



**APPLY THE PRINCIPLES AND PRACTICES OF DATA
SECURITY, GOVERNANCE AND COMPLIANCE BASED ON A
GIVEN SCENARIO.**

Program: MSc/PgDip/PgCert Cybersecurity and Digital Forensics

Module: Data Security, Governance and Compliance

Module Code: ACCA7028

Lecturer: Dr. Dipo Dunsin

Name: Sohanur Rahman

Student ID: 2434329

APPLY THE PRINCIPLES AND PRACTICES OF DATA SECURITY, GOVERNANCE AND COMPLIANCE BASED ON A GIVEN SCENARIO.

Abstract

The overall report examines how NatureGreen (NG) is able to improve its overall data security, governance along with compliance as it expands its global operation and also adopts cloud services, wireless network and others. This study reviews several cybersecurity frameworks including ISO 27001, NIST CSF, COBIT, ITIL, and Zero Trust in order to identify their both strength and relevance to NG. Based on the research, both hybrid security model and governance structure is proposed. Also, this report also includes risk assessment, compliance strategy and technical safeguards along with an incident response plan in order to support both secure and compliant operations. A critical discussion mainly highlights the need for the continuous up-to-date policies and standards for evolving cyber threats, technology change and legal requirements. The findings show that NG needs to apply continuous improvements, strong governance along with adaptive control in order to protect data, maintain data compliance and also ensures long-term business resilience.

Table of Contents

<u>I. INTRODUCTION</u>	<u>2</u>
<u>II. OVERVIEW OF THE CASE SCENARIO</u>	<u>2</u>
<u>III. RESEARCH INTO SECURITY FRAMEWORKS AND MODELS</u>	<u>3</u>
<u>IV. DESIGNING A SECURITY APPROACH FOR NATUREGREEN (NG)</u>	<u>9</u>
<u>V. DISCUSSION AND CRITICAL EVALUATION</u>	<u>15</u>
<u>VI. CONCLUSION</u>	<u>17</u>
<u>REFERENCE.....</u>	<u>18</u>

I. INTRODUCTION

NatureGreen (NG) is a global company known for selling products that mainly support healthy living. This organization operates across several countries and also uses cloud service in order to support communication, data storage along with service delivery. Almost 95% of its network is wireless and where business has a strong online and social media presence. Due to the large number of employees and international customers, NG is facing pressure in order to allow both groups to use their own personal devices to access company system. Overall, the company needs to protect sensitive staff data, customer information along with valuable intellectual property. As NG continues to depend on both cloud technology and wireless networks, where cybersecurity risks are increasing. In that case, the modern cyber threats has become more advanced where attackers are targeting systems from anywhere in the world. Multiple aspects such as cloud-based system, wireless networks along with bring your own device environments are able to create possible entry points for attackers. Without any proper controls along with clear security policies, the company may be exposed to data breaches, financial losses, and legal consequences along with damage to its reputation.

The main purpose of this report is to conduct research that is recognized security frameworks and models along with designing a proper security governance approach suitable for the NG. This report also examines the overall importance of having up-to-date regulations, policies along with industry standards. In that case, strong information security, data compliance, and governance plays an important role for NG in order to protect its assets, meet legal requirements, maintaining customer trust along with support long-term business stability.

II. OVERVIEW OF THE CASE SCENARIO

NatureGreen (NG) is an international organization that is well-known for its health-focused product range and strong global brand. The company has been overly dependent on digital technology as a means of conducting business, communicating, and interacting with the customers.

The majority of its IT infrastructure (approximately 95 percent) is wireless, and it has cloud services to store data and support internal and external services. Online platforms and social media are also relied on by NG to advertise its brand and communicate with its customers globally.

With its growing number of workforce, and international customer base, NG is increasingly required to enable personal devices like smartphones, tablets, and laptops to connect to its systems. Although it can enhance the convenience and productivity of the user, BYOD access also poses significant security issues. They consist of threats to personal data, client information, and billions worth of intellectual property. At present, NG does not have formal security policies and governance structures. In the absence of these controls, the organization is susceptible to cyber threats, data breaches, and legal compliance issues. The situation shows that an integrated security strategy should be implemented, involving frameworks, risk management, and frequent updates to safeguard company assets and guarantee safe and compliant business in a highly dynamic digital world.

ITIL Lifecycle Stage	Purpose
Service Strategy	Defines goals, policies, and service value
Service Design	Plans infrastructure, security, availability, and continuity
Service Transition	Ensures safe implementation of changes
Service Operation	Supports daily service delivery and incident response
Continual Service Improvement	Reviews and improves service performance

III. RESEARCH INTO SECURITY FRAMEWORKS AND MODELS

In order to protect organizational data and manage cybersecurity risks effectively, different companies are using recognized security frameworks and models [16]. These framework provides proper structured guidance on how to manage information, protect system along with maintaining compliance. For NatureGreen (NG), selecting a proper and suitable framework plays an important

role as the company operates through cloud technology, wireless networks and many others. The following section discusses five major security frameworks and models relevant to NG.

3.1 Information Technology Infrastructure Library (ITIL)

The information technology infrastructure works as a framework in order to manage IT services in a structured and efficient way. Its main purpose is to ensure that the IT service supports organizational goals during maintaining both operational stability and service quality [9]. It is relevant for the security management as it mainly includes processes including incident management, access control, configuration management along with change control that help to maintain several secure operations.

One of the important features of ITIL is support for the service-level agreements. It defines a measurable expectation in between the service providers and users such as security, availability and response times. For this selected company, it helps to structure the cloud service that defines BYOD usage rules and ensures consistent service quality across global operations.

3.2 ISO/IEC 27000 Series Security Model

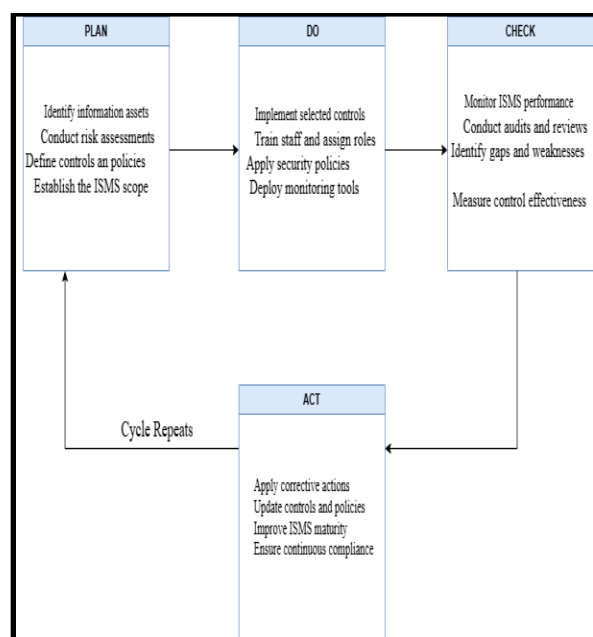
The ISO/IEC 27000 family has been widely recognized international standard for information security management [15]. It provides a structured way in order to manage risks, apply controls along with achieve compliance with several global security expectations.

Standard	Focus Area
ISO 27001	Information Security Management System (ISMS) [7].
ISO 27002	Best-practice security controls and guidelines
ISO 27005	Risk management strategy and assessment [13]

For NG, ISO 27001 is very relevant as it helps to define a full security governance system. It supports several areas such as access control, network protection, data classification, business

continuity along with compliance. It can help NG to address risks that are related to wireless networks, cloud services and personal devices.

ISO 27001: Plan–Do–Check–Act (PDCA) Cycle



The continuous cycle ensures that security practices evolve with threats. For NG, failing to update control could lead to data breaches, reputation loss along with regulatory penalties. It supports compliance, security improvement along with long-term risk reduction.

Domain	Purpose
Identify	Understand assets, risks, and environment
Protect	Apply safeguards including encryption and access control
Detect	Monitor and identify unusual and malicious activity
Respond	Takes action during a security incident
Recover	Restore systems and improve future resilience

3.3 NIST Cybersecurity Framework (CSF)

The *National Institute of Standards and Technology (NIST)* framework has been

designed in order to help organization prevent, detect and respond to cyber threats [2]. It is widely used in both public and private sectors and it provides clear guidance in order to manage cybersecurity controls. Several key domains are includes,

This above framework fits NG's cloud and wireless system as it supports a flexible environment and scalable control. For example, both detection and response stages are essential for NG as both cloud and BYOD devices increase the attack surface. NIST supports integration with the existing tools such as identify management system, monitoring software, along with automated security reporting (Aljumaiah *et al.* 2025).

3.4 COBIT Framework

COBIT (Control Objectives for Information and Related Technologies) is an enterprise governance framework. NIST, ISO and COBIT have been focused on aligning IT, business processes, compliance along with risk management [6]. It helps organization in order to create policies, assign responsibilities and measure cybersecurity performance. COBIT is suitable for NG where the company has no current security governance model, and it can provide,

- Clear roles and accountability
- Policy and compliance structure
- Proper link in between business strategy and technology decisions

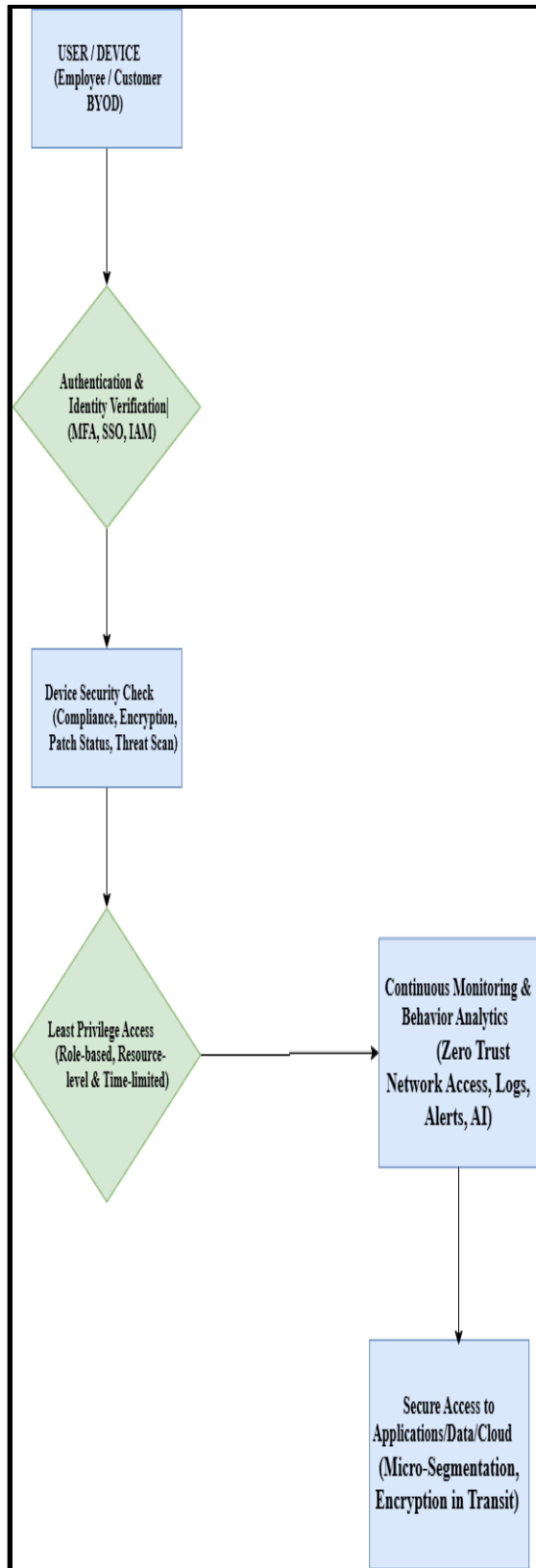
This framework helps to ensure that cloud services, wireless systems and BYOD are monitored under a controlled process rather than unmanaged access [1]. It ensures transparency, governance along with alignment with legal standards.

3.5 Zero Trust Architecture (ZTA)

Zero Trust works as a modern security model that is based on the principle ***“Never trust, always verify.”*** The traditional network security that trusts internal users where Zero Trust assumes that all users, devices and network connections may be at risk [12]. This model is very useful for the NG as this company allows personal devices, remote access along with international cloud system. Several key components are present, and these are discussed in the session below,

- Identity verification (multi-factor authentication)
- Device security checks
- Least privilege access
- Continuous monitoring

A simple Zero Trust model:



3.6 Comparison Matrix of Frameworks

Framework	Strengths	Weaknesses	Best Use for NG
ITIL	Helps to improve IT service management and SLAs.	Not focused only on cybersecurity	It helps to improve IT operations along with service delivery.
ISO 27000	Strong compliance and risk management [20]	Certification may be costly	Provide data protection, compliance and structured control.
NIST CSF	Flexible, modern, and detailed	It required integration with the other frameworks	Both cloud and wireless security operations [22].
COBIT	Strong governance along with organization-wide control	Complex implementation	Helps to build security governance and accountability.
Zero Trust	Excellent for BYOD and cloud	Requires technical maturity [8]	Mitigate several unauthorized access and help to reduce internal risks.

Each of the frameworks brings multiple strengths. For NatureGreen, a combination approach of ISO 27001 (compliance), NIST (cyber controls), COBIT (governance), and Zero Trust (technical access control) creates a strong and complete cybersecurity system that is suitable for cloud-based and wireless environments.

IV. DESIGNING A SECURITY APPROACH FOR NATUREGREEN (NG)

In order to protect its cloud system, wireless environments, BYOD access, and intellectual property where NatureGreen has required a strong and structured security approach. This section presents a proposed security governance framework, key security policies, and risk management along with contingency planning.

4.1 Proposed Security Governance Framework for NG

Based on the scenario, the hybrid security model by using *ISO 27001, NIST Cybersecurity Framework, and Zero Trust Architecture* has been recommended.

- ISO 27001 provides a structured governance system and compliance approach [19].
- NIST CSF helps NG in order to manage detection, response and recovery [5].
- Zero Trust helps to protect both cloud and wireless environment by ensuring no user and device is trusted by default.

Overall, these framework provides a balanced approach for the governance, compliance and technical security.

Before evaluating the security approach, several assumption must be made. According to the case study, NG uses public cloud SaaS and IaaS model that has a medium-maturity IT environment that operates in several jurisdiction such as GDPR and CCPA and also supports approximately 5000-10000 personal and corporate devices for the BYOD policy pressure. These assumption helps to shape the governance scope along with compliance requirements.

Governance Structure, Roles and Responsibilities (RACI Matrix)

R = Responsible, A = Accountable, C = Consulted, I = Informed

Role / Task	CISO	IT Admin	Legal/Compliance	Employees	Cloud Vendor
Create security policies	R	A	C	I	I
User access management	C	A/R	I	R	I
Incident response	A	R	C	I	C

Compliance reporting	R	I	A	I	C
Backup and disaster recovery	A	R	I	I	C

The earlier RACI matrix has been identified roles where its purpose needs interpretation. The RACI structure ensures the accountability through clarifying who approves (Accountable), executes (Responsible), supports (Consulted), and is informed (Informed). Also, it helps to prevent gaps during incident, compliance reporting along with access management. Without any model, tasks may be duplicated and ignored that creates operational risks. From the COBIT mapping perspective, it supports domain including EDM03 (Ensure Risk Optimization) and DSS02 (Manage Service Requests and Incidents).

4.2 Information Security Policies and Controls

In order to support secure operations, NG needs to introduce formal policies, and these are discussed in the below session,

Safeguard	Function
Multi-Factor Authentication (MFA)	Prevents unauthorized login
Encryption (AES-256)	Protects data storage and transmission
Firewall and IDS/IPS Systems	Blocks suspicious traffic and detects attacks
Security Operations Centre (SOC)	24/7 monitoring and response
Endpoint Protection	Protects BYOD devices and internal systems
Access Control (RBAC + Least Privilege)	Restricts access based on role and need

- **BYOD Policy**

Both employees and customers are accessing system by using personal devices that must register their devices along with comply with the security rules including multi-factor authentication, encryption and automatic updates [18].

- **Wireless Security Policy**

All the internal wireless networks need to use WPA3 encryption, segmented guest networks, and Zero Trust monitoring for data security.

- **Cloud Governance Policy**

The cloud resources need to follow role-based access control, logging requirements along with data encryption in data transit and at rest [10].

- **Intellectual Property Protection Policy**

Access to the sensitive research, formulas along with proprietary material has been required both approval and logging. In that case, data needs to be watermarked along with stored in the restricted repositories.

- **Data Classification and Retention Model**

There are four levels in the retention model where Level 1: Public, Level 2: Internal, Level 3: Confidential and Level 4: Highly Restricted (IP, customer data) [4].

A mature governance operating model has been required executive oversight. In the high-performing organization, cyber security governance is reported to the Board Cybersecurity Committee or CIO-level steering group. It ensures the alignment in between the business priorities along with regulatory requirements. The compliance

Threat	Asset at Risk	Likelihood	Impact	Risk Level	Recommended Mitigation
Cyberattack (Phishing, Malware)	Staff accounts, cloud apps	High	High	Critical	MFA, phishing training, email filtering
Unsecured BYOD devices	Data, systems	High	High	Critical	Zero Trust access, endpoint protection
Wireless network attack	IP and customer data	Medium	High	High	WPA3, segmentation, monitoring
Data breach in the cloud	Customer data	Medium	High	High	Encryption, access logs, SOC monitoring
Intellectual property theft	Research and formulas	Low	Very High	High	Access restrictions, watermarking, DLP tools

reporting needs to follow an annual cycle such as quarterly internal audit, annual ISO 27001 surveillance review, vendor compliance assessments, and KPI-based reporting for the board.

4.3 Risk Management Plan

The company needs to follow a proper risk management process based on the ISO 27005 and NIST RMF [21]. Several aspects are present such as identifying threats, classifying assets, evaluating vulnerabilities along with applying mitigation control.

4.4 Security Management and Compliance Strategy

NatureGreen must comply with both local and international regulations including **GDPR, CCPA, and ISO 27001** compliance requirements. Data compliance should be regularly monitored by

applying internal audits, security reporting along with third-party assessments. The service level agreements with the cloud provider must be included [11].

SLA Requirement	Example
Availability	Minimum 99.9% uptime
Security Controls	Encryption, access logs, vulnerability testing
Incident Response Time	1–4 hours depending on severity
Data Location & Sovereignty	Stored in approved locations

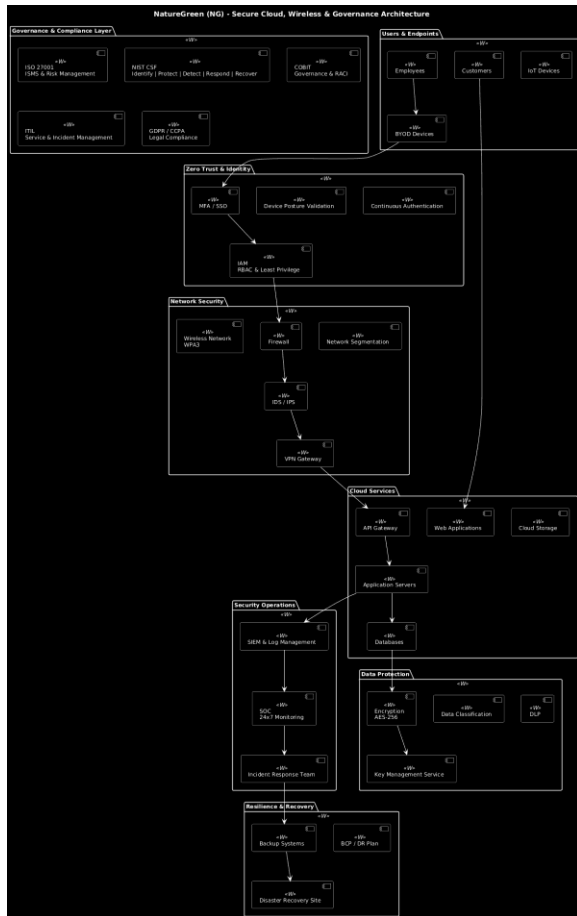
The ongoing monitoring will be supported by several vulnerabilities scans, penetration testing along with annual audits.

4.5 Protection and Technical Safeguards

In order to enforce the framework, NG needs to deploy modern technical controls.

Technical Safeguards Table

System architecture diagram



The security architecture diagram represents how the NatureGreen security controls perform together in order to protect system, cloud service and wireless networks. In that case, the governance layer guides both policies and standards by using **ISO 27001**, **NIST**, and **Zero Trust Identity and Access Management** that enforces both authentication and role-based access. Also, the network layer separates end users, wireless systems along with cloud environments that helps to reduce business risks. Several security controls such as firewalls, intrusion detection along with encryption protect data in motion [17]. For this, both backup and disaster recovery ensure resilience during monitoring and auditing provides continuous oversight.

A major weakness is many organization is the assumption that frameworks are static. The modern cybersecurity has been required adaptive control. ISO 27001 provides a strong governance in order to adopt emerging threats. NIST CSF is very flexible and it still required operational maturity. On the other hand, Zero Trust is future-focused where implementation challenges exist when the legacy system where IoT devices are involved.

4.6 Contingency Planning and Incident Response



This diagram shows the overall incident response along with the contingency planning lifecycle for NatureGreen. This process starts with the preparation where this organization creates several policies, assigns roles and ensuring staff training. Overall, threats have been detected through regular monitoring system and security alerts. If an attack occurs then the containment steps are taken in order to stop damage and isolated affected system. Overall, reviews take place in order to identify lessons and improves the plan for the future. This approach helps NatureGreen to reduce disruption, protect data along with recover faster after a security incident.

V. DISCUSSION AND CRITICAL EVALUATION

In today's digital world, cyber threats are increasing in a faster way with the proper use of cloud computing, wireless networks along with Internet of Things (IoT) devices [23]. For the fast-changing environment, the security regulations, frameworks and security standard needs to be updated. An organization like NatureGreen is being exposed to attack, compliance failures along with operational disruption. On the other hand, cybercriminals are developing several new methods including ransomware, phishing, insider attacks, and AI-powered malware. WannaCry ransomware attack in 2017 affected more than 200000 systems worldwide as the companies failed to update old security patches. This example shows that the outdated frameworks are able to create several major weaknesses. Cloud system are changing fast where many organizations now use multi-cloud environments, remote access and others model [24]. Without any updated policies, the new system is able to create vulnerabilities. A major example is 2023 Microsoft Exchange cloud breach that mainly exposed the authentication keys that is allowed attackers in order to access emails from both government and corporate users. It happens partly because security controls did not match modern cloud risks. Also, the regulatory compliance is another important reason for updating frameworks. Several laws such as **GDPR (2018)**, **California Consumer Privacy Act (CCPA)**, and **international data protection regulations** continues to evolve [14]. Companies who are not follow these requirements can faces large penalties where British Airways was fined £20 million under GDPR after customer data was stolen due to outdated security along with weak monitoring. For NG, failing compliance can damage organization's reputation that resulting in

legal costs and reducing customer trust. In that case, IoT devices are posing another challenge as they often lack built-in security along with receive fewer updates. The smart devices in the entire agriculture, buildings along with logistics that are able to use as attack's entry points. In that case, the Mirai botnet attack in 2016 that shut down several major websites such as Amazon and Netflix that happened as attackers are controlled insecure IoT devices [3]. It shows how old and simple devices are threatening even large organization. If NG continues using several outdated security policies where several consequences may occur,

- Higher risks of cyber attacks due to unpatched systems
- Can face financial loss from different aspects such as ransomware, fraud and downtime.
- Both legal and regulatory penalties for non-compliance
- Loss of customer confidence along with brand reputation
- Facing operation delays and business interruptions

The continuous improvement based on several global frameworks such as ISO 27001, NIST CSF, COBIT, and Zero Trust helps organization in order to remain secure and compliant. The regular updates ensure the proper alignment with several new technologies including AI-driven threat monitoring, advanced encryption along with automated policy enforcement. On the other hand, cybersecurity is not static and for organizations such as NatureGreen where updating frameworks, regulations along with standards are important in order to protect assets, maintain compliance and respond to new cyber threats. Without continuous improvement security has become outdated where organization have become an easy target for the attackers.

VI. CONCLUSION

In conclusion, the report has examined the current security challenges that are facing NatureGreen as it grows globally and also introduced cloud service, wireless networks along with BYOD access. The increasing level of cybersecurity threats along with sensitivity of the company's data shows a strong need for a proper, structured and well-managed security approach. By reviewing important frameworks such as ISO 27001, NIST CSF, ITIL, COBIT, and Zero Trust is clear that no single model is enough on its own. A combined approach provides the best balance in between governance, risk management, compliance along with technical protection. The proposed hybrid frameworks support business policies, risk planning, secure access control and monitoring responsibility structures. A detailed risk management plan along with protection mechanisms including encryption, MFA, firewalls, and disaster recovery helps NG in order to protect both staff and customer data while ensuring business continuity. Overall, cybersecurity must be seen as an ongoing process where threats, technology along with regulations continue to evolve, and NG needs to regularly update its standards, policies and controls. With proper governance and continuous improvement, NG is able to protect its intellectual property, maintains customer trust along with support long-term secure growth.

Reference

- [1] Al Harthy, K., 2022. A Risk Management Framework for the BYOD Environment. Available at https://pureportal.coventry.ac.uk/files/80093962/AlHarthy_2022_PhD.pdf
- [2] Aljumaiah, O., Jiang, W., Addula, S.R. and Almaiah, M.A., 2025. Analyzing cybersecurity risks and threats in IT infrastructure based on NIST framework. J. Cyber Secur. Risk Audit, 2025(2), pp.12-26. Available at <https://jcsra.thestap.com/articles/v-2025-i-2-p-2.pdf>
- [3] Al-Marsoomi, O.A.H., 2022. DDOS attack by botnet infected IoT devices detected based on deep learning models. Available at <https://openaccess.altinbas.edu.tr/items/8a736101-f698-4e7a-b05c-c52f79642c7e>
- [4] Cardona, T., Cudney, E.A., Hoerl, R. and Snyder, J., 2023. Data mining and machine learning retention models in higher education. Journal of College Student Retention: Research, Theory & Practice, 25(1), pp.51-75. Available at <https://journals.sagepub.com/doi/abs/10.1177/1521025120964920>
- [5] Dimakopoulou, A. and Rantos, K., 2024. Comprehensive analysis of maritime cybersecurity landscape based on the NIST CSF v2. 0. Journal of Marine Science and Engineering, 12(6), p.919. Available at <https://www.mdpi.com/2077-1312/12/6/919>
- [6] Efe, A., 2023. A comparison of key risk management frameworks: COSO-ERM, NIST RMF, ISO 31.000, COBIT. Denetim ve Güvence Hizmetleri Dergisi, 3(2), pp.185-205. Available at <https://dergipark.org.tr/en/pub/audas/issue/79262/1291915>
- [7] Fonseca-Herrera, O.A., Rojas, A.E. and Florez, H., 2021. A model of an information security management system based on NTC-ISO/IEC 27001 standard. IAENG Int. J. Comput. Sci, 48(2), pp.213-222. Available at https://www.researchgate.net/profile/Alix-E-Rojas/publication/362062660_A_Model_of_an_Information_Security_Management_System_Based_on_NTC-ISOIEC_27001_Standard/links/62d485bcd351bd24f51fa7c5/A-Model-of-an-Information-Security-Management-System-Based-on-NTC-ISO-IEC-27001-Standard.pdf

- [8] Ghasemshirazi, S., Shirvani, G. and Alipour, M.A., 2023. Zero trust: Applications, challenges, and opportunities. arXiv preprint arXiv:2309.03582. Available at <https://arxiv.org/abs/2309.03582>
- [9] Gunawan, H., Irianto, A.B.P. and Negara, J.G.P., 2024. Implementation of sustainable service improvement in organizations using framework information technology infrastructure library (ITIL). *Procedia Computer Science*, 234, pp.748-755. Available at <https://www.sciencedirect.com/science/article/pii/S1877050924004198>
- [10] Harper, C., 2025. ROLE-BASED ACCESS CONTROL (RBAC) AND ENCRYPTION TECHNIQUES FOR ENHANCING RELATIONAL DATABASE SECURITY. Available at https://www.researchgate.net/profile/Carter-Happer/publication/392346447_ROLE-BASED_ACCESS_CONTROL_RBAC_AND_ENCRYPTION_TECHNIQUES_FOR_ENHANCING_RELATIONAL_DATABASE_SECURITY/links/683ea7c56b5a287c3048e6c5/ROLE-BASED-ACCESS-CONTROL-RBAC-AND-ENCRYPTION-TECHNIQUES-FOR-ENHANCING-RELATIONAL-DATABASE-SECURITY.pdf
- [11] Ilori, O., Nwosu, N.T. and Naiho, H.N.N., 2024. Third-party vendor risks in IT security: A comprehensive audit review and mitigation strategies. *World Journal of Advanced Research and Reviews*, 22(3), pp.213-224. Available at https://www.researchgate.net/profile/Oluwatosin-Ilori-3/publication/381844798_Third-party_vendor_risks_in_IT_security_A_comprehensive_audit_review_and_mitigation_strategies/links/669dbae88dca9f441b8edff2/Third-party-vendor-risks-in-IT-security-A-comprehensive-audit-review-and-mitigation-strategies.pdf
- [12] Jena, K., 2023. Zero-Trust Security Models Overview. *International Journal of Scientific Research in Computer Science, Engineering and Information Technology*, 578. Available at <https://www.academia.edu/download/108965743/CSEIT2390578.pdf>
- [13] Junior, A.S.C. and Arima, C.H., 2023. Cyber risk management and iso 27005 applied in organizations: A systematic literature review. *Revista Foco*, 16(02), pp.e1188-e1188. Available at <https://ojs.focopublicacoes.com.br/foco/article/view/1188>

- [14] Khan, W.N. and Naseeb, S., 2024. Personal Data Protection in the Era of Big Data: Navigating Privacy Laws and Consumer Rights. *Mayo Communication Journal*, 1(1), pp.41-51. Available at <https://www.researchcorridor.org/index.php/mcj/article/view/146>
- [15] Koza, E., 2022. Semantic analysis of ISO/IEC 27000 standard series and NIST cybersecurity framework to outline differences and consistencies in the context of operational and strategic information security. *Med. Eng. Themes*, 2, pp.26-39. Available at <https://themedicon.com/pdf/engineeringthemes/MCET-02-021.pdf>
- [16] Kure, H.I., Islam, S. and Mouratidis, H., 2022. An integrated cyber security risk management framework and risk predication for the critical infrastructure protection. *Neural Computing and Applications*, 34(18), pp.15241-15271. Available at <https://link.springer.com/article/10.1007/s00521-022-06959-2>
- [17] Mrudula, P.S., Raj, R.D.A., Pallakonda, A., Reddy, Y.R.M., Prakasha, K.K. and Anandkumar, V., 2025. Smart grid intrusion detection for IEC 60870-5-104 with feature optimization, privacy protection, and honeypot-firewall integration. *IEEE Access*. Available at <https://ieeexplore.ieee.org/abstract/document/11083563/>
- [18] Palanisamy, R., Norman, A.A. and Mat Kiah, M.L., 2022. BYOD policy compliance: Risks and strategies in organizations. *Journal of Computer Information Systems*, 62(1), pp.61-72. Available at <https://www.tandfonline.com/doi/abs/10.1080/08874417.2019.1703225>
- [19] Pathirana, A.I.W. and Wilenius, M., 2025. ISO 27001 and Global Privacy Compliance. Available at https://www.utupub.fi/bitstream/handle/10024/182519/Pathirana_Asanka_Thesis.pdf?sequence=1
- [20] Peltonen, S., 2024. ISO27000 implementation handbook. Available at https://www.theseus.fi/bitstream/handle/10024/852451/Peltonen_Sebastian.pdf
- [21] Reimanis, D., 2025. Risk Management Framework. In *Realizing Complex Integrated Systems* (pp. 367-382). CRC Press. Available at

<https://www.taylorfrancis.com/chapters/edit/10.1201/9781003188377-35/risk-management-framework-derek-reimanis>

[22] Rohan, R., Papasratorn, B., Chutimaskul, W., Hautamäki, J., Funilkul, S. and Pal, D., 2023, December. Enhancing cybersecurity resilience: A comprehensive analysis of human factors and security practices aligned with the NIST cybersecurity framework. In Proceedings of the 13th International Conference on Advances in Information Technology (pp. 1-16). Available at <https://dl.acm.org/doi/abs/10.1145/3628454.3629472>

[23] Shafiq, M., Gu, Z., Cheikhrouhou, O., Alhakami, W. and Hamam, H., 2022. The Rise of “Internet of Things”: Review and Open Research Issues Related to Detection and Prevention of IoT-Based Security Attacks. Wireless Communications and Mobile Computing, 2022(1), p.8669348. Available at <https://onlinelibrary.wiley.com/doi/abs/10.1155/2022/8669348>

[24] Shrivastava, S. and Agrawal, Y., 2024. Multi-Cloud Deployments and Hybrid Cloud Architecture. Available at <https://pdfs.semanticscholar.org/59ee/a45e0ac3c0ac3dbd58ecd6915806e45fc9f7.pdf>