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

Application of the Principles and Practices of Data Security, Governance and Compliance Based on a Given Scenario

Submitted To:
Lecturer: Assoc. Prof. Carlene Campbell
Module code: ACCA7028

Submitted By:
Name: Shahriar Khan
Student ID: 2507023

Submission Date: 8 January 2026

Contents

1 Abstract **2**

2 Introduction **3**

3 Case Scenario : **3**

4 Literature Review: **4**

4.1 INFORMATION TECHNOLOGY INFRASTRUCTURE LIBRARY (ITIL): 5

4.2 **The ISO 27000 Series:** 6

4.3 The C.I.A. Triad: 6

4.4 **NIST Cybersecurity Framework(CSF)** 7

4.5 **COBIT – Governance-Focused Framework:** 9

5 Security Framework Diagram for NatureGreen: **10**

6 An Integrated Information Security, Governance and Compliance Approach for Nature Green: **11**

6.1 **Governance and Strategic Planning:** 11

6.2 **Proposed Strategic Planning for Nature Green Company:** 11

6.3 **Proposed Security Policy For Nature Green:** 12

6.4 **Security Design for Wireless and Cloud:** 12

6.4.1 **1)Zero Trust Architecture (ZTA):** 12

6.4.2 **Cloud Access Security Broker (CASB):** 13

6.4.3 **WPA-3 network:** 13

6.5 **Risk management:** 13

6.5.1 **Risk management Framework:** 14

6.5.2 **Potential Risk For Nature Green:** 14

6.5.3 **Risk mitigation stratigies:** 14

6.6 **Compliance (Law and Order):** 15

6.7 **Proper Contigency planning:** 16

6.8 **Protection Mechanism:** 16

7 Critical Discussion: **16**

8 Conclusion: **18**

1 Abstract

This article examines the security, governance, and compliance challenges faced by NatureGreen (NG), a worldwide perceived company in the healthy living products sec. tor, with a comprehensive international presence and a strong online and social media footprint. To manage its massive personnel and global customer base, Nature Green depends on cloud-based services to deliver IT services.
The dependency of the Nature Green company on a wireless-based network and Bring Your Own Device (BYOD) policies exponentially increases the risk of breaches of data, integrity, confidentiality, and availability. The analysis firstly identifies the Nature Green company's problem and then figures out the proper security framework for Nature Green's data protection for data breaches. Based on the literature review ITIL and the NIST framework are used for this data protection. Moreover, over-governance and compliance laws are discussed for Nature Green. critically examines the significance of regularly revising laws and guidelines to handle new technology and changing cyber threats.

Keywords: Information Security Management, ISO 27001, Risk Management, Integrated Security Frameworks for Nature Green, Zero Trust Architecture, Governance, and Compliance.

2 Introduction

In today's data-driven world, the exponential growth of the internet and information technology has inherently transformed the global business landscape. Businesses are depending on the Internet, which causes an increased threat of attacks on information assets and demand for a greater number of specialists capable of securing those assets. The threats to information assets are escalating as billions of Internet users can exploit vulnerabilities in online systems from any location at any time. Consequently, there is a significant demand for proficient Information Technology (IT) professionals equipped with the knowledge and expertise to protect sensitive data and maintain secure computing environments.
[1] [2]

Security is defined as the absence of danger. to be safe or shielded against potential loss, harm, unauthorized alteration, or other threats. Information security mainly focuses on the protection of information. Information security is not just a technical issue; it has become a strategic and governance concern for organisations operating in highly interconnected digital environments. Strong data security requires the integration of risk management, governance and compliance at the national and international level. [3] For instance, frameworks like Information Technology Infrastructure Library (ITIL) and the ISO/IEC 27000 series provide a proper structured way for managing and protecting data security, compliance with legal and ethical requirements. [3] [4]

NatureGreen (NG), a globally well-known brand, sells goods to support a healthy lifestyle. As it is a growing company worldwide with a billion-dollar net worth, the main issue is that the company has no proper security system or safety plan for managing or protecting its client data. NatureGreen uses modern tools like the cloud and wireless technology but has no proper safety and security guidelines for using them. At this point, the company is struggling with fulfilling its employees' needs, who want to use their own devices, which is a concerning issue for data security. Without an official security, compliance and management system, their most valuable data is being unprotected.

3 Case Scenario :

NatureGreen (NG) is a worldwide perceived company in the healthy living products sector, with a comprehensive international presence and a strong online and social media footprint. To uphold its massive personnel and global customer base, NG depends on cloud-based services to deliver information technology services. Although this wireless cloud-based system, Nature-Green company Endeavour, increased cost efficiency, scalability, and operational flexibility, at the same time, it simultaneously presents massive challenges regarding data security and governance.

As NatureGreen is 95 percent of the Nature-Green network, it has the basic physical and organizational facilities that are wireless. It increases the risk of unauthorized access, interception, and cyberattacks if not properly secured.

Additionally, the corporation has recently been under tremendous pressure to permit both its employees and clients to utilize their personal devices to access the company's network and services because of its sizable workforce and global clientele. NG has implemented a Bring Your Own Device (BYOD) strategy, encouraging both personnel and customers to use personal devices to access company resources. Although this improves ease of use and efficiency, it massively increases the attack surface and raises the threat of data breaches, malware attacks, and unauthorized access to critical systems.

At this point, the main concern for the Nature-Green company is the absence of an information security policy. Lack of proper security governance, policies, and procedures has resulted in an unorganized security environment, where policies, controls, and compliance requirements are not clearly defined. This ground places both personnel and customers' data in danger and exposes the Nature Green company to potential legal and regulatory consequences. Without a proper, structured security, governance, and compliance framework in place, the NatureGreen company will face potential risks related to data breaches, intellectual property theft, reputational damage, and regulatory non-compliance. These challenges highlight the urgent need for a comprehensive and well-governed information security strategy tailored to NG's operational environment.

4 Literature Review:

Information security has evolved from a purely technical issue to an important organizational and governance issue. Because organizations are more dependent on digital systems, particularly cloud computing and wireless networks, protecting information assets has become more difficult. Also, prior research tells us that companies that successfully integrate their IT processes with their business missions are more agile when it comes to combating cyberattacks.

NatureGreen also faces amplified challenges because it operates globally and its customers are organizations that need managing. Cloud services, wireless infrastructure, and BYOD policies make organizations vulnerable. Research in such environments has also shown that organizations relying on a single security framework typically are inadequately protected. They should then be proactive in combining the multiple frameworks that address their operational management, risk control, and governance responsibilities. Research indicates that companies with IT-enabled expansion not only benefit from economic effects (such as rising sales and falling expenses), but they can also develop more

core skills, a more efficient IT architecture, stronger coordination of strategies, quicker competitive responses, and improved decision-making. [5]

This literature review has been conducted with some of the most popular and accepted models of IT governance and information security management. Here focuses on widely recognized frameworks such as ITIL, ISO/IEC 27001, the CIA triad, NIST CSF, and COBIT. In doing so, the report will identify which models are most appropriate for supporting NatureGreen with its security, governance, and compliance needs.

Information Security Frameworks:

4.1 INFORMATION TECHNOLOGY INFRASTRUCTURE LIBRARY (ITIL):

ITIL is commonly used to improve the quality and consistency of IT service delivery. Its main strength lies in helping organisations manage IT operations in a structured and predictable way. For NatureGreen, ITIL can play an important role in maintaining service availability, especially given the company's heavy reliance on cloud-based systems.

A distinct facet of IT administration is covered in each book in the ITIL series. The trademarks ITIL and IT Infrastructure Library are registered with the UK's Office of Government Commerce (OGC) [1]. ITIL provides a consolidated set of best practices from the public and private sectors worldwide. [6]

The ITIL framework followed a proper lifecycle. These include service strategy, service design, service transition, service operation, continual service (CSI). [5]

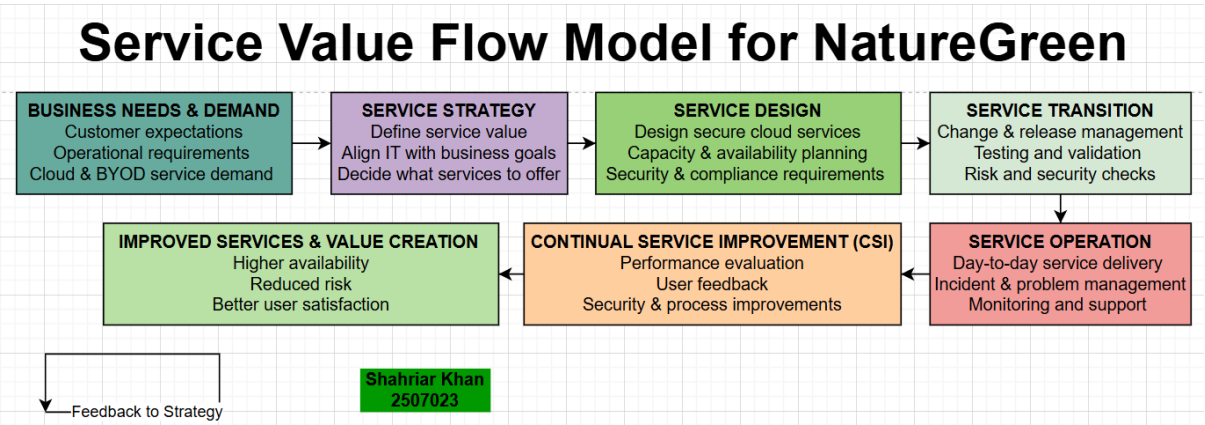

Figure 1: ITIL Framework

Figure 1 presents a service value flow model of the ITIL framework tailored to NatureGreen. The diagram illustrates how business demand is translated into IT services through strategic planning, design, transition, and operation. Continual service improvement provides a feedback mechanism that ensures services remain secure, efficient, and aligned with organisational goals in a cloud and BYOD-based environment.

4.2 The ISO 27000 Series:

International standards for information security management are offered via the ISO/IEC 27000 series. Specifically, ISO/IEC 27001 is intended to assist organizations in identifying risks and implementing suitable controls via an official Information Security Management System (ISMS). [7] For NatureGreen, this standard is especially relevant due to its global operations and responsibility to protect customer and employee data. ISO/IEC 27001 encourages a risk-based approach, which allows the organisation to prioritise security efforts based on the potential impact of data breaches. However, the standard does not prescribe specific technical solutions, meaning it must be supported by other frameworks that offer practical guidance.

ISO/IEC 27002 was first designed to provide information security management guidelines to those in charge of their company's security initiatives.

The standard was "designed to provide a common platform for defining organisational security standards and effective security management practice and to create confidence in inter-organisational dealings," according to 27000.org.

4.3 The C.I.A. Triad:

Information security mainly focuses on the protection of data.

The C.I.A. triad—confidentiality, integrity, and availability—has grown into a longer list of essential information qualities. [8]

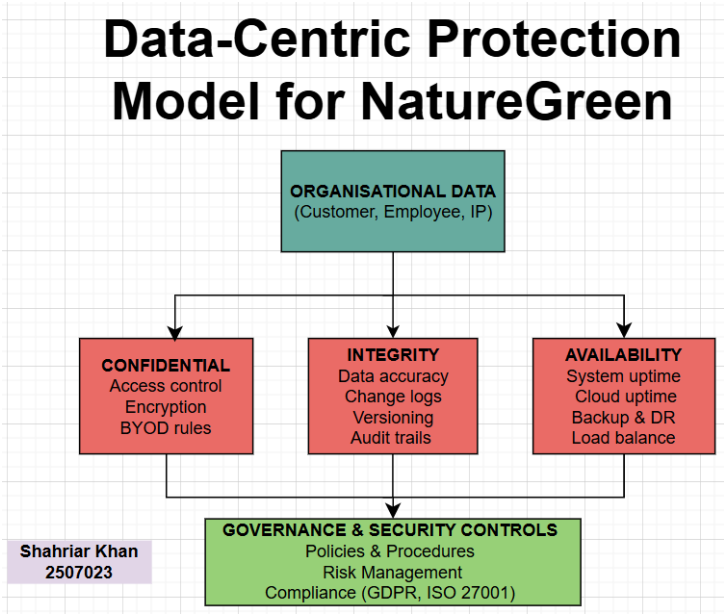

Figure 2: CIA Triad

Figure 2 presents a data-centric implementation of the CIA triad for NatureGreen. Rather than a traditional triangular model, the diagram places organisational data at the core and maps confidentiality, integrity, and availability as parallel protection domains. These domains are reinforced through governance, risk management, and compliance controls, ensuring holistic data protection in a cloud and BYOD-based environment.

4.4 NIST Cybersecurity Framework(CSF)

A methodology to help organizations in critical infrastructure sectors lower cybersecurity risk has been released by the National Institute of Standards and Technology (NIST). The NIST Cyber Security Framework for Critical Infrastructure (CSF) is the name of the framework. [9]

Alignment across these frameworks is crucial since many organizations use well-established best-practice frameworks to handle information security. In this regard, rather than taking the place of current standards, the NIST Cybersecurity Framework (CSF) is intended to complement them. Organizations can map their present security controls against the framework to find holes or weaknesses thanks to the NIST CSF, which compiles accepted industry standards and best practices.

A key strength of the NIST CSF is its flexibility, as it enables organisations to build upon their existing processes instead of introducing entirely new systems. This approach often makes the framework appear more comprehensive when compared with alternatives such as COBIT, ISO/IEC 27001, and the ISF Standard of Good Practice. However, to ensure effective alignment and compliance, it is still necessary to assess the completeness

of the NIST CSF and identify any potential gaps. Doing so helps organisations confirm that the framework adequately supports their overall information security objectives while remaining compatible with other recognised security standards. Businesses, governments, and other organizations can manage cybersecurity risks with the use of the NIST Cybersecurity Framework (CSF) 2.0. Regardless of size, industry, or degree of maturity, it provides a taxonomy of high-level cybersecurity outcomes that every firm can use to better understand, evaluate, prioritize, and communicate its cybersecurity operations. The CSF does not specify how results should be obtained. Instead, it provides links to online sites that offer more advice on strategies and safety measures that could be employed to accomplish those goals. The components of CSF 2.0 and some of its many uses are explained in this paper. [10] However, it is structured around five core functions. These are—

Identify: Recognize and understand the risks, vulnerabilities, and assets of the organization.

Protect: Protect by putting security measures like encryption and access controls in place

Detect: Using monitoring and recording to identify cybersecurity events

Respond: In order to contain and lessen events, one must respond.

Recover: After an incident, recover entails repairing systems and enhancing resilience

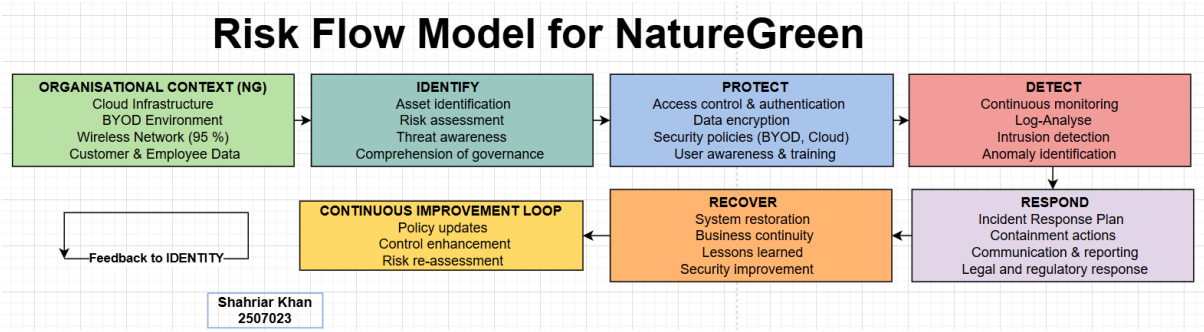

Figure 3: **Risk Flow Model for NatureGreen**

Figure 3 illustrates a customized implementation of the NIST Cybersecurity Framework for NatureGreen. The model follows a top-down risk flow beginning with organizational context and progressing through the five NIST functions. A feedback loop enables continuous improvement by feeding lessons learned from the recovery phase back into the identification of risks, ensuring adaptability to emerging threats in a cloud and BYOD-based environment.

The NIST framework is enormously adequate for cloud- and BYOD-based systems.

For as much as it does not command specific technologies but instead focuses on outcomes. This type of flexibility allows NatureGreen to adapt security controls to different cloud service providers

4.5 COBIT – Governance-Focused Framework:

It is not a coincidence that an organization has effective governance. An organization's ability to successfully implement good governance is linked to the appropriate pattern or fit for the organization, allowing it to support or enhance its strategic focus.
IT, or information technology governance, is an organizational process rather than a static concept. The IT governance structure of decentralized organizations, like universities, needs to be reviewed on a regular basis to reflect the evolving business and technology landscape.
The COBIT 5 framework offers recommendations on how IT governance should be developed by considering the domains of management of governance and enterprise governance, both of which have functions within the scope of IT management.
Higher education can use the COBIT 5 framework guide as a guide when developing IT blueprints that support both academic and extracurricular IT activities while also taking a broad view of the scope of university operations. The foundational ideas that ought to guide the governance process form the basis of the conceptual model of IT governance. [11]
The principal advantage of COBIT is distinguishing transparently between governance and management. This distinction is more important for NatureGreen because security flaws first come up with uncertainty.

5 Security Framework Diagram for NatureGreen:

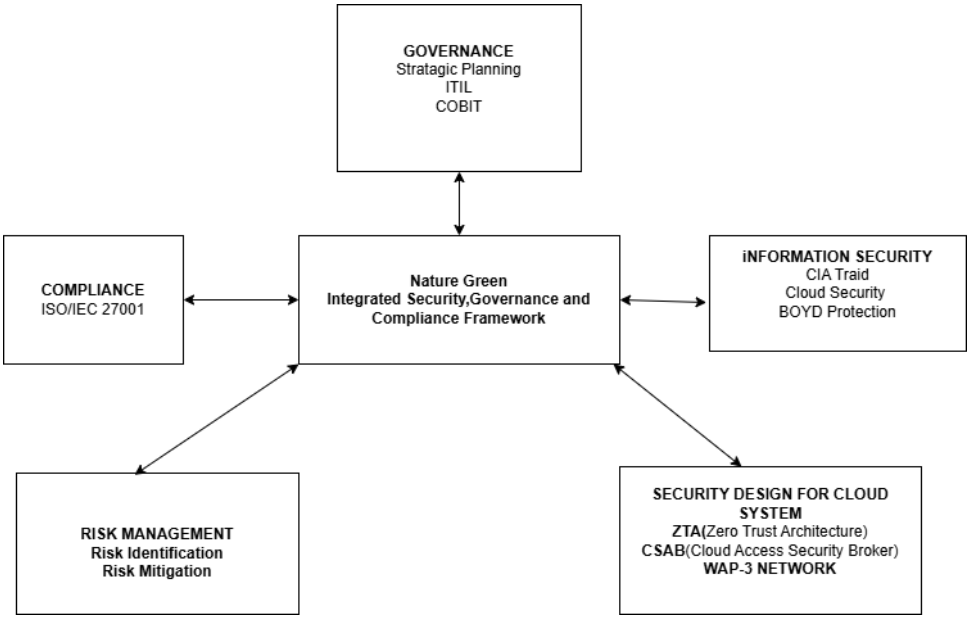

Figure 4: **Security Framework Diagram of NatureGreen**

6 An Integrated Information Security, Governance and Compliance Approach for Nature Green:

6.1 Governance and Strategic Planning:

"The process of deciding on an organization's long-term course (strategy) and allocating and acquiring the resources required to carry it out" is known as strategic planning. [12] NatureGreen should provide an expedient structure for information security governance that ensures well-defined accountability and robust strategic governance. First, a particular strategy is derived from a general strategy; second, lower-level tactical and operational planning is derived from overall strategic planning. To demonstrate organisational commitment to security, this structure should include executive-level engagement and the appointment of a Chief Information Security Officer (CISO) or Information Security Manager. Precisely well-defined dispositions and responsibilities should be documented to avoid unusual inconvenience and assure effective decision-making.
Nature Green, a globally renowned wireless firm, needs a clear, solid strategy plan that takes a defence-in-depth approach based on strong governance, risk management, and adherence to international standards like ISO/IEC 27001 and the NIST Cybersecurity Framework.
Information security mainly focuses on the protection of data.
NatureGreen should follow the C.I.A. triad—confidentiality, integrity, and availability—for their data safety and security and quality maintenance.
Organisational strategic planning processes must include security themes and align them with NG's overall business goals.

6.2 Proposed Strategic Planning for Nature Green Company:

This strategy plan was created for NatureGreen (NG), a multinational health products company that presently uses a cloud-based architecture and a 95 percent wireless network. It makes use of the ITIL and ISO 27001 standards to help the company transition from its present "security disarray" condition to one of cyber resilience and controlled expansion.

1. Executive Summary: Managing multibillion-dollar intellectual property (IP) and moving toward a flexible Bring Your Own Device (BYOD) paradigm presents a significant challenge for NatureGreen (NG). This strategic plan lays out a three-year plan for putting in place an ISO/IEC 27001-compliant information security management system (ISMS).

2. Mission, Vision, and Values Statements: Statements: Protect NatureGreen's multibillion-dollar patent portfolio and consumer data by putting a "security-first" cul-

ture into place and taking proactive steps to reduce risks.

Vision: To be a global leader in digital health services where innovation and privacy coexist. Core Values:

Confidentiality: The data is protected from unintentional or global disclosure.

Integrity: The data is protected from unintentional or deliberate change.

Availability: When needed, authorized people can access the data.

6.3 Proposed Security Policy For Nature Green:

Policy is the most vital component of an effective information security program.

The management's perspective on safeguarding data on automated systems and the policy that was developed determine how well an information resources protection program works.

Comprehensive security policies must be created and implemented in order to provide consistent guidance and enforce appropriate security practices throughout the company. NatureGreen ought to establish and enforce a set of formal, documented policies, including:

1) Bring Your Own Device (BYOD) Policy
2) Data Protection and Privacy Policy
3) Access Control Policy
4) Incident Response Policy

6.4 Security Design for Wireless and Cloud:

NatureGreen (NG) is a globally perceived company in the sector of healthy living products, with a comprehensive international presence and a strong online and social media presence. To maintain its massive personnel and global customer base, NG relies on cloud-based services to deliver information technology services.

To solve the Nature Green BOYD and cloud-based issues, they need to come out of the traditional security policy.

6.4.1 1)Zero Trust Architecture (ZTA):

Zero Trust Architecture (ZTA) or simply Zero Trust (ZT) is being hailed as a novel idea that will greatly improve an organization's security. The complexity and variety of contemporary IT systems are a major factor in the demand for ZTA. By using the ZTA Model, Nature Green Company can secure the data of its customers. [13]

No matter if someone's on their home Wi-Fi or their work network, NG's cloud stuff checks three things before letting them in: who they are, how healthy their device is, and how secret the data is.

6.4.2 Cloud Access Security Broker (CASB):

Cloud Access Security Brokers (CASBs) are intermediaries between service providers and customers who implement security measures to grant access to cloud services, typically SaaS applications.
CASB will act as a gateway between the customers and NG's Cloud service. [14]

They might also manage who has access to company resources. Authentication (passwords and credentials), enforcement of authorisation policies, intrusion prevention, anti-malware filters, security logging and auditing, and encryption are examples of security measures.

6.4.3 WPA-3 network:

Wireless networks, which link devices without the need for wires to exchange data, are the most prevalent kind of network. [15]

Whether for personal use at home or for public use at the business level, wireless networks are constantly growing.
The development of WPA3's encoding and encryption techniques demonstrated its capacity to provide both individual and business users with increased security levels.
AS NatureGreen is a 95 per cent wireless cloud-based company, they need to upgrade their protocols to WPA-3 network. WPA-3 provides a Wide range of data encryption, and it provides a massive wireless secure environment, which is the actual basic need for Nature Green company data protection.

6.5 Risk management:

When we are operating an organisation, there has always been some sort of risk. Nature GreenCompany, which is a multi-billion-dollar company, has to face some sort of risk.
At NatureGreen, managing risk means figuring out what threats our billions of dollars in IP and private data face. Then, we line up our resources to lower the chances or lessen the hit if something bad happens.

6.5.1 Risk management Framework:

1)The ISO 27000 Series: Information Technology—Code of Practice for Information Security Management, first issued as British Standard BS 7799, then as ISO/IEC 17799, and finally as ISO/IEC 27002, is one of the most frequently cited and spoken about security models. [16]

2)ITIL: ITIL is the most widely used approach to managing IT services globally. ITIL provides a consolidated set of best practices from the public and private sectors worldwide. [6]

6.5.2 Potential Risk For Nature Green:

1) Data Leakage: As Nature Green follows the Bring Your Own Device strategy, there is a high chance of data leakage and cyberattack.
2) Unprotected Wireless Network: Because 95 per cent of the network is wireless, NG is really open to man-in-the-middle attacks, fake Wi-Fi spots, and people secretly getting their hands on really expensive company secrets.

6.5.3 Risk mitigation stratigies:

The InfoSec development project team must choose one of five basic strategies to reduce such risks after identifying information assets with unacceptable levels of risk.
1) Defense
2) Transference
3) Mitigation
4) Acceptance
5) Termination

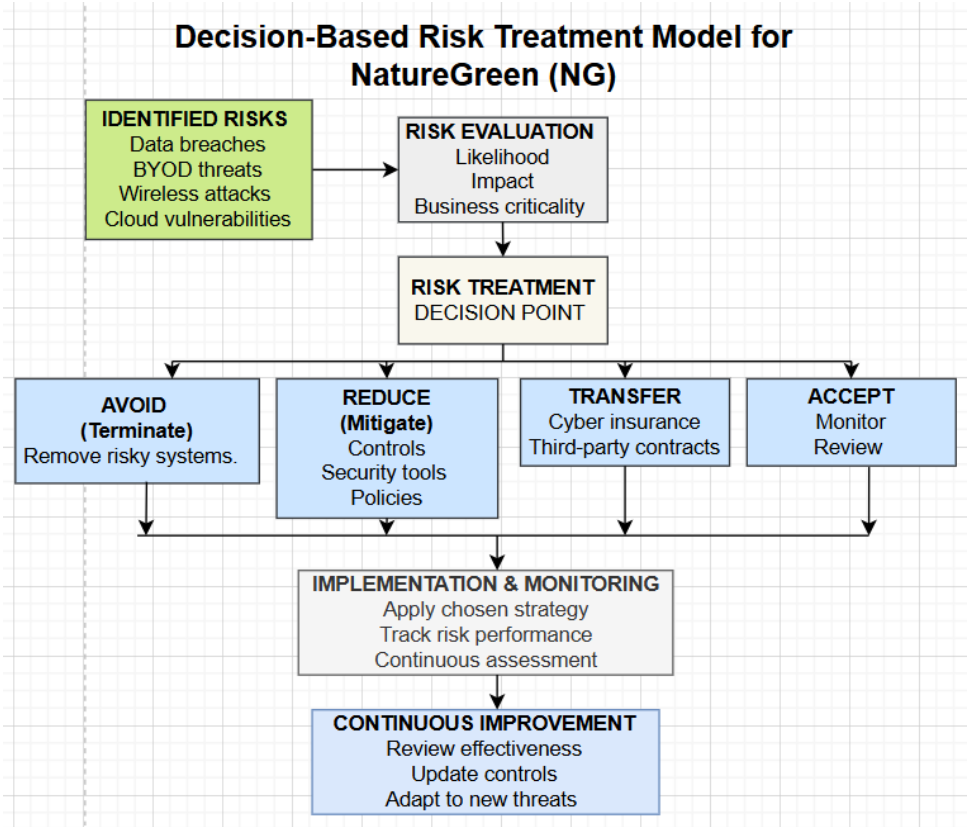

Figure 5: **Risk Mitigation Model**

6.6 Compliance (Law and Order):

Being a worldwide business organization, NatureGreen has to make sure that local and international data protection laws, such as the General Data Protection Regulation (GDPR), are followed.

Some believe that the General Data Protection Regulation (GDPR) represents the biggest shift in data privacy laws over the past 20 years. Any business that gathers and uses the personal data of EU citizens, whether they are situated inside or outside the EU, is subject to the GDPR privacy rule, which went into effect in May 2018. [17]

Additionally, the concept of personal data has been broadened. It says that information that could be used to directly or indirectly identify an individual is considered personal data. The revised definition states that identifiers like IP addresses. [18]

Similar to the 1995 directive and numerous other directives and laws, the GDPR does not specify which technologies must be utilized in order to comply. This is nothing unusual because laws that are overly prescriptive have the potential to become outdated very fast, especially considering how swiftly technology is developing in the modern world. Instead, the GDPR mandates that businesses put in place suitable operational and technological security measures. [18]

As NatureGreen is a 95 percent wireless-based company, for protecting their customer data, GDPR will be the best data protection regulation system.

Compliance initiatives should take into account ethical issues pertaining to the management of employee and consumer data in addition to legal requirements.

6.7 Proper Contigency planning:

Because businesses do more than only store or process data to provide various service platforms, contingency plans implemented in computer centers are essential for business continuity. When faced with internal or external risks that impact their investments, organizations may face a variety of consequences. It is crucial to have computer support for undesired events that impact devices. The financial harm that an illegal intrusion causes makes cyberattacks on data networks a major issue. Only technological problems can be covered by a cyberattack contingency plan. [19]

6.8 Protection Mechanism:

Although they are a crucial component of the InfoSec program, technical controls cannot secure an IT system on their own.
In situations when human conduct is hard to control, technical controls can make policy enforcement possible. Individuals within an organization can get around many of the most effective technical restrictions since they frequently have direct access to the information.
NatureGreen ought to implement the appropriate organisation and technical security protocols in order to achieve its governance and risk management objectives. These also include comprehensive data encryption, multi-factor authentication, firewalls, intrusion detection and prevention systems, secure wireless communications, and endpoint security controls for BYOD
The outcomes of the risk assessment should serve as the basis for selecting and putting into practice protective measures, and relevant security standards should be consulted. To remain effective and relevant in the face of emerging risks, risk controls should be continuously reviewed and improved.

7 Critical Discussion:

Day by day, technological advancements are increasing rapidly.
In recent years, a number of specialists and academics have revealed how susceptible wireless communication systems and technologies are to different types of cyberattacks. Both commercial enterprises and government institutions are affected by these attacks.

Attackers use advanced tools and techniques to crack any size key, and the security of private and sensitive data is still unchanged. To lessen these attacks, numerous advancements are being made. Its stability, high functional efficiency, and clarity are guaranteed by regulations and continuous updates.

Additionally, including appropriate procedures and abiding by the law will assist businesses in maintaining data security. Involving governance and compliance also aids the organization in upholding greater standards for data flow and protection.
Therefore, maintaining a robust data security system will be made easier by staying current with rules and surveillance.

8 Conclusion:

NatureGreen (NG), a globally well-known brand, sells products that are used to maintain healthy living. To uphold its massive personnel and global customer base, NG depends on cloud-based services to deliver information technology services. Although this wireless cloud-based system, NatureGreen Company Endeavour, increases cost efficiency, scalability, and operational flexibility, at the same time, it simultaneously presents massive challenges regarding data security and governance.

It also represents the complex security system, governance, and compliance.

The evaluation of the article focused on the complex security system, governance, and compliance. This paper, Addressing Security and Governance Frameworks, highlights the strategic approach to lowering the information security risk for the Nature Green organization. Additionally, the NIST Cybersecurity Framework improves threat detection, incident response, and recovery capabilities, while COBIT ensures strong governance, accountability, and alignment between IT operations and business objectives.

NIST frameworks ensure strong threat detection, understanding the risk vulnerabilities, and protecting the assets of the organization. Moreover, COBIT ensures the recommendations on how IT governance should be developed by considering the domains of management of governance and enterprise governance, both of which have functions within the scope of IT management. In conclusion, by implementing these data security frameworks and governance and compliance policies, Nature Green Company will be able to ensure data security of its customers and personnel.

References

[1] Y. A. Bena, R. Ibrahim, J. Mahmood, A. Al-Dhaqm, A. Alshammari, M. Nasser, M. Nura Yusuf, and M. O. Ayemowa, "Big data governance challenges arising from data generated by intelligent systems technologies: A systematic literature review," *IEEE Access*, vol. 13, pp. 12859–12888, 2025.

[2] L. Guerreiro, J. Martins, M. do Rosário Bernardo, H. Mamede, and F. Branco, "Impact of a master data management framework to trigger data governance maturity: A systematic literature review," *IEEE Access*, vol. 13, pp. 190644–190667, 2025.

[3] M. E. Whitman and H. J. Mattord, "Management of information security," 2007.

[4] J. Jevelin and A. Faza, "Evaluation the information security management system: A path towards iso 27001 certification," *Journal of Information Systems and Informatics*, vol. 5, no. 4, pp. 1240–1256, 2023.

[5] N. Zeinolabedin, M. Khademi, and N. Rahbar, "Assessing efficiency of itil framework to align business and it," *Research Inventy: International Journal of Engineering and Science,*, vol. 5, pp. 13–26, 2013.

[6] M. Gërvalla, N. Preniqi, and P. Kopacek, "It infrastructure library (itil) framework approach to it governance," *IFAC-PapersOnLine*, vol. 51, no. 30, pp. 181–185, 2018.

[7] M. Mirtsch, J. Kinne, and K. Blind, "Exploring the adoption of the international information security management system standard iso/iec 27001: A web mining-based analysis," *IEEE Transactions on Engineering Management*, vol. 68, no. 1, pp. 87–100, 2021.

[8] S. Deepika and P. Pandiaraja, "Ensuring cia triad for user data using collaborative filtering mechanism," pp. 925–928, 2013.

[9] S. Almuhammadi and M. Alsaleh, "Information security maturity model for nist cyber security framework," *Computer Science & Information Technology (CS & IT)*, vol. 7, no. 3, pp. 51–62, 2017.

[10] C. E. Pascoe, "Public draft: The nist cybersecurity framework 2.0," *National Institute of Standards and Technology*, 2023.

[11] H. Nugroho, "conceptual model of it governance for higher education based on cobit 5 framework.," *Journal of Theoretical & Applied Information Technology*, vol. 60, no. 2, 2014.

[12] B. George, R. M. Walker, and J. Monster, "Does strategic planning improve organisational performance? a meta-analysis," *Public administration review*, vol. 79, no. 6, pp. 810–819, 2019.

[13] N. F. Syed, S. W. Shah, A. Shaghaghi, A. Anwar, Z. Baig, and R. Doss, "Zero trust architecture (zta): A comprehensive survey," *IEEE access*, vol. 10, pp. 57143–57179, 2022.

[14] E. B. Fernandez, N. Yoshioka, and H. Washizaki, "Cloud access security broker (casb): A pattern for secure access to cloud services," in *4th Asian Conference on Pattern Languages of Programs, Asian PLoP*, vol. 15, 2015.

[15] A. Halbouni, L.-Y. Ong, and M.-C. Leow, "Wireless security protocols wpa3: A systematic literature review," *IEEE access*, vol. 11, pp. 112438–112450, 2023.

[16] C. Everett, "Is iso 27001 worth it?," *Computer Fraud & Security*, vol. 2011, no. 1, pp. 5–7, 2011.

[17] R. N. Zaeem and K. S. Barber, "The effect of the gdpr on privacy policies: Recent progress and future promise," *ACM Transactions on Management Information Systems (TMIS)*, vol. 12, no. 1, pp. 1–20, 2020.

[18] C. Tankard, "What the gdpr means for businesses," *Network Security*, vol. 2016, no. 6, pp. 5–8, 2016.

[19] V. Padilla and F. Freire, "A contingency plan framework for cyber-attacks," *Journal of Information Systems Engineering & Management*, vol. 4, no. 2, pp. 2–7, 2019.