

Global Security Governance for NatureGreen

Keval Mahendra Motivaras

Student ID- 2515743

14 December 2025

Table of Contents

1. Introduction.....	4
1.1 Background to NatureGreen	4
1.2 Problem Context.....	4
1.3 Aim, Objectives & Scope	5
2. Assumptions.....	5
2.1 Organisational Assumptions	5
2.2 Technical Assumptions.....	5
2.3 Regulatory Assumptions.....	6
3. Literature Review: Security Governance & Frameworks	6
3.1 Information Security Governance Overview	6
3.2 ISO/IEC 27001 & 27002	7
3.3 NIST Cybersecurity Framework	7
3.4 COBIT / IT Governance	9
3.5 CIA Triad & Zero Trust Model.....	10
4. Comparative Analysis of Frameworks	11
4.1 Comparison Criteria	11
4.2 Framework Comparison Discussion.....	11
5. Key Risks & Threats for NatureGreen	12
5.1 Cloud Risks & Data Residency Issues	12
5.2 Wireless Network Vulnerabilities	12
5.3 BYOD & Endpoint Security Risks.....	12

5.4 IP Theft & Insider Threats	13
6. Proposed Governance & Security Approach	13
6.1 Governance Structure & Roles	13
6.2 Policy & Standards Framework	14
6.3 Security Controls Mapped to NIST Functions	14
6.4 Risk Management, BCP & DR Planning	15
7. Third-Party & SLA Management	16
7.1 Cloud Shared Responsibility Model	16
7.2 Vendor Audit & Security Requirements	16
8. Critical Discussion: Evolving Standards & Regulations	17
8.1 Rapid Technology & Threat Evolution	17
8.2 Regulatory and Compliance Changes	18
8.3 Implications for NatureGreen	18
9. Conclusion	18
9.1 Summary of Key Insights	18
9.2 Final Recommendations	18
References	20

1. Introduction

1.1 Background to NatureGreen

NatureGreen is a global corporation that does not serve on on-premises servers and utilizes cloud services. This is typical of fast expanding technology companies. According to Gartner, over 60 percent of businesses operate the majority of their business in the cloud. It has a wireless network in nearly all its internal systems (95%). It is analogous to the current factories and biotech laboratories where individuals have to move and retrieve information immediately. The expectation of using their own devices in the workplace is on the increase. Cisco discovered over 70 percent of employees use personal phones, tablets or laptops, further providing additional access points to the company network. NatureGreen has good ideas which are very valuable and has a good online presence (Noor-A-Rahim et al., 2023).

1.2 Problem Context

NatureGreen operates in a high risk, cloud-based environment and it lacks defined information security policy. This implies that there are no defined roles, controls and responsibilities and this is one of the usual causes of breaches in growing companies. Since there is no definite governance, cyber threats such as credential theft, ransomware and wireless intrusion present a greater risk to the company. Such risks have impacted on other companies of the same nature. Indicatively, a few cloud-based breaches in IBM 2023 Cost of a Data Breach study were caused by unsecured remote access. The company has numerous regions of operation and this poses compliance issues. Regulations like GDPR or PCI DSS provide clear guidelines concerning data management and data breaching (Okusi, Obiakor and Adelaye, 2025).

1.3 Aim, Objectives & Scope

In this report, the researcher will consider the level of security of NatureGreen and propose a transparent governance process based on established cybersecurity guidelines. It has the following objectives: 1) review scholarly and commercial literature that matters, 2) learn significant standards, such as ISO 27001 and NIST, 3) draw up a tailor-made policy on governance and security that can operate in the global, wireless and BYOD environment of NatureGreen, and 4) be serious about why standards and legislation should be altered. They look merely at the context of NatureGreen itself, focusing on governance, risk, compliance, and security controls, as opposed to technical details or change in the industry more generally (Singh, 2024).

2. Assumptions

2.1 Organisational Assumptions

NatureGreen is a middle-sized international corporation consisting of approximately 800 to 1,200 workers, such as expanding technology producers serving numerous markets. The company has major units like the research, operations, IT, marketing as well as finance, which are indicative of the necessity to safeguard the intellectual property of the company. It will probably possess offices in North America, Europe, and Asia, just like other international companies, and it must be able to store data beyond national borders and ensure uniform security of the data in every region (Caudron, Promoteur and Vanleenhove, n.d.).

2.2 Technical Assumptions

It is likely that NatureGreen is operating on a public cloud which can be either AWS or Microsoft Azure. This is typical of rapid-rising technology firms since it can expand at a fast rate. Thousands of mid-market businesses are hosted by AWS alone, as reported by the

industry. It also has a 95 percent wireless coverage which implies that it has Wi-Fi networks of the enterprise nature such as those found in contemporary manufacturing facilities where people are constantly on the move. The BYOD stress implies that the staffs are frequently using their personal computers and smartphones, which aligns with the results of Cisco that showed the majority of the employees use company systems on uncontrolled devices (Kristiansson and Lundström, 2023).

2.3 Regulatory Assumptions

NatureGreen operates internationally. As such, it should adhere to GDPR, which concerns any company dealing with the personal data of individuals in the EU. In case they accept online payments, then it should also adhere to the PCI DSS, which safeguards credit card details. It can also have to comply with other privacy regulations, such as the California Consumer Privacy Act (CCPA) or the Singapore PDPA. These regulations demonstrate that it is not easy to ensure that sensitive data are secure to global digital companies (Elia, 2024).

3. Literature Review: Security Governance & Frameworks

3.1 Information Security Governance Overview

Information security governance refers to how businesses direct and oversee security-related decisions as a way of safeguarding information, adhere to regulations, and assist the business in meeting its objectives. According to researchers, governance is a board task that ensures that the security money is used on the appropriate risks and that it is in line with the plans of the company. The IT Governance Institute indicates it is a collection of relationships and actions that ensure IT supports business aspirations and manages risk. It has gained greater significance due to the increase in the use of cloud and mobile which provides more attack locations. An example is that according to PwC Global Digital Trust Insights report, over 70 % of leaders

are currently concerned with governance due to increased cyber attacks. Accountability is provided with good governance that assigns responsibility, establishes policies and measures outcomes, contributing to the avoidance of confusion in the fast-growing companies (John Agyekum Addae, Mota and António Carrizo Moreira, 2023).

3.2 ISO/IEC 27001 & 27002

ISO/IEC 27001 refers to a global standard that informs organisations on how to establish an Information Security Management System or ISMS. ISO/IEC 27002 provides more specific security control advice. The standard employs an approach that is risk based: organisations have to identify their risks, select the appropriate controls, and continue to improve. The following Hewlett-Packard 93 controls (as of 2022), which include access control, encryption, physical security, relations with suppliers, and how to dispose of incidents, are listed in Annex A. One of the reasons why many organisations opt to use ISO 27001 is that through certification, outsiders see that they are capable of satisfying security demands. Firms that use the cloud such as manufacturing firms are also certified to demonstrate that they are compliant and gain customer trust. An excellent demonstration is the use of the ISO 27001 by the numerous SaaS and technology firms that safeguard the sensitive data of their customers. The key advantages of the standard are its ability to give a clear risk approach, universal acceptance and compatibility with laws and regulations. The key weaknesses are the capital and manpower required to establish it, which may be a challenge to the medium-sized organisations (Dakić et al., 2025).

3.3 NIST Cybersecurity Framework

The NIST Cybersecurity Framework (CSF) is a universal model that consists of five major components, namely, Identify, Protect, Detect, Respond, and Recover. Many critical

infrastructure providers are using it, as well as business are adopting it since it can be applicable in a variety of situations. In the case of Identify, companies enlist their assets and assess risks. Protect also implements protective measures like permitting or prohibiting access as well as encryption of data. Detect refers to monitoring of issues. Respond entails dealing with incidents. Recover is concerned with back-up and continuity. Surveys indicate that people like the CSF and Gartner indicated that it is gaining rapid traction in the mid-size market seeking a scalable solution. One of the real-life examples is found in the United States energy and manufacturing companies, which applied the structure to create a greater resistance to operating issues. Its greatest strength is that it is flexible, and therefore the companies can select controls that are as developed as necessary and as much money as the company has, and it does not require certification to use it. The bad thing is that it never tells what specifically to do, thus it may be difficult to the newer or smaller firms to know what to work on first or at all to know where they are doing better or worse (Möller, 2023).

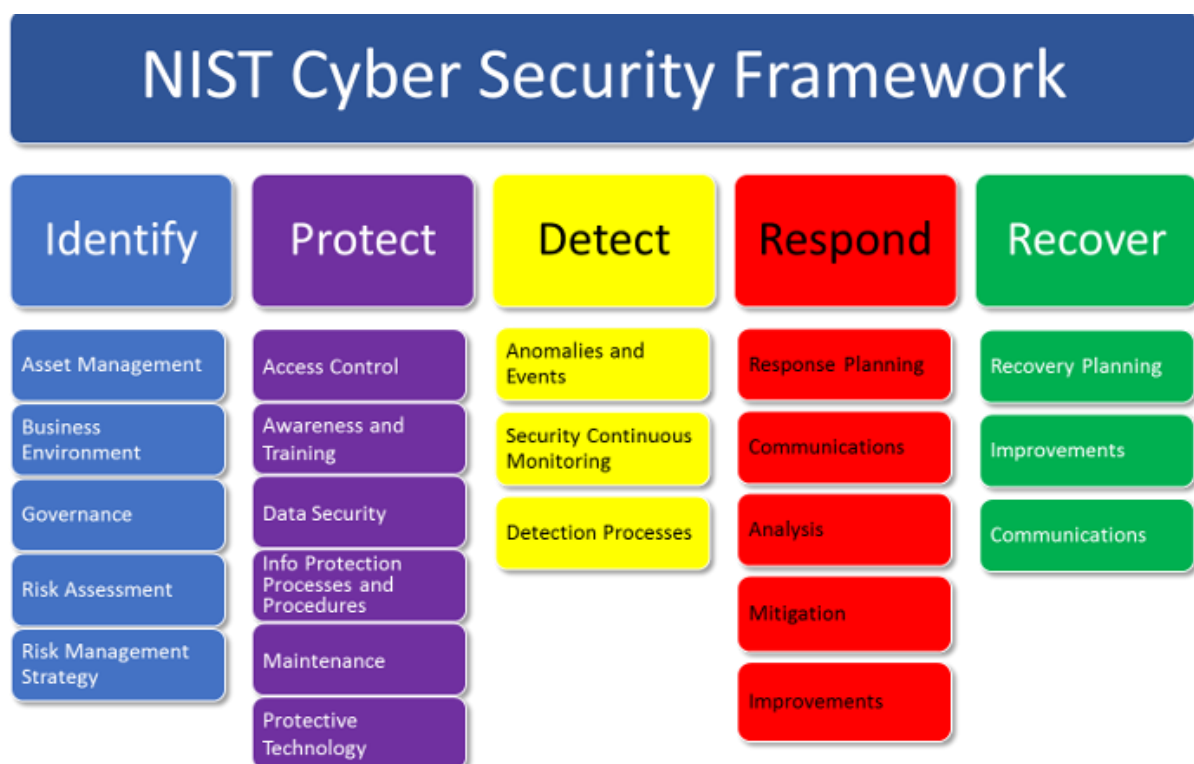


Figure 1: NIST Cybersecurity Framework

3.4 COBIT / IT Governance

COBIT (Control objectives in information and related technologies) is a model that assists firms in handling their IT. It lays emphasis on board supervision, ensuring IT aligns with the strategy of the company, and the performance of IT. COBIT provides a list of rules, actions, and objectives that assist organizations in ensuring that IT is adding value and risks are managed. It is popular in those industries where individuals require to be responsible and audits matter, e.g. finance and manufacturing. With the implementation of COBIT, the majority of organizations establish a clear decision right, and reporting line, making cybersecurity a big business risk, instead of an IT problem. The key advantages of the COBIT framework are that it explains what is done by whom and how to address problems, and supports general risk management. COBIT, however, does not provide as much specific technical guidance as such standards as ISO 27002 or NIST CSF, which is why companies tend to supplement the latter with specific standards to receive useful security measures (Bukhari et al., 2021).

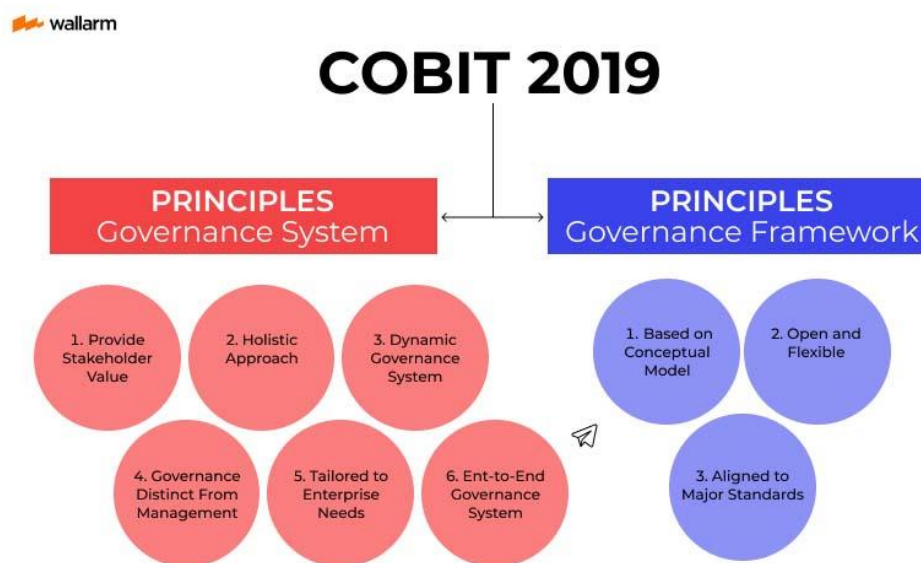


Figure 2: COBIT / IT Governance

3.5 CIA Triad & Zero Trust Model

The CIA triad; Confidentiality, Integrity and Availability assists them in the evaluation and design of security controls. Breach studies tend to identify issues with these principles such as access without permission or modifying data as contributors to large incidents. Concurrently, the rule of never trust, always verify is adhered to by the Zero Trust model that is gaining more prevalence in the cloud-based industries. It involves constant authentication, network segmentation and least privilege. Firms which migrate to cloud and wireless spaces are increasingly resorting to Zero Trust to restrict the possibility of moving laterally (HIZA, 2022).

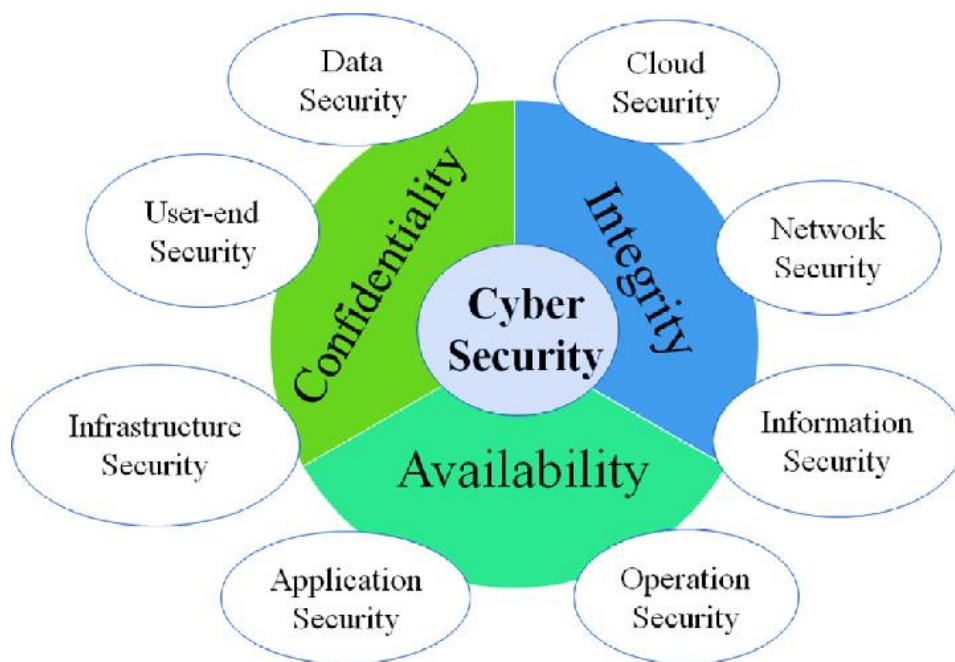


Figure 3: CIA Triad & Zero Trust Model

4. Comparative Analysis of Frameworks

4.1 Comparison Criteria

The comparison examines the four criteria that are mostly applied in industry reviews. First, the governance coverage is a check to whether the framework specifies the roles, accountability and oversight. Second, technical depth is the study of the level of guidance in the control level. Third, flexibility evaluates the ease with which the framework may integrate into other maturity levels or technologies like those of cloud and wireless systems. Lastly, certification involves whether the framework permits formal external validation which can be used to offer the customer confidence and market credibility (Heidari et al., 2024).

4.2 Framework Comparison Discussion

ISO 27001 provides robust control and numerous many controls on the basis of ISO 27002. It provides clear certification roads that the world customers appreciate. It suits organisations that have sensitive information and operate in numerous areas. The negative is that it may consume many resources. NIST CSF is highly adaptable and it is compatible with cloud and wireless environment. It is attractive to organisations, which would desire to implement it in a scaled manner without the heavy load of certification. It is versatile as it can be used in energy and industrial automation. COBIT performs well where it comes to governance and accountability by the board but requires additional operational frameworks. NatureGreen requires defined governance and relaxed security measures. A hybrid approach is reasonable: a set of decision-making and oversight with the help of COBIT, a risk-based structure and operational controls with ISO 27001, and operational maturity and incident preparedness with NIST CSF (Xiong, Shah and Wu, 2022).

5. Key Risks & Threats for NatureGreen

5.1 Cloud Risks & Data Residency Issues

Cloud services introduce risks regarding the location of the data, its owner, and those who can access it unauthorised. The corporations across the globe have experienced breaches where the data warehouses are located in countries they were not familiar with regarding rules. There is a case in point that when cloud storage was configured improperly, sensitive data were revealed. Using third-party providers also implies that they are trusting their security and their response and recovery speed. When they are not fast, then the business is not spared either (Singh and Sharma, 2021).

5.2 Wireless Network Vulnerabilities

Wireless networks contain some inbuilt risks such as eavesdropping, false access points and weak encryption. Studies indicate that a network with a loose security system has the potential to allow an attacker to access the systems that are not physically broken into without having to access the system using a security system that is lax. When businesses distribute wireless coverage on the use of the mobile, the opportunities of an assault rise, thus effective login defense and isolation are needed.

5.3 BYOD & Endpoint Security Risks

BYOD set-ups provide individuals with additional opportunities to access firm networks, and this increases the likelihood of using outdated, uncontrolled devices to connect to the network. Majority of workers work with their personal gadgets and these gadgets do not have conventional security features. In case a device is lost or hacked, it may show passwords and important files. Viruses on a personal computer can also transfer into the corporate network.

Lack of Mobile Device Management (MDM) and unclear guidelines make companies unable to coerce encryption, practice updates, and restrict access.

5.4 IP Theft & Insider Threats

In biotech and hi-tech manufacturing there are high chances of insiders abusing or stealing valuable intellectual property in organizations that possess it. Insider issues are also common when individuals have special access that is not being well tracked and reveals that labeling data, regulation of access, and observing user behavior is critical in IP-intensive environments (Carnovale et al., n.d.).

6. Proposed Governance & Security Approach

6.1 Governance Structure & Roles

To establish a well-defined governance mechanism, an initial move is to bring in a Chief Information Security Officer (CISO), who will make the security strategy, monitor risks, and maintain lawfulness within the laws. This is in line with industry trends in that CISOs provide a concise picture of technology to executives. CISO is supposed to form a Security Steering Committee that will consist of the IT, Legal, HR, and Operations individuals to make decisions that will affect all aspects of the company and all the areas of its existence. The team reports to the senior management on a quarterly basis thus everyone observes the risks, incidences and whether they are abiding by the rules. This maintains business priorities in security work. The model is similar to the one used by numerous companies across the world. It brings a stronger sense of accountability, better utilization of resources, and is able to grow and keep the intellectual property going of NatureGreen (Ciekanowski et al., 2024).

6.2 Policy & Standards Framework

NatureGreen also requires the articulate Information Security Policy stating who, what, and what. The BYOD Policy is expected to request individuals to enroll their own devices, encrypt data and properly log in, according to the common principles of using personal devices. Strong log-in procedures and different network zones should be a requirement of the Wireless Security Policy to reduce risk within a predominantly wireless environment. The Cloud and Vendor Management Policy also ought to establish guidelines concerning the location where data needs to remain, the accessibility, and the speed at which violations should be reported.

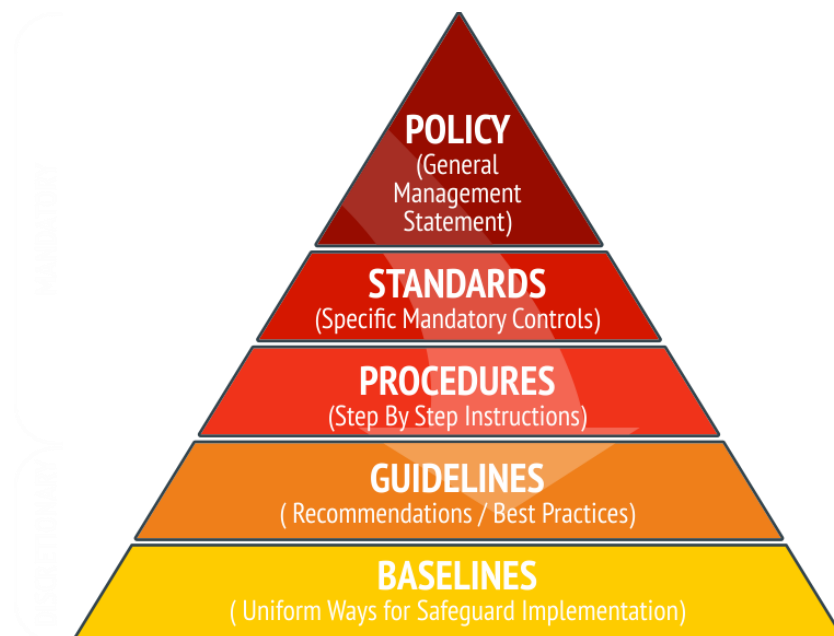


Figure 4: Policy & Standards Framework

6.3 Security Controls Mapped to NIST Functions

Identify: Make a list of every device, data, and cloud services and monitor them on a regular basis to identify vulnerabilities in wireless access and bring-the-own-device access.

Protect: Make numerous steps on the way to the login, grant access to users only when necessary, and encrypt the data. Isolate the network into distinct regions to ensure that attacks are not spread with ease, as it is the case in the current manufacturing systems. Educate individuals on security so that they can not make errors.

Detect: Monitor check systems and logs continuously to identify suspicious activity in cloud and wireless networks to enable them to detect an authorized intrusion or modification in a short time.

Respond: Prepare a clear incident response plan, which includes the way of passing the issues up the chain, the way of investigating them, and the way of discussing them. Consecutive drills and tests prove that they are ready and increase the speed of the response.

Recover: Have tested backup and restore procedure. Keep more than one backup of stores. In that manner, they can recover fast once an issue occurs, and make the cloud systems even more resistant in the global scale.

6.4 Risk Management, BCP & DR Planning

NatureGreen should ensure that the business continuity and disaster recovery plans are in place, and always monitor risks according to ISO 27005, determine recovery time (RTOs) and backup points (RPOs) and minimize downtime. These plans should be tested and updated frequently so as to ensure that they are working. The backup storage in numerous locations prevents the loss of data and aids in recovery when systems are broken or security issues are being experienced (Hamijah et al., 2025).

7. Third-Party & SLA Management

7.1 Cloud Shared Responsibility Model

In the context of using public clouds the customer and the provider have common security responsibilities. Indicatively, AWS claims to take care of the physical hardware, locations, availability zones, and virtual machines, whereas the customer has to take care of the operating system, app configuration, data, and access permissions. In the case of NatureGreen, this implies that the regulations should explicitly indicate what the provider takes care of (hardware and network) and what the company is required to secure (data, identities and applications) to avoid any loopholes in safety and separation.

Responsibility	On-premises	IaaS	PaaS	SaaS	FaaS	CIS Controls Cloud Companion Guide	CIS Foundations Benchmarks
Data classification and accountability	●	●	●	●	●	✓	✓
Client and end-point protection	●	●	●	●	●	✓	✓
Identity and access management	●	●	●	●	●	✓	✓
Application-level controls	●	●	●	●	●	✓	✓
Network controls	●	●	●	●	●	✓	✓
Host infrastructure	●	●	●	●	●	✓	
Physical security	●	●	●	●	●		
● Cloud Customer ● Cloud Provider							

Figure 5: Cloud Shared Responsibility Model

7.2 Vendor Audit & Security Requirements

NatureGreen has to include audit and security regulations in agreements with vendors and third parties, such as periodic security examinations, expeditious breach reports, and the entitlement to audit. Vendors should be made to adhere to acceptable standards such as the ISO 27001 by the company and demonstrate that controls are effective. Its frequent review of its vendors aids in dealing with external risks that are increasing due to cases of breaches of its supply chain to

make sure that its network is open and accountable throughout its extended network (Wandile Moeti, Moyo and Thereso Moropana, 2025).

8. Critical Discussion: Evolving Standards & Regulations

8.1 Rapid Technology & Threat Evolution

The locations that attackers can attack become manifold when firms rely on cloud services, wireless networks, and bring-the-own-device (BYOD) policies. Good rules ten years ago might not address emerging threats such as attacks on supply chains, going around zero-trust, or a mixed-cloud attack. According to experts, ancient controls are likely to lead to significant troubles. Thus, security plans need to be in line with new technologies and new threats in order to be effective (Srikrishna and Murthy, 2024).

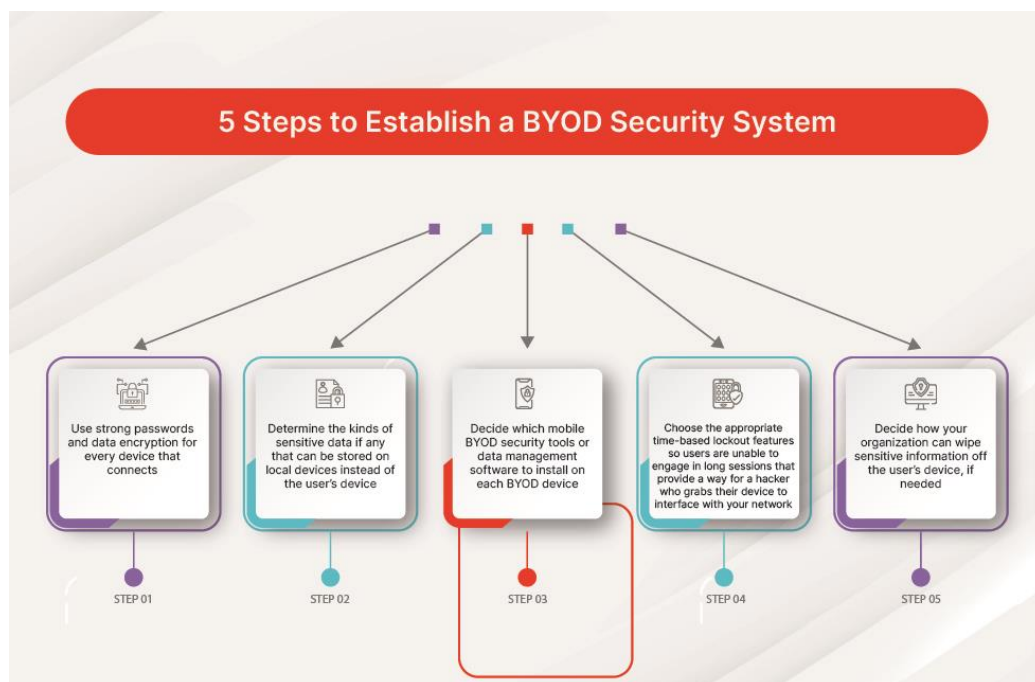


Figure 6: BYOD models

8.2 Regulatory and Compliance Changes

The world is rapidly changing cybersecurity regulations. As an illustration, in 2024, large nations proposed new cybersecurity regulations on major industries. Global working companies have to cope with evolving rule requirements such as when to disclose incidents or obligations regarding supply chains.

8.3 Implications for NatureGreen

The application of global cloud, wireless/BYOD culture and valuable IP at NatureGreen provides big risk when the rules do not match or controls are obsolete. The company requires a governing structure and a set of policies that could be revised in a short period of time and evaluated on a regular basis. Otherwise, it might disrupt rules, lose an intellectual property, and damage its brand. This is why it is necessary to add flexibility and review processes to the security program to ensure further resilience (Nookala, 2024).

9. Conclusion

9.1 Summary of Key Insights

NatureGreen is dependent on cloud, wireless and mobile technology which presents a challenging security and management requirement. Good control requires clear governance, clear rules and appropriate set of standards. The level of risks of the company should correspond to the tech controls, and the regulations of the vendors and third parties should be closely monitored (Kayode Akinsola, 2025).

9.2 Final Recommendations

To ensure that all sections of the company are on track, NatureGreen should immediately appoint a CISO and establish a security steering committee. It must develop a policy

architecture that includes BYOD, wireless, cloud, and vendor management. Practically, the company ought to employ an amalgamation of governance (i.e., COBIT), a risk-based framework (i.e., ISO 27001), and operational controls (i.e., NIST CSF). It must have SLA and audit policies with suppliers and identify clearly the responsibilities when it comes to cloud providers. Lastly, it ought to conduct regular reviews of standards, threats, and laws to ensure the security program is current and robust (Andreu, 2024).

References

- Andreu, A. (2024). The CISO Playbook. doi: <https://doi.org/10.1201/9781003477556>.
- Bukhari, T., Oladimeji, O., Etim, E. and Ajayi, J. (2021). Creating Value-Driven Risk Programs Through Data-Centric GRC Strategies. *International Scientific Refereed Research Journal* © 2021 SHISRRJ |, [online] 4, pp.2581–6306. Available at: <https://shisrrj.com/paper/SHISRRJ214437.pdf> [Accessed 24 Nov. 2025].
- Carnovale, S., Carnovale, J., Strub, D., Szalwinski, A. and Marek, J. (n.d.). Guardians of Intellectual Property in the 21st Century: The Global Supply Chain Industry. *Rutgers Business Review*, [online] 7(1). Available at: <https://rbr.business.rutgers.edu/sites/default/files/documents/rbr-070101.pdf>.
- Caudron, A., Promoteur, Q. and Vanleenhove, C. (n.d.). *How do Belgian companies deal with Chinese competition, its relentless progress and China's intellectual property protection policy?* [online] Available at: <https://matheo.uliege.be/bitstream/2268.2/15788/4/Caudron%20Quentin%20-%20thesis.pdf>.
- Ciekanowski, M., Żurawski, S., Ciekanowski, Z., Pauliuchuk, Y. and Czech, A. (2024). Chief information security officer : a vital component of organizational information security management. *Um.edu.mt*. [online] doi: <https://www.um.edu.mt/library/oar/handle/123456789/121081>.
- Dakić, V., Morić, Z., Kapulica, A. and Regvart, D. (2025). Analysis of Azure Zero Trust Architecture Implementation for Mid-Size Organizations. *Journal of Cybersecurity and Privacy*, [online] 5(1), p.2. doi: <https://doi.org/10.3390/jcp5010002>.
- Elia (2024). Navigating the landscape of EU sustainable finance regulation: challenges and imperatives to enforce sustainability financial promises in the EU through harmonized private enforcement mechanisms. *Unibo.it*. [online] doi: http://amsdottorato.unibo.it/11636/1/CERRATO_ELIA_TESI.pdf.
- Hamijah, A., Hamdan, S.N., Sulaiman, M.S., Norzalina Nasirudin, Hasan, M.H., Ismail, S., Mohd, Raja, Ghani, A., Abdullah, M.A., Radhiah Jamalludin, Noor, Hanizan Zainon, Fazli, M., Aris, M., Zakaria, M.F., Mohamad, Siti Farizawaty Sopian, Husain, A. and Mohd, S. (2025). Sustaining cyber and ICT security preparedness through disaster recovery testing and

simulations. *IOP Conference Series Materials Science and Engineering*, 1326(1), pp.012005–012005. doi: <https://doi.org/10.1088/1757-899x/1326/1/012005>.

Heidari, A., Amiri, Z., Ali, M. and Jafari, N. (2024). Assessment of reliability and availability of wireless sensor networks in industrial applications by considering permanent faults. *Concurrency and Computation Practice and Experience*, 36(27). doi: <https://doi.org/10.1002/cpe.8252>.

HIZA, D. (2022). Assessing the Significance of CIA Triad Security Model in Establishing ICT Security Controls in The Public Sector. *Iaa.ac.tz*. [online] doi: <http://dspace.iaa.ac.tz:8080/xmlui/handle/123456789/2126>.

John Agyekum Addae, Mota, J. and António Carrizo Moreira (2023). Risk governance as a line of defense: Systematic review of hotspots for future research. *Cogent Business & Management*, 10(2). doi: <https://doi.org/10.1080/23311975.2023.2215074>.

Kayode Akinsola (2025). Legal Oversight of State-Owned Enterprises: Governance Structures, Compliance, and Public Accountability. *Legal Oversight of State-Owned Enterprises: Governance Structures, Compliance, and Public Accountability*. [online] doi: <https://doi.org/10.2139/ssrn.5128102>.

Kristiansson, C. and Lundström, F. (2023). *Cloud Computing Pricing and Deployment Efforts : Navigating Cloud Computing Pricing and Deployment Efforts: Exploring the Public-Private Landscape*. [online] DIVA. Available at: <https://www.diva-portal.org/smash/record.jsf?pid=diva2:1770639>.

Möller, D.P.F. (2023). NIST Cybersecurity Framework and MITRE Cybersecurity Criteria. *Advances in Information Security*, 103, pp.231–271. doi: https://doi.org/10.1007/978-3-031-26845-8_5.

Nookala, G. (2024). Adaptive Data Governance Frameworks for Data-Driven Digital Transformations. *Journal of Computational Innovation*, [online] 4(1). Available at: <https://researchworkx.com/index.php/jci/article/view/16>.

Noor-A-Rahim, M., John, J., Firyaguna, F., Sherazi, H.H.R., Kushch, S., Vijayan, A., O’Connell, E., Pesch, D., O’Flynn, B., O’Brien, W., Hayes, M. and Armstrong, E. (2023). Wireless Communications for Smart Manufacturing and Industrial IoT: Existing

Technologies, 5G and Beyond. *Sensors*, [online] 23(1), p.73. doi:

<https://doi.org/10.3390/s23010073>.

Okusi, O., Obiakor, I. and Adeloye, F. (2025). Designing Resilient Data Risk Management Protocols for Regulatory Compliance and Cyber Incident Response. *International Journal of Advance Research Publication and Reviews*, [online] 02, pp.45–70. doi:

<https://doi.org/10.55248/gengpi.6.0725.2419>.

Singh, G.S. (2024). Cybersecurity governance framework for board directors. *Uts.edu.au*.

[online] doi: <http://hdl.handle.net/10453/187536>.

Singh, U.K. and Sharma, A. (2021). Cloud Computing Security Framework Based on Shared Responsibility Models. *CRC Press eBooks*, pp.39–55. doi:

<https://doi.org/10.1201/9781003146711-3>.

Srikrishna, H.V. and Murthy, J.S. (2024). Securing Mobile Workspaces in the Cloud.

Chapman and Hall/CRC eBooks, pp.238–262. doi: <https://doi.org/10.1201/9781003455448-13>.

Wandile Moeti, Moyo, S. and Thereso Moropana (2025). Compliance and Internal Controls: Standards and Practices in Cyber Security Governance. *SSRN Electronic Journal*. [online]

doi: <https://doi.org/10.2139/ssrn.5581811>.

Xiong, L., Shah, F. and Wu, W. (2022). Environmental and socio-economic performance of intensive farming systems with varying agricultural resource for maize production. *Science of The Total Environment*, 850, p.158030. doi: <https://doi.org/10.1016/j.scitotenv.2022.158030>.