Module: Data Security, Governance and Compliance

Module Code: ACCA7028

Submitted to:

Dr. Carlene Campbell

Associate Professor

University of wales trinity saint david

Submitted By:

MD IMRAN BISWAS

Student ID: 2436882

University Of Wales Trinity Saint David

Submitted Date: 06-01-2026

Contents

Introduction:..... 1

Comparative Analysis of Information Security Frameworks and Models:..... 2

Proposed Design of the Security Governance Framework for NatureGreen:..... 8

Critical Analysis of the Reasons Driving Continuous Updates and New Rules in Security Standards:..... 14

Conclusion:..... 15

References:..... 16

List of figures

Figure 1: The PDCA Cycle applied to an Information Security Management System (ISMS) 3

Figure 2:The ITIL 4 Service Value System (SVS) 5

Figure 3:NIST Cybersecurity Framework 7

Figure 4:Proposed Organisational Structure for NatureGreen, ensuring the independence of the Chief Information Security Officer (CISO). 9

Figure 5: Proposed Network Segmentation architecture, Utilising VLANs to isolate corporate assets from personal devices (BYOD) 12

Introduction:

In today's digital world, information security is not about technology; rather, it is about business survival. This report focuses on NatureGreen, a global pharma company facing serious problem, like 95% wireless network, no security rules, cloud management and securing personal and client data. The goal of the assignment is to analyse major security frameworks like ISO 27001,ITIL 4, NIST to find solution. Based on the research, I propose a Hybrid Governance Model. This plan uses ISO for leadership rules, NIST to secure the wireless network, and ITIL to manage cloud contracts, ensuring NatureGreen can follow the law and protect its valuable intellectual property.

Comparative Analysis of Information Security Frameworks and Models:

Information security is a critical part and plays an important role in protecting an Organisation's business. Organisations should protect their information to save the Organisation's value and reputation. Today, top management sees information security as very important. It needs more attention, support, and motivation from them. Because of this, the idea of information security governance (ISG) was created. According to Posthumus and von Solms (2004a), ISG is a set of processes determining how to address information security at the top management level. To implement the ISG in the system, the Organisations need a security framework or model. A security framework is a set of rules and steps that help Organisations protect themselves from cyber risks. On the other hand, a security model is more of a mathematical structure that defines how a system declares security policies. There are many security frameworks out there, ranging from governance-focused models like ISO/IEC 27001 (Malatji, 2023) to service management standards such as the Information Technology Infrastructure Library (ITIL), and operational guides like the NIST Cybersecurity Framework (Alumina et al, 2025). In the end, no single framework provides a perfect solution. Each model has distinct advantages and drawbacks, and its effectiveness depends on the particular operational context and use case.

ISS standards and frameworks have been playing a crucial role in the spread of now-critical holistic approaches—technical, Organisational, and managerial. Among them, ISO/IEC 27001 is arguably the most renowned one. ISO/IEC 27001 (Kitsios et al, 2023) is the international standard for information security management. It is part of the ISO 27000 series. ISO 27001 sets out a framework for all Organisations to establish, implement, operate, monitor, review, maintain, and continually improve an ISMS (information security management system). Speaking of ISO 27000 series, it refers to a series of international standards for establishing, implementing, and maintaining an information security management system (ISMS). It is not a single model but a collection of standards that provide an overview of information security best practices, risk management, and continuous improvement. Unlike other technology-centric models that focus solely on specific technical tools like firewalls, ISO/IEC 27001 focuses on an Organisation-wide, risk-based approach. ISO/IEC 27001 helps Organisations to identify the assets that need protection and then look for any threats associated with the assets. Then finally select and implement appropriate security steps to eliminate the risks.

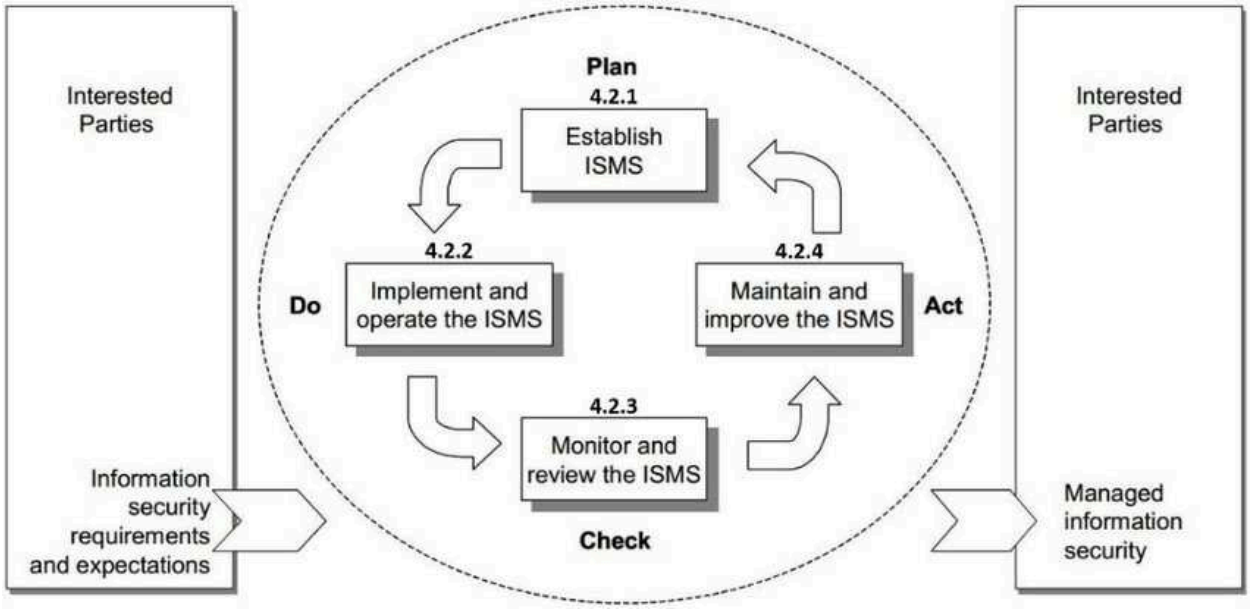

Figure 1: The PDCA Cycle applied to an Information Security Management System (ISMS)

Source: (Jevelin, and Faza, 2023)

The PDCA (Plan-Do-Check-Act) cycle is the foundational principle for the design, implementation, maintenance, and continual improvement of an Information Security Management System (ISMS) under ISO/IEC 27001. The process starts by understanding the business requirements and who the interested parties are. Then the middle cycle begins. It has 4 parts:

Plan: designing the policy and assessing the risks. It basically establishes the ISMS.

Do: Implement the policy to build the ISMS

Check: review and monitor the system

Act: continuously fixing and updating policy

The output of the cycle will be a more managed and mature ISMS system.

ISO/IEC 27001 offers a systematic approach to managing information security and provides significant benefits, but it faces notable challenges during implementation and maintenance. Its strength lies in its structured, internationally Recognised framework for managing information

security risks, enhancing security posture, and building customer trust and competitive advantage. But the primary weaknesses are the significant amount of investment in time and resources, potential for high costs, complexity for smaller businesses, and the continuous need for maintenance and cultural change.

While ISO 27001 is the gold standard for *policy*, it may lack the implementation needed for technical threats if not used with other tools.

As Organisations increasingly rely on technology to power their operations, IT teams are becoming one of the essentials of a business. ITIL (Ernawati et al, 2023) provides a framework that gives IT teams the flexibility and stability they need to support the business successfully. ITIL (also known as Information Technology Infrastructure Library) is the most widely adopted framework for IT Service Management (ITSM) globally. It provides a comprehensive set of guidelines to help Organisations manage their IT services effectively, align IT with business needs, and deliver value to customers. While ISO 27001 focuses solely on establishing a better Information Security Management System (ISMS), ITIL is focused on overall IT Service Management (ITSM) and value delivery. It also focuses on value creation for the business. As modern enterprises rely on Cloud Computing, in ITIL, security in the cloud is a reliable service, not just a firewall product. It Emphasises a service mindset, where security is an offering designed to create value by managing risk and ensuring compliance. This service is managed via the Information security management practice, which integrates activities across all Four Dimensions of Service Management (people, processes, technology, and partners).

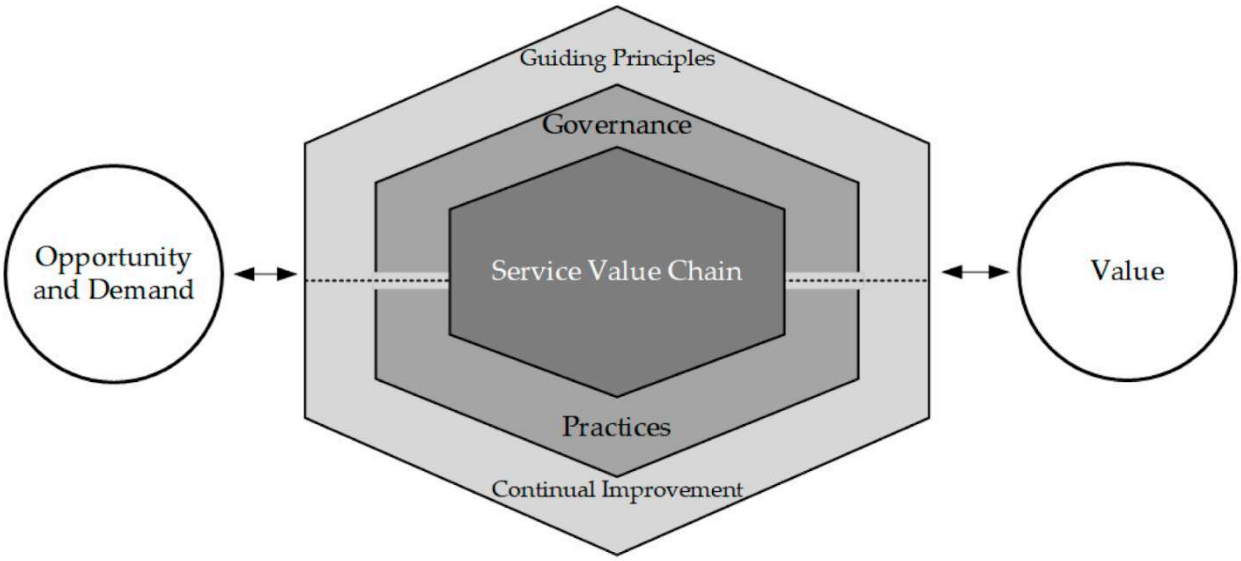

Figure 2:The ITIL 4 Service Value System (SVS)

Source: (Tuomisto, 2022)

This ITIL 4 SVS diagram describes how all the components and activities within an Organisation can work together to create value. It is a framework that takes inputs from demand and opportunities and transforms them into desired outcomes (value).

The key component of the diagram:

Opportunity and Demand: These are the inputs that trigger activities within the SVS. Opportunity refers to possibilities for adding value to stakeholders, while demand is the need for products and services among consumers.

Guiding Principles: These are foundational recommendations that guide the Organisation to make decisions and actions.

Governance: This component involves evaluating, directing, and monitoring the Organisation.

Service Value Chain (SVC): The Centre of the model that outlines the key activities

Practices: These are Organisational resources (people, information, etc) dedicated to performing work

Continual Improvement: This is an ongoing effort to align the Organisation's practices

Value: This is the resulting outcome of the SVS

ITIL 4 offers numerous advantages. It places a strong emphasis on understanding and delivering value to customers and other stakeholders. Moreover, it is a very flexible framework, which means it can be Customised to suit the specific needs of various Organisations. One of the advantages that makes it apart is its ability to integrate with other modern technologies, such as new and DevOps. The framework also guides effective governance and risk management. At last, it provides a well-defined framework for managing the ITIL service lifecycle, including design, operation, and improvement. But ITIL 4 needs a high cost to set up the framework in an organisation. While ITIL4 offers various advantages, it is also a complex implementation process. The framework can be challenging to implement, especially for Organisations without prior experience or understanding. One of the biggest disadvantages is despite its flexibility, ITIL4 is also rigid in its own way, and it may struggle to adapt to rapidly changing circumstances.

ITIL 4 offers Organisations a systematic approach that enhances efficiency and customer satisfaction. But the framework's implementation can be costly and complex, and there's a risk of resistance to change within the Organisation.

While ISO 27001 establishes the necessary governance structure and ITIL 4 ensures effective service delivery, neither of them provides the actual operational protocols to defend against active, real-time network threats. To address the gap, NIST Cybersecurity Framework (CSF) can be implemented. The NIST Cybersecurity Framework (CSF) 2.0 (Pascoe, C.E., 2023) is a voluntary, risk-based set of guidelines from the U.S. National Institute of Standards and Technology (NIST) to help Organisations manage and reduce cybersecurity risks. It's considered a standard for building a cybersecurity Programme.

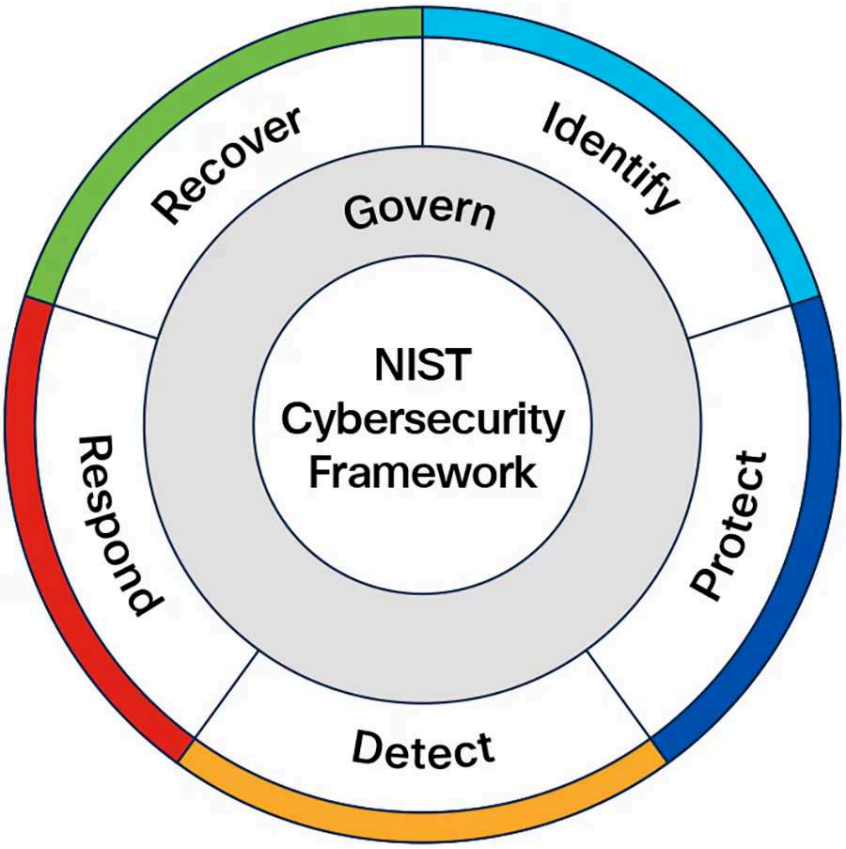

Figure 3:NIST Cybersecurity Framework

Source: (Edwards, J., 2024)

The image is a diagram of the NIST Cybersecurity Framework, which helps Organisations manage digital risks. The framework is built around six core functions:

Govern: Establishes policies, roles, and strategy for risk management.

Identify: Understands and manages risks to systems, assets, and data

Protect: Implements safeguards and controls to limit the impact of cyber events.

Detect: Finds and Analyses potential cybersecurity attacks in a timely manner.

Respond: Takes action regarding a detected incident to contain the impact.

Recover: Restores capabilities and services impaired by an incident.

Talking about the strength of NIST frameworks, it provides a structured method to identify, assess, and mitigate threats and also creates a bridge between technical and business teams. Moreover, it is highly Customisable and can adapt for Organisations of any size, industry. But it can be overwhelming and resource-intensive for smaller entities. The lack of detailed, required controls can make implementation difficult and Organisations cannot get a formal certification making its validation challenging.

The NIST CSF is a highly effective, flexible, and widely adopted framework for risk management, but its successful implementation requires careful planning and significant Organisational resources, which increases its complexity.

ISO 27001 gives you the formal rules and standards to follow for official proof. NIST CSF helps you manage security risks every day. ITIL 4 makes sure these security ideas are integrated well with the normal IT work. Together, they (Heriak et al, 2025) offer a complete plan for safety and better service.

Proposed Design of the Security Governance Framework for NatureGreen:

After evaluating the security models in the previous section, it is evident that one framework cannot be sufficient to solve the security problem of NatureGreen as on one side it has problems like Wireless Security and cloud management and on the other side it has problems like Governance disarray and Intellectual Property Risk. Therefore we need to implement an integrated hybrid governance mode designed specifically to address the company's current situation. This model will integrate the strength of three unique frameworks to create a Defence-in-Depth architecture. ISO/IEC 27001 will handle the missing governance and policy structures providing the necessary leadership oversight. Simultaneously, the NIST Cybersecurity Framework (CSF) will work on specific operational risks, such as the unAuthorised use of personal devices (BYOD) and wireless network security. Finally, ITIL 4 principles will apply to manage the external cloud dependencies through proper Service Level Agreements. This multi-layered approach ensures that NatureGreen achieves regulatory compliance and secures its intellectual property against both internal and external cyber threats.

One of the big problems of NatureGreen is it has no established policies despite the high value of its intellectual property and global presence. As a result, NatureGreen's security posture is currently in disorder. This lack of structure suggests that information security is likely treated as a lower-tier IT function rather than a strategic business aspect. To solve this problem, NatureGreen must implement a formal governance structure aligned with ISO/IEC 27001 Clause 5 (Leadership).ISO 27001 Clause 5, titled "Leadership" (Malatji, M., 2023) Emphasises the critical role of top management in the success and effectiveness of an Organisation's Information Security Management System (ISMS). It ensures that information security is a strategic priority and not just an IT issue. To ensure the structure, we need to establish Information Security Steering Committee with the CEO, Head of Legal, Head of HR, and the new Chief Information Security Officer (CISO). This committee will meet quarterly to align security objectives with business goals. The new CISO role must be structurally separated from the IT Department. This helps ensure accountability and that personnel understand their contribution to the ISMS's effectiveness. In this way, NatureGreen ensures Segregation of Duties, where the CIO builds the systems, and the CISO independently verifies their security.

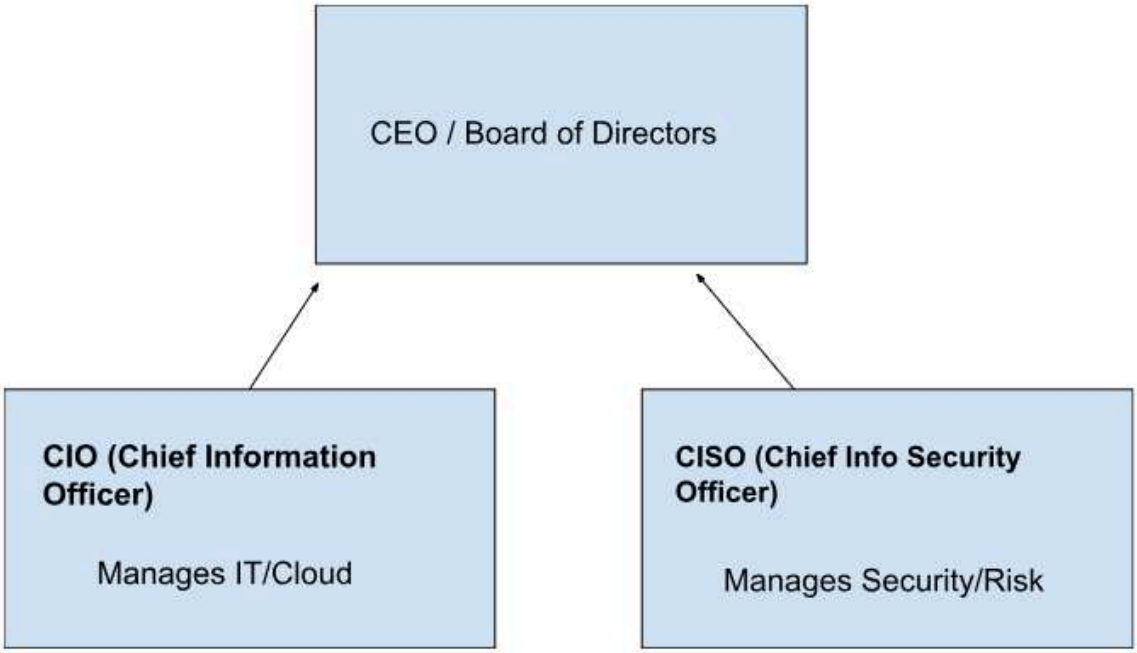

Figure 4:Proposed Organisational Structure for NatureGreen, ensuring the independence of the Chief Information Security Officer (CISO).

Source: (Ciekanowski et al,. 2024)

As a global brand, NatureGreen has an international customer base, and that' why it falls under the jurisdiction of strict privacy laws like the General Data Protection Regulation (GDPR) (EU) and CCPA (USA). Second, the "immense pressure" from staff and customers to use personal devices has created problems, leaving the company vulnerable to data leakage and legal penalties. To solve the first problem for international customers' data, we can use a Data Classification and Handling Policy aligned with ISO/IEC 27001 Annex A.8.2 (Kenyon, B., 2024). The objective is to ensure that information receives an appropriate level of protection in accordance with its importance to the Organisation. To implement it, we can apply these 3 things:

Classification Scheme: All data must be tagged as Public, Internal, or Confidential.

GDPR Mandate: "Confidential" client health data must be encrypted at rest and in transit.

Data Subject Access Rights (DSAR): A formal process must be established to allow international customers to request the deletion of their data ("Right to be Forgotten"), ensuring ethical handling of sensitive information.

To resolve the unauthorised use of personal devices, a strict Bring Your Own Device (BYOD) Policy can be introduced, aligned with ISO/IEC 27001 Annex A.6.2.Annex A.6.2 is titled "Mobile devices and teleworking" and falls under "Organisation of information security". The purpose here is to establish a management framework to ensure the security of remote working arrangements and the use of mobile devices. To implement this, a Mobile Device Management (MDM) system will be introduced, and no personal device will access corporate networks unless it is enrolled in the corporate MDM system. The MDM software will create a "sandboxed" container on the employee's phone. This separates NatureGreen's corporate data from the user's personal photos and apps, allowing the company to remotely wipe *only* the corporate

data if the employee leaves or the phone is stolen. By legalizing *controlled* access via MDM, NatureGreen balances the "pressure" for flexibility with the mandatory requirement to protect the "intellectual properties" from being synchronized to unsecured personal cloud accounts.

NatureGreen holds "intellectual properties worth billions," primarily related to its healthy living products. But there is no formal methodology for identifying or prioritizing threats to this IP. Without a structured risk assessment, the company cannot determine whether to Prioritise Defences against external hackers or internal leaks, leaving high-value assets exposed. To solve this problem, we can use a Risk Management Framework based on ISO/IEC 27005. This standard provides the guidelines for Information Security Risk Management (ISRM) and supports the general requirements of ISO 27001. We will use a Security Risk Register to identify the threat and find a solution to it.

Table 1: Proposed Information Security Risk Register for NatureGreen

ID	Risk Description	Threat Vector	Likelihood	Impact	Risk Rating	Risk Response Plan
R01	Staff devices infected with malware connect to the network.	Accidental/Internal	High	Critical	Extreme	Network Segmentation
R02	Hackers intercept IP data on the open wireless network.	External / Malicious	Medium	Critical	High	Individual logins for all staff and use VPN
R03	The Cloud Provider goes offline, halting global sales	Supply Chain	Low	High	Medium	backup on a second cloud.

One of the main problems in NatureGreen's infrastructure is of its 95% wireless network because if a single device is infected with virus or malware, The virus or malware could potentially traverse the wireless network and infect the servers holding the "billions in IP." To solve this, a Zero Trust architecture (Min et al, 2025) can be used which is based on the NIST CSF 'Protect' Function (PR.AC). The core of this design is Network Segmentation. The goal of this system is to limit access to physical and logical assets to only those users or devices that are Authorised, and only to the extent required for their specific role.

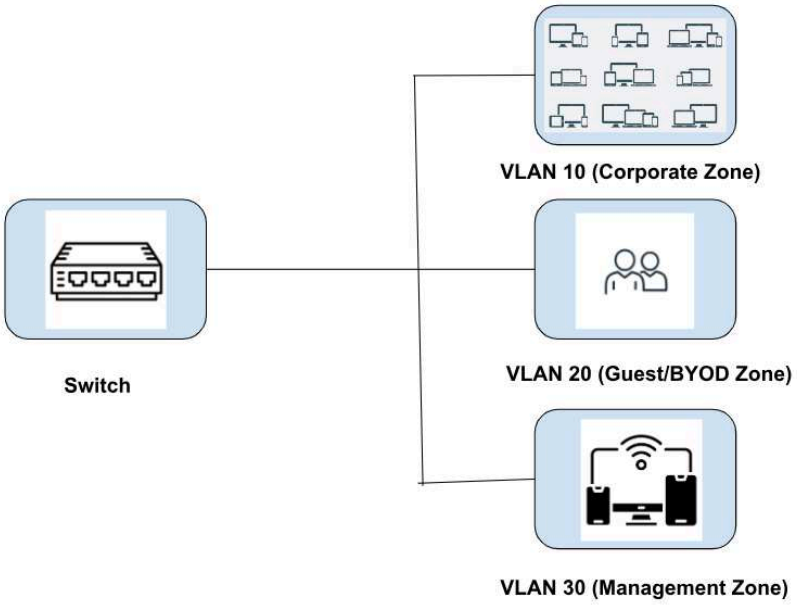

Figure 5: Proposed Network Segmentation architecture, Utilising VLANs to isolate corporate assets from personal devices (BYOD)

Source: (Kesavan et al., 2025)

As shown in the Figure, the wireless network is segmented into isolated zones to contain potential infections:

VLAN 10 (Corporate Zone): Designated for company-issued laptops containing the 'billions in IP.' Access is restricted to authenticated staff only.

VLAN 20 (Guest/BYOD Zone): Designated for personal devices and guests. This VLAN provides internet access, but is blocked by the switch from communicating with VLAN 10.

VLAN 30 (Management Zone): Reserved for VIP phones and IoT devices, ensuring they cannot be used as a gateway to attack the servers.

One more concerning fact is that NatureGreen relies entirely on "cloud services to deliver IT services" to its global staff and clients. This creates a great dependency: if the cloud provider fails, NatureGreen's business halts. To solve this supply-chain problem, the ITIL 4 'Supplier Management' can be applied. The ITIL 4 'Supplier Management' (Biswas, S., 2024) practice ensures that an Organisation's suppliers and their performances are managed appropriately to support the seamless provision of quality products and services. This system will negotiate rigorous Service Level Agreements(SLAs) with the cloud service provider. The SLAs include
Availability Target: The SLA must mandate a 99.99% Uptime Guarantee. This ensures that the global sales platform cannot be offline for more than 5 minutes per month.

Financial Penalties: The contract must include "Service Credits," meaning the vendor must pay NatureGreen if they miss the uptime target. This incentivizes the vendor to maintain stability.

The "Right to Audit" Clause: A clause must be inserted allowing NatureGreen's new CISO to review the cloud provider's third-party security audits annually.

While NatureGreen cannot physically secure the servers of a public cloud provider, applying ITIL 4 principles allows the company to ensure that the "cloud services" supporting the business are as resilient as the internal network.

Along with this thing, in case of ransomware or cloud shortage problem, NatureGreen must implement a Business Continuity Plan aligned with the NIST CSF 'Recover' function (Dimakopoulou et al, 2024). The goal of this system is to support timely recovery to normal operations and Minimise the impact of the incident on the Organisation. To implement it, we can use the 3-2-1 Backup Strategy, maintaining three data copies across two different media types, with one offline copy. This ensures safety even if the primary wireless network is compromised.

NatureGreen's lack of security rules, 95% wireless network, and inefficient cloud management put its billions in assets at huge risk. To fix this, we designed a hybrid solution: **ISO 27001** for leadership rules, **NIST** to stop wireless hackers, and **ITIL** to manage cloud contracts. This strategy turns security from a chaotic mess into a continuous, active Defence system.

Critical Analysis of the Reasons Driving Continuous Updates and New Rules in Security Standards:

Technology evolves faster than laws. A primary driver for the continuous evolution of security standards is the pace of technological innovation significantly outpaces the regulatory frameworks designed to govern it. This phenomenon is called Technological Drift (Hughes et al, 2023). A clear example is that ISO/IEC 27001:2013 didn't focus much on Cloud. Consequently, Organisations that implement this standard are vulnerable to cloud attacks. For NatureGreen, relying on outdated wireless standards for its 95% wireless infrastructure would leave the network instantly vulnerable to attack, despite following older rules. Due to this rapid change in technology, ISO/IEC 27001:2022 had to be released to offer guidance on Cloud Computing. Thus, constant updates are necessary to ensure that governance controls match the technical reality of the modern threat landscape.

Moreover, hackers change tactics (Ransomware, AI attacks). The continuous and rapid evolution of cybersecurity risks, vulnerabilities, and attacker methodologies makes it difficult to protect the Organisation. This argument is called Threat Landscape. This landscape is a complex, dynamic environment that Organisations must constantly monitor and adapt to in order to protect their assets. While defenders must secure every vulnerability, attackers need only exploit one. If an Organisation believes that a static standard that follows a certain regulation can save them from an attacker, then they will be in a big danger. Even if that regulation addresses outdated attack protocols. For instance, the rise of Ransomware-as-a-Service (RaaS) (Alwashalie el at, 2021) has made it easy for hackers to do cyber crimes, making attacks more frequent and tactical than when many older standards were written. For NatureGreen, relying on static controls is dangerous. The "immense pressure" to use personal devices creates a dynamic attack surface that static policies cannot anticipate. Therefore, continuous regulatory updates—such as the inclusion of the 'Govern' function in NIST CSF 2.0 — are essential to force Organisations to shift from a passive "checkbox" mentality to an active, threat-centric Defence posture.

Finally, Regulatory Convergence (Marotta et al, 2021) drives the need for updates. Regulatory convergence refers to the trend where different regulatory bodies and jurisdictions worldwide begin to adopt similar standards, rules, and approaches, particularly concerning data protection, privacy, and cybersecurity. As public awareness of privacy rights grows, laws become stricter.

Organisations that fail to adopt updated privacy standards face not only legal penalties but also reputational damage. So updating standards isn't just about security; it's about business survival and reputation. Thus, the continuous evolution of standards acts as a forcing function, ensuring that businesses like NatureGreen remain ethically aligned with global societal expectations regarding data privacy.

Conclusion:

To sum up, NatureGreen is currently in a dangerous position because of its reliance on a 95% wireless network without any security protocol puts its billions in assets and privacy at huge risk. This report shows that no single framework or rule can fix everything. Instead, the best solution is a Hybrid Model that combines strengths. We use ISO 27001 to fix the security management, **NIST** to stop hackers on the wireless network, and **ITIL 4** to enforce strict cloud agreements. However, security is not a one-time fix. NatureGreen must constantly update its Defences to stay ahead of new threats and keep its business safe.

References:

Jevelin, J. and Faza, A., 2023. Evaluation the information security management system: A path towards ISO 27001 certification. *Journal of Information Systems and Informatics*, *5*(4), pp.1240-1256.

Tuomisto, J., 2022. Value co-creation in ITIL 4-framework.

Edwards, J., 2024. *A comprehensive guide to the NIST cybersecurity framework 2.0: Strategies, implementation, and best practice*. John Wiley & Sons.

Ciekanowski, M., Żurawski, S., Ciekanowski, Z., Pauliuchuk, Y. and Czech, A., 2024. Chief information security officer: A vital component of Organisational information security management.

Aljumaiah, O., Jiang, W., Addula, S.R. and Almaiah, M.A., 2025. Analysing cybersecurity risks and threats in IT infrastructure based on NIST framework. *J. Cyber Secur. Risk Audit*, *2025*(2), pp.12-26.

Kitsios, F., Chatzidimitriou, E. and Kamariotou, M., 2023. The ISO/IEC 27001 information security management standard: how to extract value from data in the IT sector. *Sustainability*, *15*(7), p.5828.

Ernawati, Y. and Wang, G., 2023. Assessing IT services management with ITIL framework V3: A case study. *Journal of System and Management Sciences*, *13*(4), pp.152-164.

Pascoe, C.E., 2023. Public Draft: The NIST Cybersecurity Framework 2.0. *National Institute of Standards and Technology*.

Heriak, Y. and Berko, A., 2025. COMPARISON ANALYSIS OF METRICS AND EVALUATION SCALES OF DISTRIBUTED INFORMATION RESOURCES QUALITY PARAMETERS.

Kenyon, B., 2024. ISO 27001 controls: A guide to implementing and auditing.

Min, C.H., Kim, D.H., Yang, H. and Kwak, J., 2025. Towards Secure Legacy Manufacturing: A Policy-Driven Zero Trust Architecture Aligned with NIST CSF 2.0. *Electronics*, *14*(20), p.4109.

Biswas, S., 2024. *Ultimate ITIL® 4 Foundation Certification Guide: Master the Best Practices for IT Service Management (ITSM) and get Certified in the ITIL® 4 Foundation Framework (English Edition)*. Orange Education Pvt Ltd.

Dimakopoulou, A. and Rantos, K., 2024. Comprehensive analysis of maritime cybersecurity landscape based on the NIST CSF v2. 0. *Journal of Marine Science and Engineering*, *12*(6), p.919.

Alwashali, A.A.M.A., Abd Rahman, N.A. and Ismail, N., 2021, December. A survey of ransomware as a service (RaaS) and methods to mitigate the attack. In *2021 14th International Conference on Developments in eSystems Engineering (DeSE)* (pp. 92-96). IEEE.

Marotta, A. and Madnick, S., 2021. Convergence and divergence of regulatory compliance and cybersecurity. *Issues in Information Systems*, *22*(1).

Malatji, M., 2023, January. Management of enterprise cyber security: A review of ISO/IEC 27001: 2022. In *2023 International conference on cyber management and engineering (CyMaEn)* (pp. 117-122). IEEE.

Hughes, J. and Hutchings, A., 2023, July. Digital drift and the evolution of a large cybercrime forum. In *2023 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)* (pp. 183-193). IEEE.

Kesavan, T. and AR, R.K., 2025, April. Implementation and Optimization of VLANs in a Campus Network. In *2025 International Conference on Computing and Communication Technologies (ICCCT)* (pp. 1-5). IEEE.