



Prifysgol Cymru
Y Drindod Dewi Sant
University of Wales
Trinity Saint David

DATA SECURITY GOVERNANCE AND COMPLIANCE

ACCA7028 Assessment Report

Student Name:
Habibullah Shaikh

Student ID:
2503799

Programme:
MSc Cybersecurity and Digital Forensics

Submission Date:
Friday, 19th December 2025

Table of Contents

Abstract.....	3
1. Introduction.....	3
1.1 Background and Context.....	3
1.2 Extended Scenario Description.....	4
1.3 Problem Statement.....	5
1.4 Updated Objectives	5
1.5 Detailed Assumptions	5
2. Literature Review	6
2.1 ISO/IEC 27001:2022 Framework.....	6
2.2 ITIL 4 Framework.....	7
2.3 NIST Cybersecurity Framework (NIST CSF)	8
2.4 Framework Comparison	8
2.5 CIS Critical Security Controls (CIS v8).....	9
2.6 COBIT 2019 Governance Framework.....	9
3. Breakdown of Problems and Mapping to Models.....	10
3.1 Problem Identification.....	10
4. Selected Models to Address NG's Problems.....	11
5. Proposed Security Framework for NG.....	12
5.1 Layer 1: Governance & Strategic Planning.....	12
5.2 Layer 2: Compliance Framework.....	12
5.3 Layer 3: Security Policies.....	12
5.4 Layer 4: Risk Management.....	13
5.5 Layer 5: Security Management Models.....	13
5.6 Layer 6: Technical Protection Mechanisms	13
5.8 Layer 8: Service Level Agreements (SLAs).....	14
6. Critical Analysis: Why Standards Need Continuous Updates.....	16
6.1 Evolving Threat Landscape	16
6.2 Technological Evolution	16
6.3 Regulatory Developments.....	16
6.4 Case Studies.....	16
7. Implementation Roadmap.....	17

7.1 24-Month Timeline.....	17
7.2 Budget Estimate	18
8. Conclusion	19

Abstract

NatureGreen (NG) is a multinational wellness and health manufacturing company whose 95% of network runs on wireless infrastructure [1]. Because of extensive digital footprint, multi cloud architecture, and growing demand for BYOD access [3], NG faces serious governance, security and compliance issues. NG does not have proper information security management systems (ISMS), documented policies, or governance frameworks. While the company has billion-dollar intellectual property [7] and the company operates in multiple countries. These situations can expose the organization to operational risks, cyber attacks, and international laws such as GDPR [18], CCPA/CPRA [19], and PIPL [47]. NG's scenario is analyzed systematically, where organizational issues were identified and categorized. Cyber governance frameworks like ISO/IEC 27001:2022 [8], NIST CSF 2.0 [35], ITIL 4 [10], CIS Controls v8 [61], COBIT 2019 [62], and Zero Trust Architecture [36] were assessed. Based on these frameworks, a multi-layered security architecture will be designed for NG's governance, compliance, technical controls risk management, and operational security. By using case studies from Capital One [49], SolarWinds [50], and MOVEit [51], it was also explained why it is important to regularly update global standards. The plan also includes a cost estimate and a 24 month implementation roadmap. According to International best practices and legal requirements, this final architecture converts NG's scattered and reactive security system into organized, auditable, and resilient security ecosystem.

1. Introduction

1.1 Background and Context

NatureGreen (NG) operates in North America, Europe, Asia, and Middle East and it is a global producer and distributor of wellness products. Company's business model is technology-driven includes cloud services, digital commerce platforms, wireless-enabled workplaces, remote workers, and large scale international data flows. NG stores and processes sensitive client data, supplier information, financial records, and valuable proprietary product formulas in its systems. Nearly 95% of the NG's corporate network is based on wireless networks. This creates vulnerabilities such as rogue access points, weak authentication practices, and network-based attacks [1][6]. The company's cloud-first approach makes it more exposed to identity based attacks, insecure APIs, shared responsibility model's issues, and cloud misconfigurations [2]. Apart from that, NG's biggest online and social media footprint also increases the risk of phishing, impersonation attacks, and reputational damage. The demand for BYOD support increased exponentially from Employees and customers due to recent internal and external

pressures. This has significantly increased risks such as data leakage, mixing of personal and company data, and access to unmanaged or insecure devices [3]. Despite this different and complex environment, NG doesn't have basic governance structures, security policies, defined controls, and compliance procedure. This lack makes the organization more exposed and unsafe, and it becomes necessary that a comprehensive security framework should be developed for the organization that is compliant with regulations and effectively addresses all risks.

1.2 Scenario Description

A deeper review of NG's operational environment reveals interconnected layers of risk:

A. Organizational Complexity

- Multinational operations across multiple jurisdictions
- Global supply chains and contract manufacturers
- Billion dollar intellectual property requiring strong protection [7]
- Distributed IT operations without centralized governance

B. Technology Landscape

- Multi cloud architecture (AWS, Azure, GCP)
- 95% wireless infrastructure reliant on 802.11ac standards [1]
- E-commerce systems, APIs and mobile applications
- Extensive use of endpoints and BYOD devices

C. Regulatory Landscape

NG must comply with:

- GDPR (EU) [18]
- CCPA/CPRA (California) [19]
- PIPL (China) [47]
- PDPA (APAC countries) [20]
- PCI DSS for card payments [21]

D. Security Capability Gaps

- No ISMS or documented policies
- No CISO or security governance structures [14][15]
- No risk management methodology [32]
- Minimal monitoring, no SIEM, no incident response plan [30]
- No data classification or supplier security controls

This expanded scenario provides the foundation for problem identification and framework design.

1.3 Problem Statement

Due to the lack of formal governance mechanisms and leadership accountability, the security posture of NG has become weak, dispersed, and completely reactive [4]. To fix this situation, NG needs:

- Clear guidelines for cloud environments, BYOD devices, and wireless networks [1][3][28]
- Compliance controls as per regulations like GDPR, CCPA, PIPL, and PCI DSS [5].
- Technical protections for unmanaged devices, wireless networks, and high-risk systems [6].
- Proper procedures for supplier governance, business continuity, risk assessment, and incident management [30][32].

The lack of all these things makes the NG more of a target for major risks like data breaches, service outages, compliance fines, and intellectual property theft..

1.4 Updated Objectives

This report aims to:

1. Analyze the NG's scenario and break it down into governance, compliance, technology, and operations.
2. Identify and classify specific problems that are being faced by NG.
3. Reviewing the literature review on important security models and frameworks.
4. Assigning stable security models for each problem area.
5. Designing a custom, integrated security framework for the NG that fits its needs.
6. Real-world case studies are used to critically evaluate why it is important to regularly update security standards.
7. Provide a budget estimate and a roadmap for regular implementation.

1.5 Detailed Assumptions

A. Organisational Assumptions

- Workforce of approximately 5,000 staff with global operations in 25+ countries
- Leadership is willing to support security investments
- NG prioritises protecting intellectual property and customer data

B. Technical Assumptions

- Cloud platforms: AWS, Azure, GCP
- 95% wireless network using 802.11ac
- Approximately 6,000 corporate devices and 3,000 BYOD devices
- Critical systems include ERP, CRM, HRIS, and e-commerce platforms

C. Regulatory Assumptions

- GDPR, CCPA/CPRA, PIPL and PDPA apply to NG based on operational jurisdictions

D. Security Assumptions

- No major breach has occurred yet, but risk is significant
- Basic controls exist: firewalls, antivirus, VPN
- No SIEM, disaster recovery plan, risk register or formalised security team currently in place

2. Literature Review

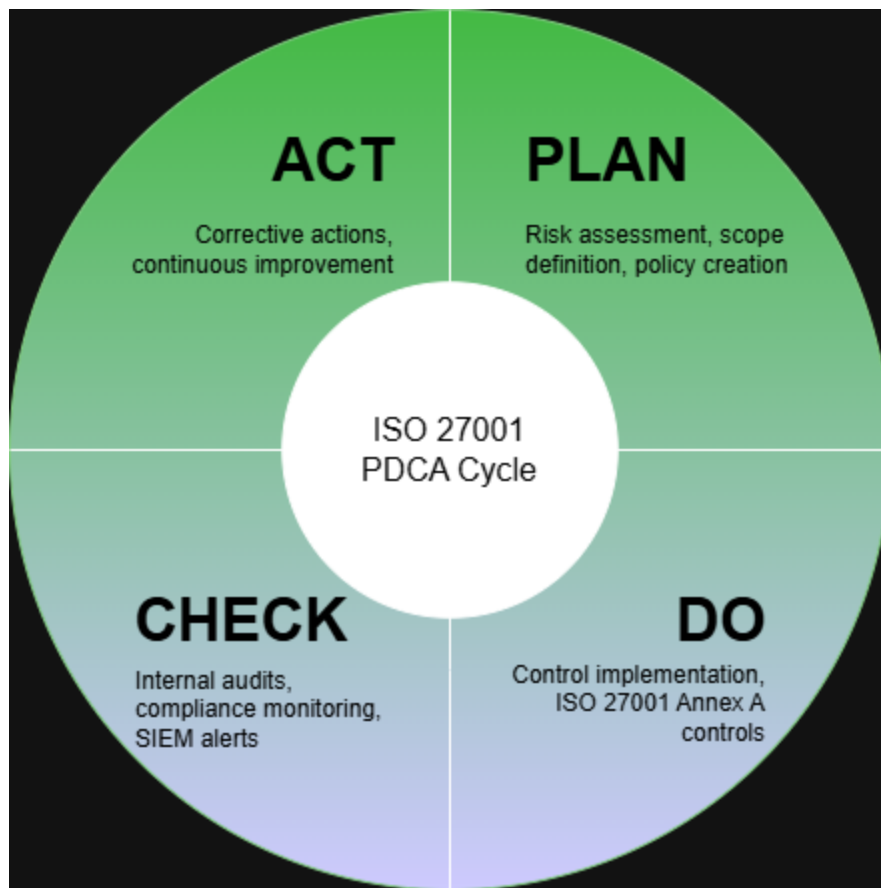
2.1 ISO/IEC 27001:2022 Framework

ISO/IEC 27001:2022 is an industry standard that is used to create, implement, maintain and improve continuously Information Security Management System (ISMS) [8]. This is based on the principles of standard governance, risk management, and systematic control implementation. 2022 update added some new control themes, like threat intelligence, cloud governance, secure coding, and ICT readiness for business continuity. These updates make the standard even more relevant for modern cloud-native, hybrid, and distributed systems [9]. The management system approach of ISO 27001, which is based on Plan-Do-Check-Act (PDCA) cycle, is one of its biggest advantages [8].

- **Plan:** Create a plan that includes identifying stakeholders, defining the scope, evaluating risks, creating policies, and risk treatment procedures.
- **Do:** Apply the controls and organizational procedures of Annex A.
- **Check:** Perform Internal audits, management reviews, and compliance monitoring.
- **Act:** Promote continuous improvement, take corrective actions, and optimize system's maturity.

Top-level management responsibilities, detailed policy documentation, performance indicators, internal audits and clearly defined governance roles, are addressed in clauses 4–10 [8]. These components are very important for an organization like NG, to become a solid security foundation, consistent governance should be maintained, and international requirements like CCPA and GDPR can be met. For better alignment with cloud and BYOD environments, Annex A (which was reduced from 114 to 93 controls) has been reorganized into four themes: organizational, people, physical, and technological [8][9]. Through the requirements of Risk-led decision making and verifiable control implementation, ISO 27001 addresses current issues of NG such as policy gaps, lack of wireless security discipline, and cloud governance vulnerabilities.

Diagram:



2.2 ITIL 4 Framework

ITIL 4 is a modern and complete framework which integrates secure operational practices throughout the entire service lifecycle and aligns services with business goals [10]. ITIL 4 also includes a Service Value System (SVS) [10], which focuses on creating value through governance, continuous improvement, guiding principles, and service management practices. It does not depend solely on processes just like previous versions. The Information Security Management (ISM) practice of ITIL 4 focuses on protecting confidentiality, integrity, and availability [11]. This makes security part of service operations, change management, configuration management, and incident response. This means that ITIL 4 does not consider security as a separate activity, but rather deals with it as an integrated part of every service.

Key theoretical foundations include [10][11]:

- Value streams that map actions that contribute in a secure service delivery;
- In service design, "fit for purpose" (utility) and "fit for use" (warranty) ensures;
- Guiding concepts such as "optimise and automate," "progress iteratively," and "focus on value."

ITIL 4 provides the operational framework that helps implement ISO 27001 controls for NG on a daily basis, especially when wireless, cloud, and BYOD services are more integrated. This

ensures that good management reduces the risk of misconfigurations. Incident handling should be organized, and policies should become practical procedures. According to cloud security research, misconfigurations are among the most common cloud security issues [2]. That's why, ITIL 4 based structured change and configuration management is very important in NG's multi cloud environment.

2.3 NIST Cybersecurity Framework (NIST CSF)

The NIST CSF is a globally recognised cybersecurity model that uses five core functions Identify, Protect, Detect, Respond and Recover to create a maturity-based approach for improving an organisation's cyber posture [12]. While ISO 27001 focuses on governance and certification, NIST CSF emphasises operational cybersecurity resilience, making it highly relevant for distributed and high-risk digital infrastructures.

The 2024 CSF 2.0 update strengthens several theoretical elements [35]:

- Greater emphasis on identity-based security, reflecting the shift to Zero Trust environments
- Expanded coverage for cloud-native ecosystems, including APIs, containerisation and serverless technologies
- Integration of supply chain security, influenced by major incidents such as SolarWinds [50]
- Stronger detection and logging guidance, supporting modern SIEM/XDR strategies

Each function is broken into categories and subcategories, providing a flexible structure that organisations like NG can map to their specific environments (wireless, multi-cloud, global operations). For example, the Detect function directly addresses NG's absence of SIEM, continuous monitoring and anomaly detection [35], while the Respond and Recover functions emphasise incident handling and business continuity both areas where NG currently lacks formal processes [30].

2.4 Framework Comparison

To understand the theoretical foundations of a combined approach, the frameworks can be conceptualised along different roles [8][10][12][35][61][62]:

Framework	Primary Focus	Strengths	Weaknesses
ISO 27001 [8]	Governance, risk management, compliance	Auditable, controls-based, policy-driven, regulatory alignment	Less technical guidance; high documentation effort
NIST CSF [12][35]	Cybersecurity operations & resilience	Strong detection/response guidance, flexible maturity tiers	Not a certification standard

Framework	Primary Focus	Strengths	Weaknesses
ITIL 4 [10][11]	Service management operations	Process consistency, operational discipline, integration with IT functions	Not primarily a security framework

The combination forms a layered theoretical model where:

- ISO 27001 acts as the governance backbone [8]
- NIST CSF provides operational cybersecurity depth [35]
- ITIL 4 integrates security across service operations [10]

This theoretical synergy is widely acknowledged in industry research and aligns with NG's need for governance, operational discipline and cybersecurity maturity.

2.5 CIS Critical Security Controls (CIS v8)

The CIS Controls v8 are a set of 18 prioritized security safeguards designed to defend against the most prevalent attacks [61]. Unlike ISO or NIST, CIS is highly prescriptive and technically detailed, offering concrete configuration steps, deployment recommendations and control verification guidelines. This makes CIS particularly valuable for NG's cloud, wireless and BYOD-driven environment.

The theoretical basis for CIS v8 includes [61]:

- Zero Trust-aligned identity controls (MFA, least privilege, SSO)
- Asset-driven security based on accurate inventories of endpoints, cloud resources and software
- Vulnerability reduction through secure configuration baselines
- Prioritisation of controls using Implementation Groups (IG1, IG2, IG3)

For NG which operates 95% wireless [1], multi-cloud and extensive device infrastructure the CIS Controls address the exact technical weaknesses identified in the scenario. Additionally, CIS cloud benchmarks provide configuration hardening standards for AWS, Azure and GCP [58], making them essential for reducing misconfiguration risks and improving cloud posture.

2.6 COBIT 2019 Governance Framework

COBIT 2019 is an enterprise-wide governance framework that ensures information and technology (I&T) align with business objectives while managing risks effectively [62]. It provides a structured model for defining responsibilities, decision-making authority and performance monitoring, making it highly suitable for organisations lacking clear governance structures, such as NG.

The framework is built on several key components [62]:

- **Governance System Principles:** COBIT promotes value delivery, risk optimisation and clear separation between governance (EDM) and management (APO, DSS, MEA) functions
- **Defined Roles and Accountability:** It emphasises leadership roles such as the CISO [14][15], governance committees and cross-functional collaboration addressing NG's current leadership and responsibility gaps
- **Design Factors:** Elements such as regulatory requirements, risk profile and enterprise strategy guide customisation of the governance model
- **Performance and Capability Models:** COBIT evaluates process maturity and performance, supporting continuous improvement in governance and cybersecurity functions

For NG, COBIT 2019 provides the necessary governance discipline, ensuring alignment between business goals, IT operations and cybersecurity requirements while establishing accountability at the executive level [14][17][62].

3. Breakdown of Problems and Mapping to Models

3.1 Problem Identification

NG's issues fall into five categories:

(1) Governance & Strategic Problems

- No CISO or steering committee
- No enterprise-wide policies
- No alignment between security and business goals

Relevant Models: COBIT 2019 [62], ISO 27001 Clauses 4–10 [8]

(2) Compliance Problems

- No data protection policies
- No DPIAs or privacy governance
- No breach notification workflow

Relevant Models: ISO 27701, GDPR [18], CCPA [19], PIPL [47]

(3) Technical Weaknesses

- Wireless vulnerabilities [1][6]
- Cloud misconfigurations [2]

- BYOD without MDM or encryption [3]
- No segmentation or Zero Trust

Relevant Models: CIS Controls v8 [61], NIST SP 800-53 [26], Zero Trust (NIST SP 800-207) [36]

(4) Risk Management Problems

- No risk methodology
- No risk register or prioritisation
- No treatment plan

Relevant Models: ISO/IEC 27005 [32], NIST SP 800-30 [33]

(5) Operational Problems

- No SIEM or logging
- No incident response plan
- No DR or BCP
- No continuous monitoring

Relevant Models: NIST CSF 2.0 [35], NIST SP 800-61 [30], ISO 22301 [39]

Diagram:

Problem Category	ISO 27001	NIST CSF	COBIT 2019	CIS v8	Zero Trust
Governance & Strategic	Primary	Related	Primary	-	-
Compliance	Primary	Related	Related	-	-
Technical Weaknesses	Supporting	Supporting	-	Primary	Primary
Risk Management	Primary	Supporting	Related	Related	-
Operational	Supporting	Primary	-	Supporting	Related

4. Selected Models to Address NG's Problems

Model	Problem Solved	Reference
ISO 27001	Governance, policies, auditability	[8]
NIST CSF	Detection, response, resilience	[35]
COBIT 2019	Strategic alignment & accountability	[62]
CIS Controls	Technical and endpoint controls	[61]
Zero Trust	Wireless, cloud, BYOD security	[36]
ISO 27701	Data privacy compliance	-
ISO 22301	Business continuity	[39]

These frameworks are integrated into a unified solution in the next section.

5. Proposed Security Framework for NG

5.1 Layer 1: Governance & Strategic Planning

NG must implement a three-tier governance model aligned with COBIT 2019 [62] and ISO 27001 [8]:

- **Board Oversight [62]**
Approves strategic security direction and ensures alignment with business objectives
- **CISO Role [14][15][16]**
Responsible for ISMS implementation, compliance and risk management
- **Security Steering Committee [17]**
Cross-functional group overseeing policies, risk treatment, supplier decisions and audit results

This governance structure aligns with COBIT 2019 and ISO 27001 Clauses 4–10.

5.2 Layer 2: Compliance Framework

NG must comply with:

- **GDPR** (data minimisation, rights, breach reporting within 72 hours as per Article 33) [18]
- **CCPA/CPRA** (access, deletion, opt-out rights) [19]
- **PIPL/PDPA** (cross-border transfer controls) [20][47]
- **PCI DSS** (payment card protection) [21]
- **SOC 2 Type II** for cloud vendor assurance [23]

Regular audits, Data Protection Impact Assessments (DPIAs) and compliance monitoring become mandatory to ensure ongoing regulatory adherence.

5.3 Layer 3: Security Policies

Required policies include [8][25]:

- **Information Security Policy** [25]
- **Access Control Policy** (MFA, SSO, RBAC, PAM) [26]
- **BYOD & Mobile Device Policy** (MDM, encryption, segmentation) [27]
- **Cloud Security Policy** (shared responsibilities, CASB, KMS) [28]
- **Data Classification & Handling Policy** [29]
- **Incident Response Policy** (NIST SP 800-61) [30]
- **Supplier Security Policy** (ISO 27036) [31]

5.4 Layer 4: Risk Management

Based on ISO 27005 [32] and NIST SP 800-30 [33]:

Step 1: Risk Identification

Identify assets, threats and vulnerabilities [32][33]

Step 2: Risk Analysis

Use likelihood × impact scoring methodology [32][33]

Step 3: Risk Evaluation

Prioritise risks using CIA (Confidentiality, Integrity, Availability) and business impact criteria [32]

Step 4: Risk Treatment

Options: Mitigate, Avoid, Accept, Transfer [25][32]

Step 5: Monitoring

Continuous monitoring using NIST SP 800-137 [34]

5.5 Layer 5: Security Management Models

- **ISO 27001 PDCA Cycle** [8][25]
- **NIST CSF Identify–Protect–Detect–Respond–Recover** [35]
- **Zero Trust Architecture (ZTA)** (continuous verification) [36]

5.6 Layer 6: Technical Protection Mechanisms

Identity & Access Control

MFA, SSO, conditional access, Privileged Access Management (PAM) [26]

Encryption: TLS 1.3+ secure data in transit and AES-256 protects data at rest [29][37].

Network & Wireless Security: 802.1 makes authentication, network segmentation, and WPA3-Enterprise wireless networks secure [38].

Endpoint & BYOD Protection: Secure containers, enterprise mobility management (EMM), mobile device management (MDM), and remote wipe features are used to protect devices [27].

Cloud Security: Implement CIS benchmarks, enable detail logging, Cloud Security Posture Management (CSPM), and Cloud Access Security Broker (CASB) are use to secure cloud [28][58].

Monitoring and Detection: Endpoint Detection and Response (EDR)/Extended Detection and Response (XDR), Security Information and Event Management (SIEM), and User and Entity Behavior Analytics (UEBA) provides advanced monitoring and threat detection [35].

Data Loss Prevention (DLP)

Protects intellectual property and customer data [26]

5.7 Layer 7: Contingency Planning

Based on ISO 22301 [39] and NIST SP 800-34 [63]:

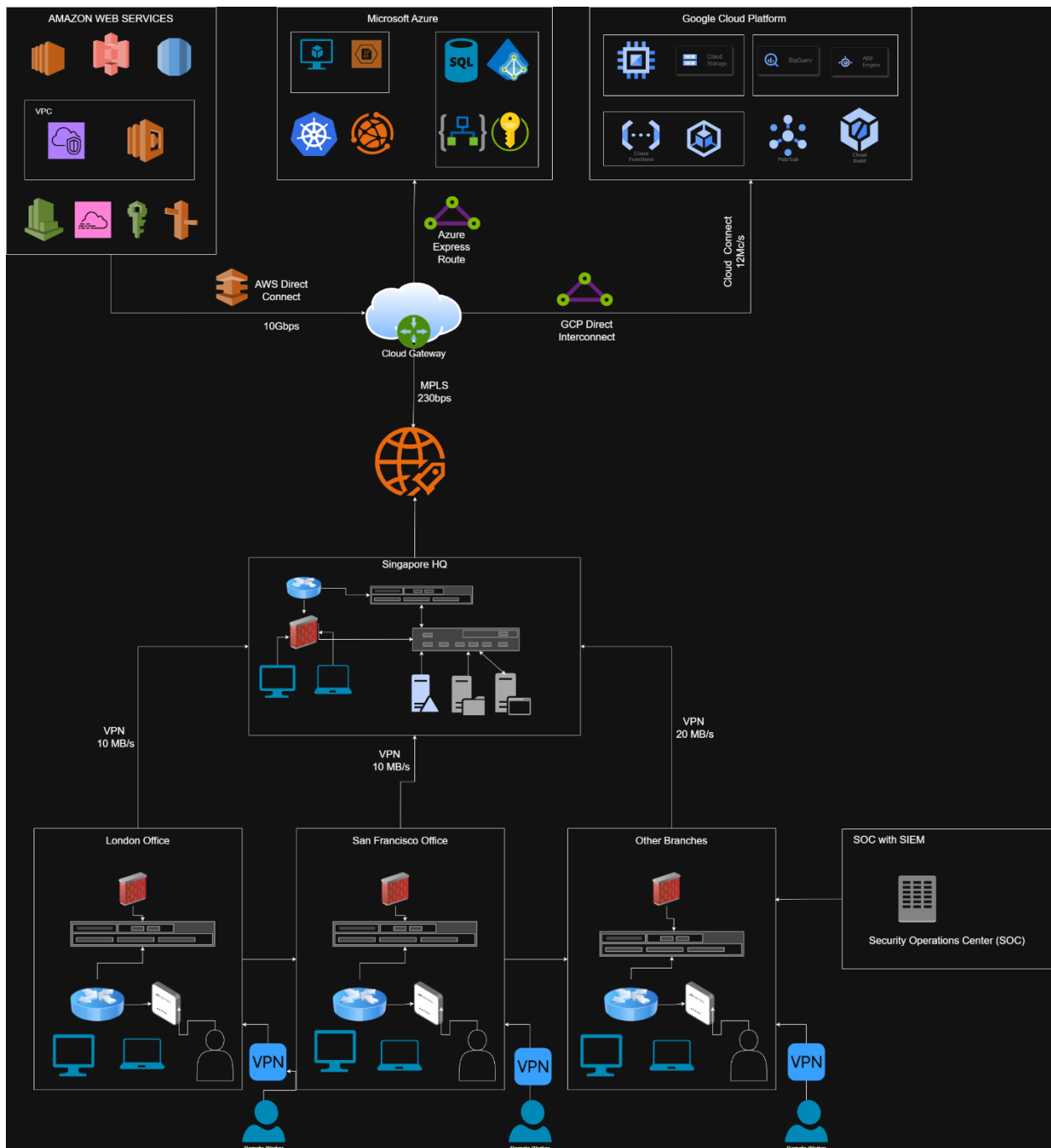
- **Business Impact Analysis (BIA)** with defined Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO) [39]
- **Disaster Recovery (DR) plan** with multi-region failover capabilities [28]
- **Incident Response** following NIST SP 800-61 [30]
- **Backup strategy** implementing the 3-2-1 rule (3 copies of data, 2 different media types, 1 offsite) [63]
- **Continuity of Operations Plan (COOP)** including redundant wireless controllers and cloud redundancy [38]

5.8 Layer 8: Service Level Agreements (SLAs)

Key components for vendor and internal service management:

- **Uptime guarantee** $\geq 99.9\%$ [40]
- **Incident response times:** Severity 1 incidents within 30 minutes based on ITIL 4 service management practices [10][11]
- **Supplier certifications:** ISO 27001, SOC 2, PCI DSS compliance required [41][42]
- **Log retention** ≥ 12 months for compliance and forensic purposes [35]
- **Data ownership and exit rights** under GDPR requirements [29]

Diagram:



6. Critical Analysis: Why Standards Need Continuous Updates

6.1 Evolving Threat Landscape

Cybersecurity threats evolve rapidly, requiring continuous framework updates:

- Cloud-focused attacks increased significantly according to recent threat intelligence reports [43]
- Credential theft and misconfiguration dominate breaches according to industry research [44]
- Ransomware tactics evolve monthly, with new variants and attack vectors emerging constantly [45]

These changes demand ongoing updates to frameworks to address emerging threat patterns and attack methodologies.

6.2 Technological Evolution

Technology advancement necessitates standard updates:

- Cloud-native architectures, serverless computing and container environments require new security controls not addressed in older frameworks [35]
- Zero Trust Architecture was introduced specifically because traditional perimeter-based security models failed in distributed environments [36]
- IoT, 5G and edge computing devices expand attack surfaces significantly, requiring updated guidance on securing these technologies [38]

6.3 Regulatory Developments

Legal and regulatory changes drive standard evolution:

- New GDPR enforcement guidelines and interpretations continue emerging [29]
- CCPA/CPRA interpretations expanded significantly between 2023–2025 [46]
- PIPL continues to introduce new cross-border data transfer restrictions [47]

ISO 27001:2022 itself was updated partly due to these regulatory developments and technological changes [48].

6.4 Case Studies

Case Study 1: Capital One (2019–2020)

A cloud firewall misconfiguration exposed over 100 million customer records, prompting major updates to cloud configuration management standards and emphasising the need for Cloud Security Posture Management (CSPM) tools [49].

Case Study 2: SolarWinds (2020–2021)

Software supply-chain exploitation affected thousands of organisations globally, forcing significant updates to NIST SP 800-161 and supply-chain security frameworks, including enhanced vendor assessment requirements [50].

Case Study 3: MOVEit (2023–2024)

Zero-day exploitation in file transfer software led to widespread data exposure across multiple organisations, highlighting the critical need for rapid vulnerability management, continuous monitoring and secure file transfer protocols [51].

These cases demonstrate that without continuous standard updates, organisations remain vulnerable to emerging attack vectors that exploit gaps in older frameworks.

7. Implementation Roadmap

7.1 24-Month Timeline

Phase 1 (Months 1–6): Foundation

- Establish governance structures, appoint CISO, create steering committee [14][15][62]
- Publish initial security policies [25]
- Deploy Multi-Factor Authentication (MFA) organisation-wide [26][52]
- Conduct initial risk assessment using ISO 27005 methodology [25][32]

Phase 2 (Months 7–12): Core Security

- Deploy Mobile Device Management (MDM) solution [27]
- Activate Security Information and Event Management (SIEM) platform [35]
- Implement network segmentation and deploy WPA3-Enterprise [38]
- Execute data classification project [29]

Phase 3 (Months 13–18): Advanced Controls

- Deploy Cloud Access Security Broker (CASB) [53]
- Implement Zero Trust Architecture principles [36]
- Deploy Privileged Access Management (PAM) solution [54]
- Establish continuous vulnerability scanning programme [54]
- Implement cloud configuration baselines using CIS benchmarks [58]

Phase 4 (Months 19–24): Optimisation

- Achieve ISO 27001 certification readiness [56]
- Conduct red-team testing exercises [55]
- Uplift Security Operations Centre (SOC) maturity [30][55]
- Implement continuous improvement processes

7.2 Budget Estimate

According to Gartner research, cybersecurity spending typically ranges from 7–12% of total IT budgets [59]. For an organisation of NG's scale and complexity, the following budget allocation is recommended based on industry benchmarks [59]:

Category	Cost Estimate (USD)
Governance & ISMS Development	\$150,000 – \$250,000
Cloud Security (CASB, CSPM)	\$350,000 – \$600,000
Identity & Access Management	\$200,000 – \$400,000
SIEM & SOC Operations	\$400,000 – \$700,000
MDM/BYOD Management	\$180,000 – \$350,000
Security Awareness Training	\$60,000 – \$120,000
ISO 27001 Certification	\$70,000 – \$150,000
Total Estimated Budget	\$1,410,000 – \$2,570,000

These estimates are based on industry-standard implementation costs for organisations with similar scale and complexity [59].

Diagram:



8. Conclusion

NatureGreen (NG) operates within a complex, wireless-dominant, cloud-centric and globally distributed environment, presenting extensive governance, compliance and cybersecurity challenges. The organisation's lack of structured policies, risk management processes, technical controls and compliance frameworks exposes it to substantial regulatory, operational and reputational risks. By adopting a comprehensive, integrated security framework combining ISO/IEC 27001:2022 [8], NIST CSF 2.0 [35], CIS Controls v8 [61], COBIT 2019 [62] and Zero Trust Architecture [36], NG can establish an auditable and resilient Information Security Management System (ISMS). The proposed multi-layered model enables NG to strengthen governance, improve risk-based decision-making, modernise technical controls, secure BYOD and cloud environments, and achieve cross-jurisdictional compliance with GDPR [18], CCPA/CPRA [19] and PIPL [47]. The inclusion of modern case studies SolarWinds [50], MOVEit [51] and Capital One [49] demonstrates that outdated standards and insufficient visibility can lead to catastrophic breaches, reinforcing the importance of continuous updates to cybersecurity frameworks. The phased 24-month roadmap and supporting budget provide NG with a realistic pathway for transformation, ensuring sustainable maturity development across governance, operations and technology. By implementing the proposed solution, NG will transition from a reactive, fragmented security posture to a proactive, standards-aligned and globally compliant security ecosystem, enabling the organisation to protect its intellectual property, customer data and operational continuity against evolving cyber threats.

References

- [1] A. C. Ijeh, A. J. Brimicombe, D. S. Preston, and C. O. Imafidon, "Security Measures in Wired and Wireless Networks," in Third International Symposium on Innovation and Information and Communication Technology (ISIICT 2009), Amman, Jordan, Dec. 2009, pp. 113–121. doi: 10.14236/ewic/ISIICT2009.10
- [2] C. Reyes and C. Mendoza, "Exploring the Impact of Shared Responsibility Models on Cloud Security Posture and Vulnerability Management," *Journal of Emerging Technologies*, Apr. 2023, pp. 2–15
- [3] T. A. M. Aljuaid, A. W. A. Wahab, and M. Y. I. Idris, "Systematic Literature Review on Security Access Control Policies and Techniques Based on Privacy Requirements in a BYOD Environment: State of the Art and Future Directions," *Applied Sciences*, vol. 13, no. 14, p. 8048, Jul. 2023. doi: 10.3390/app13148048.
- [4] S. B. Maynard, T. Tan, A. Ahmad, and T. Ruighaver, "Towards a Framework for Strategic Security Context in Information Security Governance," *Pacific Asia Journal of the Association for Information Systems*, vol. 10, no. 4, pp. 65–88, 2018.
- [5] S. K. Adabala, "Ensuring Compliance with Data Privacy Regulations in Global HR Operations," *International Journal of Innovative Research and Creative Technology*, vol. 8, no. 1, pp. 284–290, Feb. 2022.
- [6] A. C. Ijeh, A. J. Brimicombe, D. S. Preston, and C. O. Imafidon, "Security Measures in Wired and Wireless Networks," in *Proceedings of the Information Society 12th International Multi-Conference*, Ljubljana, Slovenia, Dec. 2009.
- [7] C. Mavani, H. K. Mistry, R. Patel, and A. Goswami, "The Role of Cybersecurity in Protecting Intellectual Property," *International Journal on Recent and Innovation Trends in Computing and Communication*, vol. 12, no. 2, pp. 240–258, Feb. 2024.
- [8] ISO, "ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection Information security management systems Requirements," ISO, Oct. 2022.
- [9] R. da S. Leme, J. de S. Pinto, L. G. Zanon and R. Anholon, "Management of enterprise cyber security A review of ISO/IEC 27001:2022," *ResearchGate (Request PDF)*, 2022/2024.
- [10] AXELOS, "Reader's manual: ITIL 4 practice guide," AXELOS resource hub.
- [11] "Information Security Management in an ITIL 4 world," *Invigate / ITIL resources*, blog and practice summaries.
- [12] NIST, "The NIST Cybersecurity Framework (CSF) 2.0," NIST CSWP 29, Feb. 26, 2024.

- [13] A. (various), "A high-level comparison between the NIST Cyber Security Framework and the ISO 27001 information security standard," ResearchGate, 2019
- [14] C. A. Ramezan, "Understanding the chief information security officer: Qualifications and responsibilities for cybersecurity leadership," *Computers & Security*, vol. 151, Feb. 2025. doi: 10.1016/j.cose.2025.104164
- [15] ISACA, "The Role of the CISO and the Digital Security Landscape," *ISACA Journal*, vol. 2, 2019.
- [16] Australian Cyber Security Centre, "Guidelines for cyber security roles - Chief Information Security Officer," Australian Government Information Security Manual, Mar. 2025.
- [17] I. Shakeel, "Information Security Governance Guide For the CISO," *CISO MAG*, May 2021.
- [18] European Parliament and Council, "Regulation (EU) 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)," *Official Journal of the European Union*, Apr. 2016
- [19] California Legislative Information, "California Consumer Privacy Act (CCPA)," Civil Code Section 1798.100-1798.199
- [20] G. Greenleaf, "Global Data Privacy Laws 2017: 120 National Data Privacy Laws, Including Indonesia and Turkey," *Privacy Laws & Business International Report*, 2017
- [21] PCI Security Standards Council, "Official PCI Security Standards Council Site"
- [22] ISO, "ISO/IEC 27001 Information Security Management
- [23] AICPA, "SOC 2 Reporting"
- [24] D. Chen and H. Zhao, "Data Security and Privacy Protection Issues in Cloud Computing," *International Conference on Computer Science and Electronics Engineering*, pp. 647-651, 2012
- [25] ISO/IEC 27001:2022 <https://www.iso.org/standard/82875.html>
- [26] NIST SP 800-53 Rev.5 <https://csrc.nist.gov/pubs/sp/800/53/r5/final>
- [27] <https://www.ncsc.gov.uk/collection/device-security-guidance/bring-your-own-device>
- [28] AWS Shared Responsibility Model <https://aws.amazon.com/compliance/shared-responsibility-model/>

- [29] GDPR (EU Regulation 2016/679) <https://eur-lex.europa.eu/eli/reg/2016/679/oj>
- [30] NIST SP 800-61 Rev.2 Incident Handling PDF
<https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf>
- [31] <https://hightable.io/iso-27001-supplier-security-policy/>
- [32] ISO/IEC 27005:2022 <https://www.iso.org/standard/80585.html>
- [33] <https://csrc.nist.gov/pubs/sp/800/30/r1/final>
- [34] <https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-137.pdf>
- [35] <https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf>
- [36] NIST SP 800-207 <https://csrc.nist.gov/pubs/sp/800/207/final>
- [37] csrc.nist.gov/pubs/sp/800/175/b/r1/final
- [38] <https://www.cyber.gov.au/business-government/asds-cyber-security-frameworks/ism/cybersecurity-guidelines/guidelines-for-networking>
- [39] ISO 22301:2019 <https://www.iso.org/standard/75106.html>
- [40] AWS SLA <https://aws.amazon.com/legal/service-level-agreements/>
- [41] SOC 2 Trust Services Criteria <https://www.aicpa-cima.com/resources/download/trust-services-criteria>
- [42] PCI DSS v4.0 https://docs-prv.pcisecuritystandards.org/PCI%20DSS/Standard/PCI-DSS-v4_0.pdf
- [43] IBM Security, “X-Force Threat Intelligence Index 2025.”
- [44] Verizon, “Data Breach Investigations Report (DBIR) 2025.”
- [45] ENISA, “Threat Landscape Report 2024–2025.”
- [46] California Privacy Protection Agency (CPPA), CCPA/CPRA Enforcement Updates.
- [47] <https://www.lawinfochina.com/display.aspx?id=42844&lib=law>
- [48] <https://www.bsigroup.com/en-GB/insights-and-media/insights/blogs/transition-to-the-iso-iec-27001-2022-standard/>
- [49] <https://www.jdsupra.com/legalnews/regulatory-implications-from-2019-7766499/>

- [50] <https://www.ncsc.gov.uk/collection/ncsc-annual-review-2021/the-threat/solarwinds>
- [51] <https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-317a>
- [52] <https://pages.nist.gov/800-63-4/>
- [53] <https://www.gartner.com/en/information-technology/glossary/cloud-access-security-brokers-casbs>
- [54] CISA Vulnerability Management <https://www.cisa.gov/known-exploited-vulnerabilities>
- [55] MITRE ATT&CK <https://attack.mitre.org>
- [56] <https://evalian.co.uk/transition-to-iso-270012022/>
- [57] <https://pages.nist.gov/800-63-3/>
- [58] <https://www.cisecurity.org/cis-benchmarks>
- [59] <https://www.gartner.com/en/newsroom/press-releases/2024-08-28-gartner-forecasts-global-information-security-spending-to-grow-15-percent-in-2025>
- [60] <https://www.nist.gov/itl/applied-cybersecurity/nice>
- [61] Center for Internet Security (CIS). “CIS Critical Security Controls v8.”
- [62] ISACA. “COBIT 2019 Framework: Governance and Management Objectives.”