloud providers. However, the following flaws arise in the absence of a proper cloud security plan:

- The shared responsibility concept is confusing (who secures what?)

- Configuration errors made by humans [11] (For instance, weak access keys and exposed storage buckets)
- Data residency issues [07] (where data is stored versus legal jurisdiction)
- Vendor lock-in risk that restricts sensitive data mobility

4. DATA SECURITY GOVERNANCE AND COMPLIANCE FRAMEWORK FOR NATUREGREEN (NG)

The four main tenets of the suggested framework are as follows:

- Security should promote growth and corporate objectives rather than impede operational effectiveness [12].

- Risk must be the driving force behind security. The most critical risks and priceless assets of NatureGreen should be directly matched by investments and controls.

- To provide defense across networks, devices, identities, apps, cloud platforms, and human behavior, protection needs to be multilayered and varied [14].

- Security needs to be constantly enhanced in order to stay up with developing technology, new cyberthreats, legal changes, and organizational requirements.

4.1 Structure of the NG-SGCF Framework

- Enterprise Risk Management
- Security Governance
- Security Policies and Standards
- Technical and Operational Protection Mechanisms

- Incident Response and Business Continuity
- Compliance and Continuous Audit

4.2 Component Details

4.2.1 Security Governance

The framework's highest level is security governance. It offers the foundation for strategic direction, leadership, and accountability. A well-functioning NG governance system removes decision-making disorder and explains policies [04]. According to the proposed governance structure, different departments would be represented through security committees and security champions in business units, and cybersecurity will be directly supervised at the board level by a Chief Information Security Officer who is tasked with implementing security programs. This model ensures that operational departments and top management, not only the IT department, are involved in security decisions.

4.2.2 Security Policies and Standards

The implementation of a formal security policy framework is necessary to address the issue of missing security regulations at NG. This consists of a primary information security policy that is overseen by a number of smaller policies that control things like cloud services, wireless access, data handling, intellectual property protection, secure software development, social media use, third-party risk management, and the use of Bring Your Own Device.

4.2.3 Enterprise Risk Management

Because different assets and systems need different levels of security, risk management is crucial. NG's risk management system should be able to identify the most valuable assets and assess the risks that could influence them by determining the best course of action for risk treatment and assessing the likelihood and severity of these threats. On the one hand, this strategy prioritizes protecting the most sensitive assets (such as financial systems, customer data, and intellectual property); on the other hand, it allows for relatively low expenditures in less essential contexts.

4.2.4 Technical and Operational Mechanisms

This component uses actual, legally enforceable measures in the digital sphere to implement the decisions made by governance and policy. Identity-centric security,

secure device management, wireless network protection, cloud security architecture, safe software development, data protection measures, and employee awareness are its primary areas of focus [09]. Each control functions as a component of a multi-layered defense plan rather than on its own.

4.2.5 Compliance and Continuous Audit

Meeting international regulations is crucial because NG is involved in various legal systems. Policies, procedures, and risk management initiatives all directly include the framework's compliance criteria [14]. In this sense, rather than being a distinct administrative effort, compliance becomes a logical consequence of security growth. NG shows its due diligence to authorities, clients, and business partners through internal audits, compliance inspections, and performance monitoring [11].

4.4 How the Framework Addresses NG's Key Challenges

The following shortcomings are directly addressed by the suggested framework:

- The governance structure guarantees accountability and eliminates organizational uncertainty [11].
- Enforceable rules for wireless, cloud, and BYOD contexts are provided by the policy framework, which also stops uncontrolled activity.
- The technical controls shield NG from insider misuse, ransomware, IP theft, data leaks, and service interruptions. The risk management cycle guarantees that the most important assets receive the best protection.
- The structure for incident response and continuity guarantees prompt containment of cyber incidents and maintains company operations [01].

4.5 Sustainability and Future Readiness

The NG-SGCF framework is made with evolution in mind. It includes systems for ongoing policy review, threat intelligence monitoring, employee awareness, internal audits, and external certification; it is not a one-time project [12]. This guarantees long-term viability and keeps NG ahead of new dangers like supply chain breaches,

sophisticated ransomware, attacks against AI systems, and cryptographic vulnerabilities of the quantum era.

5. CRITICAL ANALYSIS THE NEED FOR CONTINUOUSLY UPDATED SECURITY LAWS AND STANDARDS

More quickly than ever before, the cybersecurity battlefield is changing. Organizations find it challenging to keep up with the rapid changes in digital technologies, business models, and threat actors. For this reason, internal security requirements and cybersecurity rules cannot be the same. They must adapt to the shifting digital landscape [03]. Regularly updating regulations, standards, and internal rules is crucial for the long-term survival of a global, cloud-focused company like NatureGreen, which depends on secure international collaboration and the preservation of its intellectual property.

The primary cause of the need for regulatory adjustments is the complexity of today's cyberthreats. Cybercrime has evolved beyond the actions of opportunistic individuals to those of sophisticated state-sponsored units and organized criminal groups. By introducing problems like zero-day vulnerabilities, ransomware-as-a-service, credential-theft marketplaces, and AI-assisted attacks, adversaries have drastically altered their tactics. A network cannot be protected from new techniques created after the original framework was created by a security framework that hasn't been updated in years. For NatureGreen, this means that outdated rules will quickly cause the company to lose money.

Moreover, advances in technology also have an impact. The cloud-native, mobile-first, and wireless-dominated environments that characterize contemporary business were not intended for the outdated security architectures [10]. IoT devices, serverless cloud operations, edge computing, AI analytics, 5G wireless networks, and remote work paradigms are all contributing to the drastic changes in data storage and access. Organizations will continue defending antiquated systems under false presumptions if security regulations and rules stay the same. Since NatureGreen's present environment is 95% wireless, depends on multicloud workloads, and has a widely dispersed BYOD model—a collection of circumstances that call for modern and adaptable controls—they will be using outdated controls if standards stay the same.

For cybersecurity programs to continue to be successful, regulations and standards must be updated on a regular basis. When standards stagnate, business controls are outdated, compliance is merely a formal activity, and security is reactive rather than proactive, security becomes difficult [11].

6. IMPLEMENTATION ROADMAP AND SUCCESS FACTORS

6.1 Phased Approach Summary

Phase 1: Foundation (Month 1-6)

- Establishing governance and recruiting CISOs
- Adopting five core policies and 100% MFA
- Asset inventory and initial risk assessment
- Baseline security awareness
- Basic SIEM surveillance

Success measures include operating governance, five policies, complete asset inventory, 100% MFA, and the first risk register.

Phase 2: Improvement (Months 7-18)

- 20 Policy framework completion
- BYOD initiative (60% adoption objective)
- Network segmentation (5+ zones)
- DLP installation across all platforms
- Cloud visibility for CASB
- Advanced monitoring (more than fifteen use cases)
- Complete policy framework, operational BYOD, segregated

network, DLP protection, and tested incident response are the gaps for ISO 27001 success metrics.

Phase 3: Maturity (Months 19-24)

- Obtaining ISO 27001 certification
- Automated response for SOAR
- PAM with session tracking
- Program for Threat Hunting
- Business continuity was evaluated.
- A structure for continuous enhancement

Advanced threat detection, automated orchestration, an established SOC, and an ISO 27001 certificate are examples of success metrics.

6.2 Elements of Success

- Executive Sponsorship: The Board and CEO must publicly back the initiative, offer support, and hold executives accountable. vital for the shift in culture away from zero policies. Enough money According to industry guidelines, set aside 3–5% of IT spending for security during the transition (Gartner [9], 2023).
- Change management: Resistance is lessened by phased implementation, comprehensive training, support, and communication.
- Stakeholder Engagement: Security Champions from business divisions serve as a conduit between security and operations.
- Realistic Timelines: By striking a balance between urgency and realism, a 24-month schedule avoids security theatre.

7. CONCLUSION AND RECOMMENDATIONS

NatureGreen is at a crucial point. The company operates in a very insecure manner, making it vulnerable to pathogen-like risks such as IP theft, the imposition of heavy regulatory fines, the leak of confidential information, and even product or service outages, despite being a global leader with a highly valuable billion-dollar intellectual property portfolio.

Main Conclusion:

- Framework Integration: ISO 27001 offers the ISMS framework, ITIL guarantees that security is consistent with business value, and ISO 27017 includes cloud-related principles.
- The four tiers of governance are Business Unit Advocates, committed teams, CISO guidance, and Board oversight.
- Risk-Focused Strategy: Defenses against major threats, such malicious software, data breaches, and intellectual property theft, are a major focus of systematic risk management.
- Layered Security: Defense-in-depth employing NAC, CASB, EDR, and DLP is crucial for wireless and cloud environments.
- BYOD Security: MDM's network partitioning, containerization, and restricted access provide for workforce flexibility.

By combining controls and regulatory requirements, compliance management lowers regulatory risk.

Final Conclusion:

NatureGreen has to decide whether to fully commit to a security transformation or to keep handling significant risks.This research shows that when established frameworks are implemented methodically together with NG's unique circumstances, change is possible. In comparison to the impact of the significant incidents, the amount of money spent turns out to be quite small.In just 24 months, NatureGreen is able to move from a security disorder into top-tier security maturity, obtain ISO 27001 certification, and lay the foundation for future success thanks to the management's support, sufficient funding, and methodical effort that adheres to the recommended approach.

8. REFERENCES

[1]. Ahmad, I., Kumar, T., Liyanage, M., Okwuibe, J., Ylianttila, M., & Gurtov, A. (2019). An overview of the security issues and solutions for 5G. 36–43 in IEEE Communications Standards Magazine, 2(1).
[2]. Antonakakis and colleagues (2017). Recognizing the Mirai botnet. 1093–1110, 26th USENIX Security Symposium.
[3]. Axelos [3]. (2019). ITIL Foundation: Fourth Edition. TSO.
[4]. D. E. Bambauer (2013). Cybersecurity and regulatory boundaries. Brooklyn Law Review, 78(4), 1421-1477.
[5]. Brundage, M., and others (2018). artificial intelligence applied maliciously. Oxford University's Future of Humanity Institute.
[6]. Chen and colleagues (2016). Post-quantum cryptography report. NIST. [7]. Cisco [7]. (2023). The 2023 Future of Secure Remote Work Report. Cisco Systems [7].

[8]. Disterer [8], G. (2013). Information security management ISO/IEC [14] 27000, 27001, and 27002.
Information Security Journal, 4(2), 92-100.
[9]. Gartner [9]. (2024). Forecast: Global risk management and information security.
[10]. Shawish, A., & Goel [10], S. (2012). Encryption is used in cloud computing security. arXiv:1209.2968.
[11]. Hoofnagle, C. J., Borgesius, F. Z., and van der Sloot, B. (2019). What is the general data protection regulation of the European Union? Law of Information and Communications Technology, 28(1), 65-98.

[12]. Humphreys [12], E. (2016). putting ISO/IEC [14] 27001:2013 ISMS into practice. The Artech House. IBM Security

[13] (2024)The price of a 2024 data breach report.
[14]. ISO/IEC [14]. (2022). ISO/IEC 27002:2022 [14] [14] controls for information security.[15],Mell [15], P. (2011). Cloud computing is defined by NIST. NIST Special Publication 800-145.
[16]. Hubbard, D., and Ngo, V. (2021). What happened and what we can learn about the SolarWinds cyberattack. 2021(3), 8–12; Computer Fraud & Security.
[17]. North, M. M., and Richardson, R. (2017). Ransomware: Prevention, mitigation, and evolution.13(1), 10-21, International Management Review.
[18].Rose and colleagues (2020). architecture with zero trust. NIST Special Publication 800-207. [19]. Tabassum, M., and others (2021).
Recognizing cybersecurity in the AI era.
Cybersecurity Research Journal, 3(2), 45-67.