



University of Wales
Trinity Saint David
LONDON

**Department of Cyber Security and
Digital Forensics**
Master's Programme

Module Title:

Data Security, Governance, and Compliance

Module Code:

ACCA7028_LON

Assignment Title:

Apply the principles and practices of Data Security, Governance and Compliance based on a given scenario

Submitted by: **Shahriar Badhan**

Student ID: **2505521**

Submission Date: 19 December 2025

Contents

1	Introduction	4
2	Review of Security Frameworks and Models	4
2.1	ISO/IEC 27000 Series	4
2.1.1	Key Components of ISO 27001	4
2.2	ITIL (Information Technology Infrastructure Library)	5
2.2.1	Relevant ITIL Practices for NG	5
2.3	NIST Cybersecurity Framework (CSF)	6
2.4	COBIT 2019	6
2.4.1	Key COBIT Domains	7
2.5	Traditional Security Models	7
3	Tailored Information Security Governance Approach for NatureGreen (NG)	7
3.1	Governance and Strategic Planning	8
3.2	Security Policies	9
3.2.1	Essential Policies for NG	9
3.3	Risk Management	9
3.3.1	Risk Management Stages	9
3.4	Protection Mechanisms	9
3.4.1	A. Technical Controls	10
3.4.2	B. Administrative Controls	10
3.4.3	C. Physical Controls	10
3.5	Contingency and Incident Response Planning	10
3.5.1	Incident Response Lifecycle	10
3.5.2	Business Continuity and Disaster Recovery	10
3.6	Service Level Agreements (SLAs)	10
4	Importance of Continually Updated Regulations and Standards	11
4.1	Technology Evolves Faster Than Regulations	11
4.2	Constant Emergence of New Threats	11
4.3	Protecting Privacy and Complying with Laws (Compliance)	11
4.4	Maintaining Consumer Trust and Brand Integrity	12
4.5	Supporting Organisational Resilience	12
4.6	Ethical and Legal Accountability	12
5	Conclusion	13
6	IEEE References	15

List of Figures

1	ISO 27001 Plan-Do-Check-Act (PDCA) Cycle	5
2	ITIL Information Security Management Workflow	6
3	NIST CSF Core Functions	6
4	Hierarchical Governance Structure for NatureGreen (NG)	8
5	Framework	14

1 Introduction

Today's business operations heavily rely on digital infrastructure, distributed systems and interconnected devices. For NatureGreen (NG), a worldwide company established in health and wellness markets, information systems are not mere supportive devices but business enablers. With an estimated 95% of the network running as wireless, heavy reliance on cloud services, and a growing requirement to accommodate Bring Your Own Device (BYOD) for employees and visitors alike, NG is increasingly left vulnerable to security threats. Moreover, NG's IP value is counted in the billions and is another critical corporate asset that needs to be protected.

Though there has emerged an increasing realisation of its importance for cyber security, NG does not have structured policies, governance mechanisms and frameworks in place to inform its security decisions. This evaluation analyses proven security frameworks such as ISO/IEC 27000 series, ITIL, NIST frames and various models of security, with an aim to establish a specific governance and a security model for NG. It also examines critical requirements for developing and perpetually refreshing standards and regulations in the cybersecurity space.

2 Review of Security Frameworks and Models

The ISO/IEC 27000 family of standards is the topmost international reference for setting up, taking care and improving an ISMS. The core standard in this family, ISO/IEC 27001 sets out the required elements of an ISMS and is the only standard in the suite against which organizations can be audited and certified.

2.1 ISO/IEC 27000 Series

The ISO/IEC 27000 family stands as the definitive global benchmark for establishing, implementing, maintaining, and continually improving an Information Security Management System (ISMS) [1]. The foundational standard within this series, ISO/IEC 27001, provides the mandatory structural requirements and comprehensive framework for creating a resilient and effective ISMS within any organization.

2.1.1 Key Components of ISO 27001

ISO 27001 requires several key areas for an organisation, which suits NG effectively due to its emphasis on policy and commitment:

- Leadership and organizational context
- A mandatory **Risk-based methodology** for identifying and treating the threat posed to information security.
- An extensive list of **Security controls** in Annex A (covering categories A.5 to A.18).
- The focus on **Continual Improvement** using the management's **PDCA concept (Plan-Do-Check-Act)**.

The ISMS is not static, but a dynamic system that responds to emerging threats according to the Plan-Do-Check-Act (PDCA) cycle:

- **PLAN:** Identify risks and controls.
- **DO:** Implement controls.
- **CHECK:** Keep observing and auditing the project as implemented.
- **ACT:** Strengthen the program by making changes based on audits.

The focus on formal risk assessment, policy and management commitment positions ISO 27001 as a fit for purpose standard to aid NG in structuring its existing security requirements.

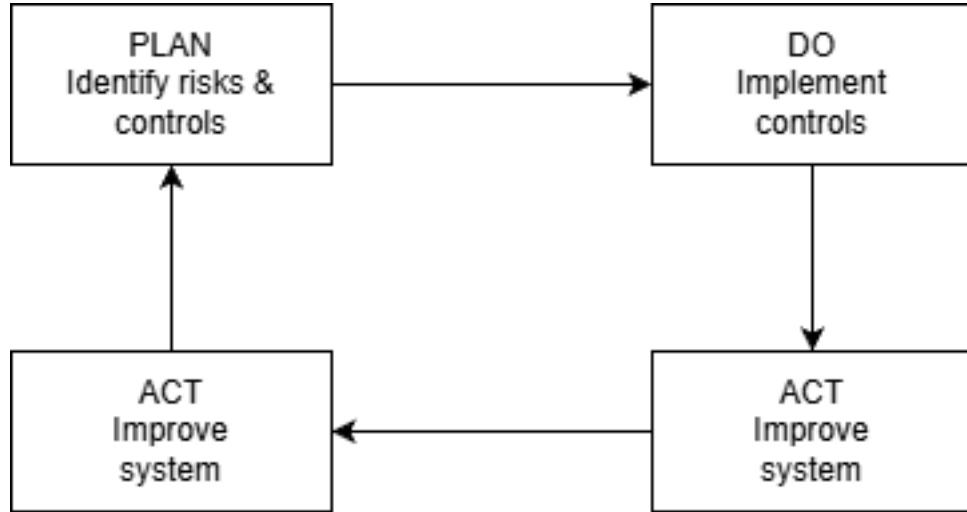


Figure 1: ISO 27001 Plan-Do-Check-Act (PDCA) Cycle

2.2 ITIL (Information Technology Infrastructure Library)

Where ISO 27000 series gives you the high-level strategic **what** (the ISMS framework), ITIL [3] is the globally-recognized service management framework that sets out the operational **how** to manage, and improve upon, the delivery and support of IT services. ITIL, while not a pure security framework, is important in that it supports security governance to the extent that it specifies structured processes and assignation of accountability. Its immediate activity is essential for NG because security must advance from a position of "disarray" to a thorough, repeatable methodology.

2.2.1 Relevant ITIL Practices for NG

There are some of ITIL's practices that can be particularly useful for NatureGreen to incorporate security in its daily operations activities and handling the cloud and wireless environment:

- **Information Security Management (ISM):** The objective of this practice is to safeguard the information and mitigate related risks.
- **Risk management:** Consistent with ISO 27001's risk focus, ITIL defines the operational processes for managing and treating risks.
- **Service Level Management:** It is an important need for managing third-party cloud service providers and establishes specific Service Level Agreements (SLAs) between the parties.
- **Incident Response and Major Incident Handling:** Offers the formalized techniques to efficiently handle and bounce back from security-related breaches provided by the Incident Response Team.
- **Change Enablement:** Guarantees security is being taken into account and enforced whenever changes merely occur in NG's large wireless network or cloud infrastructure, avoiding misconfigurations.

ITIL is then reinforcing the ISO frameworks with practical support in how operational teams at NG can meaningfully integrate the appropriate security controls and policy into their day-to-day operations.

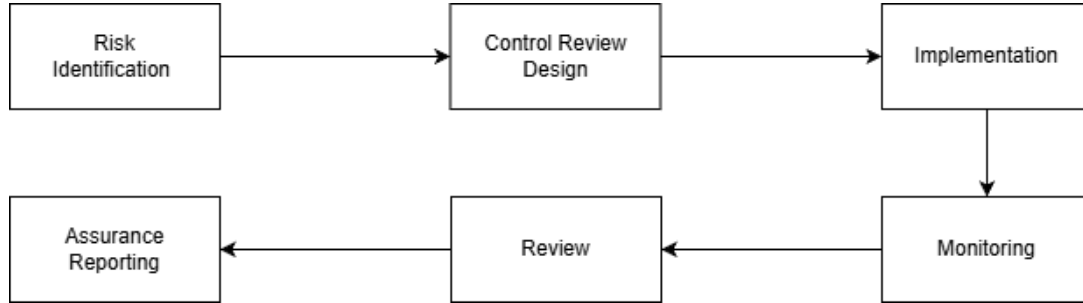


Figure 2: ITIL Information Security Management Workflow

2.3 NIST Cybersecurity Framework (CSF)

The NIST Cybersecurity Framework (CSF) [2], created by National Institute of Standards and Technology, is a simple, high-level framework that is also very comprehensive if you take the time to understand all of its components. It is very well suited for organizations such as NatureGreen (NG) who have large wireless networks and considerable cloud infrastructure.

According to the NIST, the CSF framework comprises five concurrent and continuously functioning functions that when appropriately aligned can track, understand, and incorporate an organization's cybersecurity risk management regime:

1. **Identify:** Established means of managing risk to systems, assets, data and capabilities. For NG, it is recognizing its valuable IP, customer information and wireless/cloud assets.
2. **Protect:** Developing and implementing protections to guarantee critical services. This is a security measure such as zero trust architecture, MFA and encryption for the safety of NG'S wireless and cloud infrastructure.
3. **Detect:** Activities required to detect the occurrence of a cybersecurity event. In the case of NG, this is monitoring for unauthorised activity using SIEM implementation.
4. **Respond:** Activities associated with acting in response to a cybersecurity event that has been identified. This is very much in line with NG Incident Response Policy.
5. **Recover:** Establishing and executing activities to manage the aftermath of a cybersecurity incident, maintain plans for resilience and restore any capabilities or services that were impaired due to a cybersecurity incident. This translates in-line with NG's Business Continuity/Disaster Recovery (BC/DR) strategy.

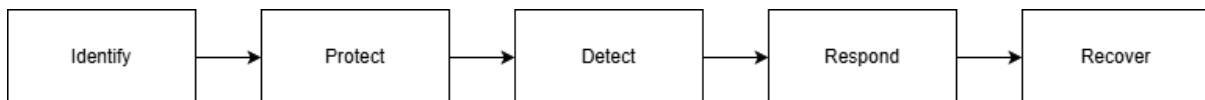


Figure 3: NIST CSF Core Functions

NIST CSF is highly effective for organisations with large wireless networks and cloud infrastructure, making it appropriate for NG.

2.4 COBIT 2019

COBIT 2019 [4] (Control Objectives for Information and Related Technology) is an overall management and governance framework that is tailored to Enterprise IT. It enables businesses to realize the maximum

value from IT by speaking the language of business objectives and delivering clear and effective IT processes.

For NatureGreen (NG), which currently does not have any security policies and governance practices in place, COBIT would be highly useful as an enabler process as it provides accountability and contributes to linking business goals with IT processes strategically. It does so by clearly delineating governance from management:

2.4.1 Key COBIT Domains

- **Governance:** Evaluate, Direct, Monitor (EDM)
- **Management:** Align, Plan, Organise (APO)
- **Management:** Build, Acquire, Implement (BAI)
- **Management:** Deliver, Service, Support (DSS)
- **Management:** Monitor, Evaluate and Assess (MEA)

Indeed, the robust and top-down nature of COBIT is necessary for NG to close the chasm between acknowledging cyber’s importance and fielding a compliant and accountable security structure.

2.5 Traditional Security Models

Complementing contemporary management perspectives, there exist many old-school security models [7] that afford natural number-theoretic foundations for policy-based access control that is strong while preserving essential concert properties of information. For NatureGreen (NG), that takes its billions in IP seriously and would like to ensure data held on the cloud is preserved, such dev models are critical for crafting granular technical controls.

The three most relevant classical models are:

Table 1: Classical Security Models and Relevance to NG

Model	Primary Security Focus	Core Rule Set	Relevance to NG
Bell-LaPadula Model [8]	Confidentiality	”No read up, No write down”	Prevents unauthorized disclosure of sensitive IP by low-clearance subjects.
Biba Integrity Model [9]	Integrity	”No write up, No read down”	Protects the quality and correctness of critical data (e.g., customer records) from unauthorized corruption.
Clark-Wilson Model	Data Integrity & Transactions	Focuses on separation of duties and well-formed transactions.	Ensures that data modification (especially for financial or crucial IP data) is done only through authorized procedures and by authorized personnel.

These base models significantly influence the building of NG’s Identity and Access Management (IAM) and Cloud Security Policy, enabling the company to support strong, multi-dimensional access control for sensitive IP assets distributed through its cloud infrastructure.

3 Tailored Information Security Governance Approach for NatureGreen (NG)

A sound security strategy for NatureGreen (NG) necessitates a tailored framework, one that not only caters to its particular mode of operation—a wireless-laden network environment (approximately 95%

wireless), dependence on the cloud, and a growing need to accommodate Bring Your Own Device (BYOD)) brought in by both employees and customers—but also ensures compatibility between each individual entity.

Assumptions: The following procedure is dedicatedly designed for the NG’s challenges only; it incorporates the best practices of reviewed frameworks (ISO 27001, NIST CSF, ITIL, COBIT and old models) to create order, accountability, and robust security measures.

3.1 Governance and Strategic Planning

Establishing good governance is the beginner’s path to pulling security from a muck and mire. NG needs to establish clear roles, reporting lines and strategic involvement. Below I introduce a governance model which translates security strategy into business objectives based on principles of COBIT [4].

Table 2: Proposed Governance Structure for NG (Table 1)

Role	Responsibility
Board of Directors	Oversees policy prioritization and risk decisions.
Chief Information Security Officer (CISO)	Leads the ISMS and manages the security strategy.
Security Steering Committee	Oversees policy prioritization and decisions.
IT Operations Manager	Implements technical controls.
Data Protection Officer (DPO)	Ensures GDPR compliance for EU/UK regions.
Incident Response Team	Handles incidents and breaches.
Internal Audit	Conducts compliance reviews.

Proposed Governance Structure for NG

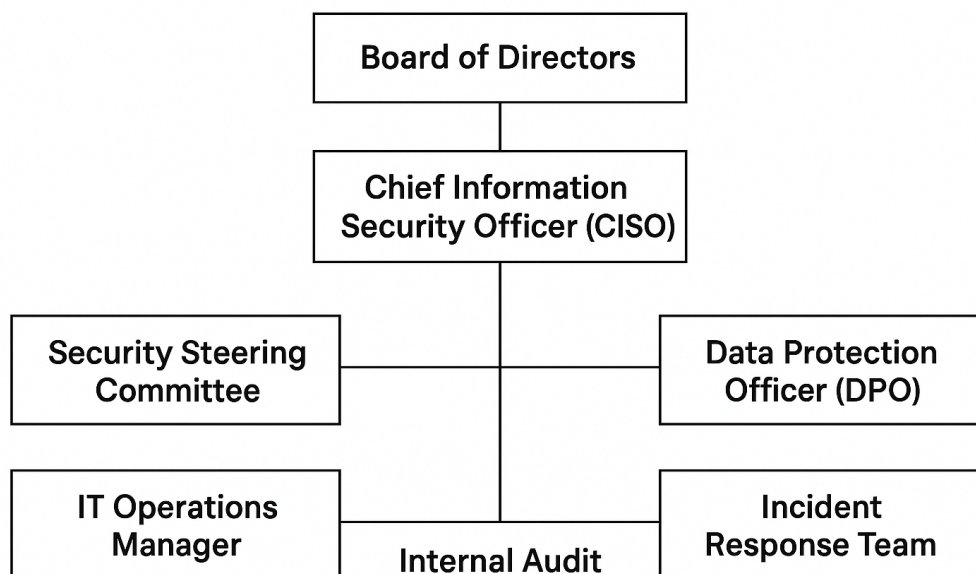


Figure 4: Hierarchical Governance Structure for NatureGreen (NG)

3.2 Security Policies

Policies are the behaviors and technical road map points, with their processes that tie to the “Plan” of ISO 27001 [1]. NG must establish an Annex A controls-based complete policy library.

3.2.1 Essential Policies for NG

- **BYOD Policy:** Necessary to control personal devices on the network.
- **Wireless Security Policy:** Mandatory for the protection of 95% wireless network.
- **Cloud Security Policy:** Compulsory for cloud-reliant architecture.
- **Access Control Policy Enforcement:** Apply controls based on traditional Models (Bell-LaPadula [8], Biba [9]).
- **Data Classification and Handling Policy:** Critical given the billions of dollars worth of IP as well as customer data.

3.3 Risk Management

The structured Risk Management Framework (RMF) based on ISO 27005 and NIST framework [6] should be used by NG. This methodical risk management is essential to protect its high-worth assets.

3.3.1 Risk Management Stages

1. **Asset Discovery:** Identification of key assets, such as Intellectual Property, customer/employee data, cloud applications and wireless infrastructure.
2. **Threat Assessment:** Predicting possible threats such as insider threats, malware, ransomware, phishing and cloud misconfiguration.
3. **Vulnerability Assessment:** Identifying weaknesses, including lack of Multi-Factor Authentication (MFA), inadequate BYOD controls, and weak wireless encryption.
4. **Risk Analysis:** Calculation based on Likelihood $\times$ Impact.
5. **Risk Treatment Alternatives:** Avoid, Transfer (i.e., Cyber insurance), Mitigate or Accept.

Table 3: Example Risk Register (Table 2)

Risk	Likelihood	Impact	Treatment
Data breach via unprotected BYOD	High	Very High	Enforce Mobile Device Management (MDM), MFA
Cloud misconfiguration	Medium	High	Cloud Security Posture Management (CSPM)
Wi-Fi interception attack	High	High	WPA3, network segmentation
Intellectual property theft	Medium	Very High	Zero Trust Architecture (ZTA)

3.4 Protection Mechanisms

These are the controls implemented during the “Do” phase of the ISMS cycle.

3.4.1 A. Technical Controls

- Enable WPA3 for all wireless connections.
- Implement Zero Trust Architecture (ZTA).
- Cloud encryption using AES-256.
- Mandatory Multi-Factor Authentication (MFA) for all systems.
- Deploy Mobile Device Management (MDM) for BYOD.
- Implement Security Information and Event Management (SIEM) for detection and monitoring.

3.4.2 B. Administrative Controls

- Security awareness training.
- Regular penetration testing.

3.4.3 C. Physical Controls

- Biometrics for server rooms.

3.5 Contingency and Incident Response Planning

NG must adopt a systematic approach to resilience, guided by NIST SP 800-61 guidelines [5].

3.5.1 Incident Response Lifecycle

1. Preparation
2. Detection and Analysis
3. Containment
4. Eradication
5. Recovery
6. Post-Incident Review

3.5.2 Business Continuity and Disaster Recovery

- Define Recovery Point Objective (RPO).
- Define Recovery Time Objective (RTO).
- Implement cloud-based backup and redundant systems/failovers.

3.6 Service Level Agreements (SLAs)

As a cloud-dependent organization, NG must use SLAs to ensure external service providers meet its internal security and availability standards.

SLAs should be reviewed quarterly to ensure continuous alignment with NG's evolving security needs.

Table 4: Essential Cloud SLA Requirements for NG (Table 3)

SLA Component			Requirement
Uptime Guarantee			99.9% or above
Data Backup	Frequency	Fre-	Every 12 hours
Breach Time	Notification		Within 24 hours
Encryption Standards			AES-256 minimum
Support Time	Response		30 minutes for critical issues

4 Importance of Continually Updated Regulations and Standards

The Cybersecurity landscape is notorious for its fast, non-linear development. Outdated regulations/standards/systems are thus in and of itself a systemic risk that can result in material financial damage and reputational harm to organizations with such wide (technology heavy) exposure as NatureGreen (NG). The need for constant updating is more than a bureaucratic requirement – it is central to organisational resilience and ethical responsibility.

4.1 Technology Evolves Faster Than Regulations

Regulatory catch-ups lag behind technology innovation. NG depends on cloud services, and 95% of its network use is done wirelessly, so security dials are turned up or down regularly.

- **Adaptation Need:** Renewed Controls (e.g., transitional from outdated Wi-Fi standards to WPA3, or moving between different cloud service delivery models) maintains technical currency in control alignment with contemporary operational risks engaged by today’s consumer-device and distributed architecture-model.
- **Avoiding Misalignment:** As long as your security policies are static, they won’t address new attack vectors brought about by the rapid influx of new technologies (such as BYOD), leaving critical security gaps.

4.2 Constant Emergence of New Threats

The threat landscape is constantly evolving with new attack tactics. The enemy constantly adapts, making yesterday’s defense today’s impediment.

- **Keeping up with the Adversary:** Updated standards – in relation to threat intelligence & incident response (e.g., updates to NIST SP 800-61 [5])—enable NG to build defenses that are equal and opposite responses to today’s attack vectors, such as cyber gangs, ransomware groups fighting dirty using increasingly sophisticated algorithms and AI-enhanced attacks.
- **Safeguarding the Core Assets:** This aspect has a big importance in over-viewing (IP) of NG that represent valuable items to defend from new exploitation patterns.

4.3 Protecting Privacy and Complying with Laws (Compliance)

NG’s international staff and client base makes it subject to a spider’s web of international data privacy laws. Compliance standards must adapt as well, or risk the legal ramifications.

- **Reducing Penalties:** International privacy laws including GDPR [10], UK Data Protection Act and CCPA are becoming increasingly widespread in application and enforcement. Failure, especially in the protection of customer and staff information, can result in catastrophic financial fines and regulatory enforcement.
- **Regulatory Authority:** As a technology hybrid cloud, NG is given the exact legal and technical standards needed to stay in compliance as opposed to nebulous promises turned into auditable controls.

4.4 Maintaining Consumer Trust and Brand Integrity

As a widely sought after international brand, NG must depend greatly on the trust of its customers. This vital reputation can be permanently and seriously damaged through a single, massive data breach.

- **Stakeholder Assurance:** Updated ongoing standards, verified through certifications such as ISO 27001 [1] and transparent reporting, provide customers and investors confidence that NG operates with industry-leading security practices.
- **Building Brand Resilience:** The proactive nature is key to building resilience for your brand against the inevitable security incident.

4.5 Supporting Organisational Resilience

Updated governance tools and security policies are key in allowing organizations to evolve with broad macro-level shifts in operations while remaining secure.

- **Operational Adaptation:** They ensure that security controls remain effective even as NG embraces modern operational trends, including:
 - Sustained Remote Work arrangements.
 - Widespread BYOD trends.
 - Integration of new technologies like AI and automation and IoT devices.
- **Scalability:** By integrating these updates, the security posture becomes scalable, ensuring that security controls remain effective and manageable as the business expands globally and adopts new technology.

4.6 Ethical and Legal Accountability

Contemporary cybersecurity governance transcends technical measures to also include morality and corporate responsibility.

- **Ethical Responsibility:** New legislation now embodies modern ethical standards which foreground transparency, honour privacy and responsible data management.
- **Director Accountability:** These changes codify the security obligations introducing a responsible or accountable line of legal and ethical responsibility for both the Directors and Executive as required under COBIT's EDM domain mitigating risks to customers at an organizational level) [4].

The need for NatureGreen is no different—adopting and consistently refreshing its security defences is the only means by which it can keep pace with technological improvements, as well as changing regulations and laws, turning a security challenge into a competitive enabler.

5 Conclusion

NG grapples with a fast-paced and ever-fluid cybersecurity environment driven by high dependence on wireless networks, cloud environments and growing BYOD demands. This appraisal illustrate how NG can leverage an ensemble of globally recognized models and standards (ISO/IEC 27000 [1], NIST CSF [2], ITIL [3], COBIT [4] and classical security models [8], [9]) to build a complete and dynamic cybersecurity governance framework.

A customized strategy was then developed containing governance structure, security policies, risk management system, defense mechanisms and disaster recovery plans. The report also underscored the need for never-sitting-still standards, ensuring that organisations must remain resistant to new threats, technologies and legal requirements.

By deploying such a systemic and proactive security model, NG will place itself in an ideal stance to secure its intellectual property, compliant with regulation requirements, streamline operations and protect the organization's personnel and customer data.

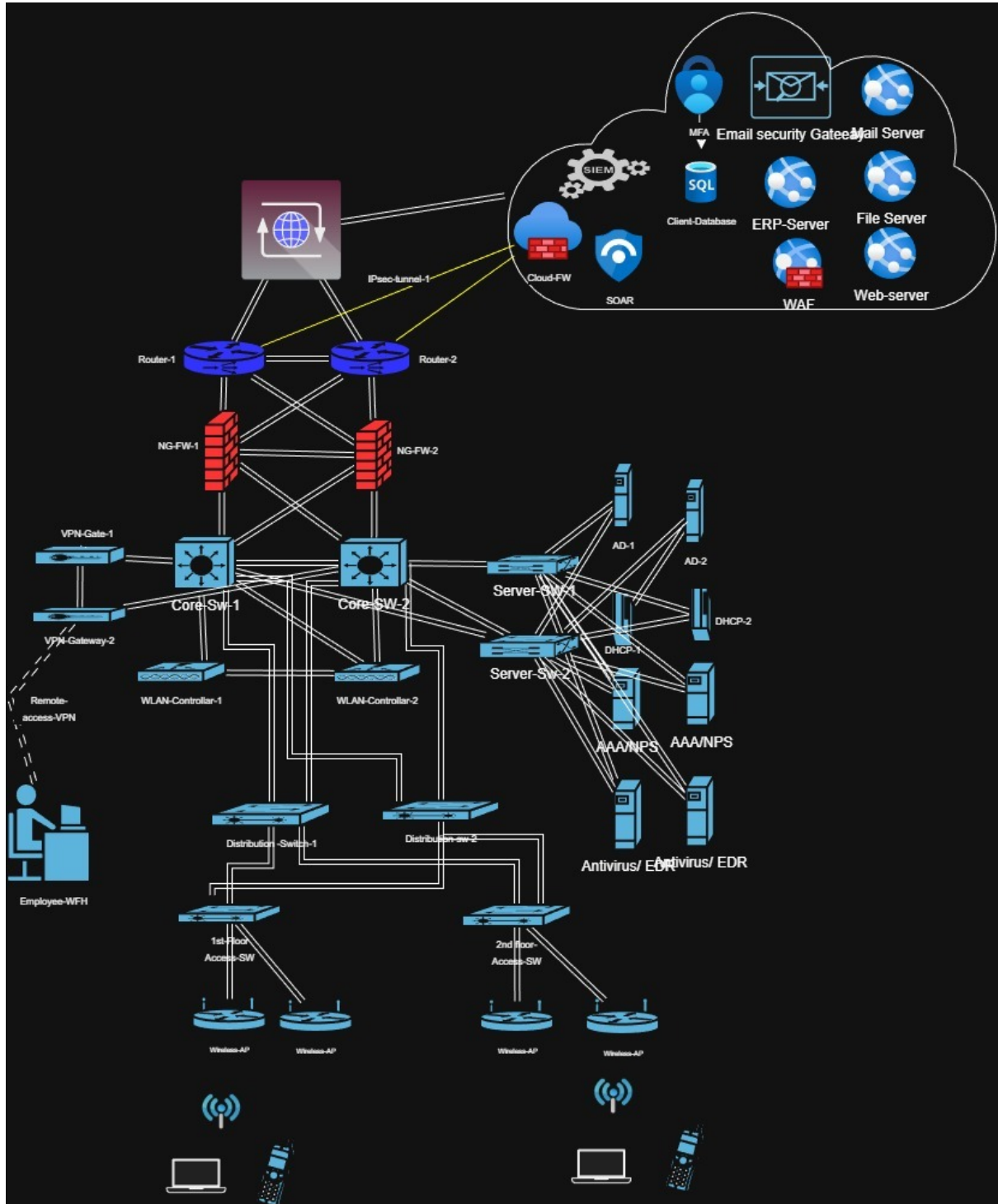


Figure 5: Framework

6 IEEE References

References

- [1] ISO, “ISO/IEC 27001: Information Security Management Systems,” International Organization for Standardization, 2022.
- [2] NIST, “Framework for Improving Critical Infrastructure Cybersecurity,” National Institute of Standards and Technology, 2020.
- [3] ITIL Foundation, “ITIL 4: Service Management Framework,” Axelos, 2021.
- [4] ISACA, “COBIT 2019 Framework: Governance and Management Objectives,” ISACA, 2019.
- [5] NIST, “NIST Special Publication 800-61: Computer Security Incident Handling Guide,” NIST, 2023.
- [6] NIST, “NIST SP 800-53: Security and Privacy Controls for Information Systems,” NIST, 2020.
- [7] B. Lampson, “Protection,” ACM Operating Systems Review, vol. 8, no. 1, 1974. (Used as a general reference for classic models, potentially referencing Clark-Wilson concepts).
- [8] D. Bell and L. LaPadula, “Secure Computer Systems: Mathematical Foundations,” MITRE Corporation, 1973.
- [9] K. Biba, “Integrity Considerations for Secure Computer Systems,” MITRE Technical Report, 1977.
- [10] GDPR, “General Data Protection Regulation (EU) 2016/679,” European Parliament, 2018.