

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

Module code: ACCA7028

Module: Data Security, Governance and Compliance

Lecturer: Dr. Dipo Dunsin

Submitted by-

Ziaur Rahman Ramim

ID- 2503796

Abstract

The current digitised and interconnected business world is more prone to the use of cloud computing, wireless networks, and the use of BYOD, which raises the threat surface dramatically in the context of cybersecurity and strongly favours the use of these three factors. This report discusses the impact of data security, governance, and compliance infrastructure that has been established on the mitigation of information security risk to a global wellness organisation, NatureGreen (NG). The paper examines the major international standards and frameworks, such as those of ISO/IEC 27001:2022, the NIST Cybersecurity Framework (CSF), COBIT 2020, ITIL 4, and ISO 31000:2021, illustrating that they are relevant to the management of information security, enterprise risk, and IT governance. Based on this discussion, the following report outlines a specific security, governance, and compliance strategy at NatureGreen that is going to embrace strategic security governance, risk management, BYOD and wireless security rules, technical security mechanisms, operational security policies, contingency planning, data governance, and third-party security by using service level agreements. In addition, the report critically appraises the significance of constantly revising regulations and standards in reacting to changing cyber threats, actual security incidents that may occur in real scenarios, and balance between innovation and compliance. The results show that a framework-based approach to integrating an organisation can help them become more resilient, safeguard sensitive data, handle regulatory compliance, and facilitate sustainable digital development, such as NatureGreen.

Table of Contents

Abstract	2
Introduction.....	4
1. Security Frameworks and Models Relevant to NG	5
1.1 - ISO/IEC 27001:2022 Information security management system (ISMS).....	5
1.2 NIST Cybersecurity Framework (CSF).	6
1.3 COBIT 2020 Governance of Enterprise IT.....	7
1.4 ITIL 4 - Management of IT Services with Inbuilt Security.	7
1.5 ISO 31000: 2021 - Enterprise Risk Management.	8
1.6 Summary of Frameworks.....	8
2(a) Tailored Security, Governance and Compliance Approach for NatureGreen.....	9
2(a) 1 Security Governance and Strategic Planning.	9
2(a) 2 BYOD and Wireless Wireless, Security Policies.	10
2(a) 3 Risk Management Process.....	11
2(a) 4 Protection Mechanisms and Technical control.....	12
2(a) 5 Security Administrative Frameworks and Practise.	13
2(a) 6 Contingency Planning and Business continuity.	13
2(a) 7 Compliance, Laws, Ethics and Data Governance.	14
2(a) 8. Service Level Agreements (SLAs) and Third-Party Management.....	14
2(a) 9. Critique of Security, Governance, and Compliance Frameworks.....	15
2(b). Why Constantly Updating Regulations and Standards Is Good Practice.....	17
2(b).1 Adapting to an Evolving Threat Landscape	17
2(b).2 Learning by Real-life cases and Sealing loopholes.....	18
2(b).3 Innovation, Compliance and Business Value Balancing.	18
Conclusion	19
References.....	20

Introduction

In the case of a global wellness brand like the NatureGreen (NG) that utilises the cloud services to a considerable extent, to use wireless network and a massive online presence. To mitigate this, organisations normally depend on established security framework and models like ISO/IEC 27001, the NIST Cybersecurity Framework (CSF), COBIT 2020, ITIL 4 and ISO31000 in managing risks. These models offer systematic support of how information security can be managed, aligned with the business strategy, and comply with the laws and regulations [10]; [13]; [8]. The report begins by tracking most important frameworks and models applicable to NG with the help of a table and conceptual figures. After that, it suggests a customised strategy in the security, governance, and compliance of NG (risk management, policies, protection mechanisms, contingency planning, and service level agreements). Lastly, it criticises and explains why regular revision of regulations and standards is a good practise in the ever-changing threat environment.



Figure: NatureGreen [13].

1. Security Frameworks and Models Relevant to NG

1.1 - ISO/IEC 27001:2022 Information security management system (ISMS).

ISO/IEC 27001:2022 is the most popular international standard of setting up, applying, sustaining and continuously enhancing an Information Security Management System (ISMS) [10]. Using this cycle, NG can evolve an ad-hoc state to a mature, documented, and audit-trainable, international best practise security state [15]; [10].

The standard is risk-based: organisations should first identify and evaluate information security risks and impose the relevant controls in Annex A that is composed of 93 controls that are categorised using the organisational, people, physical and technological themes (PacificCert, 2023). PDCA based cycle (Plan-Do-Cheque-Act) within ISO 27001 allows making sure that security is a project instead of a project [10].



Figure 1- ISO 27001 ISMS cycle of NG. [10].

- **Plan:** Scopes (global, wireless, BYOD, cloud): define, risk danger, risk treatment strategy.
- **Do:** Introduction of policies, technical controls, awareness and training.
- **Cheque:** Measure, monitor performance, internal audit.
- **Act:** Proper measures and constant developing of controls and policies.

1.2 NIST Cybersecurity Framework (CSF).

NIST CSF is a highly used voluntary model that structures the cybersecurity activity into five fundamental functions, namely: Identify, Protect, Detect, Respond, and Recover [13]. In the case of NG, the NIST CSF provides a viable road map on how it is technical and procedural controls can be implemented in its wireless, cloud and BYOD environments. The Identify function is used to motivate NG to obtain a clear vision of its assets, business environment and risks, and what systems its staff data, customer data, and IP [5]. The other most important functions are the Respond and Recover, which can be used to help NG manage incidents, communicate with stakeholders and restore normal operations in the most effective way possible [13].

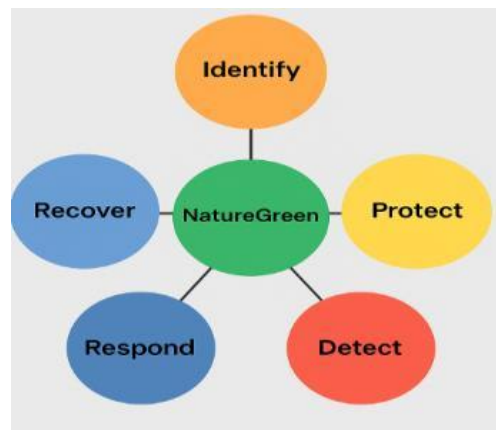


Figure 2: Map of NIST CSF functionality to NatureGreen [8]

- **Identify:** asset (corporate resources, personal devices, cloud resources: services) inventory, classification of inventory data, regulation mapping.
- **Protect:** Privilege and access administration (IAM), network division, encrypted, security conscious.
- **Detect:** Intrusion detection systems, Log monitoring, security Information and event management (SIEM).
- **Respond:** Playbooks and escalation paths, plans of incident response that are captured.
- **Recover:** Verified backup and recovery featured plans, connections with consumers and control.

1.3 COBIT 2020 Governance of Enterprise IT.

The COBIT 2020 is an enterprise IT governance structure and management framework that concentrates on value creation, risk optimisation and resource optimisation [8]. Instead of identifying technical controls, COBIT outlines governance objectives- Evaluate, Direct, Monitor (EDM) and management objectives in areas which include; Align, Plan and Organise (APO), Build, Acquire and Implement (BAI) and Deliver, Service and Support (DSS).

In the case of NG, COBIT 2020 assists in making sure that the security decisions are in line with the overall business strategy, stakeholder requirements and regulatory demands [8]. This would guarantee that security investments are in line with the objectives of NG to secure the IP, keep customers trustful and develop safe-growth in digital channels [8].

1.4 ITIL 4 - Management of IT Services with Inbuilt Security.

The recent development of the IT Infrastructure Library is ITIL 4 that offers a complete framework of IT service management [3]. To NG, where IT services, including cloud platforms, e-commerce, and internal collaboration tools, play a fundamental role, ITIL 4 will assist in integrating security throughout the lifecycle of the services [16].



Figure 3: The integration of the service value chain of ITIL 4 and security [3].

Some of the critical practises of ITIL 4 are information security management, change enablement, incident management, service continuity management and service level management [3]. The continuity of incidents and service services are directly related to contingency planning and recovery of critical systems owned by NG [3]; [16].

- Plan: Security requirements were in line with business strategy.
- Design & Transition: Principles of secure by design of new services (e.g. new customer portals or mobile apps).
- Obtain/Build: Security testing, reviewing of them, configuration management.
- Deliver and Support: Monitoring of system operation, incident response and SLA report [3].

1.5 ISO 31000: 2021 - Enterprise Risk Management.

The ISO 31000:2021 offers the principles and guidelines of the risk management applicable to any organisation [9]. In the case of NG, ISO 31000 can be used to support enterprise risk management as well as the enterprise risk-of-information secure assessment measures mandated by the ISO 27001 [15]. The standard reiterates that, risk management must create and protect value; it must be part of organisational processes and complied with organisational context [9]. The framework also makes organisations view human and cultural issues which is an important requirement in any BYOD environment where employee behaviour makes a big difference when it comes to security [12]. Using the ISO 31000, NG can establish clear risk criteria and risk appetite as well as risk tolerance and this helps in making wise decisions on the risks to accept, transfer or treat [15].

1.6 Summary of Frameworks

Framework	Main Focus	Relevance to NG
ISO/IEC 27001:2022	ISMS - policies, controls, certification	Backbone information security and policy framework.
NIST CSF	Cybersecurity operations and results	Wireless, cloud, and BYOD security operational roadmap.
COBIT 2020	Enterprise IT governance and management	Enterprises Governance Optimises security and risk and performance.
ITIL 4	IT service management	Integrates security in service lifecycle and operations.
ISO 31000:2021	Enterprise risk management	Systematised approach to risk assessment and treatment.

2(a) Tailored Security, Governance and Compliance Approach for NatureGreen

2(a) 1 Security Governance and Strategic Planning.

NG must also have an Information Security Governance Board with the corporate board reporting to it and a Chief Information Security Officer (CISO) or other executive heading it [8]. This type of governance is indicative of the principles of COBIT 2020, which include explicit roles, communication and responsibility towards the needs of the stakeholders [8]. The board must specify risk appetite on cyber and privacy risks commit security strategies and track performance on dashboards and such key indicators [17].

Risk registers, incident reports, findings of audits and updates on compliance would be discussed regularly by the governors who should make sure that the security posture of NG is up-to-date. The process of strategic planning combined with embedding security enables NG to focus on controls that will provide the highest possible risk reduction and business rewards [8]; [9].

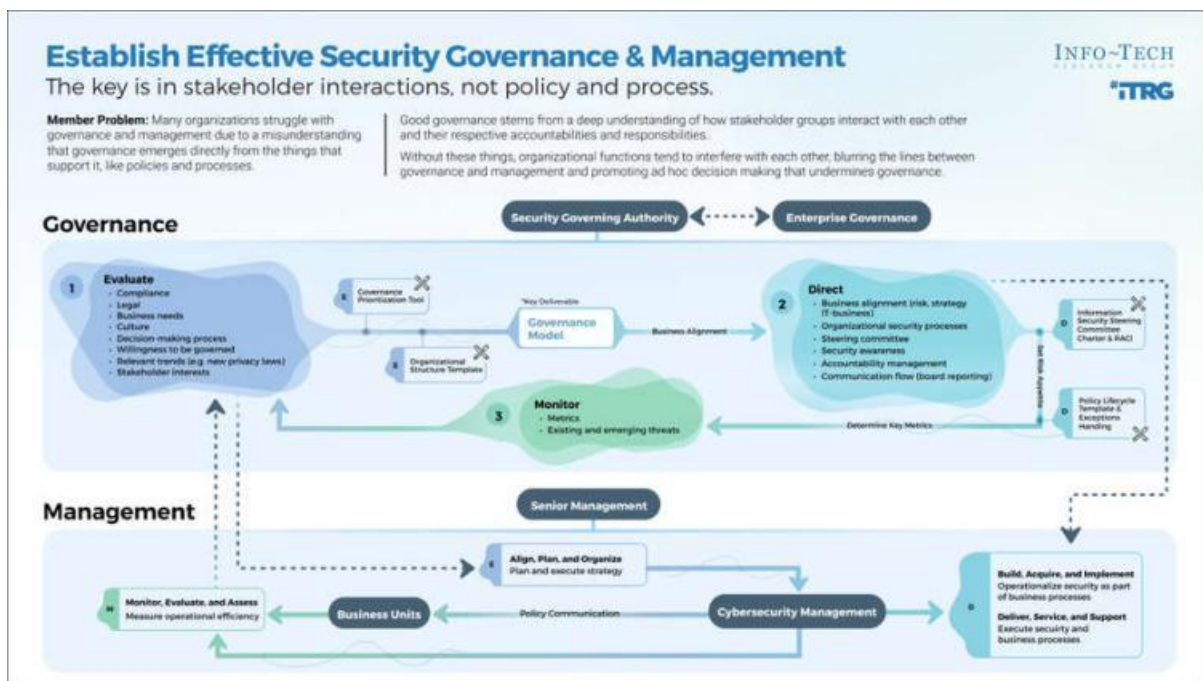


Figure: Security Governance and Strategic Planning [12].

2(a) 2 BYOD and Wireless Wireless, Security Policies.

To overcome the current state of disarray, NG needs to establish the entire security policy system based on ISO 27001. Such policies are information security, access control, acceptable use, BYOD/mobile devices, password and authentication, cloud usage, incident management, data classification and social media use [10].

According to the research, effective policies, along with training and technical implementation, are essential to the BYOD security [12]; [11]. NG must have a documented BYOD policy involving registering devices, Mobile device management (MDM) or Unified Endpoint Management (UEM), enforced encryption, screen-lock policies and capability to erase corporate data containers [2]. This shall require discriminative Wi-Fi standards (e.g. WPA3), staff, guest, and IoT device network segmentation, periodic rogue access point scanning, and powerful authentication tools [1]; [12].

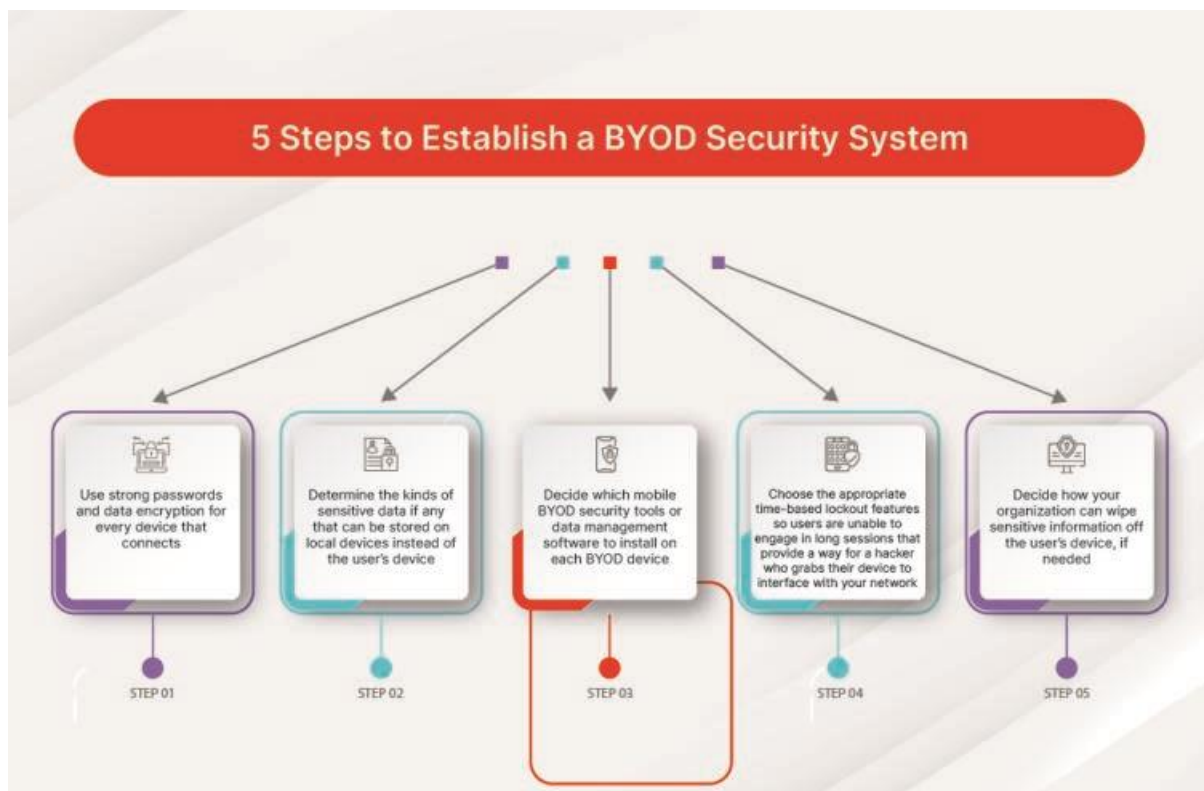


Figure: BYOD [12].

2(a) 3 Risk Management Process

The risk management approach of NG is expected to adhere to ISO 31000 that is included in the ISO 27001 ISMS [9]. Second, NG must organise the risk identification workshops in which the list of threats (e.g. phishing, ransomware, insider misuse and misconfigured cloud services), vulnerabilities (e.g. weak authentication, outdated devices, poor Wi-Fi segmentation) and potential effects on confidentiality, integrity and availability should be enumerated [15]. Qualitative/semi-quantitative matrix can then be used to analyse and evaluate risks.

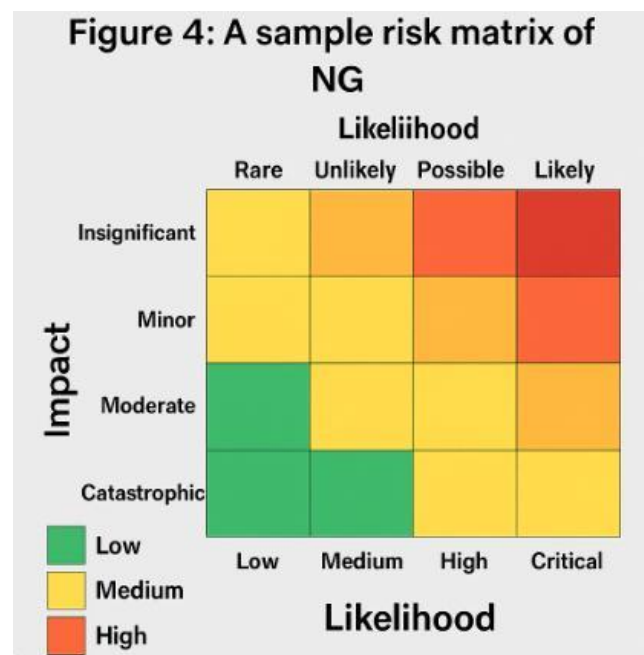


Figure 4: A sample risk matrix of NG [10].

- X-axis Likelihood (Rare, Unlikely, Possible, Likely, Almost Certain).
- Y-axis Impact (Insensitive, Latent, Trigger, Disastrous, Disastrous).
- Colour bands Low (green), Medium (yellow), High (orange), Critical (red).

The high and critical risks, including the unauthorised access of customer data on the cloud storage or the IP theft through the compromised laptops, etc., should be prioritised and treated with controls mentioned in ISO 27001 Annex A and in the NIST CSF [13]; [10].

2(a) 4 Protection Mechanisms and Technical control.

Protective measures that could be considered essential to NG are:

Identity and Access Management (IAM): Role-based access control (RBAC), the tenets of least-privilege, the strong multi-factor authentication of employees and administrators (MFA), and systematic S-O); Access reviews [10].

Endpoints and Mobile Security: MDM/UEM platform to apply encryption, patching, security constructs on the corporate and personal devices; to separate corporate and personal data using secure containers; to have anti-malware and host-firewall on the endpoints [2].

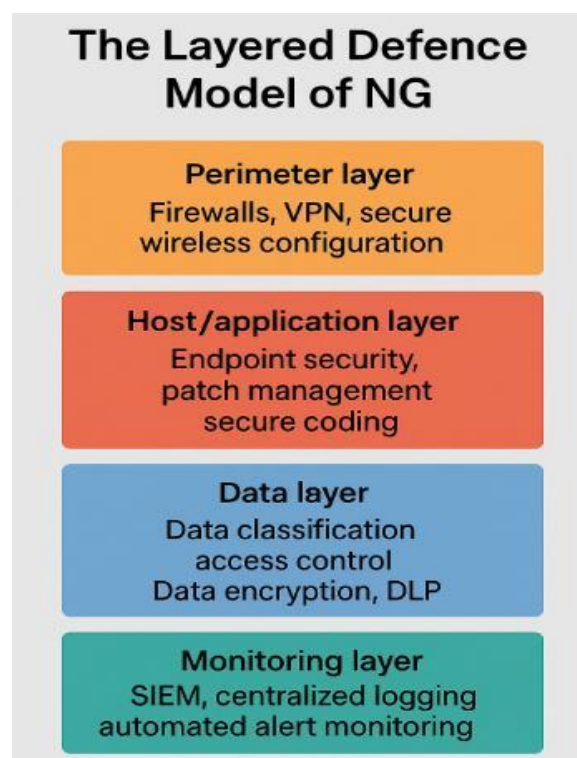


Figure 5: The layered defence model of NG [10].

Network Protection: Separated wireless networks, firewalls, intrusion defence and prevention apparatus (IDPS) and secure VPNs to access in remote locations. Strong(s) encryption and authentication tools must be utilised in wireless networks and misconfiguration must be periodically assessed [13].

Cloud Security: Economic configuration base, data transmission and rest encryption, monitoring cloud customer, and, when necessary, a Cloud Access Security Broker (CASB) to institute policies concerning SaaS applications [17].

Data Loss Prevention (DLP): Data loss prevention tools are used to track and regulate the flow of personal information and intellectual property like customer PII and IP over email, cloud storage, and endpoints to minimise accidental and intentional data leaks [4].

- Perimeter layer Firewalls, VPN, and secure wireless configuration.
- Host/ application layer Endpoint security, patch management, secure coding
- Monitoring layer: SIEM, centralised logging, automatized monitoring of alerts.
- Data layer Data classification, access control, Data encryption, DLP.

This set of controls facilitates confidentiality, integrity, and accessibility of the critical data assets of NG as per the ISO 27001 and NIST CSF recommended guidelines [13]; [10].

2(a) 5 Security Administrative Frameworks and Practise.

Security needs to be operationalised by way of regular routine operations and practises. ITIL 4 and ISO 27001 can be utilised by NG to organise the general activities of key operations like incident management, change enablement and continual improvement [3]; [10]. A SOC with the assistance of SIEM tools and threat intelligence enhances the efforts of the organisation to identify and react to attacks on time [17].

Security awareness and training should also take place continuously. The literature of BYODs demonstrates that both awareness and behaviour among employees are the key predictors of security [12]; [11].

2(a) 6 Contingency Planning and Business continuity.

The contingency planning will help guarantee that NG will be able to continue or bring online critical functions quickly following such events as cyber-attacks, outages or natural disasters. The service continuity management aspect of ITIL 4 as well as the Recover feature of the NIST CSF both offer advice on the disruption planning [3]; [13].

NG must also find out its essential services that most probably include e-commerce platforms, customer service systems, HR and payroll applications and repositories containing IP. In both cases, NG is supposed to formulate Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs) and develop a proper backup and recovery strategy [17].

2(a) 7 Compliance, Laws, Ethics and Data Governance.

As a global company, NG has to comply with various regulations on data protection, privacy, consumer and cybersecurity, including the EU General Data Protection Regulation (GDPR) and other laws in various countries [17]. Other than legal compliance, the focus of ethics is paramount to a health-oriented brand. The decisions of NG regarding data analytics, profiling and marketing activities should be guided by transparency, fairness, minimum amount of data collection and individual privacy respect [4]. Clear policies and defined roles (e.g. data owners and data stewards), data quality control and specifications on data access, data retention and deletion can make data governance good [5]; [8].

2(a) 8. Service Level Agreements (SLAs) and Third-Party Management

Because NG is largely dependent on the cloud-providers, and potentially other resourceful service providers, it will have to take care of the third-party risk by the way of robust contracts and SLAs. The ISO 27001 pays significant attention to the need to regulate the relationships with suppliers to be sure that the third party satisfies security needs of the organisation [10].

Cloud provider SLAs MDM and security vendor or partner should explicitly define security policies, such as encryption requirements, access control, incident notification span, logging and monitoring, data location, backup and recovery requirements and audit rights [13]; CSA, 2020). Effective third-party governance will make it less possible that the vulnerability of suppliers to interfere with the staff data, customer data or IP of NG [17].

2(a) 9. Critique of Security, Governance, and Compliance Frameworks

Cloud Security Failures and Misconfigurations

High-Profile Cloud Breaches: Independent research on cloud environments demonstrates that cloud misconfigurations continue to be one of the most common number of breaches that have caused a major percentage of cloud attacks due to poorly established access controls, exposed credentials, or unproductive storage environments [9].

Cyber Security News: These examples demonstrate that the adoption of the frameworks itself is not enough without organisations investing in the perpetual configuration management, real-time monitoring, and enforce the least privilege access - some of the key points that the NIST CSF and ISO/IEC 27001 highlight but are poorly practised by organisations [17].

Case Study- Football Australia: Plaintext keys on the site of a large federated organisation were exposed due to a cloud misconfiguration and poor control of changes which highlights the fact that human error and poor implementation of change controls can make cloud deployments susceptible to vulnerability in spite of overarching policies [10].

Data Exfiltration and Regulatory Consequences

Penalty imposed by the regulators on last pass: A security breach of password management provider LastPass, which was linked to hacked employee computers, caused sensitive user data to be stolen and a regulatory penalty of the UK Information Commissioner's Office due to the lack of sufficient security controls. Such cases prove that cloud compromise might be introduced to staff endpoints and development systems indirectly. They also put an emphasis on having strict access control, endpoint hardening, and management of privileged sessions - which are not always prioritised in the traditional risk registers [9].

Supply Chain and SaaS Platform Risks

SaaS Breaches related to salesforce: Millions of records of international brands were stolen due to large-scale information theft, which was associated with hacked Salesforce accounts. This example demonstrates how identity and API access management is being compromised by organisations due to third-party cloud applications, which are highly used by organisations [13].

Lessons and Framework Limitations.

Implementation Gaps: Frameworks provide best practises, and they are not secure in cases where organisations lack resources, expertise, or uninterrupted capability to provide them.

Human and Third-Party Risk: Most breaches are due to human error, vulnerability of suppliers or misconfigured clouds services, which need more powerful governance solutions and technological automation than the minimum requirement of compliance [5].

Evolving Threat Landscape: This is due to threat actors coming at the rapid pace of enhancement these actors are running out ahead of any change in policy, which highlights the significance of dynamically measuring risks and constant evolution of the framework.

2(b). Why Constantly Updating Regulations and Standards Is Good Practice

2(b).1 Adapting to an Evolving Threat Landscape

Significant security breaches, such as ransomware attacks or mass data breach, often demonstrate the emergence of new vulnerabilities in cloud services, supply chains and end-user devices [17]. As an illustration, the recent updates of ISO 27001 and ISO 31000 focus on risk-oriented decision-making, leadership and communication with business operations, which is a manifestation of the fact that security is not a technical process anymore [9]. Similarly, post-executive order 14028 guidance on the topic in the United States has emphasised the significance of zero-trust architectures, supply chain security and enhanced incident reporting [13]; [17].



Figure: Evolving Threat Landscape [4]

2(b).2 Learning by Real-life cases and Sealing loopholes.

Standards and regulations do not remain in their places since the incidents that happen in the real-life reveal holes in the practise being exercised now. Policymakers and standards organisations can assist organisations in methodically sealing these gaps by modifying regulatory requirements and regulators [17]; [5].

Traditional structure in the case of NG would pose a threat of forgetting key concerns namely BYOD, current wireless security, cloud misstating and sophisticated social engine assaults. The maintenance of standards will keep the security posture of the company in line with current best practise and not previous assumptions.

2(b).3 Innovation, Compliance and Business Value Balancing.

Frequently revised laws and regulations also stimulate organisations to modernise their systems and processes that may enhance efficiency and aid innovation. Effective data management and data security might facilitate reliable data analytics, enhanced customer insights and assertive digital services [4]; [8]- In the case of NG, complying with the existing standards should enable the company to form an alliance with other organisations that need strong security assurances and certifications.

Conclusion

NatureGreen has a digital and global connected business environment whereby data and networks wirelessly, cloud services and personal devices are core to the business model. This report has considered some of the important frameworks such as ISO/IEC 27001, NIST CSF, COBIT 2020, ITIL 4 and ISO 31000 and it includes how they can be interrelated into a unified security and governance model of NG. It has also given a customised strategy, which incorporates the governance set-ups, broad security policies, process of risk management, technical security protocols, operational security, contingency planning, data governance and solid SLAs with third parties. Lastly, the report has asserted that constantly revising regulations and standards is a good practise as it assists organisations to adapt to the changing threats, learn upon the actual incidences and strike the balance between innovation and compliance.

References

- [1] M. Alenezi et al., “Systematic Literature Review on Security Access Control Policies and BYOD,” *Applied Sciences*, vol. 13, no. 14, p. 8048, 2023.
- [2] A. Alshahrani, H. Al-Samarraie, and L. Moody, “Hospital Bring-Your-Own-Device (BYOD) Security Challenges and Solutions,” *JMIR mHealth and uHealth*, vol. 8, no. 6, p. e18175, 2020.
- [3] Axelos, ITIL® Foundation: ITIL 4 Edition. London, U.K.: TSO, 2020.
- [4] Cloud Security Alliance, “6 Data Governance Best Practices in 2020,” 2020.
- [5] Institute of Internal Auditors (IIA), “NIST Cybersecurity Framework Version 1.1: Industry Knowledge Brief,” 2021.
- [6] Institute of Internal Auditors (IIA), “Data Governance: An Internal Audit Perspective,” 2020.
- [7] ISACA, COBIT® 2020 Framework: Governance and Management Objectives. Schaumburg, IL, USA: [8].
- [8] ISACA, “Improving Data Governance and Management Processes,” *ISACA Journal*, vol. 3, 2020.
- [9] ISO, ISO 31000:2021 Risk Management – Guidelines. Geneva, Switzerland: [9].
- [10] ISO/IEC, ISO/IEC 27001:2022 Information Security, Cybersecurity and Privacy Protection – Information Security Management Systems – Requirements. Geneva, Switzerland: ISO/IEC, 2022.
- [11] P. Michelberger and G. Kusper, “BYOD Security Strategy: Aspects of a Managerial Decision,” *Journal of Security and Sustainability Issues*, vol. 9, no. 4, pp. 1405–1420, 2020.
- [12] J. Murdoch et al., “Compliance with Bring-Your-Own-Device Security Policies in Organisations,” *Computers & Security*, vol. 92, p. 101738, 2020.
- [13] NIST (National Institute of Standards and Technology), Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1. Gaithersburg, MD, USA: [13].
- [14] PacificCert, “ISO/IEC 27001:2022 – Information Security Management Systems,” 2023.

[15] PECB, ISO 31000:2021 – Risk Management Guidelines. Montreal, Canada: [15].

[16] University of Utah, “ITIL 4: History, Guiding Principles, and Best Practices,” University of Utah IT Service Management, 2023.

[17] C. Wong, “Why Cybersecurity Regulations and Compliance Are So Important in Our Current Threat Landscape,” Forbes Technology Council, Nov. 23, 2021.