

University of Wales

Trinity Saint David

An Assignment
on

Data Security, Governance & Compliance
Module code: ACCA7028

Submitted To:

Dr. Dipo Dunsin

Lecturer

Department of Cybersecurity and Digital Forensics
University of Wales Trinity Saint David

Submitted By:

Md Obaydul Hoque

ID: 2435442

Programme:

M.Sc. in Cybersecurity and Digital Forensics
University of Wales Trinity Saint David

Date of Submission
19th December 2025

Table of Content

1	Introduction	3
2	Background & Assumptions	3
3	Literature Review	4
	3.1 ISO/IEC 27000 Family	5
	3.2 COBIT Framework	6
	3.3 ITIL / IT Service Management (ITSM)	6
	3.4 NIST Frameworks	7
	3.5 Risk-Management Best Practices	7
4	Security Frameworks and Models (with diagrams)	
	4.1 Governance Models in Data Security	
	4.2 Risk Assessment & Compliance Analysis	
	4.3 Risk Assessment	
	4.4 Vulnerability Assessment	
	4.5 Compliance Analysis	
	4.6 Risk Evaluation and Prioritization	
5	Technical, Procedural, and Organizational Controls	
	5.1 Technical Controls	
	5.2 Procedural Controls	
	5.3 Organizational Controls	
6	Proposed Security Framework for Nature Green (NG)	
7	Conclusion	
8	References	

Introduction:

With digital transformation rapidly taking hold across the globe, businesses are relying more on cloud services, remote working arrangements, and Bring Your Own Device (BYOD) initiatives to gain scale while at the same time boosting collaboration and productivity. Ambitious as these may sound, they also carry with them substantial risks in terms of data protection, governance and compliance. Nature Green (NG) is a company with rapid growth that highlights the trade-off faced by organisations between operational agility and security robustness in today's world.

This evaluation examines NG's existing information security posture and recommends a model to protect its information resources. The model complies with the international standards such as ISO/IEC 27001, NIST cyber security framework and Zero Trust Architecture (ZTA). This guarantees a rational and risk-based plan for the security of confidentiality, integrity, and availability (CIA) of NG's data [5].

Through evaluations of governance and risk management, regulatory requirements, technical controls and related processes, the assessment also uncovers gaps in a client's organization and offers focused assistance to help clients make strides in bolstering information security and compliance on an ongoing basis.

Literature Review

With breaches on the rise, regulations becoming more complex and organizations being challenged by increasing amounts of data – how can you stay ahead? Research and industry submissions continually emphasize the importance of layering technical, procedural and organizational controls for strong security postures. Based on ISO/IEC 27001, organizations are required to set up a risk-based Information Security Management System (ISMS) to secure the confidentiality, integrity and availability of information assets [1]. The standard highlights the importance of continuous evaluation, monitoring and improvement to keep controls effective in an evolving threat landscape.

The NIST Cybersecurity Framework (CSF) offers an alternative model of information security management. It categorizes cybersecurity activities into five broad functions: Identify, Protect, Detect, Respond and Recover [2]. This structure enables enterprises to focus resources based on risk, to align security investments with business objectives, and to remain resilient in the face of

known and emerging threats. Studies demonstrate that those that have implemented both the ISO/IEC 27001 and NIST CSF frameworks report increased understanding of risk, stronger organisational internal controls and enhanced regulatory compliance [2].

Zero trust architecture (ZTA) has emerged as an important security model, particularly for cloud-first and bring-your-own-device (BYOD) environments. Unlike conventional security models which are based on perimeters, ZTA trusts no one—whether user or device—by default, even those already inside corporate network. Every access-request passes through on-line authentication, authorization and validation before access is granted [5]. Based on academic research and NIST publications, ZTA was found to mitigate risks associated with insider threats, stolen credentials and compromised endpoints, which is particularly relevant for organizations with extensive remote and mobile workforces.

Studies also reveal that cloud adoption and BYOD policies significantly expand the attack surface. Research studies reveal that unprotected personal devices, unmanaged applications and misconfigured cloud resources lead to data leakage and regulatory noncompliance [3]. The risk associated with mobile devices can be mitigated through the use of Mobile Device Management (MDM), endpoint security and access controls, which also contribute toward enhanced employee productivity and operational agility.

In addition to this, GDPR and the UK Data Protection Act 2018 compliance is becoming more and more significant for corporate governance. Both legislations mandate that the organisations should take “appropriate technical and organisational measures” to protect data by design and by default [3]. Organizations that marry security frameworks with GDPR compliance programs demonstrate better accountability, risk management and earned trust in stakeholders."

There are many organisation wide frameworks and governance models that help shape how to manage technical, organisational or regulatory requirements imposed on a system by developing a cybersecurity strategy. This section outlines key international standards and frameworks applicable to NG, namely ITIL/ITSM model [13], ISO/IEC 27000 series of standards, COBIT [20], NIST SP 800-53/30/34 security frameworks ("recommendations"), as well as established risk management methodologies.

3.1 ISO/IEC 27000 Family

The ISO/IEC 27000 family of standards is believed to be the best-known standard for information security management. An ISMS is a systematic approach to managing sensitive company information, based on an assessment of risk, and includes processes for establishing, implementing, operating, monitoring, reviewing and maintaining the quality of an organization's information security. It should be noted in literature that ISO/IEC 27001 is considered as a foundation for organization governance through its inclusion of risk-based decision-making premise, leadership commitment, documentation and continual improvement [1].

Relevance to NG:

- Participates in governance documentation requirements

- Provides strong data protection and auditability
- Supports GDPR/UK DPA accountability principles

3.2 COBIT Framework

COBIT (Control Objectives for Information and Related Technology) is an enterprise IT governance framework that provides a systematic approach to govern business operations. It also provides a best practice method of control activities in compliance with regulation. Key is that COBIT 2019 focuses on governance elements like processes, organisational structures, culture, information flows, and people [2]. It is a commonly used tool for accountability and to ensure that leaders are aligned with tech teams.

Relevance to NG:

- Assists in the definition of governance roles (CISO, DPO, Data Owners)
- Cloud policy lifecycle management
- IT controls are in line with strategic objectives

3.3 ITIL / IT Service Management (ITSM)

A non-IT-specific set of good practices for IT service management, based on ASL and other models. Image An ISO/IEC standard to guide the certification of an organisation's capability to deliver quality services. Performance Appraisal The assessing or judgment of something. Policy Defines rules that stipulate what is allowed or not allowed to happen. Quality Control Systematic measurements against established standards. Portfolio Managing a portfolio includes balancing conflicting demands from a variety of sources. Notes 1.

The ITIL 4 framework provides advice on managing IT services, such as incident management, change control, service-level management and continual improvement. ITIL focuses on a service-oriented approach and to form a coherent IT security practices with daily operation [3].

Relevance to NG:

- Support the drafting of SLA.
- Allows for formal incident response and change control
- Augments the ISO/NIST controls via operational Routine and practices

3.4 NIST Frameworks

These types of frameworks are offered by US-based National Institute of Standards and Technology (NIST) in the context of cybersecurity:

3.4.1 NIST Cybersecurity Framework (CSF)

The NIST CSF is organized around five high-level categories (Identify, Protect, Detect, Respond, Recover). There is a lot of research on its suitability for the cloud and distributed systems [4].

3.4.2 NIST SP 800-53

Offers extensive technical controls for federal systems and is often referenced in conjunction with the ISO standards.

3.4.3 NIST Zero Trust Architecture (SP 800-207) The NIST has also released SP 800-207, the Zero Trust Architecture with a detailed review of its components and characteristics.

Describes the foundations of Zero Trust-like continuous authentication and device attestation and micro-segmentation [5].

Relevance to NG:

- Assists in cloud security and BYOD requirements
- Aids in the Enhancement of Visibility & Monitoring
- Offers technical detail to address/to complement ISO/COBIT

3.5 Risk-Management Best Practices

The literature on cybersecurity highlights risk management as an important part of governance. De-risking actions are based on risk assessment performed using methods like ISO 31000 and NIST SP 800-30 that consider threat identification, vulnerability analysis, likelihood rating, and impact calculation. Sound risk management strategies determine the relative ranking or prioritisation of controls according to quantifiable levels of measureable exposure rather than intuition or convenience [6].

Relevance to NG:

- Assists to rank BYOD threats
- Enables cloud misconfiguration scanning
- Evidence-based investment decision making

3.6 Synthesis: Proposed Security Governance & Compliance Approach for NG

According to existing sources of information, a mixed governance approach is proposed for NG:

This holistic strategy helps NG achieve efficient governance, strong technical controls, regulatory adherence, and continual improvement.

Framework	NG's Use Case
ISO/IEC 27001 (ISMS)	Governance, compliance, documentation, audits
NIST CSF	Operational security alignment
Zero Trust	BYOD, cloud access, remote/hybrid workforce
COBIT	Organizational roles, oversight, strategic alignment
ITIL/ITSM	Incident management, change control, SLA tracking
ISO 31000 Risk Management	Formal risk-assessment lifecycle

4.1 Governance Models in Data Security

As effective governance is essential in coordinating security across an organization. Weak governance is known to result in disconnected controls, uncontrolled risk and penalties for noncompliance. A good governance model should take into consideration:

Roles and Responsibilities: Clearly specifying responsibility for making decisions relating to risk management, policy enforcement, and compliance will make them easier to manage. The collect responsibilities are communicated in delegations - the CISO dealing with security strategy and one a DPO man aging regulatory compliance [3].

Policies and Standards: This addresses the organization's policies regarding acceptable behavior, security requirements for operations. ISO/IEC 27001 also makes a recommendation of developing access control policy, mobile device use policy, incident response plan and business continuity plan [1].

Risk Management Policies: If scored and prioritized, organizations can place appropriate resources in the most effective way. NIST CSF promotes dynamic risk assessment so security posture can be updated in response to changing environment [2].

Audits and Monitoring: Ongoing monitoring, internal audits and reports to demonstrate that security controls are effective and in compliance. Regular evaluation against standards, regulatory and organisational requirements Governance frameworks assist with regular assessment against standards, regulations and organizational policies.

Training and Awareness: According to studies, human error is a significant factor in data breaches. Formal Governance Elements Regular training, in particular for staff members, awareness creation and role based security education are must have governance denominators [3].

Cloud-first / BYOD environments require governance to go beyond traditional lines. Organisations should create cross-functional committees, implement vendor risk management and ensure that security policies extend to both personal and corporate devices. The literature indicates that an all-encompassing governance strategy that integrates ISO/IEC 27001, NIST CSF, and Zero Trust approaches greatly contributes to organizational preparedness and alignment with regulations to improve business processes 1[5].

4.2 Risk Assessment & Compliance Analysis

Risk assessment is a fundamental aspect of data security, governance and compliance. Businesses need to identify what they perceive as threats, assess vulnerabilities and implement the necessary steps in order to protect sensitive information and adhere to any regulations. For an organization like Nature Green (NG), a cloud-first and BYOD (Bring Your Own Device) business, risk management is crucial to be understood for the reasons that include increasing attack surface area, remote working habits and involvement of third-party CSPs.

This section examines NG's strategic information security risks, assesses the regulatory environment and governance and operational control deficiencies.

4.3 Risk Assessment

The key threats to NG are:

Cyber-threats: Malware, ransomware, phishing and advanced persistent threats (APTs) are major dangers for systems that support cloud-enabled and remote work. Adversaries may take advantage of unpatched systems, weak authentication, or misconfigured cloud-based resources 2.

Insider threats: Staff, temporary workers or trusted third-parties who have authorized access can be either intentionally or unintentionally acting against the organization. The insider threats are aggravated by the BYOD (Bring Your Own Devices) policies which allow employees to access private computers without an adequate security infrastructure [3].

Leaks: Your company's or customer's sensitive data is at risk on unsecured endpoints, removable media, and shared improperly. That risk would only be increased by the lack of encryption and oversight.

Third-party vendor risks: Cloud service providers and SaaS applications create dependencies that can influence security and compliance. Vendors that are unthreatened can wind up targets of attacks.

Regulatory risk: Failure to meet GDPR, the UK Data Protection Act 2018, or industry specific regulation can result in fines and financial harm along with reputational damage 3.

4.4 Vulnerability Assessment

NG has weaknesses in the technical as well as organizational environment:

- **Technical weaknesses:** Poor access controls, fragmented use of multi-factor authentication (MFA) and absent monitoring for Bring Your Own Device devices.
- **Process attack surfaces:** Weak security policy enforcement, infrequent risk assessments and poor incident response planning.
- **Human weaknesses:** The members of the staff do not know security risks, or make password only work without passwords maintaining and phishability in device using [3].

NG can map threats onto vulnerabilities in order to rank risks according to their probable impact and likelihood to assist with its risk treatment plan.

4.5 Compliance Analysis

The GDPR stipulates that entities shall take appropriate technical and organisational measures to ensure the security of personal data. Key obligations for NG include:

- **Minimization Of Data:** To minimize data collection and storage to the extent necessary [3].
- **Consent and transparency:** Ensuring that processing is lawful, and providing clear information to data subjects.
- **Security:** Encrypting personal data, limiting access to it and recording changes.
- **DPIAs:** High-risk processing is subject to this obligation.

GDPR also stresses accountability. Compliance needs to be demonstrated by policy, training and documentation. NG is partially in the right direction with current BYOD developments, but has little visibility of BYOD devices and experiences challenges to apply uniform cloud security policies.

4.5.1 UK Data Protection Act 2018

UK Data Protection Act operates in conjunction with GDPR to detail further responsibilities:

- Adopting technical and organizational measures (TOMs) that ensure data protection [4].
- Lawful processing and storage of data in line with the organization's internal governance.
- Holding the giant companies accountable for transparency and individual rights.

NG may lack compliance in audit logging, third-party vendor risk management and incident response. These need to be resolved to avoid them from being penalized.

4.6 Risk Evaluation and Prioritization

Using a risk-based approach, the most critical risks for NG include:

Risk	Likelihood	Impact	Priority
Unauthorized cloud access	High	High	Critical
BYOD data leakage	Medium	High	High
GDPR/DPA non-compliance	Medium	High	High
Insider threat	Medium	Medium	Medium
Vendor failures	Medium	Medium	Medium

By focusing on risks, NG can better allocate resources and address information security threats that might compromise the integrity, confidentiality or availability of data.

The risk analysis and compliance development proved that the current private data safety condition of NG is being confronted with multiple difficulties because cloud firsts and BYOD policies. There is also partial access control, as well as device control and incident response deficiencies. Incomplete GDPR and UK Data Protection Act 2018 compliance leaves NG exposed to regulatory challenges and reputational

damage.

Mitigating these threats calls for a formal governance process, technical controls, and procedures, based on international standards and security frameworks. The following chapter will summarize the technical and procedural measures, as well as organizational controls, and elaborate on their phased arrangement to mitigate risks and compliance.

Part 5:

Technical, Procedural, and Organizational Controls

Now that we have discovered some of those risks and failings in compliance in Part 3, this final section will create a strategic plan for Nature Green (NG) to develop a comprehensive policy approach to minimize threats and adhere to the demands of regulation. Deploying a series of technical, procedural and organisational controls complements each other and therefore provides holistic protection to information assets while minimising security vulnerabilities; it is well-aligned with global standards such as ISO/IEC 27001, the NIST Cybersecurity Framework (CSF) 1, Zero Trust Architecture (ZTA) [5]. This chapter describes the proposed controls and a transition model for NG, to increase its security measures.

5.1 Technical Controls

Operational controls serve to mitigate security risks in the system and infrastructure. For NG, the following should be advised:

5.1.1. Zero Trust Architecture (ZTA)

ZTA is a concept in cybersecurity that does not trust anything inside or outside the organization and instead verifies services before granting access. Key features include:

- Dynamic authorisation and authentication: Evaluates each access request with respect to the user identity, device posture and risk [5].
- Microsegmentation: The network and applications are divided up to stop lateral movement if there is a hack.
- Principle of least privilege: Users receive only as much privilege as is necessary to perform their function.
- Using ZTA on NG will dramatically lower the risk of insider threats, credential loss, and cloud misconfigurations.

5.1.2 Multi-Factor Authentication (MFA) and Identity Management

MFA should also be mandatory in the cloud and on-prem to protect against unauthorised access. Integration with an Identity and Access Management (IAM) [1] system allows role based access controls, automatic provisioning, and de-provisioning of accounts.

5.1.3 Mobile Device Management (MDM)

As NG has BYOD policy, MDM is important to:

- Implement device-level encryption and strong passwords
- Enable remote wipe for lost or stolen devices
- Check adherence to security procedures and patch requirements
- Manage access to company apps and data [3]

5.1.4 Encryption and Data Protection

Sensitive types of data should be encrypted at transit and inactive. Employ effective encryption methods like AES-256 for storage and TLS 1.2+ for communications across networks. This also requires you to regularly test backup and recovery methods even in disaster conditions to keep business running.

5.1.5 Persistent Monitoring & Attack Display

The NG shall deploy Security Information and Event Management (SIEM) and Intrusion Detection System (IDS) as follows:

- Keep an eye on users and network traffic
- Identify suspicious activities leading to potential attacks
- Alerts: Fast incident response [2]

5.2 Procedural Controls

Control measures are actions, policies, procedures or management practices that are designed to implement the controls in a defined way.

5.2.1 Security Policies and Procedures

NG is to have written policies addressing:

- Appropriate use of business and personal devices
- Classification of Data and Handling
- Access control and identity management
- Incident handling and escalation [1]

5.2.2 Response to Incidents and Continuity of Business

The IRP should establish who does what and in which order when dealing with security incidents. Alongside a business continuity plan (BCP), such processes reduce the impact of failure or breach.

5.2.3 Employee Training and Awareness

Human factors are one of the main reasons for security incidents. Scheduled course programs should train employees on the following:

- Phishing and other scams
- Proper use of BYOD devices
- Secure data treatment and report of suspicious events [3]

5.2.4 Audit and Compliance Checks

NG should periodically conduct internal and external audits to test PI, ISO 27001, NIST CSF, GDPR, or UK DPA compliance. Audit outcomes need to form part of continuous improvement loops.

5.3 Organizational Controls

Management actions ensure that governance structures, roles and responsibilities are conducive to effective security operations.

5.3.1 Governance Committees and Roles

- Security Steering Committee: Manages strategic security initiatives, budget approval and risk treatment execution.
- CISO: Manages security strategy and sets/reinforces policy.
- Data Protection Officer (DPO): responsible for overseeing GDPR and UK Data Protection Act 2018 compliance.
- IT security team: Enforces technical controls, observes networks and responds to incidents 3.

Proposed Security Framework for Nature Green (NG)

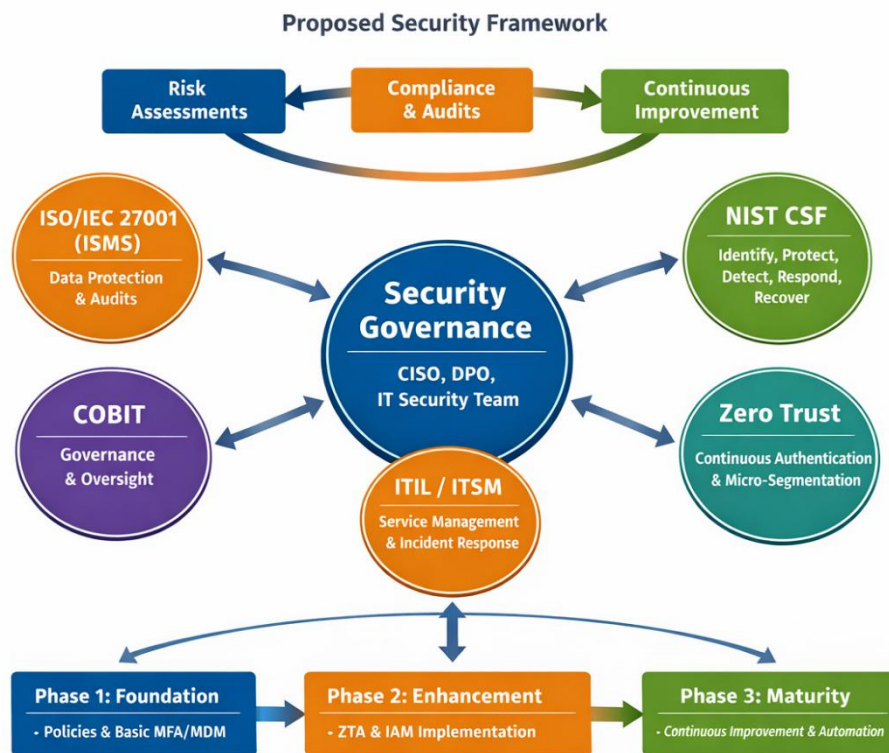


Fig: Proposed Security Framework diagram

For the risks and compliance issues identified in NG, a formalized/integrated security framework is recommended to implement. This model incorporates different security models and standards to secure the safeguard of the sensitive data, adherence with the regulatory requirements as well as improving organization's security standards. The framework is a mix of technical, procedural and organizational controls aligned into phased implementation plans.

Security Governance

The cornerstone of the proposed model is Security Governance, ensuring that the security strategies are in line with the business strategies. Key stakeholders in this governance are CISO, DPO's and the IT Security Team. These positions have very crucial functions, which is to manage risk, ensure compliance and enforce the appropriate policies and procedures. This is the governance model for overseeing and monitoring of security maturity.

Core Security Frameworks

The security model is based on global standards, working hand in hand to form the comprehensive security approach:

- **ISO/IEC 27001 (ISMS):** This standard provides the requirements for establishing an Information Security Management System (ISMS) to manage sensitive information through risk management, data protection and auditing. It underpins all NG's security operations and governance.
- **NIST Cybersecurity Framework (CSF)** – This approach to cybersecurity is based on five core functions: Identify, Protect, Detect, Respond, and Recover. This system provides an organized set of prioritized resources which helps to correlate security and the enterprise objectives.
- **Zero Trust Architecture (ZTA):** With the cloud-first and BYOD policies, it is necessary to prove all access decisions. There is no trusted user or device, and each attempt of access must be strictly verified. ZTA also involves micro-segmentation for the containment of lateral movement during a breach, and least privilege access to restrict the surface area.
- **COBIT Framework:** The Control Objectives for Information and Related Technologies (COBIT) harmonizes IT governance with business delivery and establishes clear lines of oversight and accountability. It assists in defining governance roles, and can help manage the life-cycle of policies and controls across the business.
- **ITIL/ITSM:** The ITIL framework means that Service Management and Incident Response processes are formalized, which in turn assist NG manage their IT services more efficiently and respond to security incidents effectively. It combines well with ISO and NIST controls for operation security.

Phased Implementation Approach

The security framework itself consists of three stages which enable step-by-step adoption and iteration:

Phase 1: Foundation

Early on, NG will concentrate on “establishing and renewing security policies, plus governance.” An enterprise MFA and MDM solution, with basic functionality will be implemented to prevent unauthorised access. The CISO and DPO roles will be appointed, and an initial risk assessment shall be undertaken to identify the worst threats.

Phase 2: Enhancement

In addition, NG will go one level up and implement Zero Trust Architecture (ZTA) while integrating Identity and Access Management (IAM), in order to have a strong authentication and authorization event handled. Establish Continuous Monitoring will use/implemented Security Information and Event Management (SIEM) systems to detect and/or respond to any anomalies. While technical and human factors are going to be addressed via employee training and penetration testing as well.

Phase 3: Maturity

The maturity state concentrates on optimization and automation. NG will implement a strong PDCA (Plan-Do-Check-Act) structure for ongoing assessment and integration of security mechanisms using this ISO/IEC 27001 PDCA model. Automation of Identity Management and Compliance Reporting, along with ongoing audits of third party vendors and cloud services, will help maintain security standards.

Feedback Loops

For the security framework to retain its relevance and potency, Risk Assessments, Compliance Audits, and Continuous Improvement are essential parts of the puzzle. These feedback loops allow security measures to adapt to various threats and governmental regulations while they emerge.

Conclusion

In today's rapidly evolving digital landscape, organizations like Nature Green (NG) must navigate complex challenges surrounding data security, governance, and compliance. With the company's adoption of cloud-first strategies and Bring Your Own Device (BYOD) policies, the attack surface has expanded, bringing about significant vulnerabilities that need to be addressed systematically. This assessment has thoroughly examined NG's current security posture and identified key risks, including unauthorized access, data leakage, and compliance gaps with critical regulations such as **GDPR** and the **UK Data Protection Act 2018**.

The proposed **security framework** is designed to mitigate these risks by integrating globally recognized standards like **ISO/IEC 27001**, the **NIST Cybersecurity Framework**, and **Zero Trust Architecture (ZTA)**. By employing a combination of **technical, procedural, and organizational controls**, NG can significantly enhance its data protection measures, ensuring a robust defense against evolving threats while meeting regulatory requirements.

The **phased implementation approach** proposed ensures that security measures are not only introduced gradually but also evolve continuously in response to emerging risks. From establishing strong foundational policies to implementing advanced security models like Zero Trust, the framework will guide NG towards long-term success and resilience.

Ultimately, this assessment underscores the importance of a structured, holistic approach to cybersecurity that goes beyond mere compliance to foster a culture of continuous improvement, risk management, and organizational accountability. By adopting the proposed framework, NG will not only safeguard its data but also build trust with stakeholders, strengthen its competitive position, and ensure sustainable growth in the digital era.

References:

- [1] ISO/IEC 27001: Information Security Management Systems — Requirements. International Organization for Standardization (ISO), 2013/2022 Revision.
- [2] National Institute of Standards and Technology (NIST). *Cybersecurity Framework (CSF)*. NIST Special Publication 800-53 & CSF 1.1.
- [3] Information Commissioner's Office (ICO). *Guide to the UK GDPR: Accountability and Governance*. ICO, United Kingdom.
- [4] UK Parliament. *Data Protection Act 2018*. United Kingdom.
- [5] National Institute of Standards and Technology (NIST). *Zero Trust Architecture*, NIST Special Publication 800-207.