

ACCA7028 Data Security, Governance and Compliance

Name: ONJON SUTRADHAR

ID: 2431963

MSc Data Science and Artificial Intelligence,
University of Wales Trinity Saint David

Contents

Abstract	2
1 Governance and Compliance	3
1.1 Initial Assessment and Direction	4
2 Policies Design (Zero Trust Microsoft)	5
2.1 Introducing Zero Trust as the Policy Foundation	5
2.2 Policy Areas Required for NG	6
3 Security Program	7
4 Risk Management	9
4.1 Understanding NG's Risk Landscape	9
4.2 Risk Assessment Approach	9
4.3 NG's Risk Register and Mitigation Framework	11
5 Protection Mechanism	12
5.1 Wireless Network Protection	12
5.1.1 Stronger Wireless Authentication	12
5.1.2 Network Segmentation	13
6 Ethics and Laws	14
7 Conclusion	15

Abstract

This report outlines how NatureGreen (NG), a global company with valuable intellectual property, can move from its current chaotic and unprotected state to a properly governed and well-secured environment. NG relies heavily on cloud systems, wireless networks, and personal devices, yet it lacks even the most basic security policies or governance practices.

To fix this, the report applies structured frameworks, simplified for practical use, and integrates Microsoft Zero Trust as the guiding philosophy. By combining governance, policy design, risk management, and strong protection mechanisms, NG can build a security program that is stable, modern, and able to adapt over time.

The goal is to help NG establish leadership-driven governance, define clear policies, implement layered protections, and align with ethical and legal expectations across its global operations.

1. Governance and Compliance

NatureGreen's (NG) most critical issue is the absence of governance, leaving high-value research data and sensitive customer information exposed. Governance is the method for directing and controlling security decisions. Effective governance begins when leadership acknowledges security as an organizational responsibility, which must be formalized through defined roles and decision-making structures.

Strong governance is built upon the ISO 27001 structure:

Clause 5 (Leadership): NG must establish a senior committee of executive leaders responsible for approving security policies, allocating resources, and ensuring alignment with business objectives, thereby establishing a clear chain of accountability. This corrects the current reliance on informal communication by mandating defined roles and formal approval of the security program.

Clause 6 (Planning): Introduces risk-based planning, which helps NG prioritize and manage its varied, multi-regional compliance obligations (e.g., data handling and breach reporting) as an integral part of security planning, not an afterthought.

Clause 7 (Support): Addresses NG's lack of competence and awareness by requiring mandatory employee training and clear understanding of responsibilities. This ensures governance extends to day-to-day behavior, crucial in an environment heavily utilizing cloud and wireless systems.

Clause 8 (Operation): Requires NG to plan and control all operational security processes, including access management, system monitoring, and enforcing secure configurations. This defines which security activities fall under NG's responsibility versus its cloud service providers.

Clause 9 (Performance Evaluation): Mandates monitoring and measurement to replace NG's current unreliable reporting, giving leaders accurate visibility into the security posture and the effectiveness of controls.

Clause 10 (Improvement): Reinforces the need for continual improvement—correcting weaknesses, reviewing incidents, and updating policies. This structured approach is essential for adapting to NG's rapidly changing cloud and wireless capabilities.[1] [2]

Compliance forms the second foundation. Because NG operates across multiple regions, it must adhere to various data protection requirements for personal and sensitive information. Compliance isn't just following rules; it requires integrating data protection into routine business practice and demonstrating responsible management through

regular assessments, documentation, and reporting.

Organizational structure is key. NG needs defined security leaders to translate governance decisions into daily operations. This structure must include personnel responsible for critical functions like cloud security, network management, monitoring, privacy, and incident response. Establishing this distribution of labor prevents reliance on informal, inconsistent processes.

Before making security decisions, NG must perform a comprehensive environmental assessment. This means understanding what data is held, how information flows across cloud and wireless networks, and which systems support essential business functions. This foundational understanding is necessary to establish a reliable governance model and prioritize immediate versus long-term protection needs.

1.1 Initial Assessment and Direction

The first step toward stability is a full assessment of the current situation. NG must understand:

- what data it holds,
- where that data is stored,
- how systems are accessed,
- how employees use devices,
- the vulnerabilities of the wireless network,
- the state of configurations in cloud services.

This assessment becomes the base for planning, letting the leadership prioritise which risks need immediate action and which can be addressed over time.

2. Policies Design (Zero Trust Microsoft)

NatureGreen cannot rely on outdated or informal rules to run its security operations. The company depends on cloud systems, wireless networks, and a large number of personal devices, all of which require clear and modern security policies. This chapter redesigns NG's policy environment using simplified language and the Microsoft Zero Trust framework as the central foundation.[3]

Microsoft Zero Trust is based on one core idea: never trust any user, device, network, or application by default. Instead, verify everything continuously. This approach is ideal for NG because it is cloud-first and heavily wireless, with users connecting from different devices and locations.

2.1 Introducing Zero Trust as the Policy Foundation

Zero Trust turns policy design into a practical and structured process. NG's policies must ensure that every access request—whether from a laptop, phone, or cloud application—is verified, limited, and monitored.

The key Zero Trust pillars NG should include in its policies are:

- **Identity verification:** Strong authentication such as MFA for all users.
- **Device compliance:** Only secure, updated, and registered devices can connect.
- **Least privilege access:** Users get only the access they need.
- **Network segmentation:** Wireless and cloud access separated into secure zones.
- **Data protection:** All sensitive information classified and monitored.
- **Continuous monitoring:** Access patterns checked constantly to detect anomalies.

Zero Trust does not replace existing standards, but it provides a practical structure that fits NG's environment better than generic high-level frameworks.[4][5]

2.2 Policy Areas Required for NG

NG needs formal, written policies covering all major security operations. The absence of such policies is the root cause of its disorder. These policies must be approved by leadership and enforced consistently.

The most important policy areas include:

- Acceptable use of systems and devices.
- Cloud service usage and configuration.
- Wireless network access rules.
- BYOD (Bring Your Own Device) guidelines.
- Data classification and handling rules.
- Access control and authentication.
- Device management (corporate and personal).
- Encryption rules for stored and transmitted data.
- Monitoring, logging, and audit processes.

NatureGreen (NG) must rebuild its security policy framework using Microsoft's Zero Trust model to unify inconsistent practices across its cloud-heavy, wireless, and device-diverse environment. Zero Trust verifies every access request, assuming no user or device is trusted by default.

Core Zero Trust Policies Identity: Policies must enforce Multi-Factor Authentication (MFA) and the principle of least privilege to mitigate the risk of compromised accounts.

Device: Require device compliance, ensuring only secure, registered, and up-to-date devices connect to corporate systems.

Network: Treat internal wireless networks with caution. Policies must mandate certificate-based authentication, encryption, and strict network segmentation.

Cloud: Require all cloud applications to follow secure configuration guidelines, use centralised identity management, and submit logs for monitoring.

BYOD: Personal device use must be conditional, requiring compliance with baseline requirements (e.g., encryption, MDM enrollment). Policies must protect corporate data on these devices using containerisation or remote wipe features.

Data: Implement a modern data classification policy (e.g., Confidential, Restricted) to define clear rules for access, storage, and sharing of sensitive information and intellectual property.

3. Security Program

A strong security program gives structure to the policies and governance decisions created earlier. For NatureGreen, this program must be practical enough to operate daily yet flexible enough to adapt when technology or business needs change. The most suitable structure is the Plan–Do–Check–Act (PDCA) cycle, which creates a continuous improvement loop. This means NG does not treat security as a one-off project but as an ongoing commitment that matures with time and experience.

The Plan phase sets the groundwork. NG must begin by building a clear picture of its systems, data, and business processes. This includes identifying what information must be protected, where it resides, how it moves between users and applications, and who is responsible for each part of the environment. Planning also involves creating formal documents such as policies, risk assessments, and security objectives that reflect NG’s priorities. With this understanding, the company can begin shaping controls that are realistic rather than theoretical.

The Do phase is where NG implements the technical and organisational controls defined during planning. This includes enforcing identity protections, securing the cloud environment, and improving wireless network configurations. NG must also roll out management tools such as mobile device management for controlling access from personal devices, and data loss prevention tools for monitoring sensitive information. Training programmes should also be established in this phase, giving employees the knowledge required to follow the new policies. Implementation must be coordinated to avoid disruption and ensure that each control aligns with Zero Trust principles.

The Check phase ensures NG does not rely on assumptions about its security posture. Instead, it uses audits, monitoring, and testing to determine whether the controls in place are functioning as expected. Logs from the cloud, wireless network, and endpoints provide real-time insight into user activity, access patterns, and possible attempts to bypass controls. Vulnerability scanning and penetration testing highlight misconfigurations or gaps that attackers could exploit. Reports generated during this phase should be presented to leadership, allowing them to stay informed and make decisions based on accurate visibility rather than guesswork. The Cloud Security Alliance Cloud Controls Matrix (CSA CCM) provides cloud-specific security controls that strengthen NG’s ISO 27001 framework by addressing risks unique to hosted environments. It clarifies shared responsibility between NG and its cloud providers, ensuring encryption, identity, logging, and configuration du-

ties are explicitly assigned. The CCM also supports continuous monitoring by offering detailed expectations for cloud governance and technical oversight. Integrating CCM ensures NG's cloud operations remain aligned with Zero Trust principles and industry best practices. [6]

The Act phase focuses on improvements. When the Check phase exposes weaknesses, NG must respond by updating processes, changing configurations, or enhancing training. This might include strengthening authentication rules, applying patches faster, rewriting unclear policies, or adding additional monitoring points. Over time, the Act phase ensures that NG's security program evolves naturally and intelligently instead of stagnating.

Surrounding the PDCA cycle is the need for operational discipline. NG requires reliable processes for incident response, change control, and asset management. Incident response plans must outline the exact steps to follow during a security event, including how incidents are detected, contained, and communicated. Change management ensures that updates to systems or cloud configurations do not inadvertently introduce new vulnerabilities. Asset management allows NG to track devices, software, and cloud applications as they enter or leave the environment, preventing blind spots that attackers could exploit.[7]

A mature security program blends technology, processes, and human behaviour. For NG, this programme represents a shift from reactive management to proactive defence, creating a stable environment that supports modern operations and reduces the likelihood of impactful security incidents.

4. Risk Management

Risk management is one of the most important components of NG's security approach. Without a structured way to identify and prioritise risks, the company cannot protect its most valuable assets, including customer data, employee information, research formulas, and intellectual property. Because NG operates in a cloud-first environment and relies on a mostly wireless infrastructure, risk levels are higher than in traditional on-premise organisations.[8]

This chapter explains how NG should identify risks, evaluate them, and assign controls to reduce their impact. The goal is not to eliminate all risks—no organisation can—but to manage them intelligently and consistently.

4.1 Understanding NG's Risk Landscape

NG faces several types of risks due to its current environment:

- lack of formal security policies,
- dependence on cloud services,
- a wireless network that covers nearly the entire company,
- employee demand for BYOD,
- handling of sensitive personal data,
- storage of high-value intellectual property.

Because these risks affect different assets and systems, NG must map out where its most sensitive information sits and how it is accessed. This forms the basis of a proper risk assessment.[9]

4.2 Risk Assessment Approach

The risk assessment process should include:

- **Asset Identification:** listing all critical data, services, systems, and devices,

- **Threat Identification:** identifying what can go wrong (e.g., unauthorised access, data leakage, misconfiguration),
- **Vulnerability Identification:** finding weaknesses that could allow threats to cause harm,
- **Risk Evaluation:** scoring risks based on likelihood and impact,
- **Risk Treatment:** determining how to reduce, avoid, transfer, or accept each risk.

4.3 NG's Risk Register and Mitigation Framework

Table 4.1: NatureGreen (NG) Risk Register and Mitigation Framework

Identified Risk	Affected Assets	Relevant Areas	Proposed Mitigation Control	Supporting Standards/Guidance
No established policies, company in disarray	Entire organization	Governance and leadership	Create and enforce core security policies and assign clear security roles	Internal governance frameworks
Heavy use of cloud services	Staff and client data, IP, service availability	Cloud governance, supplier management	Enforce cloud security controls, define provider responsibilities, monitor compliance	Cloud security best practices
Wireless network covers 95% of operations	All data transmitted over Wi-Fi	Network security	Apply strong encryption, authentication, and segmentation	Wireless security guidelines
Pressure for personal device usage (BYOD)	Staff and client data, network access	Remote working and endpoint security	Enforce device enrolment, apply MDM, restrict unmanaged devices	BYOD management practices
Protecting personal and client data	Sensitive personal information	Data privacy and storage	Enforce privacy rules, encrypt data, apply access control and audit logs	Data privacy principles
Protecting intellectual property worth billions	Research data, formulas, analytics	Data classification and IP security	Classify data, enforce strict access rules, monitor for data leakage	Information protection standards

5. Protection Mechanism

Protection mechanisms form the practical layer of NatureGreen’s security model. They turn policies and risk assessments into real safeguards that defend the organisation from threats. Because NG operates in a modern environment with cloud systems, extensive wireless networks, and personal devices, its protection strategy must combine several layers of defence. No single control is sufficient on its own; strength comes from combining technology, process, and user awareness into a coherent whole.

The first layer concerns identity. In a cloud-first business, identity becomes the new perimeter. NG must ensure that every login is based on verified user identity, strong authentication, and clear authorisation. Multi-factor authentication should be mandatory for all accounts, and privileged accounts require additional protections such as conditional access and continuous monitoring. Least privilege access must be enforced so that users interact only with the data and systems required for their roles. This reduces the likelihood of accidental misuse and limits the impact of compromised accounts.[10]

Device security forms the next layer. NG employees use a combination of corporate and personal devices, which creates an unpredictable environment. To regain control, the company must implement a device compliance model that checks whether a device is secure before allowing it to connect. Device encryption, updated software, secure configurations, and mobile device management enrolment become non-negotiable requirements. These controls ensure that even if a device is lost or stolen, corporate data remains protected.[2]

5.1 Wireless Network Protection

With 95% of NG’s network operating on Wi-Fi, the wireless environment must be one of the most secure parts of the company. Strong protections prevent attackers from intercepting or manipulating network traffic.

5.1.1 Stronger Wireless Authentication

NG must implement:

- WPA3-Enterprise encryption,

- IEEE 802.1X authentication,
- certificate-based EAP-TLS authentication for all employee devices.

These controls ensure that only authorised users and devices connect to the network.

5.1.2 Network Segmentation

The wireless network must be separated into zones:

- corporate network for trusted devices,
- BYOD network for registered personal devices,
- guest network with limited internet-only access,
- quarantine VLAN for non-compliant devices.

Segmentation limits the impact of compromised devices.

6. Ethics and Laws

Ethics and legal responsibility are essential components of NatureGreen’s security approach. While technical protections and governance structures create the framework for securing systems, the organisation must also operate with respect for the individuals whose data it handles. Ethical behaviour builds trust with customers, employees, partners, and regulators. For NG, this trust becomes especially important because the company manages sensitive personal information alongside high-value intellectual property.

Ethical data handling begins with transparency. Individuals should understand what information NG collects, why it is needed, and how long it will be kept. Being transparent helps prevent misuse and builds confidence that data is treated fairly. An ethical approach also requires limiting access to personal and sensitive information. Even within the organisation, not all employees should view all types of data. The principle of least privilege applies not only as a security measure but also as a reflection of respect for privacy.[1]

NG must also act responsibly when designing systems and selecting technologies. The organisation should prioritise solutions that minimise unnecessary data collection and reduce the chance of accidental exposure. When deploying monitoring tools, for example, NG must ensure that they are used only to support legitimate security and operational needs, not for invasive scrutiny of employee behaviour. This balance ensures that security practices reinforce ethical standards rather than undermine them.

The organisation must remain aware of cross-border data transfer restrictions as well. Since NG is cloud-first and distributes workloads globally, it must confirm that data stored in one region is processed in accordance with the laws of another. Contracts with cloud providers must specify responsibilities related to encryption, data residency, and deletion. By setting these expectations clearly, NG ensures that external partners meet the same ethical and legal standards that it imposes internally. [8] .

7. Conclusion

NatureGreen is currently operating in a risky environment due to a lack of governance, policies, and structured security practices. At the same time, it depends heavily on cloud services, wireless networks, and personal devices. This combination makes strong security essential for protecting customer data, employee information, and valuable intellectual property.

By implementing clear governance, adopting Microsoft Zero Trust, establishing structured policies, managing risks properly, and applying layered protection mechanisms, NG can transform from a disorganised organisation into a secure and resilient one. Continuous monitoring, improvement, and ethical behaviour ensure that security remains strong and aligned with both legal and moral responsibilities.

A well-designed security program is not just a defence—it is a long-term investment in trust, stability, and business success.

Bibliography

- [1] A. Cyber, “How to efficiently implement iso 27001 for cloud-based companies.” https://www.approach-cyber.com/wp-content/uploads/2025/02/iso_whitepaper_2022_0.pdf, 2025. Accessed: 2025-11.
- [2] C. for Internet Security, “Cis controls mapping to cloud security alliance cloud controls matrix.” <https://www.cisecurity.org/insights/white-papers/cis-controls-mapping-to-cloud-security-alliance-cloud-control-matrix>, 2023. Accessed: 2025-11.
- [3] Microsoft, “Zero trust strategy and architecture.” <https://www.microsoft.com/en-us/security/business/zero-trust>, 2025. Accessed: 2025-11.
- [4] Microsoft, “Zero trust guidance center.” <https://learn.microsoft.com/en-us/security/zero-trust/>, 2025. Accessed: 2025-11.
- [5] Microsoft, “Microsoft zero trust vision paper.” https://download.microsoft.com/download/f/9/2/f92129bc-0d6e-4b8e-a47b-288432bae68e/Zero_Trust_Vision_Paper_Final10.28.pdf, 2025. Accessed: 2025-11.
- [6] C. S. Alliance, “Cloud controls matrix v4.” <https://cloudsecurityalliance.org/artifacts/cloud-controls-matrix-v4>, 2024. Accessed: 2025-11.
- [7] C. S. Alliance, “Security guidance for critical areas of focus in cloud computing v4.0.” https://www.anskaffelser.no/sites/default/files/csa_security_guidance_v4.0.pdf, 2024. Accessed: 2025-11.
- [8] M. K. Khalil, M. Al Jahdhami, and V. Dattana, “Cloud storage security compliance: An analysis of standards and regulations,” *Journal of Student Research*, 2022. Accessed: 2025-11.
- [9] T. Group, “What is the cloud controls matrix?.” <https://cpl.thalesgroup.com/faq/data-security-cloud/what-cloud-controls-matrix>, 2025. Accessed: 2025-11.
- [10] Microsoft, “The microsoft zero trust assessment.” <https://techcommunity.microsoft.com/blog/microsoft-security-blog/>

the-microsoft-zero-trust-assessment-helping-you-operationalize-the-hardening-of-
4468729, 2025. Accessed: 2025-11.