

Name : MD RIAD HOSSAIN

STUDENT ID: 2434324

MODULE: ACCA7028

Data Security, Governance and Compliance

Lecturer: Dr. Dipo Dunsin

SUBMISSION DATE: 19/12/2025

Table of Contents

1. **Introduction**
2. **Research on Security Frameworks and Models**
 - 2.1 Overview of IT Security Frameworks
 - 2.2 Information Technology Infrastructure Library (ITIL)
 - 2.3 ISO/IEC 27000 Security Model
 - 2.4 Relevant Diagrams, Figures, and Charts
3. **Proposed Information Security Approach for NatureGreen (NG)**
 - 3.1 Governance and Strategic Planning for Security
 - 3.2 Security Policies for Staff and Customer Device Usage (BYOD)
 - 3.3 Compliance with Laws, Ethics, and Regulations
 - 3.4 Risk Management Framework for NG
 - 3.5 Protection Mechanisms for Staff, Client Data, and Intellectual Property
 - 3.6 Service Level Agreement (SLA) Considerations
 - 3.7 Contingency and Continuity Planning
 - 3.8 Tables and Diagrams Supporting the Proposed Approach
4. **Analysis and Critique of Updating Regulations and Standards**
 - 4.1 Importance of Constantly Updating Security Standards
 - 4.2 Organisational, Legal, and Ethical Implications
 - 4.3 Impact on Governance, Risk, and Compliance (GRC)
5. **Conclusion**
6. **References**
7. **Appendices**
 - Appendix A: Security Framework Diagrams
 - Appendix B: Risk Assessment Tables
 - Appendix C: Security Policy Samples

Introduction

The modern enterprise are characterized by internet access, mobile workforces, and dependence on technologies, faces complex array of information security challenges. Most of organizations are rapidly reliant on advanced dynamic infrastructure, such as cloud platform and extensive wireless technologies which reduce traditional security perimeters. NatureGreen(NG), a global leading health and wellness brand, exemplifies this modern complexity. The organizations operational basement is heavily depend on cloud service and

almost full of its network activity is wireless based. Crucially, NG is under huge pressure to accommodate the use of devices for both staff and its international customer base.

While NG recognizes information security as a priority, the current environment is explain as being in disarray with no stable policies to govern security needs. The main idea are multifaceted: the prevention of the data of staff and user, securing the high value intellectual property worth billions, and ensuring compliance from vast global operational footprint. This situation represents a significant risk exposure that must be immediately addressed through structured governance.

NatureNaere Security Problems and Solutions

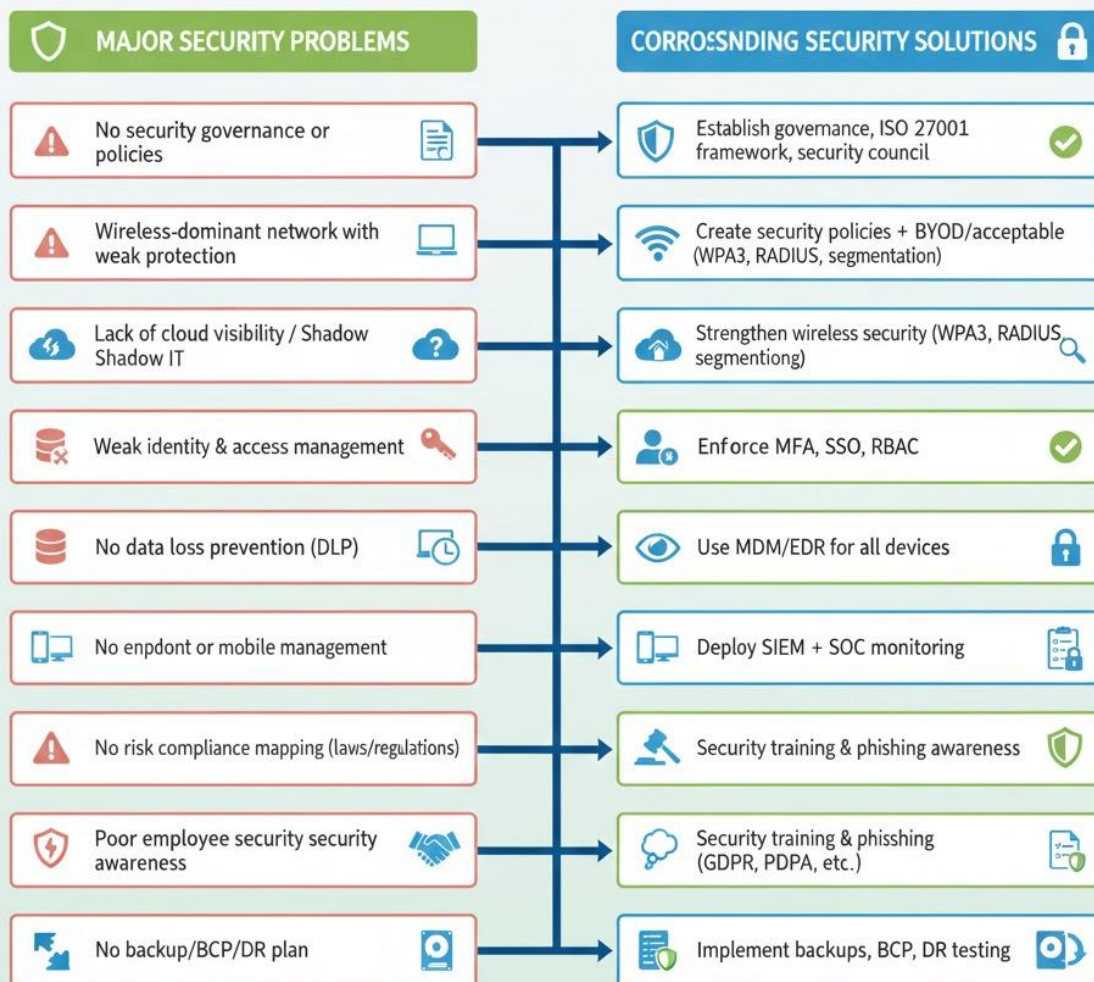


Fig 1

The aim of this report is twofold: first, to conduct comprehensive research into established security frameworks and models, using diagrams and figures help to understanding, and second, to effort this knowledge to design a bespoke info system security, governance, and compliance approach for NG. Additionally, this report will analyze, and discuss the core necessity for the xonstant review and upgrade fo security regulations and standards in response to the advanced threat landscape. This comprehensive approach to utlize authoritative references, including COBIT, ISO 27000 series, and NIST special publications, to establish a robust and defensible solution for NG.

II. Research on security Frameworks and Models

The foundation of robust information security management lies in the adoption of internationally recognized frameworks and models. These infrastructures offers necessary control objectives and management processes to move NG from state of disarray to one of disciplined governance and operational security.

2.1 Overview of IT security frameworks

Security frameworks offers a comprehensive structure which aids organizations in managing and reducing their cybersecurity risks [1]. They can be generally structured by their major focus: Governance and operational. For NatureGreen, a holistic method is required, necessitating the integration of all three categories. Security Frameworks are designed to be adaptable, allowing an organization to pre select related controls that aling with objective of business, risk appetite, and legal obligations such as GDPR, CCPA.

2.2 Information Technology Infrastructure Library

While ITIL is fundamentally a service management framework, its latest iteration, ITIL4, and its focus on service value system, offers essential operational allow for implementing security controls [2]. How security policies and standards are translated into day to day operations ITIL dictates.

The ITIL practices are most relevant to NG's security needs include:

1. Change of enablement which ensuring security monitoring are mandatory for all infrastructure changes, particularly those concerning the wireless and cloud space.
2. Incident management which establishing a defined, quick and efficient way for corresponding to security breaches or unauthorized BYOD access, directly allow NG's need for data protection.
3. Service level management defining, negotiating, and monitoring the security requirements integrated into agreements with NG's cloud providers and internal IT teams.

2.3 ISO 27000 Security Model

The **ISO/IEC 27000** series represents the globally recognized standard for establishing, implementing, maintaining, and continually improving an infosec management system [3]. This is the critical framework needed to impose order on NG's current policy vacuum.

The main standard is ISO/IEC 27001:2022, which defines the necessity for an ISMS. It is founded on the plan do check act cycle:

- Plan: Define the scope of the ISMS and establish the security policy.
- Do: implement the controls verified in the statement of applicability based on ISO/IEC 27002:2022
- Check: reviewing, measure, and audit the task performance of the ISMS.
- Act: Take right actions for continuous improvement.

ISO/IEC 27002:2022 offers catalog of precise security controls like data leakage prevention and identity management, vital for securing IP and client data across the wireless, BYOD environment.

2.4 Relevant Diagrams, figures and charts

- Figure 1: competitive focus of key IT frameworks and ISO/IEC 27001 ISMS PDCA Cycle

- This figure illustrates how COBIT provides the strategic governance mandate, ISO 27001 provides the management system, and ITIL offers the operational execution loop.

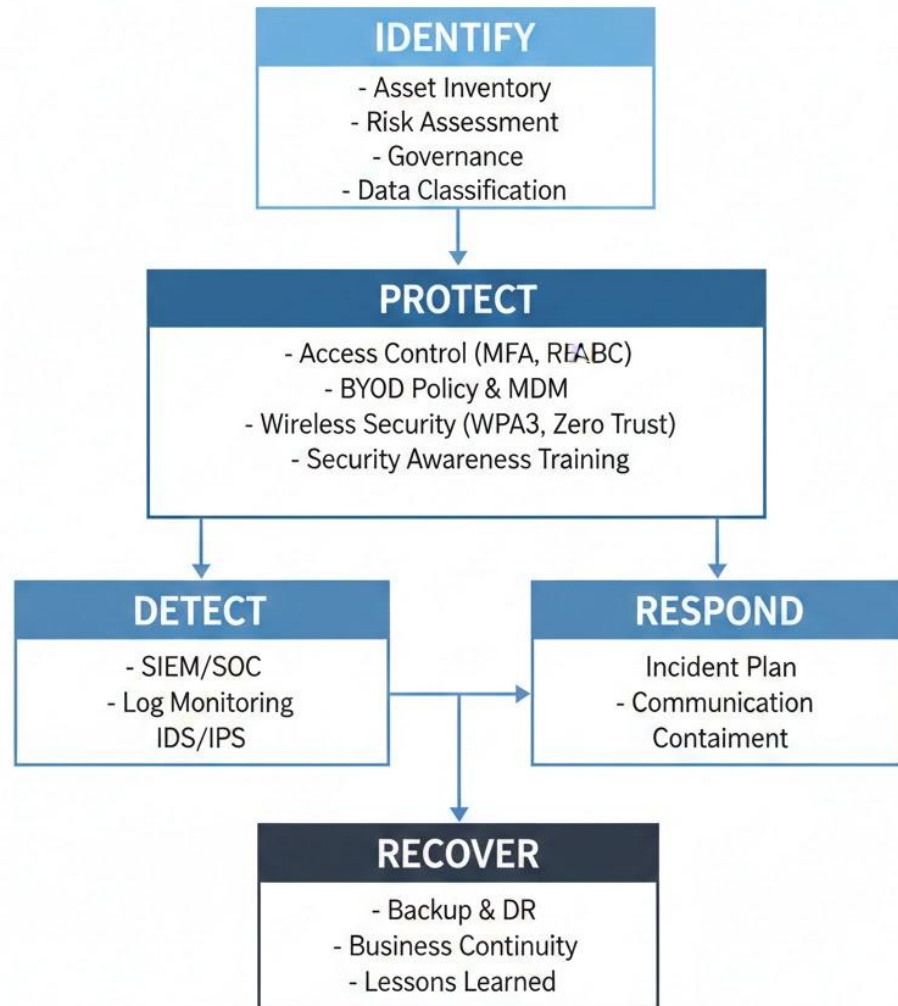


Fig 2

3. Proposed information security approach for NatureGreen (NG)

The proposed approach integrates the Governance principles of COBIT 2019, the Management requirements of ISO 27001, and the tech controls by NIST publications to make robust and compliance security architecture for NatureGreen.

3.1 Governance and Strategic Planning for Security

To move beyond the current state of disarray NG must immediately implement strong IT governance. The COBIT 2019 Framework is suggested as the organizational layer, as it bridges the gap between the business required and the technical requirements [4].

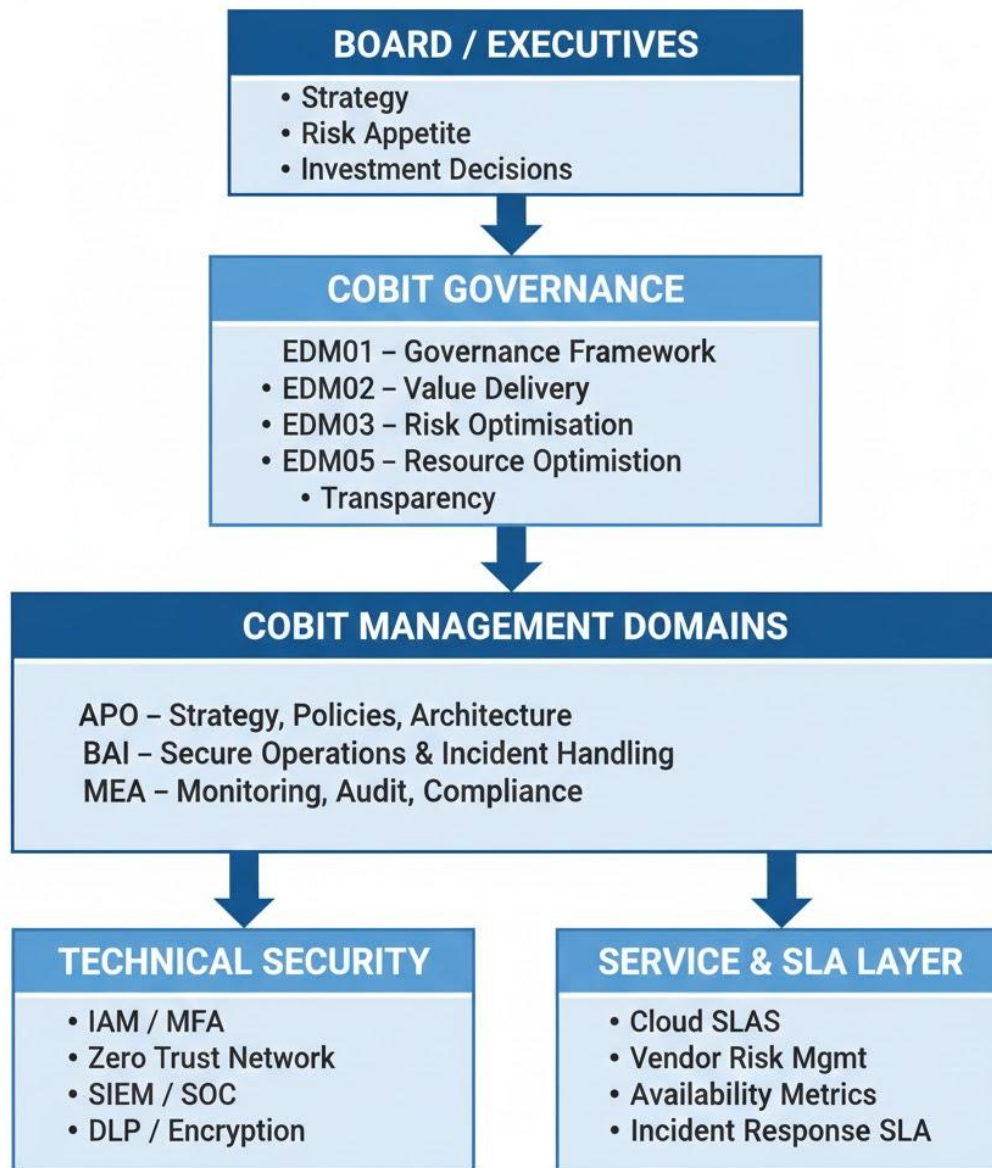


Fig 3

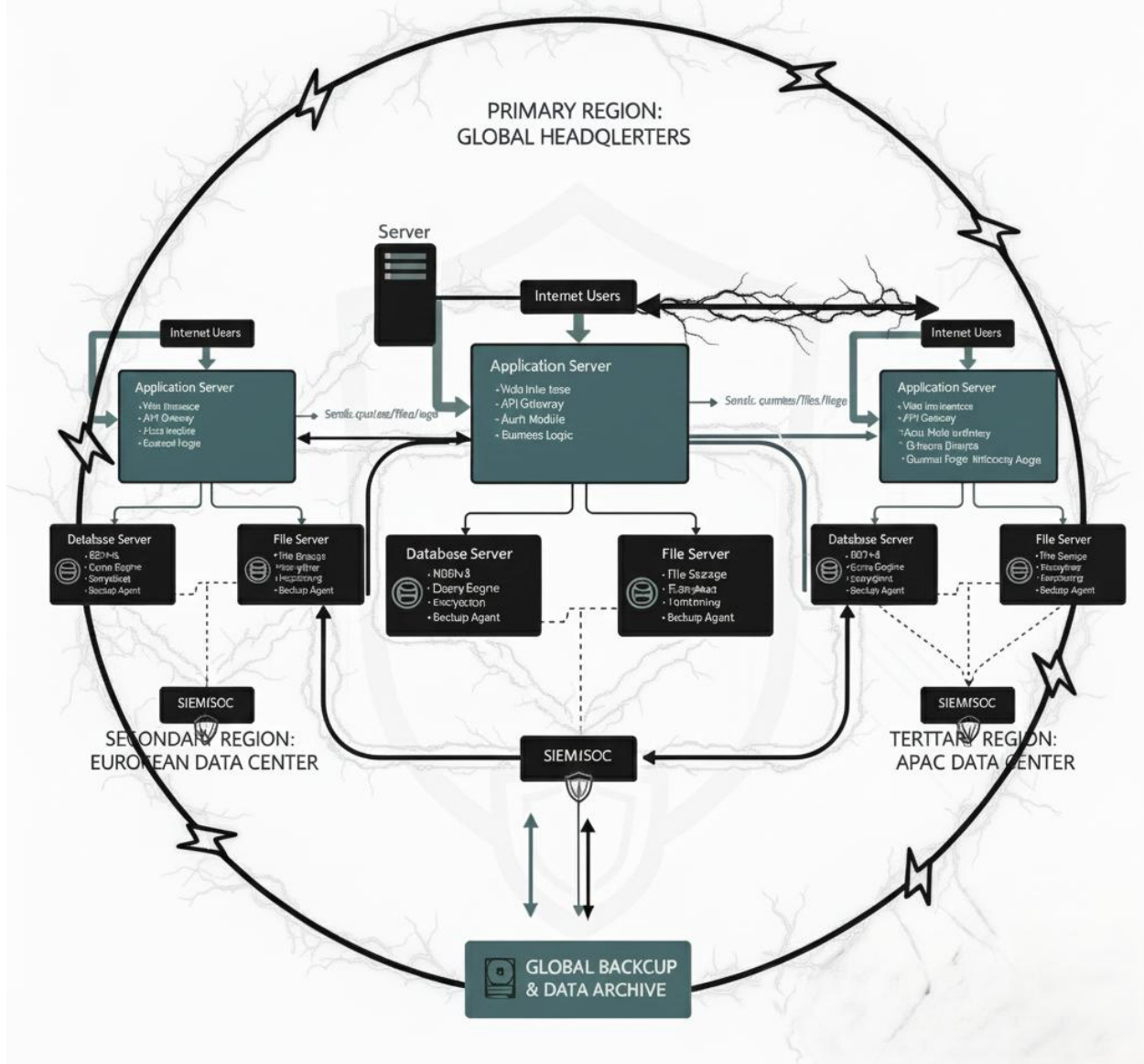
- Figure 3: COBIT 2019 Governance this diagram demonstrates how stakeholder necessity are process into IT goals, providing the required strategic direction for NG's security investment.
- Establish a security steering management to comprised the executive leadership and the CISO which will be responsible for the security policy and the risk appetite.

- Define security planning to map the security program to get the business objective which ensures the protection of the millions worth of IP is prioritized.
- Adoption COBIT goal cascade for translate higher level of business goals down to IT Goals and the control objective of specific security

3.2 security policies for staff and customer device usage

The extensive wireless network and BYOD required policies that focus on access control and data separation system. There are some suggested policy and components down below with diagram:

NatureGreen Global Replicated Application & Security Architecture



- Zero trust architecture: Implement a ZTA infrastructure where no user or device is inherently trusted [5]. Access to confidential resources must be verified and authentic dynamically based on the context and the health of the device.
- Mobile device management: all staff BYOD devices having permission using NG DATA must be enrolled in MDM solution . this procedure allows containerization and remote wiping capacity for corporate info.
- Network access control: Implements NAC to separate unauthorized data or unhealthy devices onto a guest network and strictly prohibiting access to core of the ip system.

3.3 compliance with Ethics, Law and Regulations

NG's international presence required more strict adherence to multiple data protection and laws enforcement.

EU General data protection regulations (GDPR) needs explicit consent and mandatory breach notification. 27002 controls directly help NG meet these requirements.

US state regulation needs some specific consumer rights regarding each individual information.

Ethical data handling Given NG's focus on health, establishing ethical policy regarding the anonymization and responsible use of customer health related data and info is essential to maintain brand trust. Increase the demand among the consumers.

3.4 Risk management framework for NatureGreen:

NG must adopt a structured process for analysis, identify, assessing, and mitigating risks, particularly those who concern IP theft and BYOD device compromise. The NIST risk management Framework

Sp 800-37 is ideal for this structured [6].

1189: NIST Risk Management Framework

A circular, iterative approach to managing information



Fig 4

Fig 4: NIST RISK Management framework

Well this diagram shows the major 7 cyclical procedure for manage businesses security and privacy risk at NatureGreen

NIST RMF steps applied to NG

1. Categorise : based on impact its divide into few categories.
2. Select: chose to cotrols from Nist sp 800-53 based on system catalog.
3. Implement and assess: deployment controls and aduit their effectiveness.
4. Monitor and Authorize : the ssc grants authorizations to operate based on the acceptable risk, followed by continuous monitoring.

3.5 protection mechanism for staff, user data and intellectual property

- IP protection refers deploy data loss prevention from all cloud services and endpoints. DPL must surveillance and block unauthorized movement of the intellectual property. Strict access control should implement for all IP repsoitiories.
- User and staff's data protection refers enforce multi factor authentication and end to end encypton for the all data has been transmitted from wireless network. Utilize cloud security posture management tools to keep monitoring cloud config.

3.6 service level agreement considerations

NatureGreen must ensure it security patch requirements are embedded in its contracts

- Cloud SLAs: need the cloud provider services to adhere to precise security standards with some ISO 27001 Level certificaion. Mandate strict incident respose time guarantees.
- Internal SLAs refers internal IT task performance metrics for security operation, like patch deployment run time and incident resolution time ensuring ITIL processes support the security framework.

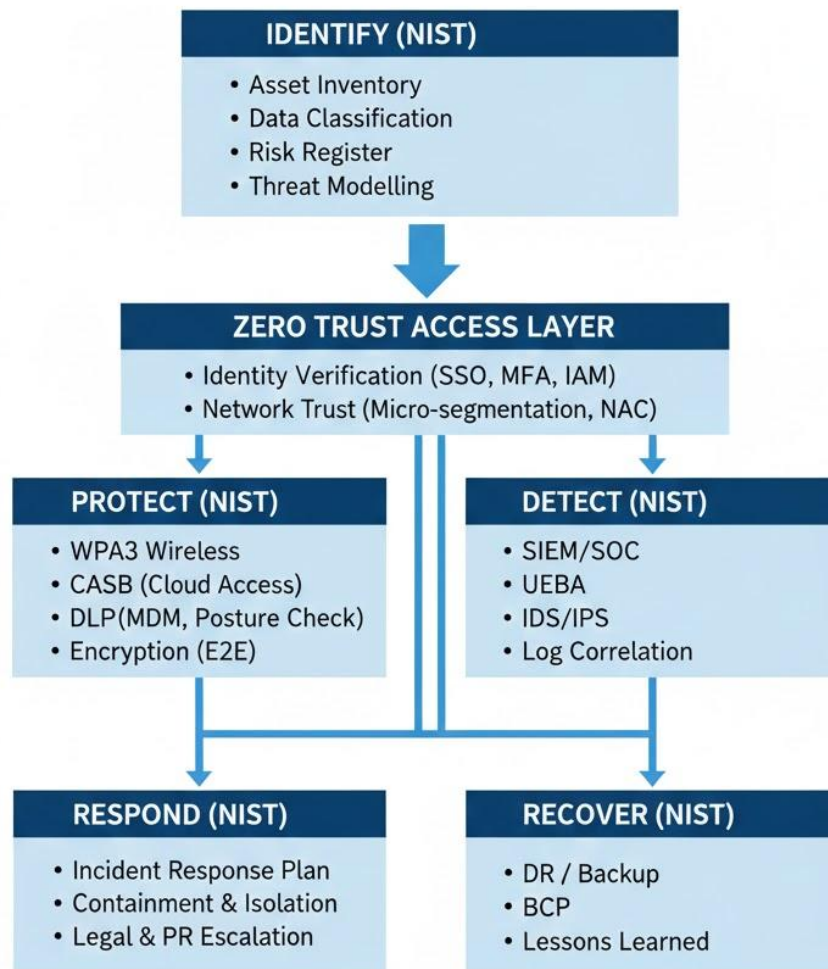
3.7 contingency and continuity planning

To ensure business resilience a robust plan is needed.

- Business continuity planning : defines a aligned withn iso 22301 business continuity management.
- Recovery metrics : refers clear recovery time objective and point objectives for the whole system.

3.8 Diagrams supporting the proposed approach

NatureGreen zero trust network diagram.



This diagram demonstrates the isolate of highly trusted of corporate devices from BYOD devices accessing allocated and contined resource, based on NIST 880-207 zero trust architecture principles.

4 Analysis and critique of updating regulations and standards

4.1 Importance of constantly updating security standards

The standards and the regulation of security are not static, they need constant revision. This need is driven by the dynamic and the asymmetrical nature of the threat landscape.

Key drivers for updates:

- The evolving threat landscape. Threat actors continually innovate. Standards must evolve to mandate controls that address these new attack vectors. For example ISO 27002:2022 update introduces new controls for cloud services especially [7].
- Technological evolution: The rapid adoption of new tech introduces fundamentally new security perimeters and risks. Failure to update standards could leave organizations trying to secure 21st century's network infrastructure with outdated rules.

4.2 organizational, legal, and Ethical implications

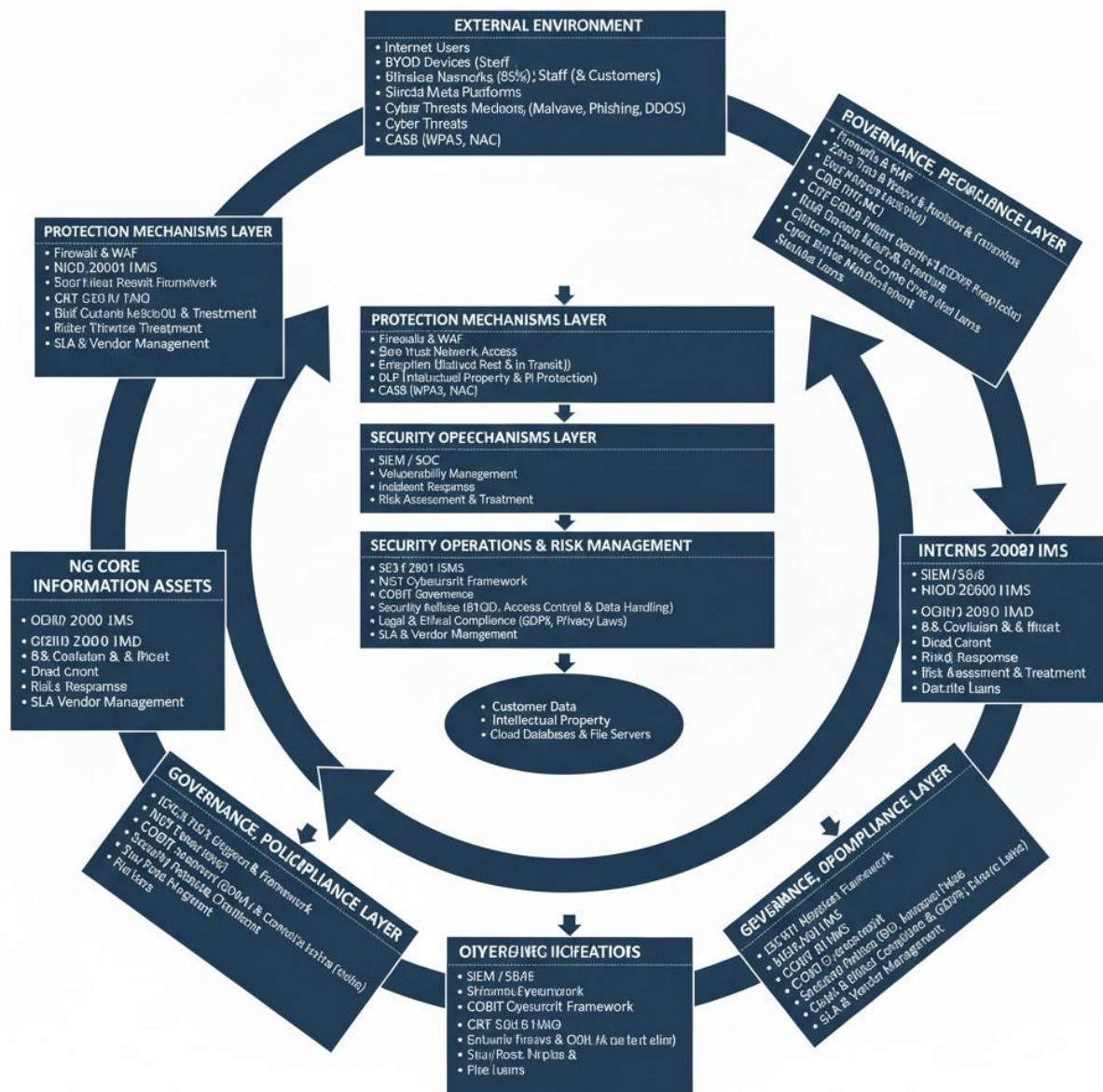
The continuous update of security standards carries important implications for the organization.

- Organizational cost vs Risk: the capital in updating policies and controls is essential as the cost of breach far outweighs the cost of maintaining current compliance due diligence.
- Legal Liability: courts often consider adherence to the latest established standard like NIST or ISO as the proof of due care[8]. Organizations failing to adopt updated standards expose themselves to enhanced legal liability regulatory fines under GDPR.
- Ethical responsibility: For a brand like NatureGreen, there is an ethical imperative to protect customer data using the best security practices. Outdated standards do not meet this ethical obligation.

4.3 Impact on governance, risk, and compliance

Keeping standards updated fundamentally transforms the nature of GRC within an organization.

Diagram below



- Governance : updating ensure governance is advanced dynamic and adaptive. This required the COBIT mandated SSC to continually review the risk appetite and make the decisions based on current best practices.
- Risk : latest stands introduce new control baseline, lowering the whole residual risk to the organization. Regular updates force the RMF procedures to reassess controls against the new threats.

- Compliance : updates turn compliance onto a keep monitoring activity , need ongoing audits, check and corrective actions, shifting compolance from time to time into a business process

5.conclusion

NatureGreen's multi operational environment, represent it's global scale, cloud reliance, wireless technology and acute BYOD demand. Also presents significant security challenges compounded by its current policy vacuum. The proposed method resolve this disarray through the strategic integration of all three authoritative frameworks COBIT establishes the required top down governance; ISO/IEC 27001:2022 implement a robust managing system and the NIST RISK management framework provides the structured process for continuous risk assessment and the deploy of specific controls such as ZTA, DLP. This multi layersolution make sure the data safety and the protection of billions in intellectual property and compliance with international data privacy laws as well. Furthermore the analysis confirms that compliance is not static, the required of constantly updating regulations is driven by evolved technologies and threats requiring nature green to adopt a posture of continuous security. By implementing this GRC frameworks NG can transform its security posture from one of reactive disarray to one proactive resilience management.

6. References :

1. [1] A. Sadeghi, T. Z. Aref, and M. A. Serhani, "Cybersecurity Frameworks," *Journal of Information Systems Engineering and Management*, vol. 9, no. 4s, 2024.
2. [2] D. Berger, N. K. Shashidhar, and C. Varol, "Using ITIL 4 in Security Management," in *Proc. IEEE International Symposium on Digital Forensic and Security (ISDFS)*, 2020, pp. 1–6, doi: 10.1109/ISDFS49300.2020.9116257.
3. [3] G. Disterer, "ISO/IEC 27000, 27001 and 27002 for Information Security Management," *Journal of Information Security*, vol. 4, no. 2, pp. 92–100, Apr. 2013, doi: 10.4236/jis.2013.42011.
4. [4] K. Leonardo and R. Latuperissa, "Information Technology Governance Design in Trading Companies Using the COBIT 2019 Framework," *Journal of Information Systems and Informatics*, vol. 6, no. 3, pp. 1466–1483, Sep. 2024, doi: 10.51519/journalisi.v6i3.798.

5. [5] R. Rose, N. Mitchell, and I. Connelly, "Zero Trust Architecture: Principles and Practice," *Journal of Cybersecurity and Privacy*, vol. 2, no. 4, pp. 627–648, Dec. 2022, doi: 10.3390/cybersecurity2040041.
6. [6] A. Efe, "A Comparison of Key Risk Management Frameworks: COSO-ERM, NIST RMF, ISO 31000, COBIT," *Denetim ve GÜvence Hizmetleri Dergisi*, vol. 3, no. 2, pp. 185–205, Jul. 2023.
7. [7] R. Nykänen, "Analysis of the Next Evolution of Security Audit Criteria," *Information Security Management*, vol. ??, pp. ??, 2023. (Discusses ISO/IEC 27002:2022 and how the updated control set reflects modern security concerns.)
8. [8] S. J. Shackelford, A. Proia, B. Martell, A. Craig and et al., "Toward a Global Cybersecurity Standard of Care? Exploring the Implications of the NIST Cybersecurity Framework on Shaping Reasonable National and International Cybersecurity Practices," *Texas International Law Journal*, vol. 51, no. 2, pp. ???–???, 2015.