

Table Of Content

1 Abstract	1
2 Introduction	1
3 Methodology and Research Approach	2
3.1 Assumptions	2
4 Critical Evaluation of Security Frameworks and Standards.....	2
4.1 ISO/IEC 27000 Series.....	2
4.2 NIST Cybersecurity Framework (CSF) 2.0	3
4.3 COBIT 2019	4
4.4 ITIL Information Security Management (ISM).....	5
4.5 SOC 2, HIPAA, NERC CIP, FISMA and Other Frameworks	5
4.6 Regulatory Requirements: GDPR and NIS 2	6
5 Integrated Security Governance Model for NatureGreen.....	6
5.1 Governance and Strategic Planning	7
5.2 Compliance and Legal Obligations.....	8
5.3 Security Policies and BYOD/Wireless Strategy	8
5.4 Risk Management	9
5.5 Securing the Management Models andModes	9
5.6 Contingency Planning and Business Continuity	10
5.7 Protection Mechanisms	10
5.8 Service Level Agreements (SLAs)	10
5.9 Proposed Security Program Overview.....	11
6 Why Regulations and Standards Must Continuously Evolve	12
7 Conclusion	12

Table Of Figure

Figure 1: Comparative Overview of Major Cybersecurity Frameworks.....	2
Figure 2: NIST Cybersecurity Framework (CSF) 2.0 Core Functions (NIST CSF 2.0 adopts lifecycle-based model).....	4
Figure 3: Integrated Security Governance Model	7
Figure 4: BYOD and Wireless Security Control Architecture.....	8
Figure 5: NatureGreen’s Proposed Security Programme Pillars.....	11

Integrated Security Governance and Compliance Strategy for NatureGreen

1 Abstract

Driving the expansion of organizational attack surface is the growth in cloud services, wireless network and bring-your-own-device (BYOD) access. Nature Green, an international horticultural company, has a mostly wireless cloud environment that plans to accommodate personal devices and realizes their intellectual property is something of value but do not have cohesive security policies. This whitepaper provides an analysis of modern security frameworks, including ISO/IEC 27000, NIST Cybersecurity Framework 2.0, COBIT 2019 and ITIL Information Security Management, as well as supplementary ones (such as SOC 2, HIPAA, NERC CIP and GDPR or ISO 31000). It provides a critical discussion of strengths, limitations and practical utility, with reference to current empirical research and to the potential uses suggested by legislation. Based on that overview, the report offers a specific governance, risk and compliance (GRC) approach customized for Nature Green's business. The model encompasses the most crucial building blocks from the frameworks and standards reviewed, covering governance, legal compliance, security policies, risk management practices (measures), operational controls (procedures) contingency planning, protection mechanisms and SLAs. The main recommendations are to update standards and regulations on an ongoing basis for AI-driven threats and emerging technologies, along with where Nature Green leadership should focus in implementing a resilient and compliant security program.

2 Introduction

Digital Transformation is a mandate for global enterprises. Enterprises like Nature Green, a leading horticulture brand with customers worldwide, increasingly depend on cloud services and wireless networks for provisioning IT resources. About 95 % of Nature Green traffic goes through wireless networks and both the company's employees and customers demand more BYOD access. Nature Green's high-value IP and PD, in its possession and under management by Nature Green staff and other parties acting for it whom would have access to such information, needs this strong security governance; however policies are not consistent or structured within the enterprise. This is a classic example of the pull between agility, flexibility and security: keeping employees productive and customers happy, while also safeguarding sensitive data and complying with regulations. The Data Security, Governance and Compliance module focuses on a coherent understanding of security models, and the critical assessment of current research. This report serves that mission by reviewing these widely accepted models and standards. It concludes by integrating its findings to develop a holistic security program for Nature Green and discusses the importance of ongoing regulatory and standard revision. Throughout, the report references relevant scholarly articles, standards documents and industry reports that have appeared in the last several years to maintain currency and credibility.

3 Methodology and Research Approach

The research used a systematic literature review of peer-reviewed publications, conference articles and authoritative industry sources. The queries were conducted targeting the framework such as ISO/IEC 27001/27002, NIST Cybersecurity Framework (CSF) 2.0, COBIT 2019, ITIL Information Security Management and ISO 31000 for risk management and regulatory standards such as GDPR, NIS -2 Directive, SOC 2, HIPAA, NERC CIP and FISMA. Search phrases included “cybersecurity governance,” “cloud security framework,” “BYOD security,” “wireless network policies” and “business continuity planning.” The research included 2024–2025 sources to ensure that the latest revisions of frameworks (e.g., NIST CSF 2.0) and current legislation (e.g., NIS 2, EU AI Act discussions) were incorporated. The citations in this report reference the specific lines from sources using tether IDs.

3.1 Assumptions

1. Organizational scope: Nature Green operates in multiple jurisdictions but primarily follows UK and EU regulations, thus compliance with GDPR and NIS 2 is assumed mandatory.
2. Cloud architecture: Nature Green adopts public and private cloud systems for offering Infrastructure-as-a-Service (IaaS) and Software-as-a-Service (SaaS). Data is stored locally on company devices and in cloud servers.
3. 3. Wireless/ BYOD: About 95% of network access is wireless. Nature Green will encourage employees and customers to access resources on employee-owned devices, expanding the BYOD attack surface.
4. 4. Resource burden: Nature Green has resources to invest in certification and how it complies with these programmes, but is looking for ways to do so cost-effectively. As a result, I am considering these cert-heavy frameworks with great caution.

4 Critical Evaluation of Security Frameworks and Standards

This section analyses key security frameworks and regulations. It identifies how each contributes to Nature Green’s requirements and highlights limitations that must be addressed when designing a bespoke model.



Figure 1: Comparative Overview of Major Cybersecurity Frameworks

4.1 ISO/IEC 27000 Series

The ISO/IEC 27000 family is a series of internationally accepted standards for best practices in information security management. ISO 27001 lays down the necessary elements needed for a

security management system, and there are many more standards in ISO/IEC 27000 family covering these topics. An article by bit sight explains that ISO 27001/2 certification verifies an organization's security program, but says it is resource intensive and provides a single test for one (point-in-time) assessment and as such must evolve with current threats [1]. Despite the cost, 27001 carries worldwide credence and plays well with other standards and regulations. An MDPI study from 2024 emphasizes that ISO 27001 offers a full set of controls and aligning to GDPR, NIS2 or the EU AI Act results in holistic security management. [2]

Strengths:

- Comprehensive control set: ISO 27002 provides an organized list of controls that address physical, technical and organizational aspects. For Nature Green, this offer a wide reference to policies in Cloud, Wireless and BYOD environments.
- Certification and credibility: By obtaining ISO 27001 certification, Nature Green demonstrates to customers and business partners that it adheres to stringent security procedures.
- Compliance alignment: The framework is aligned to GDPR, NIS 2 and other regional legislations making it easier for organizations to be compliant. Weaknesses

Limitations:

- Resource intensity and static audits: The cost of certification may lead the final destination not to necessarily, day-to-day reflect [1]. For Nature Green, firebreaks of periodic check-ups should be enforced by continuous surveillance.
- One size fit none: ISO 27001 is purposely vendor neutral, and as such, businesses will need to customize the controls for wireless and BYOD risk.

4.2 NIST Cybersecurity Framework (CSF) 2.0

HITRUST CSF is a prescriptive standard and therefore is more detailed and operational in comparison to other frameworks like NIST. 14 The NIST CSF, offers a top-down approach of how cyber risk should be managed. Version 2.0 focuses on the alignment of cybersecurity with enterprise risk management and adds a new Governance component. NIST state that the CSF provides a set of non-mandatory controls for use by organizations of all sizes to understand, manage and reduce risk[3], and it “is flexible designed to be tailored” across industries. [3] The framework is divided into six functions -Govern, Identify, Protect, Detect, Respond and Recover – each with a set of sub-categories for specific outcomes.



Figure 2: NIST Cybersecurity Framework (CSF) 2.0 Core Functions (NIST CSF 2.0 adopts lifecycle-based model)

- Risk-based and adaptable: CSF is structured to enable organizations prioritize their risks based on business objectives, not a pre-determined set of factors. For Nature Green it will enable the mapping in the ISO 27001 controls.
- Enterprise governance integration: The Govern function is focused on roles, responsibilities and policies that align with board oversight and risk appetite.
- Widely used: Organizations leverage CSF to measure maturity and present your security posture to stakeholders.

Limitations:

- Non-Prescriptive: Although flexibility is a strong point, it can also be cause for confusion. order to tightly control Provide controls and measure in Nature Green's wireless/BYOD environment.
- **Lack of certification:** Unlike ISO 27001, CSF is voluntary and does not offer formal certification; thus it may not satisfy external stakeholders seeking assurance.

4.3 COBIT 2019

COBIT 2019 is a framework for IT management that emphasizes meeting business objectives through IT goals. In MDPI 2025, COBIT is described as strong in governance but not a conclusive framework for cybersecurity; the authors suggest amalgamating it with ISO 27000 to have a complete security strategy[4]. The components of COBIT are Governance system, and components (processes and organizational structures) Policy, Implementation guideline, Management objectives. These are specific to [gathering] IT risk management with enterprise strategy.

Strengths:

- **IT governance orientation:** COBIT helps Nature Green’s leadership align security initiatives with strategic goals and risk appetite. It emphasizes board responsibility and performance measurement.
- **Integration with other standards:** The framework can integrate with ISO 27001 and NIST CSF, providing a governance “wrapper” around technical controls.

Limitations:

- **Lacks technical detail:** COBIT does not specify detailed cybersecurity controls. Without complementary frameworks, it may not address the specific requirements of cloud and wireless networks.
- **Complexity:** COBIT’s extensive guidance may be overwhelming for small teams. Nature Green must carefully select relevant components.

4.4 ITIL Information Security Management (ISM)

ITIL is a framework for IT service management. Information Security Management (ISM) is intended to Safeguard the Confidentiality, Integrity and Availability of Information. ITIL ISM ITIL Information Security Management (ISM) is all about the proper management of information security[5]. It highlights risk assessment, incident management, compliance and continual improvement[5].

Strengths:

- **Service orientation:** ITIL integrates security into service design and operation, ensuring that Nature Green’s cloud and wireless services remain secure while meeting service-level expectations.
- **Process-focused:** It provides detailed process guidance for incident response, change management and continual improvement.

Limitations:

- **Less emphasis on governance:** ITIL is service-centric rather than governance-centric. It must be combined with frameworks like COBIT to ensure strategic alignment.
- **Not security-specific:** While it includes ISM, ITIL covers broader IT service management and may not offer detailed security controls for BYOD.

4.5 SOC 2, HIPAA, NERC CIP, FISMA and Other Frameworks

While the assignment is informed by ISO 27000 and ITIL, it is helpful to consider other relevant standards briefly: • SOC 2 It’s an auditing standard for service providers’ controls based on five principles of security, availability, processing integrity, confidentiality and privacy. Bit Sight mentions that SOC 2 constitutes trust for customers but mandates third-party audits [1]. For Nature Green, SOC 2 certification might provide a comforting insurance policy to partners but adds expense. •HIPAA governs healthcare data. It focuses on risk analysis, administrative safeguards, and privacy standards [1]. Horticulture is at Nature Green’s core; privacy standards guided by HIPAA dictate the management of such information. • NERC CIP is actions control-oriented to the critical infrastructure, and it pays attention to incident response and supply chain

risk[1], which can guide NG's vendor management. • Continuous monitoring and systems inventories are required by FISMA [1]. Continuous monitoring can be borrowed by Nature Green from FISMA. • ISO 31000 (Risk Management) provides a framework that helps organizations to identify, analyze and evaluate the risks as well as treating them. It adds to ISO 27001 and NIST CSF by offering a framework for staged risk management.

4.6 Regulatory Requirements: GDPR and NIS 2

In the EU/UK market, compliance with GDPR is legally required in all cases. Organizations under GDPR must apply technical measures, organize with organizational ones and engage in data protection impact analysis and breach notification. One summary of the GDPR is that it has 99 articles, and requires breach notification and high fines for non-compliance[1]. In addition, the NIS 2 Directive (as of October 2024) entails more stringent incident reporting obligations, board-level responsibility and cooperation arrangements[6]. Nature Green will need to have an organizational structure that is designed to meet these obligations and can respond rapidly to incidents.

5 Integrated Security Governance Model for NatureGreen

To meet the multifaceted security requirements in Nature Green, in this paper we present an integrated model that integrates multiple models and overcomes their weaknesses. This is represented in Figure 1, the integrated model placed Nature Green's custom security program in the middle of the primary models; ISO 27001, COBIT 2019, NIST CSF 2.0 and ITIL ISM. This second layer exchanges with the other two layers (2), and is intertwined with and supplies the central governing mechanisms. Specific aspects are further affected by other external these frameworks and regulations (SOC 2, HIPAA, NIS 2, GDPR, ISO 31000 etc.).

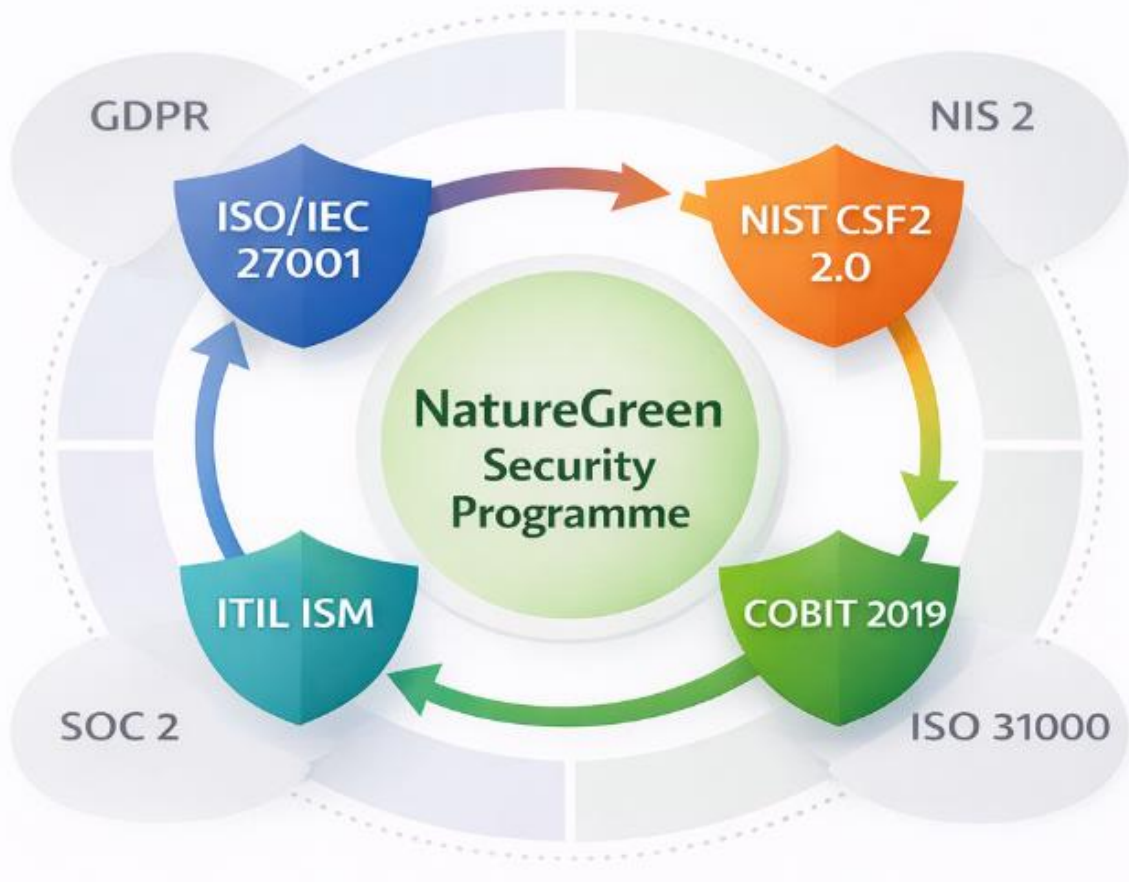


Figure 3: Integrated Security Governance Model

5.1 Governance and Strategic Planning

1. Form a Security Steering Committee: Driving the creation of a Security Steering Committee that is chartered to be led by a board member and have members from IT, legal, human resources and marketing in partnership with the CISO and leveraging COBIT governance. This committee sets the organization's risk appetite, approves policies and oversees compliance.
2. Take a Risk with ISO 31000: Marry the risk management process from ISO 31000 to NIST CSF's Identify and Govern functions. Potential threats for cloud services, wireless networks and BYOD need to be evaluated according to their probability and effectuation. The committee should priorities high-risk assets (e.g., intellectual property) and implement appropriate controls.
3. Alignment to Business Goals: COBIT stresses the importance of alignment between IT goals and business objectives. _Source If it is then Next Generation Nature Green should be aligning security objectives to organizational goals (e.g., that a customer trusts an online channel) and has access in corporate strategy direction. It shows that: security = business enabler, not merely an IT function.

5.2 Compliance and Legal Obligations

1. GDPR and Data Protection Requires Nature Green to engage in data minimization, encryption and pseudonymization of personal data. Consider making DPIAs part of the life cycling of projects. However, incident response plans need to be in alignment with GDPR's 72 hours data breach notification requirement[1].
2. NIS 2 Directive: Nature Green must be ready for mandatory incident reporting and board accountability by implementing clear escalation paths and training board members on cybersecurity oversight[6]. Ongoing tabletop exercises will be conducted to test the organization's prompt reporting of incidents.
3. Monitoring: Adapt from FISMA's continuous monitoring. Implement compliance checks within ITSM tools so any drift with standards pop up alerts. [1]

5.3 Security Policies and BYOD/Wireless Strategy

The usage of personal devices and wireless access significantly increase the space for attacks. A study on BYOD in hospitals indicates that though the use of personal devices at workplace helps productivity but it also causes security piggybacking through loose controls, human error and policy workarounds[7]. A multidimensional maturity model is suggested, and the three critical dimensions are technology, policy and people[7].



Figure 4:BYOD and Wireless Security Control Architecture

4. **BYOD Policy:** Define eligibility, acceptable use, device registration, and minimum security requirements. Devices should adhere to baseline controls: strong authentication (multi-factor), device encryption, screen timeouts, and remote wipe. The policy should restrict access based on user roles and device security posture.
5. **Mobile Device Management (MDM):** Implement MDM solutions to enforce compliance, deploy updates and monitor device health. MDM will support remote wiping of lost devices and separation of personal and corporate data through containerization.
6. **Wireless Security:** All wireless access points must support the WPA3 standard, segmentation of guest networks and certificate-based authentication. Network access control (NAC) should be used to restrict devices that do not meet policy standards.
7. **Privacy and Consent:** Staff and customers must consent to monitoring for security purposes. Data collected from personal devices should be limited to security metadata and not personal content.

5.4 Risk Management

1. Risk identification: Utilize ISO 31000 for identification of risks, such as those presented by cloud providers (e.g., data compromise and misconfigurations), wireless networks (e.g., rogue access points/ eavesdropping), BYOD (malware/data leakage) and insider threats. Consider also external threats – ransomware or supply-chain attacks.
2. Risk Analysis and Evaluation: prioritize risks by probability consequences. For example, the 2024 ransomware spike that cost billions and which is prevented through solid backup and disaster recovery[8] points to a great deal of potential for cloud data to be impacted by this attack. This risk should be prioritized.
3. Risk Treatment: Mitigation includes the application of least-privilege access controls, encryption, periodic vulnerability scanning, and supply-chain risk management. Remaining risks should be Tolerated by the Security Steering Committee or Transferred (e.g., to cyber insurance).

5.5 Securing the Management Models and Modes

1. Access Control and Identity Management: Practice the principle of least privilege and use role-based access control (RBAC). Enable multi-factor authentication (MFA) for all users, especially remote bring your own device (BYOD) users. Identity and access management (IAM) tools must connect with cloud platforms and offer single sign-on (SSO).
2. Asset & Configuration Management: Utilize ITIL process to keep track of physical, software and cloud resources. The practice is reinforced by the FISMA mandate for system inventories[1]. Server, network device and endpoint configuration baselines should be established and managed.
3. Incident Response: ITIL and NIST CSF functions analogous to Detect and Respond help in creating an incident management procedure. Clarify escalation paths, roles and communication plans. Practice Continuous practice and incorporate learnings into best practices.
4. Security Awareness and Culture: Human-centered is important as in the case of BYOD maturity model[7]. Nature Green should deliver frequent education on phishing, device

hygiene and policy adherence. Engagement can be improved through gamification and scenario-based training.

5.6 Contingency Planning and Business Continuity

Ransomware and business interruption Meanwhile, escalating ransomware attacks and operational disruption point to the urgency of continuity. A 2024 article observes that ransomware attacks are becoming both more expensive and dangerous, underscoring backup-and-disaster recovery planning, such as the 3-2-1-1 backup rule (three copies of your data, on two different media formats, one of which is off-site and one is offline to ensure no errors) [8].

1. **Disaster Recovery Planning:** Nature Green shall maintain a disaster recovery plan (DRP) that replicated across regions, on-premises backups should 3-2-1-1-0[8]. It is necessary to periodically test the recoverability of backup.[8]
2. **Business Continuity Planning:** Create a business continuity plan (BCP) with key functions (e.g., e-commerce, supply chain, customer service) outlined and develop strategies to continue operations during interruptions. This plan should cover alternate communication methods, remote working processes and interaction with cloud providers.
3. **Tabletop and Live Workouts:** Do regular workouts to replicate ransomware, breaches or network outages. These tests help ensure that competences, and weaknesses in the DRP and BCP are identified.

5.7 Protection Mechanisms

1. **Technical Controls:** Deploy endpoint detection and response (EDR) solutions on all devices, including BYOD endpoints, to detect malware and suspicious behaviour. Network segmentation and micro-segmentation reduce lateral movement.
2. **Encryption:** Encrypt data at rest and in transit. Use strong key management practices and hardware security modules (HSMs) for key protection. For BYOD devices, enforce full-disk encryption and secure VPN tunnels.
3. **Application Security:** Employ secure development practices, including threat modelling, secure coding, static/dynamic analysis and penetration testing. Protect APIs and cloud interfaces with authentication, throttling and input validation.
4. **Monitoring and Logging:** Implement continuous monitoring across cloud and on-premises environments. Centralized log management with correlation and anomaly detection improves visibility. Apply zero-trust principles: verify explicitly, use least privilege and assume breach.

5.8 Service Level Agreements (SLAs)

SLAs define the expectations between Nature Green and its cloud providers or managed service providers. According to Databank, key components of an SLA include service availability (e.g., 99.99 % uptime), support response time (e.g., 15-minute response), issue resolution time (e.g., four hours), performance metrics (e.g., latency < 10 ms), security measures, penalties for non-compliance, and monitoring/reporting [9]. Nature Green should negotiate SLAs that:

1. **Specify Availability and Performance:** Guarantee high availability across geographic regions with defined RTOs and RPOs. Cloud providers must deliver resilience and redundancy.
2. **Define Security Responsibilities:** Clarify shared responsibility models, including data protection, vulnerability management and incident notification. Providers should commit to strong encryption, regular security audits and compliance with standards.
3. **Ensure Transparent Reporting:** Require monthly reports on uptime, security incidents, patch management and performance metrics. Include provisions for independent audits and rights to audit.
4. **Include Remedies and Penalties:** Define financial penalties or service credits if providers fail to meet SLA targets. This motivates compliance.

5.9 Proposed Security Program Overview

Figure 5 summarizes Nature Green’s security programmed, incorporating the above elements and aligning them with the corresponding frameworks.



Figure 5:NatureGreen’s Proposed Security Program Pillars

The program is based on 8 pillars: Compliance & Legal, Governance & Strategic Plan, BYOD & Cloud Environment (from Dec 2015), Working Model of SLA, Security Mechanism Factor; Safety Management Practice, Emergency Response Plan and Security Policy/ Risk Management. Each pillar is grounded in pragmatic models. For instance, the Compliance pillar builds upon GDPR and NIS 2, Governance on COBIT and NIST CSF, while Security Management on ITIL and ISO 27001. Collected together, these all contribute to a healthy and well-rounded picture of security.

6 Why Regulations and Standards Must Continuously Evolve

Cyber Threat Adversaries' methods are evolving in the face of technology advancements (AI-enabled attacks and geopolitical tensions, for example). The World Economic Forum states that major economies implemented new cybersecurity regulations in 2024 (e.g., the EU's NIS 2, US's National Cybersecurity Strategy and Singapore's OT Cybersecurity Masterplan) and 60 % of business executives believe that effective regulation can reduce risk [6]. The former aims at two measures: incident reporting with accountability for the board [6], and the latter pushes responsibility back to those that are most capable of mitigating risk [6]. Such a new development emphasizes the necessity of up-to-date information.

Drivers for evolution:

Emerging technologies: Artificial intelligence, machine learning, quantum computing and 5G create fresh openings for human mischief. Standards need to look at challenges including AI-generated phishing, model poisoning and data poisoning.

Supply chain risk: As third-party software and cloud providers become more prevalent so do supply-chain security requirements.

Regulatory convergence: Multinational companies serve customers in multiple geographies; aligned standards ease the path to compliance and trade. For example, updates of ISO 27001 include mapping with NIS 2 and GDPR [2].

Human factors: BYOD and remote work emphasize the need for approaches dealing with user behavior, training and cultural change [7].

An incident report card: Big breaches expose holes in the current system of questions. Steady improvement relies on turning lessons into new standards.

Failing to update regulations causes compliance lag (where old standards don't accommodate new threats); legal uncertainty (businesses are unsure of what they must do); and competitive shortfall (slow movers aren't meeting customer demands for security).

7 Conclusion

Nature Green works in this intricate digital environment: cloud computing, wireless and BYOD. In the course of this report, a thorough analysis based on literature review was carried out regarding the most important security frameworks and standards in commercial use (ISO/IEC 27000, NIST CSF 2.0, COBIT 2019, ITIL ISM), as well as other asset management models (SOC 2, HIPAA, NERC CIP, FISMA and ISO31000). This research concluded that "there is no one-size-fits-all framework, a nonergative approach will be necessary. ISO 27001 for all of its controls (albeit customized ones[1]); NIST CSF is flexible and risk based [3]; COBIT has the strategic alignment [4]; and ITIL has security embedded in service management [5]. Compliance standards and regulations (such as GDPR 3 and NIS 24) introduce legal obligations. Mixing these frameworks, a customize security governance model for Nature Green depicting governance, compliance with

(governance, compliance, BYOD policies A risk management, operational controls A contingency planning protection mechanisms A SLAs) was designed in the report. The integrated model and the proposed security program are shown in Figures 1 and 2. Lastly, it maintains that the statutes and standards need to be updated constantly to keep up with new threats and technologies recognized globally¹⁹.

Utilizing the integrated security governance method presented here, Nature Green can safeguard its intellectual property, meet legal requirements and earn customer and partner trust. It is all about having a strict discipline whilst still remaining flexible, understanding that security isn't some fixed point you can reach and maintain but rather an ongoing route with constant changes and challenges.

Reference

- [1] E. Cisternelli, “7 Cybersecurity Frameworks to Reduce Cyber Risk,” BitSight, Feb. 27, 2024. <https://www.bitsight.com/blog/7-cybersecurity-frameworks-to-reduce-cyber-risk>
- [2] Š. Grigaliūnas, R. Brūzgienė, M. Schmidt, P. Smyrli, S. Andreou, and A. Lopata, “Holistic Information Security Management and Compliance Framework,” *Electronics*, vol. 13, no. 19, pp. 3955–3955, Oct. 2024, doi: <https://doi.org/10.3390/electronics13193955>.
- [3] Bilgin Metin, Sibel Berfun Sevim, and M. Wynn, “Cybersecurity Strategy Development: Towards an Integrated Approach Based on COBIT and ISO 27000 Series Standards,” *Standards*, vol. 5, no. 4, pp. 33–33, Dec. 2025, doi: <https://doi.org/10.3390/standards5040033>.
- [4] Bilgin Metin, Sibel Berfun Sevim, and M. Wynn, “Cybersecurity Strategy Development: Towards an Integrated Approach Based on COBIT and ISO 27000 Series Standards,” *Standards*, vol. 5, no. 4, pp. 33–33, Dec. 2025, doi: <https://doi.org/10.3390/standards5040033>.
- [5] P. Griffon, “ITIL Information Security Management,” Purple Griffon, Aug. 21, 2023. <https://purplegriffon.com/blog/itil-information-security-management> (accessed Jan. 14, 2025).
- [6] S. Feingold and F. Beato, “Cybersecurity rules saw big changes in 2024,” *World Economic Forum*, Oct. 17, 2024. <https://www.weforum.org/stories/2024/10/cybersecurity-regulation-changes-nis2-eu-2024/>
- [7] T. A. Wani, A. Mendoza, and K. Gray, “A Socio-Technical Approach to BYOD Security in Hospitals: Development and Pilot Testing of a Maturity Model Using Mixed-Method Action Research (Preprint),” *JMIR Human Factors*, Jan. 2025, doi: <https://doi.org/10.2196/71912>.
- [8] A. Data, “The Importance of Cybersecurity and Business Continuity Planning,” Atomic Data®, Oct. 03, 2024. <https://www.atomicdata.com/the-importance-of-a-resilient-disaster-recovery-practice-lessons-from-catastrophic-2024-ransomware-cyberattacks/> (accessed Aug. 14, 2025).
- [9] K. MacLean, “The Critical Role Of Service Level Agreements (SLAs) In Ensuring Data Center Reliability,” *DataBank | Data Center Evolved*, Jul. 08, 2024. <https://www.databank.com/resources/blogs/the-critical-role-of-service-level-agreements-slas-in-ensuring-data-center-reliability/> (accessed Oct. 06, 2024).

Figure 1 – Comparative Overview of Major Cybersecurity Frameworks Adapted by the author based on ISO/IEC 27001, NIST Cybersecurity Framework 2.0, COBIT 2019, ITIL Information Security Management, GDPR and the NIS 2 Directive.

Figure 2 – NIST Cybersecurity Framework (CSF) 2.0 Lifecycle Adapted from National Institute of Standards and Technology (NIST), Cybersecurity Framework (CSF) 2.0, 2024.

Figure 3 – Integrated Security Governance Model for NatureGreen Author’s original integrated model developed using ISO/IEC 27001, NIST CSF 2.0, COBIT 2019, ITIL Information Security Management, ISO 31000, GDPR and the NIS 2 Directive.

Figure 4 – BYOD and Wireless Security Architecture Adapted by the author based on NIST SP 800-124 Rev.2, NIST SP 800-153, ISO/IEC 27002:2022 and recent BYOD security research.

Figure 5 – Security Programme Pillars Author's adaptation based on integrated security governance and management concepts derived from ISO/IEC 27001, COBIT 2019, NIST Cybersecurity Framework 2.0 and ITIL Information Security Management.