Module: Data Security, Governance and Compliance
Module Code: ACCA7028

Submitted To:
Dr. Carlene Campbell
Associate Professor
University of Wales Trinity Saint David

Submitted By:
MD. Eyamin Molla
Student ID: 2425028
University Of Wales Trinity Saint David

Table of Contents

Introduction 3

1. Research into Security Frameworks and Models 3
   1.1 Information Technology Infrastructure Library (ITIL) 3
   1.2 ISO/IEC 27000 Family 4
   1.3 Comparison of ITIL and ISO/IEC 27001 5

2. Designing a Security, Governance, and Compliance Approach for NatureGreen 5
   2.1 Overview of the Proposed Approach 5
   2.2 Governance Structure 6
   2.3 Information Security Management System (ISMS). 7
   2.4 Technological and Operational Controls. 8
   2.5 Data Protection and Intellectual Property Security 9
   2.6 Compliance and Continuous Improvement. 10

3. Why Continuous Updates Are Necessary in Practice 11
   3.1 Compliance, Laws, and Ethics 12
   3.2 Governance and Strategic Planning for Security 13
   3.3 Security Policies 13
   3.4 Risk Management 14
   3.5 Security Management Models and Practices 14
   3.6 Contingency Planning 15
   3.7 Protection Mechanisms 16
   3.8 Service Level Agreements 16
   3.9 Critical Challenges and Trade-offs of Frequent Updates 16

Conclusion 17

References 18

Introduction

The increasing dependence on Internet-based technologies, cloud computing, and wireless networks has changed the way organisations are run and at the same time raised vulnerability to cyber threats as well as regulatory risks (Stallings, 2023). In multinational organisations like NatureGreen, information security, governance, and compliance have become vital organisational priorities because employees, customers, and partners access corporate resources remotely and on personal devices, which means that the digital ecosystems are highly interconnected (Whitman and Mattord, 2022). The result of the lack of formalised security framework may be disjointed controls, differing decision-making, and a higher susceptibility to data breaches, intellectual property theft, and reputational damages (von Solms and van Niekerk, 2019). It should be managed in systematic ways through recognised IT service management structures and information security structures. ITIL, ISO/IEC 27000, and other frameworks assist the organisations by aligning the security controls with business goals and by ensuring confidentiality, integrity, and availability of information assets (ISO, 2022). This chapter analyses the major security frameworks and uses their concepts to develop a customized security, governance, and compliance strategy for NatureGreen.

1. Research into Security Frameworks and Models

1.1 Information Technology Infrastructure Library (ITIL)

ITIL is a popular IT service management tool that concentrates on integrating IT services with the business requirements using well-organized procedures and continuous enhancement (Axelos, 2020). ITIL is not a security framework, but the security aspect is integrated throughout service design, transition, operation, and continuous improvement of service. ITIL focuses on governance, risk management, and service value systems by making sure the security controls are aligned with the organisational goals and not working independently (Cartlidge et al., 2021). The information security management within ITIL is taken care of by policies, risk assessment, incident management, and change management. It is especially applicable to the case of NatureGreen, where cloud services and wireless connectivity prevail in the network infrastructure. ITIL promotes standardised management of security incidents, clearly assigned responsibilities, and well-organised change management, minimising the chance of errors in the configuration and unauthorised entry (Axelos, 2020).

1.2 ISO/IEC 27000 Family

The ISO/IEC 27000 is a series of internationally recognised standards that can be used to develop, deploy, support, and continually (continuously) enhance an Information Security Management System (ISMS) (ISO, 2022). The standard that is at the core of this family of certifiable standards is ISO/IEC 27001, and it is informed by a risk-based approach to information security. It asks organisations to determine information assets, risk analysis and appropriate controls whether people, processes, or technology (Humphreys, 2018).

One of the strengths of ISO/IEC 27001 is that it provides an in-depth coverage of the governance, compliance and operational security. The domains of control identified in the annex A of the standard include access control, cryptography, supplier relationship, mobile device management, and incident response. The mentioned controls can be directly applied to the issues that NatureGreen has to deal with through bring-your-own-device (BYOD), the use of clouds, and access to data worldwide (ISO, 2022).

Fig 01: ISO/IEC 27001 Compliance Lifecycle for Information Security Management Systems (ISMS).

1.3 Comparison of ITIL and ISO/IEC 27001

Although ITIL is based on service management and operational efficiency, ISO/IEC 27001 offers specific security controls and compliance mechanisms (Peltier, 2016). ITIL is process-based basedNew and ITIL supports governance by supporting service lifecycle management as opposed to ISO/IEC 27001, which is control-based and focuses on risk assessment and constant security enhancement. These frameworks provide a comprehensive strategy when unified, which incorporates governance, operations management, and technical security (Whitman and Mattord, 2022). In the case of NatureGreen, both frameworks can be used to ensure that security is integrated into the everyday IT processes, and at the same time, regulatory requirements and safeguarding of sensitive information resources.

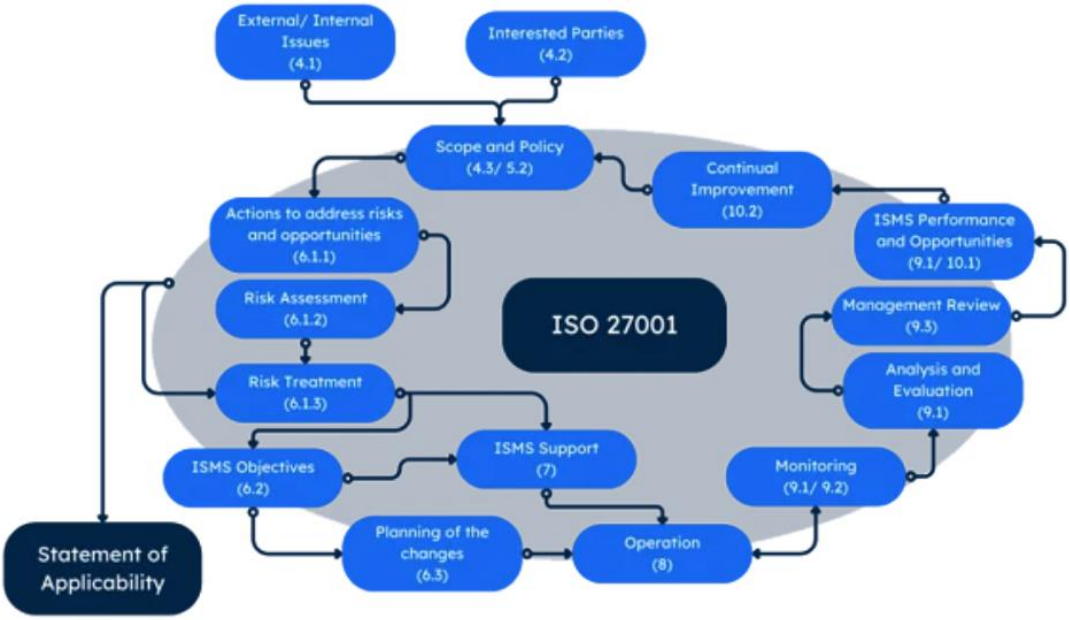


Fig 02: ISO/IEC 27001 – ISMS (Information Security Management System) Framework Diagram.

2. Designing a Security, Governance, and Compliance Approach for NatureGreen.

2.1 Overview of the Proposed Approach

An Overview of the Proposed Approach. In the case in question, the researcher will utilize several techniques to ensure that the risk factors are identified and mitigated.

NatureGreen is proposed to use a hybrid framework based on the analysis of ITIL and ISO/IEC 27001. The practice is a combination of the service management framework of ITIL with risk-based security measures of ISO/IEC 27001. The aim is to develop a single model of security governance that accommodates cloud usage, wireless infrastructure, BYOD access, data protection, and intellectual property security (von Solms and van Niekerk, 2019).

```
Business Objectives
        ↓
Security Governance
        ↓
ISO/IEC 27001 ISMS (Risk-Based Controls)
        ↓
ITIL Processes (Incident, Change, Access)
        ↓
Continuous Monitoring & Improvement
```

Fig 03: Model of NatureGreen Hybrid Security

2.2 Governance Structure

There should be a clear governance framework that would make the existing messy security environment at NatureGreen orderly. It is important that senior management develops an Information Security Steering Committee that will play a role in overseeing information security, approving policies, as well as aligning strategies. The security decisions of NatureGreen are complicated due to their vast international presence, cloud implementation, wireless network, and the usage of personal devices (Weill and Ross, 2004). Studies conducted on ITIL and ISO/IEC 27001 show that no framework is adequate to manage such challenges singly. An integrated strategy allows NatureGreen to balance the goals of the security measures with the general business and execute efficient risk-based controls. Strengthening governance, introducing an ISMS, applying technical and operational controls, and focusing on unceasing improvement, NatureGreen could secure its information resources, guarantee that the rules are

followed, and the stakeholders will trust the organization in an ever-unfriendly online space (ISO, 2022).

Table 2: Proposed Security Governance Structure

Role	Key Responsibilities
Board of Directors	Strategic oversight and risk acceptance
Information Security Steering Committee	Policy approval and monitoring
Chief Information Security Officer	ISMS leadership and enforcement
IT Operations Manager	ITIL process implementation
Employees & Users	Policy compliance and awareness

2.3 Information Security Management System (ISMS).

An ISMS that NatureGreen must adopt is based on ISO/IEC 27001 to offer a more structured and auditable means of information security. The ISMS must involve identifying the assets, assessing the risks, treating the risk, and monitoring the risks. This makes sure that the security controls are commensurable to the risks that the organisation is exposed to (Humphreys, 2018). Seeing that personal devices are widely used, BYOD policy ought to be included into the ISMS. Such policy must require the encryption of the devices, robust authentication, ability to remote wipe and endpoint security software to safeguard the corporate information accessed via personal gadgets (Behl and Behl, 2017).

Fig 04: Diagram of the Organization Structure for Cyber Defense

2.4 Technological and Operational Controls.

The excessive use of wireless networks by NatureGreen necessitates the use of stringent network security controls. These must contain effective encryption measures, network division, and constant control to identify illegal usage (Stallings, 2023). Identity and access management, secure configuration baselines, and periodic security audits must also be used as a means of enforcing cloud security controls. These controls should be operationalised by use of ITIL processes like incident management and change management. Security incidents should undergo a specified lifecycle with quick containment, investigation, recovery and that modifications to systems should be assessed as to risk before implementation (Axelos, 2020).

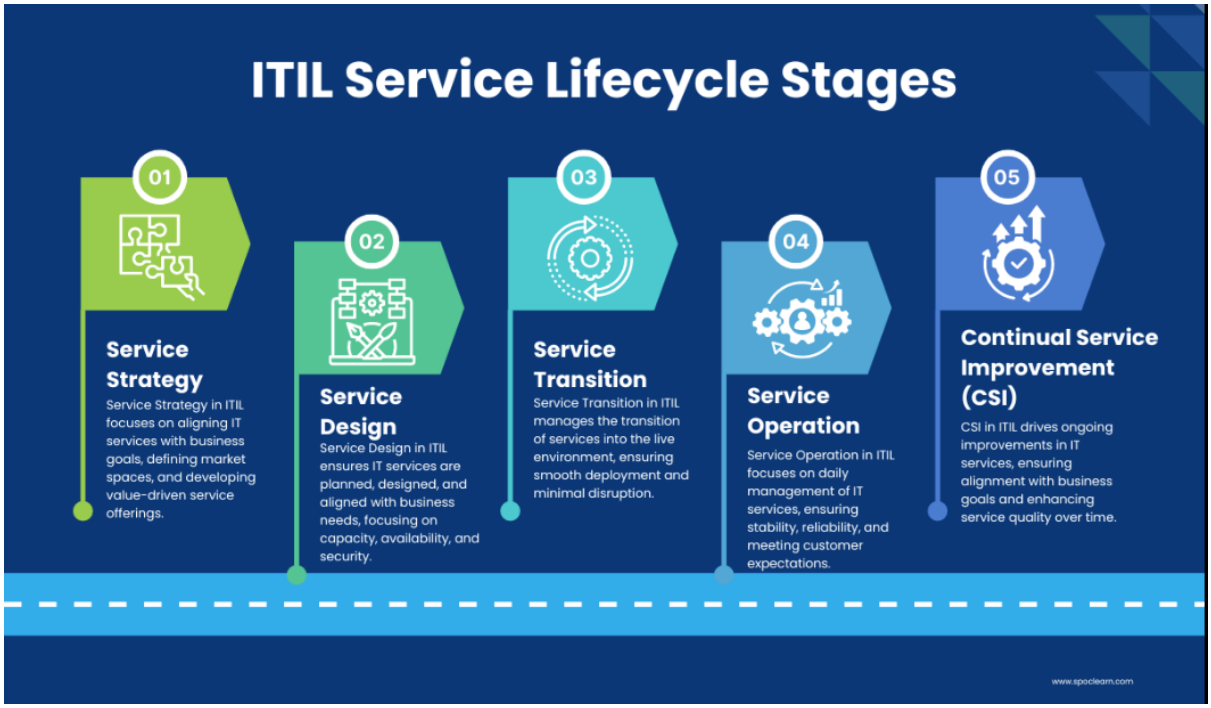


Fig 05: Diagram of the ITIL Service Lifecycle Stages

Table 3: Key Technical and Operational Controls

Area	Control Measures
Wireless Networks	Strong encryption, segmentation
Cloud Services	IAM, secure baselines
BYOD	Device encryption, MDM
Incident Management	Detection, response, recovery
Change Management	Risk assessment and approval

2.5 Data Protection and Intellectual Property Security

One of the central needs of NatureGreen is to protect customer records, employee information, and intellectual property. Data classification schemes must be brought in order to discriminate between the public, internal, confidential, and highly sensitive information. The levels of classification should then be imposed with access controls and encryption requirements (Peltier, 2016). The intellectual property, as a major financial asset of NatureGreen, must be secured by means of access control, digital rights management, and tracking of data-leaking attempts. Such actions minimize the insider threat and industrial spying (Whitman and Mattord, 2022).

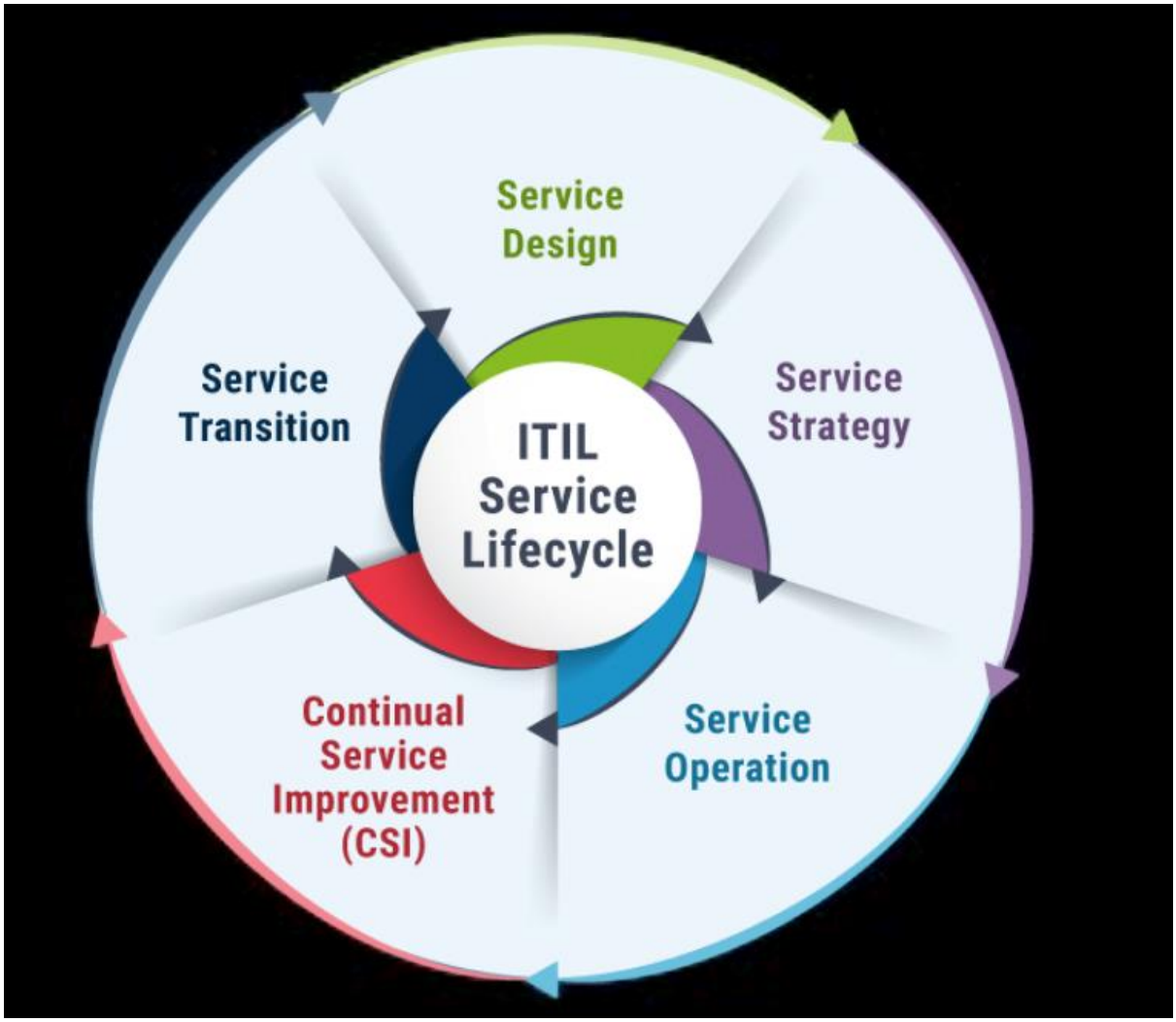


Fig 06: Diagram of the ITIL Service Lifecycle

2.6 Compliance and Continuous Improvement.

Adherence to the international data protection laws and the industry should be integrated into the security plan of NatureGreen. The ISO/IEC 27001 requires frequent internal audits, risk assessment, or management reviews. The model of continuous improvement of services provided by ITIL can assist in continuous assessment and optimization of the security process (Cartlidge et al., 2021). Security awareness training is also necessary so that employees would be aware of their duties and the threats of using personal devices and communicating on social media. Human factors are still among the most important sources of security violations, so training is an essential measure of control (Behl and Behl, 2017).

3. Why Continuous Updates Are Necessary in Practice

The main cause of constant changes in regulatory and standards is that cyber risk does not remain the same. The attackers swiftly keep up with the defensive strategies, and they use new systems as organisations migrate to cloud services, mobile work, Internet of Things, and AI-powered workflows (Stallings, 2023). The lack of evolution of standards often serves to preserve the infrastructure of yesterday, so gaps occur in current settings like identity-based access, cloud misconfiguration, and third-party software supply chain (NIST, 2024). Revised standards serve as a process of institutional learning in any industry: significant incidents unveil shared failures, and changes translate the lessons into better control expectations, audit advice, and baseline practices (ENISA, 2023). Most importantly, changes in society in the shape of expectations cause updates too. The customers and employees demand more privacy-by-design, safe access to mobile devices, clarity regarding the use of the data, and responsibility when violations take place (ICO, 2023). To react against these expectations, regulations are used to clarify the meaning of personal data, notification of breaches, cross-border transfers, and governing roles. In the multinational setting, such as that of NatureGreen, revised legal frameworks influence the data flow between jurisdictions, the consent mechanism, and the fact that security controls will have to be demonstrated in audits (European Parliament and Council, 2016). Unless it is continuously aligned, organisations may end up having legal non-compliance regardless of their own reasonable technical security by older standards.

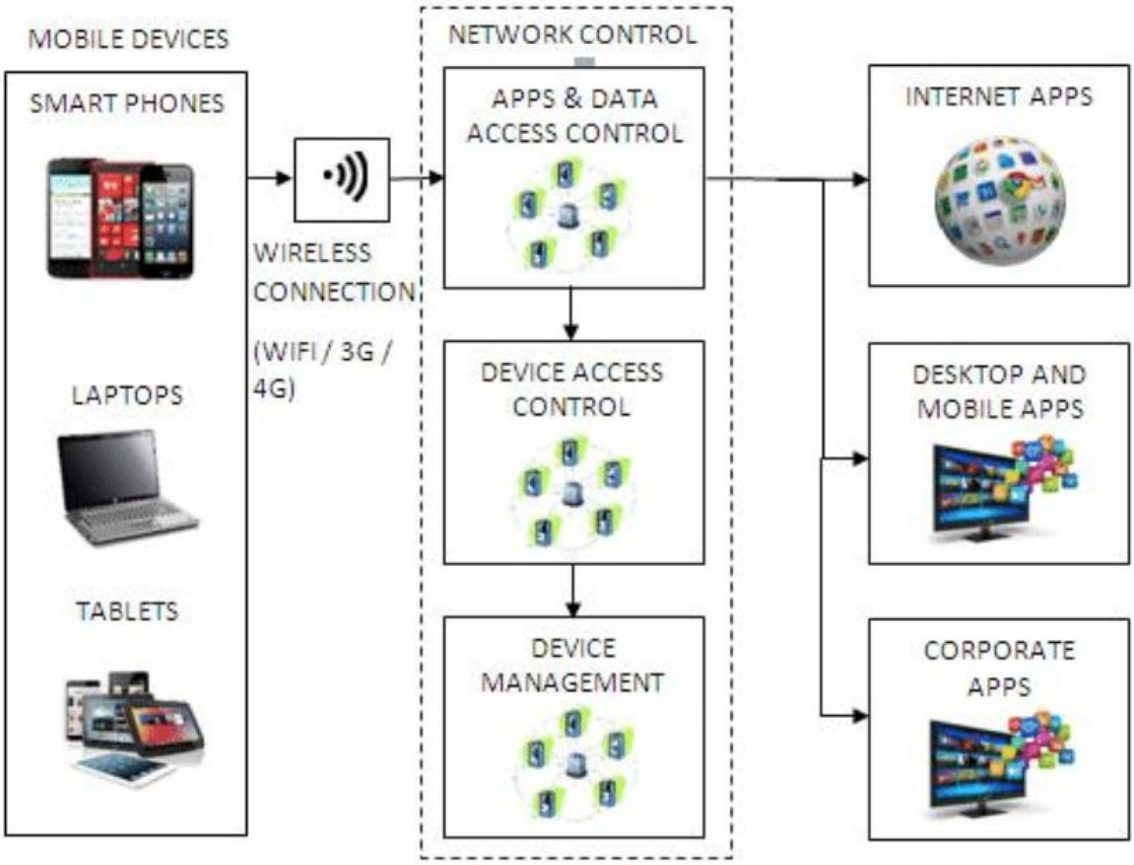


Fig 07: Architecture Diagram for Mobile Device Management (MDM) and Enterprise Mobility Management (EMM).

3.1 Compliance, Laws, and Ethics

Regulatory changes enhance compliance by eliminating grey areas and minimizing cases of inconsistent interpretations. Previously established regulatory documents permit a wide-ranging reasonable security claim, whereas the current revisions are more specific about governance obligations, reporting schedules, and provider and vendor responsibility (European Parliament and Council, 2016). This is relevant since ambiguity will generate preferential treatment towards underinvestment: since organisations can claim that they acted reasonably, this allows them to defer costly reforms until a breach occurs. New policies bring the minimum expectations more precise and less appealing to consider security as a secondary issue (ICO, 2023). Continuous updates also indicate changing norms of harm, ethically. The case in point is that mobile-first workplaces and BYOD impose new ethical obligations on employers: they have to ensure that employees do not intercept corporate data on their personal devices at the same time as ensuring corporate assets are not compromised, and imposing strict policy limits and technical constraints is less invasive than full-scale surveillance (Whitman and Mattord,

2022). Compliance should, therefore, be treated by organisations as a floor rather than a ceiling, and to go beyond the minimum in case the harm is high through risk management (Power, 2021).

3.2 Governance and Strategic Planning for Security

Staying pertinent standards are useful as they advance security to a new level beyond a technical issue to a governance one. A number of modern frameworks also mandate leadership, risk ownership, and decisional structure, which is the opposite of the typical failure mode in which IT is assigned security but lacks the authority or budget to do so (Weill and Ross, 2004). In the case of NatureGreen, where everything is in disarray, updates are especially useful since they create the recognised reference point to establish governance: who is authorising policy, who is accepting risk, who is making sure audits are completed, and controlling how security is performed. Good practice is not simply a matter of updating because the standard has changed, but applying governance to prioritise changes among exposure of threats, importance of business, and quantifiable benefits, such as fewer incidents or fewer privileged access (ISO, 2022).

3.3 Security Policies

Recent changes in regulations and standards enhance security policies and ensure that they are periodically reviewed and adapted to the present-day practice. Policies are the artefacts that are usually outdated since they indicate assumptions regarding gadgets, networks, and roles that evolve with time. In the case of wireless and BYOD reality at NatureGreen, policy should deal with mobile device management, authentication requirements, acceptable use, data classification, encryption expectations, and incident reporting requirements (Behl and Behl, 2017). Excessively complicated policies lower compliance and promote workarounds, especially in busy business fields such as customer service and marketing teams operating social media accounts (Power, 2021). Importantly, the policies should be put into practicality through training, equipping, and implementation. Strong authentication is just another meaningless policy that lacks identity systems capable of implementing it over cloud services and user experience designs that can reduce friction (NIST, 2024).

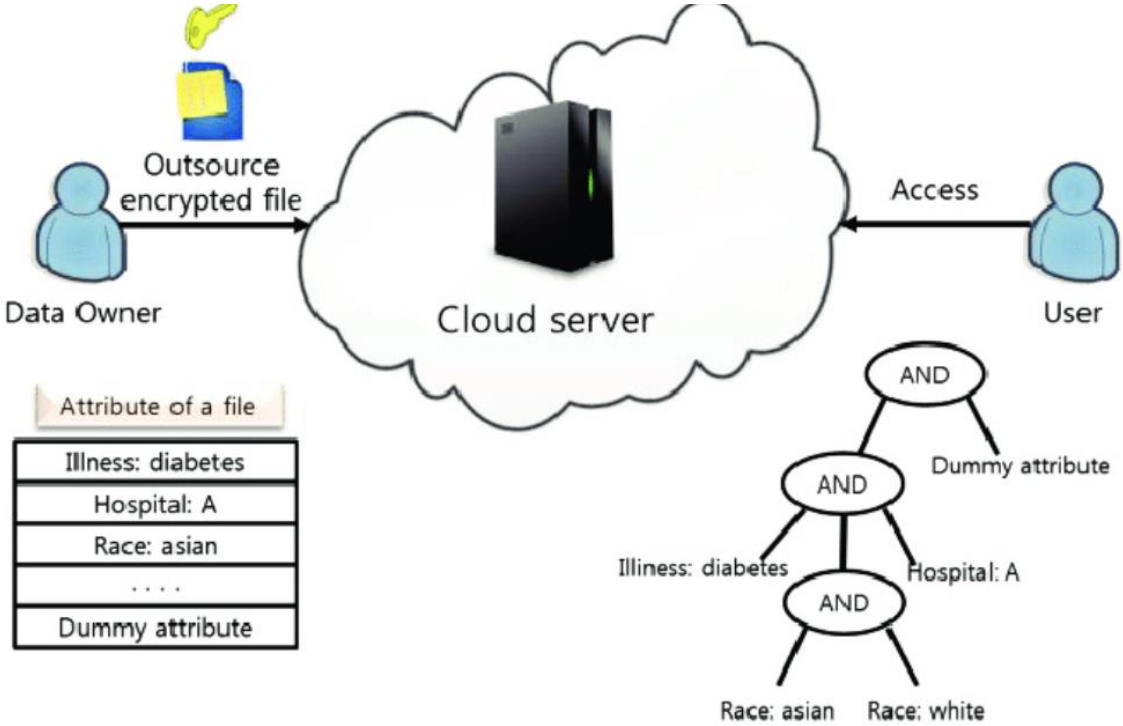


Fig 08: Cloud security diagram for attribute-based encryption (ABE) and attribute-based access control (ABAC).

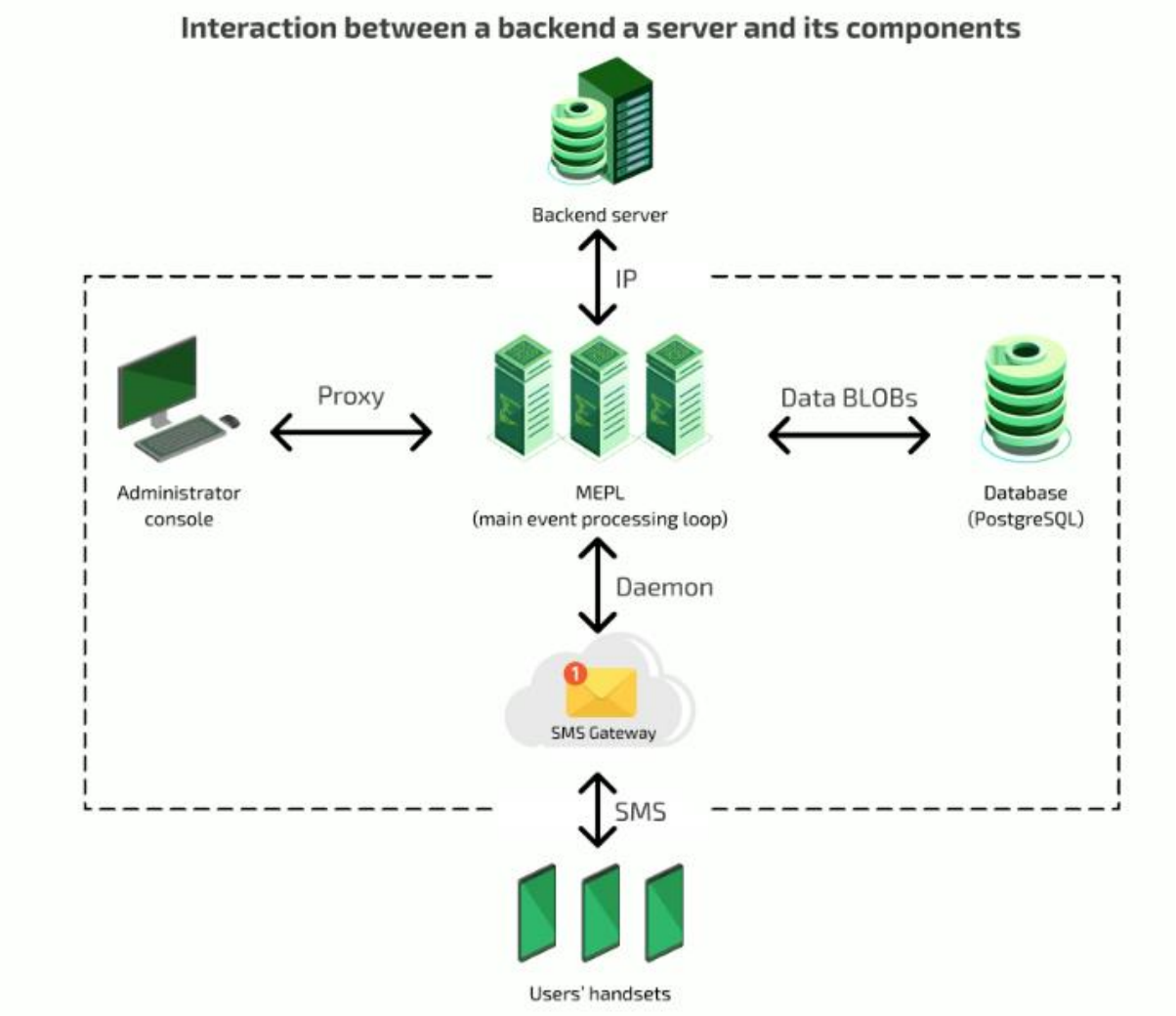
3.4 Risk Management

The most powerful case in favor of the ongoing updating of standards is that the updated standards enhance better risk management by updating the control base to suit new risks. Risk management involves the identification of assets, threats, vulnerabilities, and impacts and a selection of controls that reduce the risk to manageable levels. In case of the standards update, new categories of risks are frequently added, and they include cloud shared-responsibility failures, ransomware operational impacts, and supply-chain compromise (ENISA, 2023). Newer guidance is placing more focus on continuity and resilience and incident response maturity, instead of a one-off assessment (NIST, 2024). The weakness is that risk models will turn into a bureaucratic process when updates are considered a checklist. Best practices include adding new control requirements in risk registers, linking them to business services, and tracking the leading indicators, including patch latency, phishing resilience, and number of privileged access (ISO, 2022).

3.5 Security Management Models and Practices.

Updates in security management models are advantageous since they promote continuous enhancement, quantification, and adjustment. The trend of modern standards tends to

encourage the process of planning, implementation, monitoring, and improvement, which is consistent with the notion that security is a process rather than a product (ISO, 2022). The generic standard might not give priority to the controls that will benefit most to the nature of the organisation, including good identity governance, IP data loss prevention, and wireless network segmentation (Stallings, 2023). As a rule of thumb, one can consider using standards as a reference and subsequently customize by threat modelling and criticality of assets, as such that compliance alignment does not substitute security effectiveness (Power, 2021).



3.6 Contingency Planning

New standards and regulations address resilience and contingency planning as necessary ones. This is a healthy practice as the query has been transformed into, that is, can we prevent all breaches, and then, how fast we can contain, recover, and keep delivering essential services (ENISA, 2023). Newer standards tend to call toward tabletop exercises, technical recovery exercises, and lessons-learned loops to demonstrate operational preparedness (NIST, 2024). In the case of NatureGreen, frequent incident simulations would be particularly useful as it has a

very large online presence and social media coverage, the reputational damage in the case of which may spread rapidly. The cost and disruption are the limitations, but the price of failure to test can be devastating in case an event happens, and the teams realize that their assumptions were mistaken (Whitman and Mattord, 2022).

3.7 Protection Mechanisms

Mechanisms of protection should be upgraded since the attacker follows the weakest layer. Recent standards stimulate the implementation of current controls, including multi-factor authentication, zero-trust access principles, default encryption, the idea of constant protection of the endpoints, and the enhancement of logging and monitoring (NIST, 2024). One critical solution is to introduce new mechanisms under the change management discipline: pilot, measure impact, train users, and monitor adoption (Axelos, 2020). In the case of the BYOD environment that NatureGreen is implementing, new protections must prioritize the least invasive yet effective solutions, including containerisation, mobile device control with privacy protection, conditional access, and effective identity governance (Behl and Behl, 2017).

3.8 Service Level Agreements

New rules and guidelines enhance SLAs because what vendors should assure, and what evidence they should present, are defined anew. In cloud-heavy environments, there is distributed responsibility. In case the SLAs are obsolete, they might not address the most important aspects, including the timeframes of incident notification, forensic support, audit rights, data location requirements, subcontractor controls, and recovery objectives (ISO, 2022). However, a good practice to integrate revised SLA requirements with supplier assurance: third-party risk assessment, regular reviews, compliance reports, and shared incident exercises among critical vendors (ENISA, 2023).

3.9 Critical Challenges and Trade-offs of Frequent Updates

Constant updates are a good principle, but they pose actual difficulties. To begin with, regulatory overload may afflict organisations that have to work in more than one jurisdiction and need to balance between competing requirements and create voluminous paperwork (European Parliament and Council, 2016). Second, constant change may cause security fatigue in employees and make them less compliant and more inclined to informal workarounds (Power, 2021). Third, these speedy updates can expand the difference between large companies

and smaller vendors that are unable to match the rapidity, and this can give rise to a systemic vulnerability in supply chains. One radical response would be to take an outcomes-driven position: use standards as a guide but focus more on controls that limit risk in a significant way. Mature governance assists in mapping the requirements to business services, establishing a realistic roadmap and assessing performance against paperwork volume (Weill and Ross, 2004).

Conclusion

This report has demonstrated that effective information security for NatureGreen requires a structured, risk-based, and continuously evolving approach. As shown in this report, successful information security of NatureGreen must be an organised, risk-based, and constantly changing process. With the adoption of acknowledged models, powerful governance, and the constant provision of updates to the regulations and standards, as well as controls, the organisation is able to respond to the emergent threats, legal compliance, and ethical adherence, and high-value data and intellectual property security. Ensuring that resilience, trust, and long-term sustainability of the organisation is maintained by continuous improvement is crucial.

References

Axelos (2019) *ITIL Foundation: ITIL 4 Edition*. London: TSO (The Stationery Office). Available at: https://www.axelos.com/best-practice-solutions/itil (Accessed: 28 December 2025).

Behl, A. and Behl, K. (2017) 'An analysis of cloud computing security issues', *Journal of Information Security and Applications*, 36, pp. 1–8. Available at: https://www.sciencedirect.com/science/article/pii/S2214212617301110 (Accessed: 28 December 2025).

Center for Internet Security (CIS) (2024) *CIS Critical Security Controls Version 8.1*. Available at: https://www.cisecurity.org/controls/v8-1 (Accessed: 28 December 2025). CIS

Center for Internet Security (CIS) (2021) *CIS Critical Security Controls Version 8*. Available at: https://www.cisecurity.org/controls/v8 (Accessed: 28 December 2025). CIS

Cloud Security Alliance (2024) *Cloud Controls Matrix (CCM) and CAIQ v4*. Available at: https://cloudsecurityalliance.org/artifacts/cloud-controls-matrix-v4 (Accessed: 28 December 2025). Cloud Security Alliance

Cloud Security Alliance (2025) *Cloud Controls Matrix (CCM) Research Page*. Available at: https://cloudsecurityalliance.org/research/cloud-controls-matrix (Accessed: 28 December 2025). Cloud Security Alliance

European Parliament and Council of the European Union (2016) *Regulation (EU) 2016/679 (General Data Protection Regulation)*. Available at: https://eur-lex.europa.eu/eli/reg/2016/679/oj (Accessed: 28 December 2025).

ENISA (2024) *ENISA Threat Landscape 2024*. Available at: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024 (Accessed: 28 December 2025). enisa.europa.eu

ENISA (2024) *ENISA Threat Landscape 2024 (PDF)*. Available at: https://securitydelta.nl/media/com_hsd/report/690/document/ENISA-Threat-Landscape-2024.pdf (Accessed: 28 December 2025). securitydelta.nl

ENISA (2024) *2024 Report on the State of Cybersecurity in the Union (Condensed Version)*. Available at: https://www.enisa.europa.eu/sites/default/files/2024-11/2024%20Report%20on%20the%20State%20of%20Cybersecurity%20in%20the%20Union%20-%20Condensed%20version.pdf (Accessed: 28 December 2025). enisa.europa.eu

Humphreys, E. (2018) *Implementing the ISO/IEC 27001:2013 ISMS Standard*. 4th edn. Boston: Artech House. Available at: https://us.artechhouse.com/Implementing-the-ISO-IEC-27001-2013-ISMS-Standard-Fourth-Edition-P1917.aspx (Accessed: 28 December 2025).

Information Commissioner's Office (ICO) (2025) *Guide to the General Data Protection Regulation (UK GDPR)*. Available at: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/ (Accessed: 28 December 2025).

ISO (2022) *ISO/IEC 27001:2022 Information security management systems — Requirements*. Geneva: ISO. Available at: https://www.iso.org/standard/27001 (Accessed: 28 December 2025). iso.org

ISO (2022) *ISO/IEC 27002:2022 Information security controls*. Geneva: ISO. Available at: https://www.iso.org/standard/75652.html (Accessed: 28 December 2025). iso.org

ISO (2022) *ISO/IEC 27005:2022 Guidance on managing information security risks*. Geneva: ISO. Available at: https://www.iso.org/standard/80585.html (Accessed: 28 December 2025). iso.org

ISO (2018) *ISO 31000:2018 Risk management — Guidelines*. Geneva: ISO. Available at: https://www.iso.org/standard/65694.html (Accessed: 28 December 2025). iso.org

ISO (2019) *ISO 22301:2019 Business continuity management systems — Requirements*. Geneva: ISO. Available at: https://www.iso.org/standard/75106.html (Accessed: 28 December 2025). iso.org

ISACA (2025) *COBIT (Resource Centre)*. Available at: https://www.isaca.org/resources/cobit (Accessed: 28 December 2025). ISACA

NIST (2024) *The NIST Cybersecurity Framework (CSF) 2.0*. NIST CSWP 29. Available at: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf (Accessed: 28 December 2025). NIST Publications

NIST (2024) *Cybersecurity Framework (CSF) 2.0 Resource Center*. Available at: https://www.nist.gov/cyberframework (Accessed: 28 December 2025). NIST

NIST (2020) *Security and Privacy Controls for Information Systems and Organizations (SP 800-53 Rev. 5)*. Available at: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf (Accessed: 28 December 2025). NIST Publications

NIST (2025) *Computer Security Incident Handling Guide (SP 800-61 Rev. 3)*. Available at: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r3.pdf (Accessed: 28 December 2025). NIST Publications

NIST (2024) *CSF 2.0: Resource and Overview Guide (SP 1299)*. Available at: https://csrc.nist.gov/pubs/sp/1299/final (Accessed: 28 December 2025). NIST Computer Security Resource Center

NIST (2024) *CSF 2.0: Quick-Start Guide for Creating and Using Organisational Profiles (SP 1301)*. Available at: https://csrc.nist.gov/pubs/sp/1301/final (Accessed: 28 December 2025). OWASP Foundation

OWASP (2021) *OWASP Top 10: 2021*. Available at: https://owasp.org/Top10/2021/ (Accessed: 28 December 2025). OWASP Foundation

PCI Security Standards Council (2025) *PCI Security Standards Document Library*. Available at: https://www.pcisecuritystandards.org/document_library/ (Accessed: 28 December 2025). PCI Security Standards Council

Peltier, T.R. (2016) *Information Security Policies, Procedures, and Standards: Guidelines for Effective Information Security Management*. Boca Raton: CRC Press. Available at: https://www.routledge.com/Information-Security-Policies-Procedures-and-Standards-Guidelines-for-Effective/Peltier/p/book/9781439836953 (Accessed: 28 December 2025).

Stallings, W. (2023) *Effective Cybersecurity: A Guide to Using Best Practices and Standards*. Boston: Addison-Wesley. Available at: https://www.pearson.com/en-us/subject-catalog/p/effective-cybersecurity/P200000005683 (Accessed: 28 December 2025).

Verizon (2025) *2025 Data Breach Investigations Report (DBIR)*. Available at: https://www.verizon.com/business/resources/reports/dbir/ (Accessed: 28 December 2025). Verizon

Verizon (2025) *2025 Data Breach Investigations Report (PDF)*. Available at: https://www.verizon.com/business/resources/reports/2025-dbir-data-breach-investigations-report.pdf (Accessed: 28 December 2025). Verizon