



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

ACCA7028 LON ASSESSMENT

**Data Security, Governance, and
Compliance**

Habibur Rahman | 2428138

To

Dr. Dipo Dunsin

Submission Date: 19/12/2025

Table of Contents

Table of Figures and Diagrams	3
1 Abstract	4
2 Introduction	4
3 Literature Review	4
4 Case Scenario: Nature Green (NG)	5
5 Identify the Problem of Nature Green (NG)	5
6 Breakdown of the problem of Nature Green (NG)	5
7 Discussing Frameworks and Models	6
7.1 ISO/IEC 27000 Series (Information Security Management)	6
7.2 ITIL (Information Technology Infrastructure Library) and IT Service Management	7
7.3 COBIT (Control Objectives for Information and Related Technologies) and IT Governance	7
7.4 NIST Cybersecurity Framework (CSF)	7
7.5 Risk Management Frameworks	8
8 Proposed Security Governance and Compliance Approach for Nature Green (NG)	8
8.1 Governance	8
8.2 Policies and minimum rules	8
8.3 Cloud-only layered technical controls	9
8.4 Operational integration	9
8.5 Continuous risk assessment and improvement	9
9 Proposed Diagram	10
10 Conclusion	11
11 References	11

Table of Figures and Diagrams

Figure 1: Logic Flow of the Literature Review for Nature Green (NG) 5

Figure 2: NG Security Blueprint Process 6

Figure 3: Cloud security governance model for Nature Green (NG) 10

1 Abstract

This review paper discusses the importance of information security, governance, and compliance in today's business environments, working with significant digital connectivity. As companies rely on cloud deployments, wireless connections, or personal devices, they face greater challenges protecting sensitive data, intellectual property, and customer confidence. Findings of this study call for a methodical approach to security management with clear guidelines and rules, risk assessment, disaster recovery planning strategies, and security countermeasures in accordance with ethical and legal compliance. It then goes on to offer a high-level framework that shows the direction in which businesses should be thinking, in terms of the strategic planning process, when it comes to incorporating governance and compliance, but also being agile enough to take on new challenges. The debate ends with a discussion of laws and standards that would guarantee the effectiveness of security and the durability of organizations in an ever-evolving technological landscape.

2 Introduction

Organizations have stored and are still collecting tons of data, some of which is very personal indeed [1]. In contrast, the regulatory landscape has itself been reshuffled, meaning that compliance with laid-down rules is mandatory [1]. Data breaches have also put the spotlight on data governance, and it is now seen as an integral part of the data protection life cycle [1]. Setting up data governance is a constant and iterative process that brings together data quality, security, privacy, and access policies [1]. Authorizing data governance by design involves adopting rules, processes, and a systematic method to ensure openness and traceability [1]. Privacy has been an issue in the computer era from its earliest days [2]. Back in the 1960s, fears of how governments and other large organizations might abuse personal information led to laws such as the U.S. Privacy Act of 1974 [2]. As the internet has expanded since the 1980s, risks to privacy, such as cookies or tracking software, have become more pronounced [2]. Measures such as encryption and anonymization were developed. Nowadays, with the massive use of social networks and recurring privacy troubles with big tech enterprises, these worries are even greater [2].

3 Literature Review

In this paper, the discussion will be about a company called Nature Green (NG). After that, there will be an understanding of the problem, a breakdown of it, and how to solve that problem. Later, proposed a comprehensive security model for the company, ensuring strong defenses against hackers and safeguarding its digital assets. Figure 1 reviews the framework, which indicates the description of the use case scenario and its major security concerns for Nature Green (NG). The issues are then examined to investigate their underlying causes. With this deep comprehension, applicable security models and principles in the literature are noted, then informally used as guidelines to recommend a suitable strategy to mitigate the observed problem.

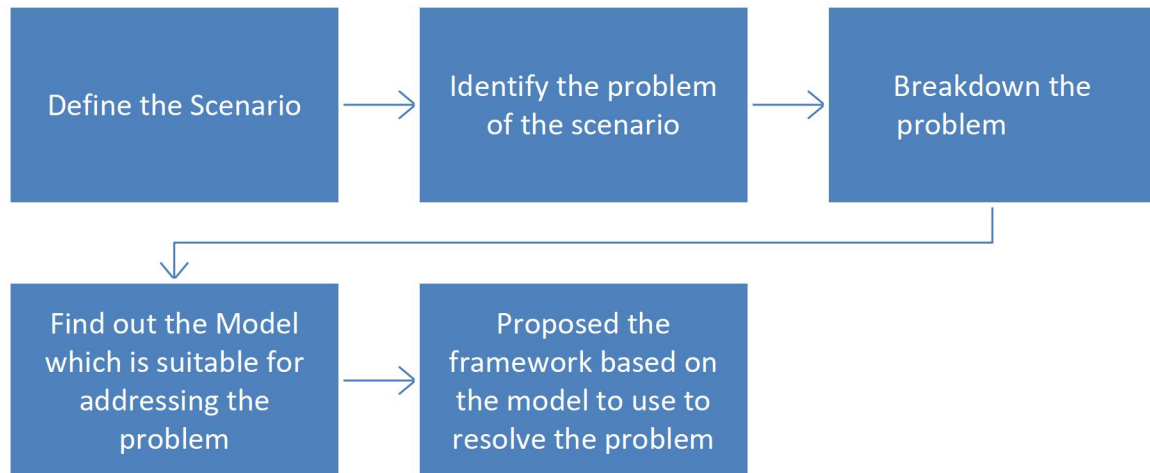


Figure 1: Logic Flow of the Literature Review for Nature Green (NG)

4 Case Scenario: Nature Green (NG)

Nature Green (NG) is a large global network where 95% infrastructure is mobile, and it has an influential online population. Its employees and customers request more bring-your-own-device (BYOD) access to their corporate resources. While this is good in terms of business agility, it leads to a much wider attack surface. Your own device and public Wi-Fi are threats to data leakage, malware, and unsanctioned access. It's NG's IP, and potentially sensitive customer data privacy laws come into play here.

5 Identify the Problem of Nature Green (NG)

Nature Green (NG) does not have a security policy or governance framework, making it vulnerable to cyber threats and compliance issues.

6 Breakdown of the problem of Nature Green (NG)

After breaking down the problem, it is identified that:

- Most of NG's infrastructure is wireless, which is easier to attack.
- BYOD introduces risks like data leakage and malware.
- There is no formal security policy or governance structure.
- Sensitive data is at risk, and privacy laws require protection.
- The attack surface is growing, but there is no risk management plan.

7 Discussing Frameworks and Models

In this section Figure 2 discusses the security models suitable for integration at Nature Green (NG) to improve its security policy. It then explains the security frameworks that guide governance, risk management, and operations. Finally, the section presents a security blueprint that combines these models and frameworks into a practical, cloud-only security approach for NG.

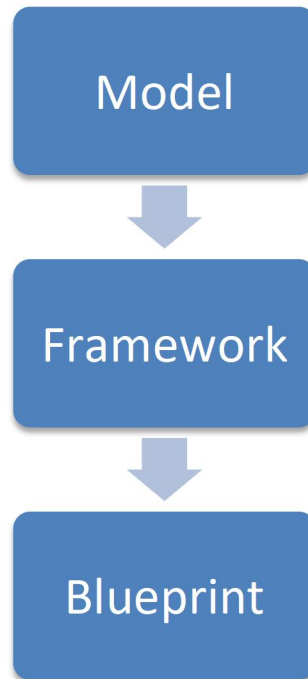


Figure 2: NG Security Blueprint Process

7.1 ISO/IEC 27000 Series (Information Security Management)

The ISO/IEC 27000 family is a set of standards that helps organizations build an Information Security Management System (ISMS) [3], [4]. An ISMS is how the company manages security as a business process rather than doing security only when something goes wrong. ISO/IEC 27000 provides a shared vocabulary and an overview, so people write policies and evidence in a consistent way [4], [3]. The most important standard for NG is ISO/IEC 27001, which sets requirements for establishing, implementing, maintaining, and continually improving an ISMS [4]. ISO/IEC 27001 is risk-based; on NG, it defines scope, assesses risks, chooses treatments, and checks whether controls work. ISO/IEC 27002 supports ISO/IEC 27001 by providing practical guidance for selecting and implementing security controls, such as access control, encryption, logging, incident handling, and supplier security [4].

Examples for NG under ISO 27001/27002:

- BYOD security only allows registered devices that are enrolled in MDM, encrypted, and compliant before accessing NG resources.
- Data protection classifies customer and finance data as confidential/restricted, restricts access using roles, and encrypts data in transit and at rest.
- Incident response evidence keeps an incident log, lessons learned, and control updates as proof of continual improvement.

7.2 ITIL (Information Technology Infrastructure Library) and IT Service Management

ISO standards help NG define what to manage, but ITIL helps NG run security day-to-day as part of service management. ITIL's information security management practice focuses on protecting the information required by the organization and managing risks to its confidentiality, integrity, and availability across the service lifecycle [5]. For NG, ITIL is valuable because many security failures happen through operational gaps: rushed changes, missing approvals, weak documentation, and inconsistent incident handling. ITIL reduces these risks by embedding security into change enablement, incident management, and continual improvement.

Examples for NG using ITIL:

- Changing management cloud firewall rules, IAM roles, and application releases must go through approval, testing, and rollback planning before releasing.
- Incident management attacks such as phishing or DDoS are logged, prioritized, escalated, resolved, and documented consistently.
- Service continuity, clear recovery steps using backups, failover, and defined service targets, reduces downtime during outages.

7.3 COBIT (Control Objectives for Information and Related Technologies) and IT Governance

COBIT is a governance framework that helps make sure IT and security support business goals, risks are controlled, and responsibilities are clear [6]. For NG, COBIT is helpful because leadership needs visibility, which can include factors such as the biggest risks, any improvements, and security measurements. COBIT supports reporting, accountability, and auditability. It encourages management to review metrics such as incident trends, downtime, compliance status, and risk treatment progress.

Examples for NG using COBIT:

- Executive oversight: quarterly dashboards summarize security incidents, availability, and compliance progress to support decision-making.
- Accountability: clear ownership for identity management, cloud configuration, incident response, and supplier management.
- Audit trail: approvals and logs for critical changes (IAM roles, WAF rules, security groups) provide traceability.

7.4 NIST Cybersecurity Framework (CSF)

The NIST Cybersecurity Framework (CSF) allows a flexible way to manage and reduce cybersecurity risk [5]. It is widely used because it has a simple structure and shared language for executives and technical teams. CSF is commonly explained through five functions, which are to identify, to protect, to detect, to respond, and to recover [6]. For NG, this lifecycle helps organize security work and track maturity over time, especially in a cloud-only environment where monitoring and configuration are crucial.

Mapping for NG using the CSF functions:

- Identify: keep an inventory of cloud resources, endpoints, data stores, and supplier connections.
- Protect: enforce MFA, RBAC, encryption, segmentation, secure baselines, and WAF/DDoS protection.
- Detect: central logging and SIEM alerting for unusual sign-ins, abnormal downloads, and web attack patterns.
- Respond/Recover: incident playbooks, containment actions, backup restoration, and post-incident improvements.

7.5 Risk Management Frameworks

Risk frameworks help NG decide what to fix first, based on business impact and likelihood, rather than trying to do everything at once. ISO 31000 provides general risk management guidelines for identifying, analyzing, evaluating, treating, monitoring, and communicating risk across an organization [7]. For information security specifically, ISO/IEC 27005 guides the management of information security risks to support the implementation of an ISMS based on ISO/IEC 27001 [8]. This is especially important for NG because cloud risks such as exposed storage, insecure APIs, and overly permissive IAM roles can change quickly and need continuous review.

Examples for NG using risk frameworks:

- Cloud risk assessment: before launching new services, check misconfigurations such as public buckets, open ports, weak IAM, and mainly check risks before going live.
- Vendor risk: assess third parties and cloud providers for security responsibilities and evidence to reduce supply chain risk.
- Continuous monitoring: update the risk register when incidents occur, or new threats emerge, and track residual risk after treatment.

8 Proposed Security Governance and Compliance Approach for Nature Green (NG)

The proposed approach for NG is cloud-only, and it is based on the frameworks discussed in Discussing Frameworks and Models. The authors proposed that NG should combine: ISO/IEC 27001 for the ISMS foundation, ISO/IEC 27002 for control guidance, ITIL for operational security processes, COBIT for governance and accountability, NIST CSF for continuous lifecycle improvement, and ISO 31000/ISO/IEC 27005 for structured risk management [4], [8], [9].

8.1 Governance

NG should set clear ownership, so security decisions are not left unclear. Under COBIT-style governance, top management sets risk allowance, approves key budgets, and reviews performance metrics [6]. The ISMS owner (security lead) maintains policies, the risk register, internal audits, and an improvement plan under ISO/IEC 27001 requirements [4]. IT service owners embed security into daily work using ITIL practices such as change control, incident handling, and service continuity [5].

8.2 Policies and minimum rules

NG should keep policies simple and focused on the highest risks. Key policies should cover BYOD, access control, data classification/handling, secure change management, incident response, backup/disaster recovery, and supplier security. These policies provide consistent expectations and create evidence for audits. ISO/IEC 27001 requires documented processes and continual improvement, while ISO/IEC 27002 provides practical control guidance [3],[4],[10].

Minimum policy set for NG:

- BYOD & endpoint policy: MDM enrolment, device encryption, patching, and compliance checks before access.
- Access control policy: MFA everywhere, RBAC/least privilege, and privileged access controls for admins.
- Data classification & handling policy: label sensitive data, restrict access, encrypt, and define retention.
- Secure change policy: security checks before deployment; approvals and a rollback plan required.
- Backup & DR policy: regular backups, tested restores, and defined recovery targets.

8.3 Cloud-only layered technical controls

Because NG is cloud-only, protection must be layered. At the edge, NG should use DDoS protection and a web application firewall (WAF) to filter attacks before they reach the application. Inside the cloud, NG should use segmentation and cloud firewall/security groups to separate public services from private application services and restricted data stores. Identity should be ‘front and center’, IAM with MFA and RBAC should control who can do what, with stronger controls for privileged admin access. Sensitive data should be encrypted in transit and at rest, with strong key management. Finally, NG should centralize logs into a SIEM for detection and rapid response. This matches the NIST CSF outcomes for Protect and Detect and aligns with ISO control guidance [11],[4],[9].

8.4 Operational integration

NG should embed security into daily processes. Changes to cloud resources (IAM roles, firewall rules, WAF policies, deployments) should follow a controlled change process with security checks and approvals. Incidents should follow a consistent workflow of detection, triage, containment, eradication, recovery, and post-incident review. NIST and CSF provide lifecycle framing (Detect/Respond/Recover), while ITIL provides operational discipline (incident management and continual improvement) [5],[9].

8.5 Continuous risk assessment and improvement

NG should maintain a living risk register and update it whenever major changes occur and on a routine schedule. ISO 31000 encourages embedding risk management into governance and decision-making [7] . ISO/IEC 27005 supports information security risk assessment and treatment aligned to ISO/IEC 27001 [8] . This keeps security focused on the biggest risks and ensures that residual risk is understood and accepted by management when necessary.

9 Proposed Diagram

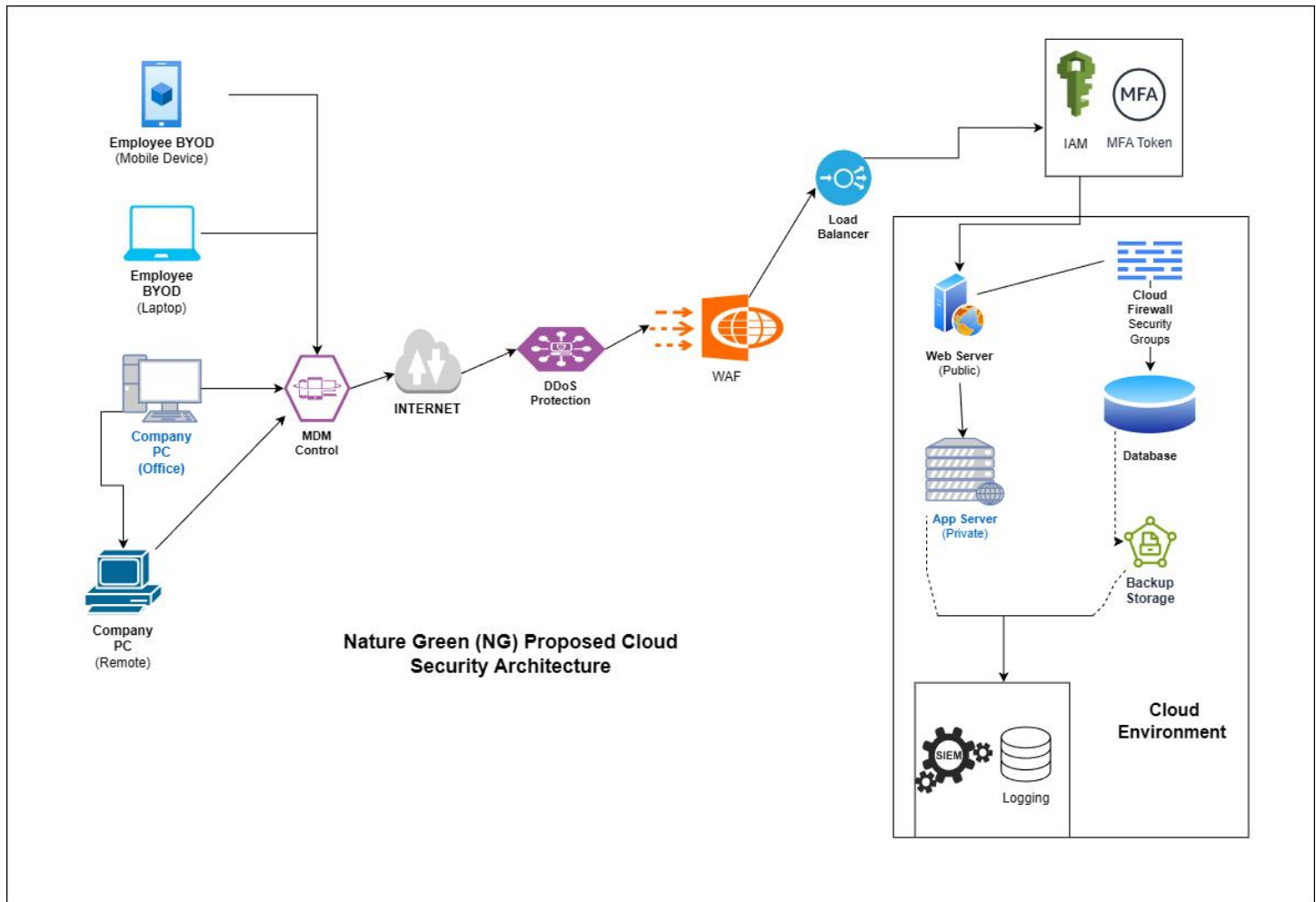


Figure 3: Cloud security governance model for Nature Green (NG)

According to Figure 2 presents proposed diagrams that visually support the recommended security governance and compliance approach for Nature Green (NG). It explains how Nature Green (NG) can secure its cloud-only environment, supporting a large BYOD and mobile workforce. It shows how users, security controls, governance, and monitoring work together to reduce risk and meet compliance requirements.

NG employees have to access their system using BYOD mobile devices, laptops, and company PCs, which are managed by NG. All devices are controlled through Mobile Device Management (MDM) to ensure they meet security requirements such as encryption, patching, and compliance before access is allowed. This reduces the risks associated with personal devices and public Wi-Fi. All traffic passes through some layer protections, which include DDoS protection and a Web Application Firewall (WAF), which block attacks before they reach NG's cloud services. A load balancer securely routes traffic to the public web server, while IAM with Multi-Factor Authentication (MFA) ensures only authorized users can access NG's application. Inside the cloud environment, network segmentation and cloud firewalls separate public services from private application servers and databases. Sensitive data is protected using encryption and regular backups, reducing the impact of data loss or breaches. All activities are logged and sent to a central SIEM, enabling real-time monitoring, detection, and incident response.

Overall, the diagram supports NG's security governance approach by aligning with ISO/IEC 27001 for security management, ITIL for operational processes, COBIT for governance and accountability, and the NIST Cybersecurity Framework for continuous protection, detection, response, and recovery.

10 Conclusion

To summarize, developing a clear and comprehensive security policy is vital for addressing the problems and objectives in this scenario. A strategic approach will bring clarity, enhance the security posture, role definition, and maintain alignment between security-intensive processes and business objectives. The ongoing refresh and flexibility are essential to remain effective as threats and technology evolve.

For Nature Green (NG), they need to have explicit policies, strong cloud security, and good governance to mitigate risks from mobility BYOD and a wide attack surface. By embedding security into daily operations, it ensures that changes, incidents, and risks are dealt with consistently and effectively. Regular monitoring, reviewing, and updating will help the company to keep ahead of possible threats, comply with privacy laws, and protect sensitive data. Overall, a formal, evolved, and well-structured plan helps NG ensure that it can provide security, resilience, and trustworthiness while the business grows.

11 References

- [1] J. Osakwe and I. Haitula-Waiganjo, "DATA SECURITY AND COMPLIANCE THROUGH EFFECTIVE DATA GOVERNANCE," *IJIS*, vol. 4, no. 1, -04-10 2025. doi: 10.34218/ijis_04_01_004.
- [2] M. Zostant and R. Chataut, "Privacy in computer ethics: Navigating the digital age," *Comput Sci Inf Technol*, vol. 4, no. 2, -07-01 2023. doi: 10.11591/csit.v4i2.pp183-190.
- [3] International Organization for Standardization. "ISO/IEC 27000 family — Information security management." International Organization for Standardization. <https://www.iso.org/standard/iso-iec-27000-family> (accessed 18 December).
- [4] M. Malatji, "Management of enterprise cyber security: A review of ISO/IEC 27001:2022," 2022-10-25. doi: 10.1109/cymaen57228.2023.10051114.
- [5] S. Lopes, et al., "Using ITIL as part of the NIST Cybersecurity Framework," 2024-04-29. doi: 10.1109/isdfs60797.2024.10527256.
- [6] A. C. Amorim, et al., "Using agile methodologies for adopting COBIT," *Information Systems*, vol. 101, -02-19 2020. doi: 10.1016/j.is.2020.101496.
- [7] G. H. Silva Rampini, H. Takia and F. T. Berssaneti, "Critical Success Factors of Risk Management with the Advent of ISO 31000 2018 - Descriptive and Content Analyzes," 2019. doi: 10.1016/j.promfg.2020.01.400.
- [8] A. Z. Mahfud, et al., "Information Security Risk Management Design Based on ISO/IEC 27005:2022, ISO/IEC 27001:2022, and NIST SP 800-53 Revision 5 (A Case Study at ABC Agency)," 2024-08-07. doi: 10.1109/ice3is62977.2024.10775428.

- [9] National Institute of Standards and Technology, "Framework for Improving Critical Infrastructure Cybersecurity," 2014. Accessed: 18 December 2025. [Online].
<https://www.nist.gov/system/files/documents/cyberframework/cybersecurity-framework-021214.pdf>
- [10] ISO/IEC (International Organization for Standardization / IEC). "ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection — Information security management systems — Requirements." ISO – International Organization for Standardization. <https://www.iso.org/standard/27001> (accessed 18 December).
- [11] V. Diamantopoulou, A. Tsohou and M. Karyda, "From ISO/IEC27001:2013 and ISO/IEC27002:2013 to GDPR compliance controls," *ICS*, vol. 28, no. 4, -06-08 2020. doi: 10.1108/ics-01-2020-0004.