



**Prifysgol Cymru**

Y Drindod Dewi Sant

**University of Wales**

Trinity Saint David

Submitted by

Shamsuddin Mahmud (2432880)

Supervisor: Dr Dipo Dunsin

Course: Data Security, Governance and Compliance

Project submitted as part of the requirements for the  
award of MSc

## Table of Contents

|                                                                |    |
|----------------------------------------------------------------|----|
| Abstract .....                                                 | 3  |
| I. Introduction – NatureGreen Scenario .....                   | 4  |
| II. Problem Analysis .....                                     | 5  |
| A. High-Level Problems .....                                   | 5  |
| B. Dissertation on the Problems.....                           | 5  |
| III. Literature Review .....                                   | 7  |
| A. ISO/IEC 27001 and the ISO/IEC 27000 .....                   | 7  |
| B. ITIL Information Security Management .....                  | 7  |
| C. COBIT for IT Governance.....                                | 7  |
| D. NIST Cybersecurity Framework (CSF) .....                    | 8  |
| E. BYOD and Wireless Security Guidance.....                    | 8  |
| F. Data Protection Regulations and Cloud Security.....         | 8  |
| IV. Methodology .....                                          | 9  |
| V. Proposed Security Governance Framework for NatureGreen..... | 10 |
| A. Graphical View .....                                        | 10 |
| B. Governance and Policy .....                                 | 11 |
| C. Risk Management .....                                       | 11 |
| D. Compliance Management.....                                  | 12 |
| E. Technical Controls and Security Architecture.....           | 12 |
| F. Incident Response and Continuity.....                       | 14 |
| G. Awareness and Training .....                                | 14 |
| H. Monitoring and Continuous Improvement .....                 | 14 |
| VI. Discussion.....                                            | 15 |
| VII. Conclusion.....                                           | 16 |
| References.....                                                | 17 |

# Abstract

NatureGreen (NG) is a global wellness brand that relies heavily on cloud services, wireless networking and social media. Almost all its corporate network is wireless, allowing staff and even customers to use their own devices to access NG resources. The company holds valuable intellectual property and large volumes of personal data. However, there is no formal information security policy or governance structure in place. Security is a stated priority, but its implementation is ad hoc and reactive.

In this paper, I design a security governance framework tailored to NG. I begin by explaining NG's business and technology environment, then identify and decompose the key problems: absence of security governance, unmanaged bring-your-own-device (BYOD) practices, insecure wireless and cloud architectures, weak data protection for personal and intellectual property, and lack of incident response capability. I review established frameworks and standards, ISO/IEC 27001 and the broader ISO/IEC 27000 family, ITIL security management, COBIT, and the NIST Cybersecurity Framework (CSF), as well as guidance on BYOD, guest Wi-Fi, privacy regulations such as the GDPR, and cloud security best practices [1] [2] [3] [4].

Using these models, I adopt a design-science methodology to construct a practical framework consisting of seven domains: (1) Governance and Policy, (2) Risk Management, (3) Compliance Management, (4) Technical Controls and Security Architecture, (5) Incident Response and Continuity, (6) Awareness and Training, and (7) Monitoring and Continuous Improvement.

The proposed framework converts NG's fragmented practices into a coherent, risk-based information security management system aligned with international best practice. It enables NG to protect personal data and intellectual property, meet regulatory obligations, and support business growth while maintaining an agile and innovative environment.

# I. Introduction - NatureGreen Scenario

During my examination of NatureGreen (NG), I observed that it is a company that has invested heavily in digital innovation but has given very little attention to structured information security. NG sells wellness products worldwide and promotes a healthy lifestyle brand. Its operations depend on several modern technologies:

- **Cloud services** deliver IT services to staff and host business applications and data, enabling seamless access and management.
- **A massive online and social media presence** is being used for marketing and customer engagement.
- **An almost fully wireless internal network** supports staff mobility across offices and sites.
- **Bring Your Own Device (BYOD)** is a widely accepted practice. Staff, contractors and even customers are encouraged to use their personal smartphones, tablets or laptops to access NG's network and services.

These characteristics give NG agility and a competitive customer experience. However, the case scenario makes clear that *everything is in disarray*. There is no established information security policy, no formal governance structure, and no consistent approach to managing risk. Security is considered necessary, but it competes with business pressure to maximise accessibility and convenience.

At the same time, NG holds two categories of highly sensitive assets:

1. **Personal Data:** NG holds personal data of its staff and customers across multiple platforms. That is a serious issue related to data protection. That falls under the data protection laws of the EU's General Data Protection Regulation (GDPR) [3].
2. **Intellectual Property (IP):** Their product formulas, research data, ingredient extraction, preparation of raw materials, market analysis, marketing plans, and business strategies all carry the potential value of billions of dollars.

The company is under increasing pressure from regulators and customers to demonstrate that these assets are adequately protected. Any serious breach could result in regulatory fines, lawsuits, reputational damage and competitive loss.

This situation motivated me to design a comprehensive security governance framework for NG.

## II. Problem Analysis

### A. High-Level Problems

From the scenario, I identified five problems:

1. **Lack of information security governance and policy.** There is no formal information security management system, no clear roles and responsibilities, and no approved security policies. Decisions are ad hoc and undocumented.
2. **Uncontrolled BYOD and pervasive personal device access.** Staff and customers connect personal devices directly to NG's wireless network and cloud services with almost no technical or procedural control.
3. **Insecure wireless and network architecture.** With 95% of the network wireless, any weaknesses in Wi-Fi configuration or segmentation could allow attackers to pivot into core systems.
4. **Weak data protection for personal data and IP.** Personal information and trade secrets are stored and processed without a coherent data classification scheme, access control model or encryption strategy.
5. **No structured incident response or continuity capability.** If a breach or outage occurs, NG lacks defined processes, teams or tested plans to respond, communicate and recover.

### B. Dissertation on the Problems

I identified the key reasons or sectors that contribute to these problems and what the gap is.

1. **Governance gaps**
  - No information security steering committee or accountable executive.
  - No formally approved information security policy.
  - No policy framework (BYOD, acceptable use, data handling, cloud, social media).
2. **Risk and compliance gaps**
  - No formal risk assessment process.
  - Lack of visibility of key risks (BYOD, cloud misconfiguration, social engineering).
  - Unclear understanding of obligations under GDPR and other privacy laws.
3. **Technology and architecture weaknesses**
  - Single flat wireless network for staff and guests.

- No network segmentation is in place to protect critical systems or IP repositories.
- Absence of centralised identity and access management and multifactor authentication.
- Lack of endpoint protection, patch management and device encryption on BYOD devices.
- Cloud resources are configured on a "best effort" basis by IT staff without reference to standards.

#### **4. Operational and organisational issues**

- No documented incident response plan or security incident response team.
- No formal backup and no disaster recovery plans to test against realistic scenarios.
- Limited security awareness among staff, and no regular training or phishing simulation.

#### **5. Lack of monitoring and improvement**

- No central logging or Security Information and Event Management (SIEM) capability.
- No security metrics or key performance indicators.
- No regular internal security audits or management reviews.

### III. Literature Review

After identifying the problems and the key reasons behind them, I aim to resolve the issues for NG. To address this, we need to develop a robust security framework for the company. In designing the security framework, I tried to build it on mature and established security frameworks that are already well accepted globally.

#### A. ISO/IEC 27001 and the ISO/IEC 27000

ISO/IEC 27001 defines requirements for an Information Security Management System (ISMS) built around a Plan–Do–Check–Act (PDCA) cycle [5]. It requires organisations to define their scope, perform risk assessments and treatments, implement controls (referencing ISO/IEC 27002), monitor effectiveness, and continually improve. The standard explicitly mandates top management commitment, information security policy, defined roles and responsibilities, and regular internal audits and management reviews [5].

For NG, ISO/IEC 27001 offers a comprehensive blueprint for governance, risk management and control selection. Additional members of the ISO/IEC 27000 family provide more specific guidance, including ISO/IEC 27017 for cloud security, ISO/IEC 27018 for the protection of personal data in cloud environments, and ISO/IEC 27005 for risk management. Recent revisions also include explicit controls on user endpoint devices and BYOD, which are central to NG's challenges [5].

#### B. ITIL Information Security Management

The IT Infrastructure Library (ITIL) is a best-practice framework for IT service management. Its Information Security Management practice aims to ensure confidentiality, integrity and availability of information in cooperation with business and IT service management [1]. ITIL emphasises integrating security into incident, change and configuration management processes and explicitly aligns its security management practice with ISO/IEC 27001 [1].

For NG, ITIL provides process-oriented guidance for embedding security into day-to-day IT operations and improving incident and change management areas where the case scenario shows apparent weaknesses.

#### C. COBIT for IT Governance

COBIT is a framework developed by ISACA for the governance and management of enterprise IT. COBIT 5 and COBIT 2019 define principles such as "meeting stakeholder needs," "covering the enterprise end-to-end," and "separating governance from management" [4]. COBIT positions information security as part of overall IT governance, linking security objectives to business goals and risk appetite, and explicitly integrates with ISO/IEC 27001 and ITIL [4].

For NG, COBIT informs the design of a security governance structure, including an executive-level committee, defined decision-making processes, and a set of governance objectives that align security with corporate strategy, rather than treating it as a purely technical concern.

## D. NIST Cybersecurity Framework (CSF)

The NIST CSF provides a risk-based approach organised around five core functions: Identify, Protect, Detect, Respond and Recover [6]. Each function contains categories and subcategories of desired outcomes, mapped to existing standards such as ISO/IEC 27001 and NIST Special Publication 800-53. The CSF is widely accepted because it is flexible, technology-neutral and explicitly designed to connect cybersecurity activities with business [6].

For NG, the CSF provides a simple yet powerful lens that ensures the framework maintains balance across the identification of assets and risks, preventive controls, detection, incident response, and recovery.

## E. BYOD and Wireless Security Guidance

BYOD and central Wi-Fi are the focus of NG's scenario. Research and vendor whitepapers highlight key BYOD risks, including data leakage from lost or stolen devices, malware from unthoroughly examined apps, insecure public Wi-Fi, weak or reused passwords, and compliance issues when regulated data is stored on personal devices [7]. Recommended controls include mobile device management (MDM), device encryption, strong authentication, containerisation of corporate data, and virtual private networks (VPNs) [7].

For guest and staff Wi-Fi, best practices include segmenting guest networks from corporate networks, enforcing WPA2-Enterprise or WPA3 encryption, utilising captive portals with acceptable-use terms, and monitoring for rogue access points [8]. These practices are highly relevant to NG's essentially wireless infrastructure.

## F. Data Protection Regulations and Cloud Security

The GDPR requires organisations to implement "appropriate technical and organisational measures" to ensure the security of personal data, considering risks and state-of-the-art controls [3]. It also mandates breach notification within strict timelines and emphasises accountability and documentation of processing activities [3]. Similar requirements are also found in other privacy laws worldwide.

Cloud security best-practice documents summarise how ISO/IEC 27017, NIST SP 800-53, and frameworks like the Cloud Security Alliance Cloud Controls Matrix can guide the secure configuration of cloud environments and clarify the shared-responsibility model between the cloud provider and customer [2].

Together, these models and regulations gave me a toolbox of concepts and controls to address the problem chunks identified for NG. In the next section, I explain how I used them to design a tailored framework.

## IV. Methodology

I followed a design-science methodology to move from NG's scenario to a concrete security governance framework.

1. **Context and requirement analysis:** By re-reading the case scenario and mapping all business activities, assets, technologies and pain points. From this, I derived the set of problem chunks described in Section II.
2. **Framework mapping:** For each problem, I identified which external frameworks or standards provided a relevant solution. For example, ISO/IEC 27001 and NIST CSF address governance and risk, while BYOD guidance addresses endpoint controls. Wi-Fi best practices address network architecture, and GDPR and cloud standards address data protection and privacy obligations.
3. **Domain definition:** I grouped related controls and processes into a small number of logical domains that would be understandable to NG's management: governance and policy, risk management, compliance, technical controls and architecture, incident response and continuity, awareness, and monitoring and improvement.
4. **Iterative design:** For each domain, I proposed objectives, roles and key activities, checking that every problem is covered by at least one domain. The design is to minimise overlap and keep the framework practical for NG's current maturity level.
5. **Conceptual diagram:** I've attached a diagram (Fig. 1), which illustrates how the domains interact and how external standards are mapped onto them. This visual model helped me validate that the framework formed a coherent whole.
6. **Critical reflection:** Ultimately, I considered the implementation challenges and the need for continuous updates to policies and controls in light of emerging threats and regulatory changes. This informed the monitoring and improvement domain, as well as the emphasis on management review.

## V. Proposed Security Governance Framework for NatureGreen

### A. Graphical View

Fig. 1 illustrates the framework I propose for NG. At the centre is a governance and policy layer mainly based on ISO/IEC 27001 and COBIT. Around it are six operational domains—risk management, compliance, technical controls and architecture, incident response and continuity, awareness and training, and monitoring and improvement—aligned with NIST CSF functions (Identify, Protect, Detect, Respond, Recover) [5] [4] [6].

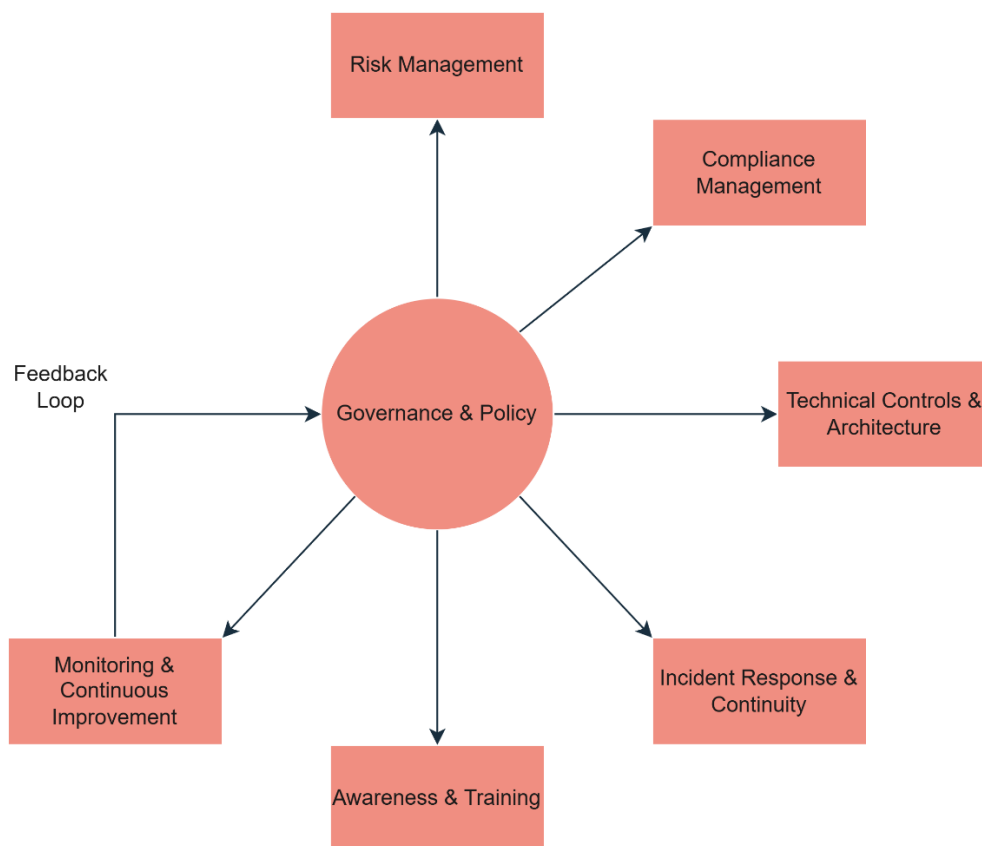


**Fig. 1. High-level security governance framework for NG.**

A circular model with *Governance & Policy* at the core. Surrounding it are six segments: *Risk Management*, *Compliance Management*, *Technical Controls & Architecture*, *Incident Response & Continuity*, *Awareness & Training* and *Monitoring & Continuous Improvement*. Arrows show governance feeding each segment; monitoring feeds back to governance, forming a continuous improvement loop. ISO/IEC 27001 and ITIL influence governance, risk and operations; COBIT shapes governance; NIST CSF aligns the outer functions.

Below, I describe each domain from my perspective and show how it addresses specific NG problems.

## B. Governance and Policy

To establish a robust information security governance framework for NG

- I propose an **Information Security Steering Committee**, chaired by a senior executive (ideally a CISO or CIO), and comprising representatives from IT, Legal, HR, and key business units. This body approves policies, sets risk appetite and monitors performance, following COBIT principles for enterprise IT governance [4].
- I drafted a top-level **Information Security Policy** aligned with ISO/IEC 27001 [5]. It defines scope (encompassing all NG sites, systems, and data), core principles (including confidentiality, integrity, and availability), and responsibilities for management, system owners, and users.
- Under this umbrella, I create specific policies and standards:
  - **BYOD Policy** specifying allowed devices, mandatory controls (device lock, encryption, MDM enrolment), corporate rights (remote wipe of corporate data), and prohibited actions (storing classified IP in personal cloud accounts) [7].
  - **Acceptable Use Policy** covering the use of NG networks, the internet and email.
  - **Data Classification and Handling Policy** define categories (Public, Internal, Confidential, and Highly Confidential) and outlines the required safeguards (e.g., encryption, restricted access) for each.
  - **Access Control Policy** that enforces least privilege, role-based access, and multifactor authentication for sensitive systems.
  - **Cloud Security Policy** requires the use of approved cloud providers, secure configurations, and compliance with relevant standards, including ISO/IEC 27017 and 27018 [2].
  - **Social Media Policy** limiting what staff may share online about NG and mandating security on corporate social media accounts.

These governance measures directly tackle NG's lack of policy and clarify expectations for every stakeholder.

## C. Risk Management

To transition from intuition to evidence-based decisions, I introduce a formal risk management process that aligns with ISO/IEC 27005 and the NIST CSF's *Identify* function [5] [6].

- I lead a **risk assessment** that inventories NG's assets (customer databases, R&D repositories, e-commerce platforms, cloud workloads, wireless infrastructure), identifies threats and vulnerabilities, and estimates likelihood and impact.

- I document results in a **risk register**, assigning owners and treatment options (mitigate, accept, transfer, avoid) to each risk. For example, the risk "personal data breach via lost BYOD device" is mitigated by MDM, encryption and incident response procedures [7].
- I develop a **risk treatment plan** prioritising high-impact issues such as BYOD, guest Wi-Fi and cloud misconfiguration, and recommend projects (Implementing MDM, network segmentation, and SIEM) with timelines and budgets.
- I ensure the steering committee reviews the risk register regularly so that risk appetite and resource allocation remain aligned.

This structured approach turns NG's vague concern about "security" into a manageable portfolio of risks with clear actions and owners.

## D. Compliance Management

Given NG's global footprint and large volumes of personal data, compliance is a dedicated area of focus.

- I compile a **compliance inventory** that lists relevant regulations and standards, including the GDPR and other national privacy laws, consumer protection laws, payment card standards (such as PCI DSS, if applicable), and contractual security requirements from partners.
- I recommend appointing a **Data Protection Officer (DPO)** or a privacy officer to oversee GDPR compliance, maintain records of processing, and coordinate responses to data subject requests [3].
- Together with Legal, I map **legal obligations to controls** in our framework. For example, the GDPR's requirement for "appropriate technical and organisational measures" corresponds to encryption, access control, logging, and incident response controls; breach-notification obligations align with specific steps in the incident response plan [3].
- I establish processes to assess **third-party risk**, ensuring cloud and service providers meet required security and privacy standards, ideally evidenced by ISO/IEC 27001 or SOC 2 reports [2].

By integrating compliance into governance rather than treating it as an afterthought, NG can demonstrate due diligence to regulators and partners while reducing legal risk.

## E. Technical Controls and Security Architecture

This domain converts policies and risk decisions into concrete protections. I divide it into four sub-areas.

### 1. Network and Wireless Security

- I redesigned NG's network to enforce **segmentation**, creating a separate guest Wi-Fi network for customers and visitors that is isolated from internal systems, as well as additional VLANs for highly sensitive systems, such as R&D and finance [8].
- I enforce **WPA2-Enterprise or WPA3** on staff networks, using individual credentials and 802.1X authentication [8].
- Perimeter and internal **firewalls** enforce "deny by default" rules, while **IDS/IPS** and, where feasible, a **web application firewall** monitor and block suspicious traffic.
- A **VPN** with multifactor authentication secures remote access, especially from BYOD devices.

## 2. Endpoint and BYOD Security

- I deploy a **Mobile Device Management (MDM)** solution and require enrolment of any device accessing NG email or internal applications. Policies enforce device encryption, lock-screen PINs or biometrics, basic antivirus and OS version requirements [7].
- Company-owned laptops and desktops are protected by **endpoint detection and response (EDR)** tools, full-disk encryption and centralised **patch management**.
- I restrict or monitor the use of **removable media** and personal cloud storage for sensitive data, where feasible, using data loss prevention (DLP) tools.

## 3. Application and Data Security

- I introduce a **data classification scheme** operationalised through access controls, DLP and encryption. Highly Confidential IP and personal data receive the strongest controls.
- I work with development teams to embed **secure SDLC** practices, including code reviews, static analysis, and regular penetration testing.
- All critical applications and APIs are fronted by **TLS encryption** with strong ciphersuites, and sensitive data at rest is encrypted in databases and file systems.

## 4. Cloud Security

- I implement **secure configuration baselines** for cloud platforms guided by cloud security benchmarks and ISO/IEC 27017 [2].
- Logging and monitoring (CloudTrail-equivalent services) are enabled for all cloud accounts, feeding into a central monitoring system.

- I consider using **cloud security posture management (CSPM)** tools to continuously scan for misconfigurations such as open storage buckets [2].

These controls drastically reduce NG's attack surface and directly address the BYOD, wireless, IP and cloud risks highlighted in the scenario.

## F. Incident Response and Continuity

Assuming incidents *will* occur, I define how NG will respond:

- I developed a **Security Incident Response Plan** based on NIST guidance, which includes stages for preparation, detection, analysis, containment, eradication, recovery, and lessons learned. The plan defines escalation paths, internal and external communication, and regulatory breach-notification steps, all of which are aligned with the GDPR [6] [3].
- I form a **Security Incident Response Team (SIRT)** comprising IT, information security, legal, HR and communications. I recommend periodic tabletop exercises and technical drills to keep this team ready.
- In parallel, I work with business continuity managers to create **Business Continuity and Disaster Recovery (BC/DR)** plans. These include a business impact analysis, recovery time objectives (RTOs), backup strategies, and regular recovery testing.

With these capabilities, NG can limit the damage from breaches or outages and quickly restore critical services.

## G. Awareness and Training

Technology alone cannot protect NG; people must be part of the defence.

- I design a **security awareness programme** that all staff must complete annually. Modules cover phishing, password hygiene, safe use of BYOD devices, incident reporting, and data-handling rules.
- I run **phishing simulations** to reinforce training and measure resilience.
- I provide targeted training for administrators and developers on secure configuration and secure coding.

This domain addresses human-factor risks, including phishing, accidental data leaks, and policy non-compliance.

## H. Monitoring and Continuous Improvement

Finally, I embed mechanisms to keep the programme alive and evolving:

- I implement central **logging and Security Information and Event Management (SIEM)** to collect events from firewalls, endpoints, servers and cloud platforms.

- I define **key performance indicators** (patch compliance rates, incident numbers, time to detect and contain incidents, and training completion rates) and report them to the steering committee.
- I schedule **internal audits** and management reviews at least annually, in line with ISO/IEC 27001's PDCA cycle [5]. The findings inform an updated security roadmap.
- I monitor changes in threats and regulations and update policies and controls accordingly. This directly satisfies the requirement to show why it is good practice to keep rules and standards up to date. Without continuous improvement, NG's controls would quickly lag behind evolving attack techniques and new legal expectations [5] [6] [3].

## VI. Discussion

The framework I have proposed transforms NG's security posture from a fragmented and reactive one to a structured and risk-based one. Importantly, it does so without simply banning the practices that give NG business agility. I do not prohibit BYOD or guest Wi-Fi; instead, I regulate them through policy, MDM and network segmentation [7] [8]. Staff still enjoy flexibility, but under clear conditions that protect NG's assets.

Aligning with ISO/IEC 27001, ITIL, COBIT, and NIST CSF ensures the framework is recognisable to auditors, partners, and regulators [5] [1] [4] [6]. NG could later formalise this alignment with external certification (ISO/IEC 27001) if desired.

Implementation will require investment and change management. Some staff members may resist using MDM on personal devices or complain about the need for stronger authentication. To address that, I must communicate the business reasons: protecting customer trust, avoiding fines, and safeguarding jobs that depend on NG's reputation. Senior management sponsorship, facilitated through the steering committee, is critical.

The continuous improvement loop is essential. Threat actors constantly evolve, and standards are periodically revised to incorporate new lessons [5] [6]; regulations like GDPR are sharpened by enforcement actions and guidance [3]. By institutionalising management review, risk reassessment and policy updates, NG avoids treating security as a one-off project and instead manages it as an ongoing capability.

## VII. Conclusion

From my analysis of the NatureGreen scenario, it was clear that the company had not established a mature information security governance framework to accompany its rapid digital growth. Uncontrolled BYOD, pervasive wireless access, heavy reliance on cloud services, and the absence of formal policies left NG exposed to data breaches, IP theft, regulatory penalties, and operational disruption.

In this paper, I explain NG's environment, identify and decompose the key problems, review relevant frameworks and standards, and design a tailored security governance framework. The framework's seven domains, governance and policy, risk management, compliance management, technical controls and architecture, incident response and continuity, awareness and training, and monitoring and continuous improvement jointly address NG's challenges while remaining aligned with ISO/IEC 27001, ITIL, COBIT and NIST CSF [5] [1] [4] [6].

If NG implements this framework, it will move from informal, fragmented practices to a coherent ISMS with clear accountability, consistent policies, risk-based control selection and continuous oversight. Personal data and intellectual property will be significantly better protected, regulatory compliance will be demonstrable, and the company will be able to respond confidently to security incidents. Just as importantly, the framework is designed to evolve, ensuring that as NG grows and as threats and regulations change, its security posture keeps pace.

From my perspective as the practitioner who designed it, this framework is not merely a theoretical model but a practical roadmap that NG can follow step by step to embed information security into its culture and operations, supporting long-term business success.

## References

- [1] AXELOS, ITIL Foundation: ITIL 4 Edition, London: The Stationery Office (TSO), 2019.
- [2] Check Point Software Technologies Ltd., “Cloud Security Standards You Need to Implement,” Check Point, 2023. [Online]. Available: <https://www.checkpoint.com/>. [Accessed 25 11 2025].
- [3] European Union, “Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (General Data Protection Regulation),” Official Journal of the European Union, Brussels, 2016.
- [4] ISACA, COBIT 2019 Framework: Introduction and Methodology, Schaumburg, IL: ISACA, 2018.
- [5] International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC), “Information security, cybersecurity and privacy protection — Information security management systems — Requirements,” ISO, Geneva, 2022.
- [6] National Institute of Standards and Technology (NIST), “Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1,” NIST, Gaithersburg, MD, 2018.
- [7] SentinelOne, “BYOD Security Risks: How to Protect Your Organization,” 2024. [Online]. Available: <https://www.sentinelone.com/>. [Accessed 2 12 2025].
- [8] Cisco Systems, Inc, “Best Practices for Guest Wi-Fi Security,” Cisco, 2024. [Online]. Available: <https://www.cisco.com/>. [Accessed 1 12 2025].