



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

Data Security, Governance and Compliance

ACCA7028 Accessment Report

Student Name: Gandhi Raj Rakeshkumar

Student ID: 2503898

Program: MSC Cybersecurity and Digital Forensics

Submission To: Dr. Dipo Dunsin

Table of Contents

Abstraction.....	1
1. Introduction.....	2
2. Literature Review: Frameworks and Models.....	2
2.1 ISO 27000 Series	2
2.2 Information Technology Infrastructure Library (ITIL).	3
2.3 COBIT (Control Objectives of Information and As applied Technologies)	3
2.4 Visual Aids	4
2.5 ISO 27001 PDCA cycle.....	4
2.6 NIST CSF five function wheel	5
2.7 ITIL service lifecycle	6
3. NatureGreen risk and requirements analysis.....	6
3.1 NG has a number of threats with high impact:.....	7
3.2 Risk Assessment.....	7
4. Proposed security, governance and compliance approach.....	8
4.1 Topline Technology, Inc. Security Governance Structure.....	8
4.2 Core Policy Framework	8
4.3 Technical Protection Mechanisms.....	9
4.4 Risk Management Process.....	10
4.5 Implementation roadmap.....	10
4.6 Cloud Service Provider Service Level Agreements (SLAs)	11
4.7 Metrics and KPIs.....	12
5. Discussion: Need for Updated Regulations and Standards.....	12
5.1 Major Reasons to update the information on a regular basis.....	12
5.2 Direct Benefits for NatureGreen	13
5.3 Difficulties and Solutions to Problems:	13
5.4 Critical Analysis	14
6. Conclusion	15
7. References	16

Abstraction

NatureGreen (NG) is an international health products enterprise that uses a largely wireless network, vast cloud computing and increased Bring Your Own Device (BYOD) application alongside containing very delicate personnel, customer and intellectual property information. This analysis determines the main information security threats faced by NG, such as the vulnerability of wireless networks, a misconfigured cloud network, unmonitored BYOD-based devices, and the impact of regulatory requirements in the framework of GDPR and similar regimes. Based on the well-established frameworks, like ISO 27001, NIST Cybersecurity Framework, ITIL, and COBIT, the report considers best practices in governance, risk management, and data protection within the environment of NG. It has then suggested a customized security, governance and compliance strategy that incorporates policy formulation, operational controls and a definite pathway towards the implementation which is fitted to the goals of the NG. The final objective of the report will be to enhance the security posture and the long-term survival of the NG through the introduction of constant improvement and regulatory conformity to its data security and governance competencies.

1. Introduction

The information technology has revolutionized the nature of businesses being conducted in business giving fast access, cloud computing and easier access to information. Nonetheless, it is also important to note that this new digital world poses more threats through cyber attacks that must be well controlled by companies. NatureGreen (NG) is an international organization that manufactures health products, and it has to endure such challenges. It uses wireless network in 95 per cent of its connections, uses cloud heavily and provides it employees and partners the opportunity to bring their own devices, based on a Bring Your Own Device (BYOD) policy. NG possesses valuable intellectual property and sensitive personal information, and, however, at the moment, it has disorderly security controls, unfinished policies, and a weak governance structure [1].

The report closely examines such security threats as NG is exposed to, including attacks on its wireless network, error or gap in cloud-based migration, uncontrolled BYOD threats, insiders threats, and social engineering threats. It also takes into consideration the confusing rules that NG should comply with with GDPR in Europe or CCPA in the US, and other legal regulations in all countries in which it operates.

This report aims at developing a security, governance, and compliance framework to suit the needs of NG. It checks internationally standardized and frameworks such as ISO 27001, NIST Cybersecurity Framework, ITIL, and COBIT [2].

2. Literature Review: Frameworks and Models

As a specification vital during the design of a strong security, governance and compliance program of NatureGreen (NG), this segment thoroughly discusses four popular information security frameworks and models of the company. These models can accommodate vital organizational requirements such as risk management, governance, process-based and alignment of security with business aim [3].

2.1 ISO 27000 Series

The ISO 27001, specifically the ISO 27000 family offers an internationally recognised standard of Information Security Management System (ISMS). It focuses on the avoidance of risks, constant

enhancement, and adherence to its legal and regulatory standards. The framework provided in ISO 27001 addresses asset and access control controls, cryptography, physical control, and incident control.

2.2 Information Technology Infrastructure Library (ITIL).

ITIL is an IT service management focused ITIL has a good governance and process orientation. It assists in matching IT services to the business requirements as it aids in security at service lifecycle, change management, and incident response. ITIL completes the ISO 27001 in that it integrates security into the operation process of IT [4].

Overview: NIST Cybersecurity Framework (CSF) provides a structure that assists and supervises the incorporation of the required security features in HIEs, thereby aiding patients' privacy and confidentiality.

Description: NIST Cybersecurity Framework (CSF) offers an outline that facilitates and manages the integration of the necessary security functionalities in HIEs, thus contributing to the privacy and confidentiality of patients.

2.3 COBIT (Control Objectives of Information and As applied Technologies)

COBIT offers practices embraced by governance and management of any enterprise IT, where renders high focus on regulatory compliance, performance measurement and strategic alignment.

Summary Table of Frameworks:

Framework	Focus Area	Strengths	Relevance to NatureGreen
ISO 27001	ISMS, Risk-based Security	International standard, certification readiness, continuous improvement	Foundation for NG's comprehensive security program and audits
NIST CSF	Cyber risk management	Flexible, detailed controls for cloud & wireless	Addresses NG's technical vulnerabilities & incident handling

ITIL	IT Service Management & Governance	Operational integration, incident/change management	Embeds security within NG's IT service processes
COBIT	IT Governance & Compliance	Strategic alignment, audit & compliance focus	Establishes governance, policy enforcement, accountability

2.4 Visual Aids

Use the diagrams of ISO 27001 PDCA cycle, NIST CSF five function wheel and ITIL service lifecycle. There are control areas and compliance requirements summarised in tables.

2.5 ISO 27001 PDCA cycle



The PDCA cycle of ISO 27001 is a continuous improvement model that is employed to control the safety of the information. During the Plan phase, an organisation determines the regions of its risks and determines the controls and policies required. These controls are introduced and the employees are trained in the Do stage. The Check phase involves audits and reviews conducted to determine that everything is proceeding as anticipated. Lastly, during the act stage the correction of any problems detected and the enhancement of the situation is completed. The cycle also makes the ISMS up to date, efficient and responsive to the dynamic security requirements [5].

2.6 NIST CSF five function wheel



1. Know your assets, risks, and environment- identify (ID).
2. Protect (PR): Implement a system of safeguards to ensure systems and data integrity.
3. Detect (DE): Observes and identifies threats or incidents within a short duration of time.
4. Respond (RS): Respond to contain and mitigate actions of incidents.
5. Recover (RC): Reestablish impaired services and enhance resiliency.

2.7 ITIL service lifecycle



1. Service Strategy (SS): Determines the services to be delivered and their reason. Pay attention to business objectives, needs of the market, value of services.
2. Service Design (SD): Transforms strategy to service blueprints. Design processes, technology, people, SLAs.
3. Service transition (ST): Results in the release of new/modified services into production. Dwelling on change management, testing, release & deployment.
4. Service Operation (SO): Identifies the management of service on daily operations. Special attention to accidents, issues, order requests, control of operations.
5. Continuous Service Improvement (CSI): Moves straight on. Concentrate on monitoring, reviewing, optimisation services [6].

3. NatureGreen risk and requirements analysis

NatureGreen (NG) functions in a complex and active cyber environment that offerings multiple safety challenges rising from its organization, operational performs, and regulatory requirements. Sympathetic these risks is crucial for designing an operative security outline.

3.1 NG has a number of threats with high impact:

- **Wireless Security Risks:** NG is open to Wi-Fi vulnerability because 95 percent of it refers to rogue access points, evil twin attacks, deauthentication, and the absence of WPA3 encryption. Lack of wireless intrusion detection system (WIDS) makes exposure to such attacks even worse.
- **Cloud Misconfigurations:** The misconfigured cloud services are dangerous threats like data leaks in open S3 buckets and poor identity and access management (IAM) systems.
- **BYOD Risk:** BYOD policy brings in uncontrolled endpoints that are likely to be infected with malwares, leak data and unauthorized access because of the lack of mobile device management (MDM) and endpoint controls [7].
- **Insider Threats:** The Data loss prevention (DLP) systems and stringent access panels are not essentially in place to host the threat of knowledgeable property theft, unplanned information leaks, or disruption.
- **Social Engineering:** NG has numerous online appearances, which kinds it a board of the phishing movement and other types of scheming attacks trusting on the inherent susceptibilities of humans.

3.2 Risk Assessment

Risk Category	Threat	Likelihood	Impact	Risk Score	Key Vulnerabilities
Wireless Security	Rogue AP/Evil Twin	High	High	Critical	95% wireless, no WPA3/WIDS
Cloud Security	Misconfiguration	High	Critical	Critical	Unmanaged IAM, no CSPM
BYOD Access	Malware/Data Leak	Medium-High	High	High	No MDM, inadequate endpoint control
IP Theft	Insider Threat	Medium	Critical	High	No DLP, insufficient access control

Social Media	Phishing Campaigns	High	Medium	High	No monitoring or user awareness
--------------	--------------------	------	--------	------	---------------------------------

4. Proposed security, governance and compliance approach

In order to mitigate severe security-related gaps observed in the NatureGreen environment, an all-inclusive and combined set of security, governance, and compliance controls are suggested.

4.1 Topline Technology, Inc. Security Governance Structure.

- The company will have a Chief Information Security Officer (CISO) who will report straight to the CEO. This makes certain that security has a voice in the executive level and is also in line with the general business strategy [9].
- It will establish a Security Steering Committee, which will consist of the CIO, CISO, Legal, HR, heads of major business units and Data Protection Officer. Policies and top priorities in investments and monitoring performance based on KPIs will be approved by this committee and it will review high-risk issues.
- A day-to-day surveillance, incident response, and vulnerability management and security tools will be the responsibility of a Security Operations Team (SOC analysts, incident responders, and engineers).
- A Policy and Compliance Officer will be in charge of ensuring the security policy framework, organizing the internal or external audits and monitoring regulatory provisions.
- Regional Security Leads will assist the international location whereby the global policies will be put into practice in a manner that reflects the local legal and cultural criteria.

4.2 Core Policy Framework

- BYOD Policy: It is a mandatory mobile device management (MDM) enrolment of any personal device to the corporate resources. Screen lock, encryption, anti malware and remote wipe. Definitely isolate the personal and corporate information using secure containers.

- Data Classification Policy: Public, Internal, Confidential and Restricted. The Intellectual Property automatically falls under the Restricted category. Customers and staff personal information as Confidential with extreme access limits and histories.
- Acceptable Use Policy: Company and BYOD internet, social media and email use policy. Ban on unauthorised software, back-door IT and unsecured storage (e.g. personal cloud accounts). Rules are enforced by integrating with technical controls e.g. web filtering and DLP [10].
- Cloud Security Policy: need to utilize licensed cloud service providers and conventional models (e.g. private endpoints, VPN). There is least privilege IAM role use, which is mandatory, encrypted at rest and in transit, and logging. Baselines and auto checks with Cloud Security posture Management (CSPM).

4.3 Technical Protection Mechanisms

- Identify: Automated discovery and maintenance of servers and endpoints, cloud resources and potentially critical applications maintained in a configuration management database (CMDB)
- Protect: Implement multi factor authentication (MFA) to vpn, email and privileged accounts and key applications. Install Endpoint Detection and Response (EDR) on the laptops, server and BYOD where feasible.
- Detect: Invest in cloud based Security Information and Event Management (SIEM) platform, which is used to gather endpoint, cloud, network and application logs. Install wireless intrusion detection systems (WIDS) and rogue access point detection in order to safeguard 95 percent of wireless environment [11].
- Define incident response playbooks Playbooks Not previously described Playbooks Unify the list of scenarios to include in the playbooks Intruder Spoiler: Ransomware, data exfiltration, insider misuse and cloud misconfiguration Driver: Definitions Intruder Spoiler: Intruders: The list can include ransomware, data exfiltration, insider misuse and cloud misconfiguration.
- Recover: Have immutable, and versioned backups of critical systems and data, which have off sidings with multi region replicas. Establish Recovery Time Objectives (RTO)

and Recovery Point Objectives (RPO) of essential services as well as certify that backup/DR architectures comply with it.

4.4 Risk Management Process

- Identify: Have quarterly business and IT workshops to determine new assets, changes and emerging threats.
- N.B. the combination of qualitative (high/medium/low) and quantitative (e.g. CVSS to prioritize technical problems, score business impact) should be used to rank risks.
- Decisions on each risk: - mitigate, transfer (e.g. insurance), avoid (change process) or accept with justification and sign off (documented).
- Monitor: To monitor key risks and mitigation controls using the SIEM dashboards, vulnerability management tools and audit reports [12].
- Review: Annually review the control effectiveness, revise risk appetite statements and reconcile with the change in strategy and regulation.

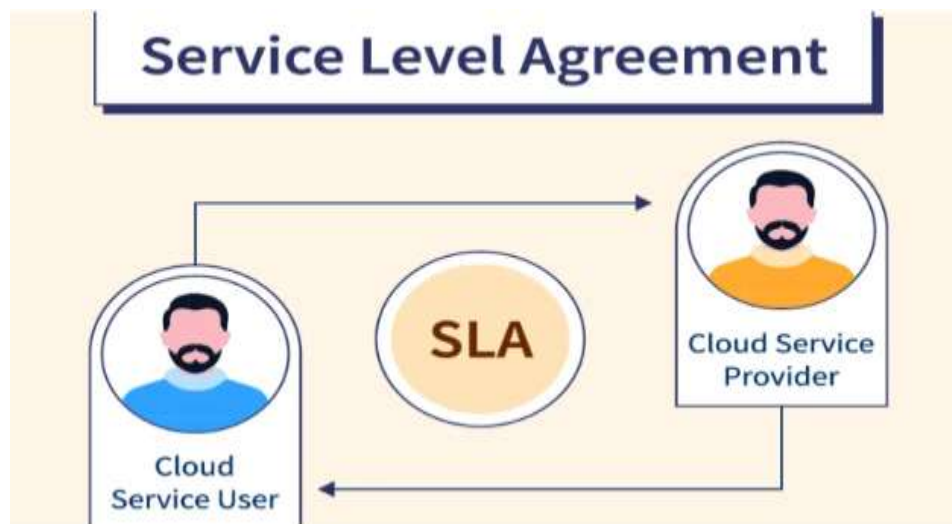
4.5 Implementation roadmap



Phase	Timeline	Key Deliverables	Owner

Phase 1: Foundation	Q1 2026	Governance structure, MFA, core policy rollout	CISO
Phase 2: Protect/Detect	Q2 2026	EDR, SIEM, Wireless hardening, BYOD MDM	Security Ops
Phase 3: Respond/Recover	Q3-Q4 2026	Incident response, BCP/DR, ISO 27001 certification efforts	All teams
Phase 4: Optimize	2027+	AI-driven threat hunting, zero-trust, continuous compliance	CISO

4.6 Cloud Service Provider Service Level Agreements (SLAs)



- Proximity: The services would be obtainable at slightest 99.99% of the period.
- Incident response: prescribed timelines within which security incidents should be notified (e.g. one hour with high severity incidents) and distinct roles in the shared responsibility model [13].
- Compliance: Operations have been demonstrated in terms of independent audits like ISO 27001, SOC 2 Type II and data residency support measures.
- Security measures: Customer controlled key encryption keys, logging, IAM, and network controls, like the integration of private endpoints and the WAF.

- Consistency in data management Data location, data holding, data removal, and data handling are obviously defined at the conclusion of agreement.

4.7 Metrics and KPIs

- Coverage: EDR installations Percentage of employment furnishings installed. Fraction of accounts safeguarded by MFA. The percentage of systems that are adhered to by SIEM logging.
- efficacy of control: Patching percentage on critical security flaws in agreed SLA (e.g. 14 days). Count of high risk misconfigurations that CSPM identified and improved every month. Phishing simulated percentage and reporting rate.
- Incident metrics Mean time to detect (MTTD) and mean time to respond (MTTR) security incidents. Major incidents recorded and how they affect the business per quarter [14].
- Governance and awareness: Rate of policy acknowledgement. Conclusions of security training and awareness. Count of uncovered audit findings and their remediation status.

5. Discussion: Need for Updated Regulations and Standards

The high pace of the technological growth requires constant changes in security regulations and standards. NatureGreen (NG) is a business that competes in an environment that is dynamically bound by threats that force relative frameworks out of use within a very short amount of time, rendering the regulatory evolution not only useful, but a necessity to survive.

5.1 Major Reasons to update the information on a regular basis.

- Technological Acceleration: Cloud-native infrastructure, 5G wireless networks, etc., and IoT proliferation, and AI-enabled attacks have surpassed standards. The ISO 27001:2022 now had an expanded cloud services control, supply chain security control, and threat intelligence control, which was not previously included in the 2013 edition. NIST CSF 2.0 new Govern function is explicitly related to executive oversight and supply chain risks after similar incidents such as the SolarWinds [15].
- Changing threat landscape: Agreements involving ransomware affect healthcare directly affecting the sector of NG. Since the implementation of GDPR, the enforcement has been

even stricter since Schrems II that imposes fines up to 1.2B against Meta (2023) due to poor data transfer regulations.

- Fragmentation: NG will have to deal with GDPR (EU), CCPA/CPRA (California), PIPL (China), and DORA (EU financial services) globally. All of them develop separately, though DORA requires more severe resilience testing, and NIS2 Directive increases critical infrastructure requirements.

5.2 Direct Benefits for NatureGreen

Benefit	Impact on NG
Risk Reduction	Updated NIST controls mitigate zero-day wireless/cloud exploits targeting health IP
Compliance Assurance	ISO 27001:2022 aligns with DORA and NIS2 for NG's international operations
Competitive Advantage	SOC2 Type II + ISO certification differentiates NG in health products market
Insurance Eligibility	Cyber policies increasingly require current framework compliance

5.3 Difficulties and Solutions to Problems:

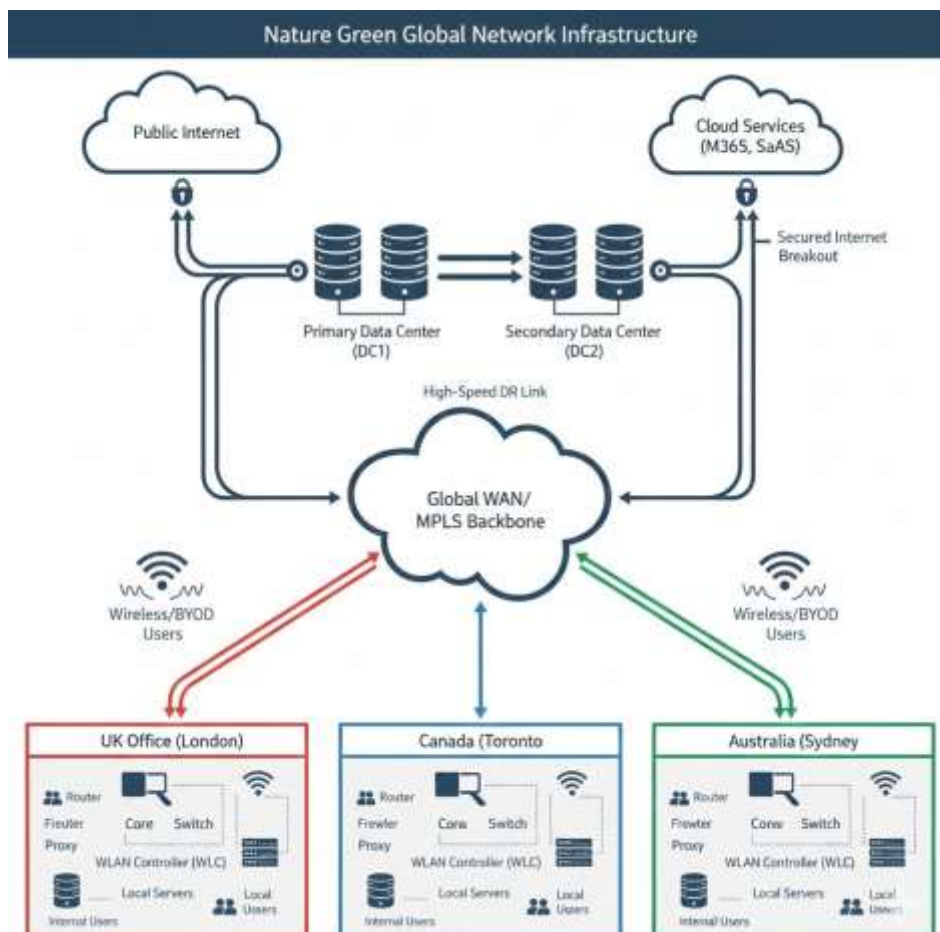
- Resource Strain: Resource intensive (~50 staff) Annually updating standards. Recommendation: Obedience concluded Cloud Security Posture Management (CSPM) and Governance, Risk, and Compliance (GRC) tackles and stages like as ServiceNow or Archer would be automatic.
- Jurisdictional Conflicts: GDPR data residency and business requirements of international cloud. Solution Regional security takes the lead in the form of centralized policy governance and data residency mapping [16].
- Implementation Lag: Standards are developed at a higher rate as compared to enterprise adoption. Recommendation: The phased roadmap of NG (Phase 4: continuous compliance automation) where the horizon is scanned quarterly.

5.4 Critical Analysis

Older standards have harmful vulnerabilities - 95 percent of wireless networks should require WPA3 but lots will still have WPA2. BYOD pressure at NG necessitates updated MDM that was not present in outdated frameworks. One can expect average breach detection on on-oznake with the use of static compliance, whereas with constant updates, one can guarantee under 48 hours to date.

The market structure ought to be equitable to all participating in the market. NG-Specific Policy Recommendation:

- Sergeant: There have to be annual reviews of standards by the Security Steering Committee [18].
- Implementation planning of critical updates in 90 days.
- Biannual tabletops (emulating emergent pressures (significant risks, AI social engineering, 5G achievements))



6. Conclusion

The 95% wireless network, high use of clouds, BYOD forces, lack of governance, and billion dollar IP portfolio face naturegreen (NG) with a serious security threat [18]. This report addresses them effectively in a coordinated attempt to encompass them in an integrated system based on ISO 27001 (systematic risk management), NIST CSF (technical controls), ITIL (operational integration), and COBIT (strategic governance).

The solution provided will bring about immediate reduction risk through priority controls - MFA rollout, EDR rollout, SIEM rollout, WPA3/WIDS wireless hardening, and strategic governance (CISO-led Security Steering Committee, extensive policy framework, Q1-Q4 2026 staged roadmap). It minimally alleviates the vulnerability areas that NG is most vulnerable to: rogue AP attacks, cloud misconfigurations, BYOD malware, insider IP theft. The achievement of success will be guaranteed by measuring KPIs: MFA ≥ 95 , MTTR 01-hour, patch compliance 92.

Impairments: High-level design: the requirements presuppose moderate IT maturity; the specifications (SIEM rulesets, wireless heatmaps) are to be NG-aware, which is to be confirmed throughout penetration testing.

Recurrent regulatory changes (ISO 27001:2022, NIST CSF 2.0) are also important to the global activities of NG. The governance form legalizes flexibility, secures IP, and responds to GDPR demand, as well as customer assurance. The realization of roadmaps makes NG a leader in the security of the health sector.

7. References

- [1] S. Qu, H. Wu, and Y. H. Ng, “Clean production of hydrogen peroxide: A heterogeneous solar-driven redox process,” *Advanced Energy Materials*, vol. 13, no. 36, Aug. 2023, doi: 10.1002/aenm.202301047.
- [2] R. Fedorov *et al.*, “Zooming in on Arctic urban nature: Green and blue space in Nadym, Siberia,” *Environmental Research Letters*, vol. 16, no. 7, p. 075009, Jun. 2021, doi: 10.1088/1748-9326/ac0fa3.
- [3] R. C. Prince, G. N. George, and A. L. Stevens, “Nature green with avarice and greed,” *Plant Physiology Reports*, vol. 27, no. 4, pp. 625–631, Nov. 2022, doi: 10.1007/s40502-022-00696-3.
- [4] C. Demanuele *et al.*, “Considerations for conducting bring your own device (BYOD) clinical studies,” *Digital Biomarkers*, vol. 6, no. 2, pp. 47–60, 2022, doi: 10.1159/000525080.
- [5] C. I. Eke, A. A. Norman, and M. Mulenga, “Machine learning approach for detecting and combating bring your own device (BYOD) security threats and attacks: A systematic mapping review,” *Artificial Intelligence Review*, Jan. 2023, doi: 10.1007/s10462-022-10382-3.
- [6] J. Jevelin and A. Faza, “Evaluation of the information security management system: A path towards ISO 27001 certification,” *Journal of Information Systems and Informatics*, vol. 5, no. 4, pp. 1240–1256, Nov. 2023, doi: 10.51519/journalisi.v5i4.572.
- [7] A. Calder and S. Watkins, *IT Governance: An International Guide to Data Security and ISO 27001/ISO 27002*, 8th ed. Ely, U.K.: IT Governance Ltd., 2024.
- [8] B. Kenyon, *ISO 27001 Controls: A Guide to Implementing and Auditing*. Ely, U.K.: IT Governance Ltd., 2020.
- [9] J. Carlos and C. Valeria, “Aplicación de la norma ISO 27001 para la seguridad de los sistemas de información,” *Dominio de las Ciencias*, vol. 8, no. 3, p. 14, 2022. [Online]. Available: <https://dialnet.unirioja.es/descarga/articulo/8635191.pdf>
- [10] D. P. F. Möller, “NIST cybersecurity framework and MITRE cybersecurity criteria,” in *Advances in Information Security*, vol. 103. Cham, Switzerland: Springer, 2023, pp. 231–271, doi: 10.1007/978-3-031-26845-8_5.
- [11] G. B. White and N. Sjelin, “The NIST cybersecurity framework,” in *Research Anthology on Business Aspects of Cybersecurity*. Hershey, PA, USA: IGI Global, 2022. [Online]. Available: <https://www.igi-global.com/chapter/the-nist-cybersecurity-framework/288672>
- [12] M. F. Delgado, D. Esenarro, F. F. J. Regalado, and M. D. Reátegui, “Methodology based on the NIST cybersecurity framework as a proposal for cybersecurity management in government

organizations,” *3C TIC: Cuadernos de Desarrollo Aplicados a las TIC*, vol. 10, no. 2, pp. 123–141, 2021. [Online]. Available: <https://dialnet.unirioja.es/servlet/articulo?codigo=8091397>

[13] D. Wang, D. Zhong, and L. Li, “A comprehensive study of the role of cloud computing on the information technology infrastructure library (ITIL) processes,” *Library Hi Tech*, early access, Jul. 2021, doi: 10.1108/LHT-01-2021-0031.

[14] A. Rusman, R. Nadlifatin, and A. P. Subriadi, “Information system audit using COBIT and ITIL framework: A literature review,” *Sinkron*, vol. 7, no. 3, pp. 799–810, Jul. 2022, doi: 10.33395/sinkron.v7i3.11476.

[15] A. C. Amorim, M. Mira da Silva, R. Pereira, and M. Gonçalves, “Using agile methodologies for adopting COBIT,” *Information Systems*, vol. 101, p. 101496, Feb. 2020, doi: 10.1016/j.is.2020.101496.

[16] F. Muttaqin *et al.*, “Measurement of the IT helpdesk capability level using the COBIT 5 framework,” *Journal of Physics: Conference Series*, vol. 1569, no. 2, p. 022039, Jul. 2020, doi: 10.1088/1742-6596/1569/2/022039.

[17] A. J. Fernandes, H. Hartono, and C. Aziza, “Assessment of IT governance of human resources information system using COBIT 5,” *Int. J. Open Information Technologies*, vol. 8, no. 4, pp. 59–63, 2020. [Online]. Available: <https://cyberleninka.ru/article/n/assessment-it-governance-of-human-resources-information-system-using-cobit-5>

[18] F. Lorè, P. Basile, A. Appice, M. de Gemmis, D. Malerba, and G. Semeraro, “An AI framework to support decisions on GDPR compliance,” *Journal of Intelligent Information Systems*, Mar. 2023, doi: 10.1007/s10844-023-00782-4.