

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



Deep Shaileshbhai Patel (2504308)
DATA SECURITY, GOVERNANCE AND COMPLIANCE (ACCA7028)

Table of Contents

1. Introduction.....	2
2. Organisational Context and Security Challenges at NG.....	2
2.1 Overview of NG's IT Environment	2
2.2 Key Information Security Issues.....	2
3. Review of Information Security Frameworks and Models.....	3
3.1 Information Technology Infrastructure Library (ITIL)	3
3.2 ISO/IEC 27000.....	4
3.3 Other Relevant Security Models	5
4. Designing a Custom Information Security Approach for NG	7
4.1 Security Governance and Strategic Planning.....	7
4.2 Information Security Policies	8
4.3 Risk Management Framework.....	9
4.4 Compliance, Legal and Ethical Considerations	10
4.5 Security Management Models and Practices	12
5. Security Controls and Protection Mechanisms	13
5.1 Technical Controls	13
5.2 Administrative and Physical Controls	13
5.3 Contingency and Business Continuity Planning.....	13
6. Service Level Agreements (SLAs) and Vendor Management.....	14
7. Critical Discussion: Importance of Continuous Updates to Regulations and Standards	14
8. Conclusion	15
References.....	16

1. Introduction

NatureGreen (NG) is an internationally recognised brand that endorses living healthily through its products and digital services. The organisation is primarily dependent on cloud computing, wireless networks, and BYOD practices for the support of its global workforce. Information security is important since cloud systems are more likely to be exposed to data breaches and cyber threats [1]. NG combats essential challenges related to wireless security, personal device applications, data protection, and defending precious intellectual property. This report's intention is to examine pertinent information security frameworks and to draw up a security approach that is specifically suited to NG. This report has a plan of reviewing security models, proposing solutions, and, after that, considering the significance of its updated regulations and standards in a critical way.

2. Organisational Context and Security Challenges at NG

2.1 Overview of NG's IT Environment

NatureGreen (NG) has a digitalised IT infrastructure based on heavy use of cloud solutions to provide applications, data storage, and customer collaboration solutions to its employees and customers globally. Over 95% of the network infrastructure in NG is wireless, allowing flexible network access between the offices and remote offices. The organisation accommodates the globally distributed workforce and the international consumers, which increases the number of access requests on the system. Moreover, NG has a robust online presence and social media to sell its products, communicate with its customers, and promote the brand worldwide.

2.2 Key Information Security Issues

Bring Your Own Device (BYOD) is one of the biggest information security problems of NatureGreen (NG). When such flexibility is provided to the staff and customers by allowing them to use their personal devices, the organisation is exposed to malware, unsecured applications and data leakage. Personal devices typically do not have standard security measures like encryption and periodic patching, which is why they are easily attacked by cybercriminals [2]. The network is highly wireless, and insecure devices find easy access to the network and break down critical systems in such an environment of NG.

Another important issue is data privacy and confidentiality since NG has a global workforce and its customers are also international. The company channels and processes considerable

amounts of personal and sensitive data on the cloud and online platforms. Although cloud-based systems are efficient, they take risks of unauthorised access in case the access controls and monitoring are not strong [3]. The violation of customer or employee data might lead to the loss of money, legal consequences, and embarrassment.

Intellectual property (IP) protection is of special concern to NG because its product information and business strategies are worth billions as proprietary. Organisations that do not have sound internal security controls are more susceptible to industrial espionage and insider threats [4]. Without stringent access control and classification rules, sensitive IP can either be revealed intentionally or by chance, particularly on personal devices and cloud sharing solutions.

The inadequacy of formal security policies adds even more risk to NG. Employees can, without knowledge, perform certain unsafe activities if there are no definite policies on BYOD usage, data handling, access control, and incident response. Security policies are the initial step toward unity and accountability in the security actions of the organisation, and their absence generally produces uncoordinated and defensive security management [5].

Lastly, NG deals with a considerable amount of compliance and regulatory exposure. Operating in various regions, the company is required to adhere to various data protection laws and ethical standards. Failure to comply with security practices and regulatory requirements will result not only in sanctions but also in a loss of stakeholder trust [6]. In the absence of proper governance and compliance, NG may be at risk of breaching legal obligations regarding data protection and privacy.

3. Review of Information Security Frameworks and Models

3.1 Information Technology Infrastructure Library (ITIL)

The Information Technology Infrastructure Library (ITIL) is a popular framework of IT service management, which aims at aligning IT services to the business requirements. ITIL offers organised IT services lifecycle management practices, such as service design, delivery, and operation, as well as constant improvement [7]. ITIL refers to information security management as a collective responsibility integrated into service management processes in terms of information security. According to scholarly studies, ITIL assists organisations to incorporate security measures into normal IT processes as opposed to considering security as a separate practice [8].



Figure 1: ITIL Framework

Source: [7].

ITIL facilitates risk mitigation by encouraging well-defined roles, documented processes and constant monitoring. In the case of organisations such as NG that depend extensively on the services of the clouds and wireless networks, ITIL can be used to ensure that the security requirements are factored into service level agreements, incident management, as well as change management processes. Research indicates that ITIL enhances service reliability and accountability, which indirectly enhances information security governance [9].

3.2 ISO/IEC 27000

The ISO/IEC 27000 is a set of standards that are internationally recognised and specifically designed to deal with information security management [10]. The most substantial standard, ISO/IEC 27001, offers specifications for setting up, carrying out, upholding, and developing

an Information Security Management System (ISMS) constantly [11]. ISO 27002 supplements this, providing specific guidance on security controls, including access control, cryptography, incident management and supplier relationships.

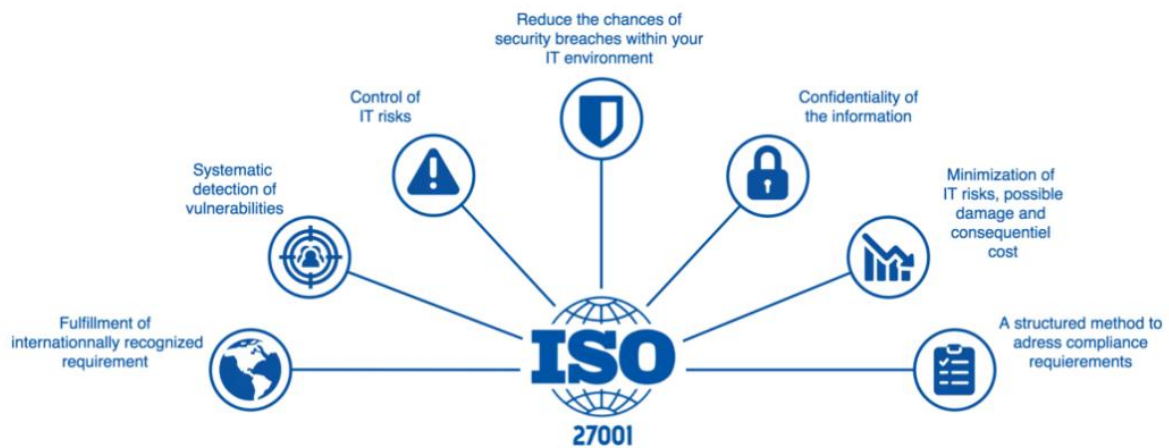


Figure 2: ISO 27002 Framework

Source: [12]

ISO 27001 is a best-practice model of preventing confidentiality, integrity, and availability of information because this standard employs a risk-based model whereby organisations can detect threats, vulnerabilities implement appropriate controls [12]. In cases of a global organisation such as NG, ISO 27001 would be especially beneficial, given that it would facilitate regulatory adherence and grant a certain sense of security to customers and partners. Studies show that organisations with certification to the ISO 27001 have enhanced trust, incidents and enhanced compliance results [13].

3.3 Other Relevant Security Models

Alongside ITIL and ISO standards, various other security models are applicable. One of the widely employed is the NIST Cybersecurity Framework for managing cybersecurity risks through the five core functions, such as identifying, protecting, detecting, responding, and recovering. NIST is practical and flexible, and hence is a suitable framework for organisations with complex digital environments [14]



Figure 3: NSIT Framework

Source: [12]

The other significant model is the COBIT, which is centred on IT governance and management. COBIT ensures the implementation of IT processes that are associated with business objectives while simultaneously managing risk and compliance. COBIT is in synergy with ISO 27001 by means of governance, accountability, and the strategic oversight [15].

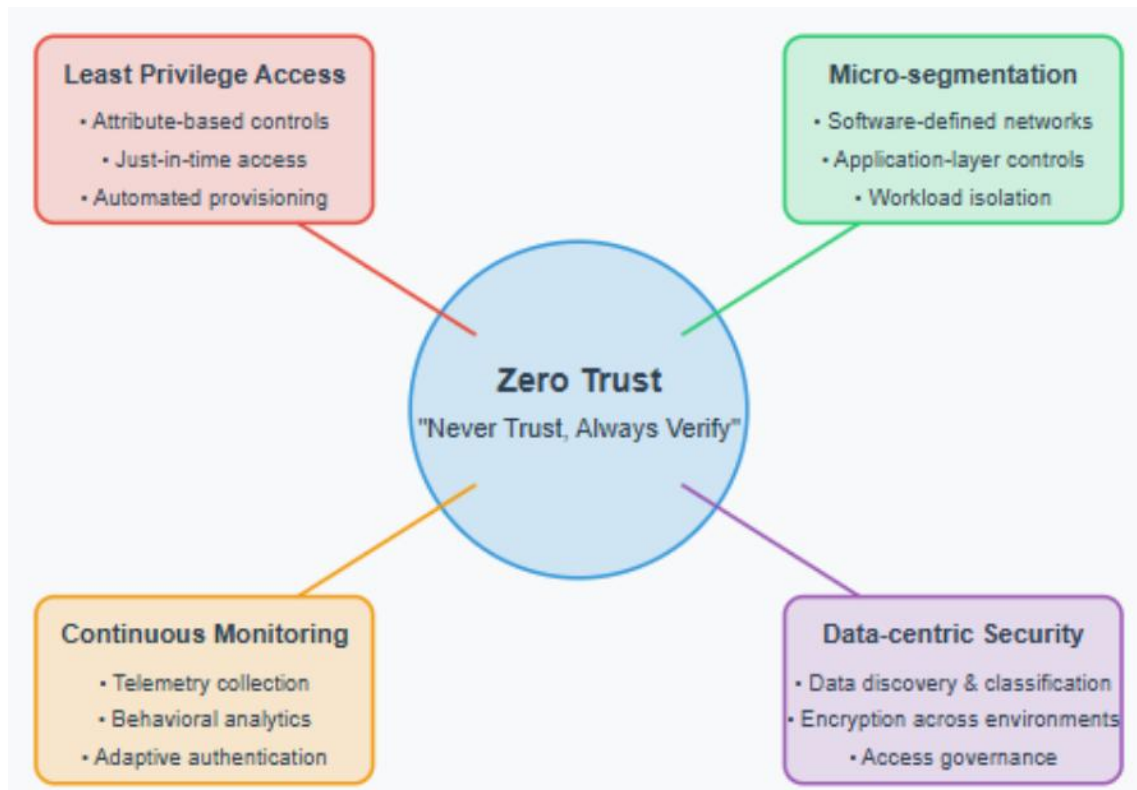


Figure 4: Zero Trust Security Model

Source: [16]

Zero Trust Security Model is based on the premise of never trust, always verify, where there is no automatic trust of a user or device, whether it is within or outside the organisational network [16]. The permission is provided under the condition of constant authentication, authorisation, and risk analysis. The model is best applied in the cloud-based and wireless environment of NatureGreen, involving BYOD, which has many smaller components, thereby making traditional perimeter-based security ineffective. Through Zero Trust, NG has the potential to minimise the threat of unauthorised access, lateral movement of attackers and data leakage. It has been proven that Zero Trust architectures make the systems more resilient to contemporary cyber threats and achieve better security governance [17].

4. Designing a Custom Information Security Approach for NG

4.1 Security Governance and Strategic Planning

NatureGreen need to consider good security governance to be aligned with organisational strategy and be aided on an executive level to enable accountability and resilience in the long run. *ISO/IEC 27001 Information Security Management System (ISMS)* should be the leading

governance tool to be implemented by NG because it offers a systematic methodology of integrating information security targets to business objectives. This structure underpins the definition of roles, duties, and control systems, which are essential in the complex cloud-based and wireless environment of NG. The process of strategic planning must be risk-oriented, where the security investments are focused on high-value assets, including customer data and intellectual property. The institution of a security steering committee and the appointment of a CISO-level position would offer better decision-making and global operations coordination. It has been found that organisations that have security governance at the board level are more mature in their management of cyber risks and regulatory compliance [18]. Moreover, it is better to incorporate security goals into corporate strategy to enhance the resilience of organisations to changing threats [19]. When governance is incorporated into strategic planning, NG will be able to shift its reactive security practices to a proactive and responsible security culture.

4.2 Information Security Policies

The operational basis of imposing security controls in NG is through information security policies. An information security policy framework that is coherent with **ISO/IEC 27002 security controls** must be embraced to normalise acceptable behaviour, especially in terms of BYOD, cloud usage, access control and incident response.

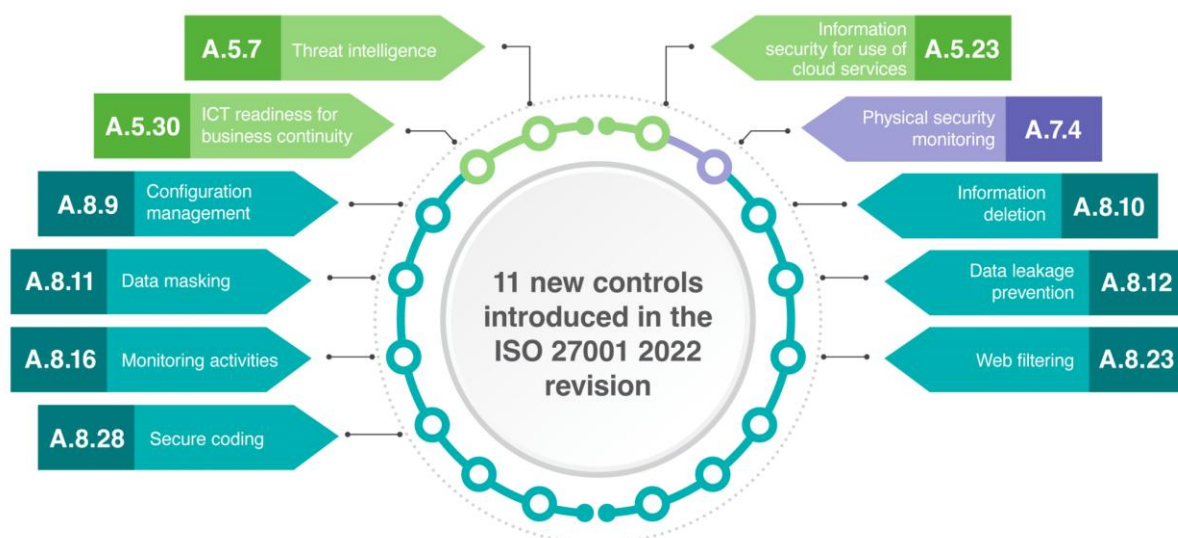


Figure 5: ISO/IEC 27002 security controls

Source: [20]

With the use of personal devices and the use of wireless access being instrumental to the operations of NG, there is a need to have a definite BYOD policy to require encryption, endpoint protection, and the use of secured authentication. Awareness training should be carried out to support the policies to make employees aware of their security roles. Research indicates that policy awareness and enforcement have a significant impact on accidental data breaches and insider-related incidents [21]. In addition, the effectiveness of the policy requires frequent review cycles to adapt to the emerging threats and regulatory changes, particularly in cloud environments [22]. The means of enforcement, such as monitoring and disciplinary measures, must be well-written to create accountability. The adoption of an organised and enforceable set of policies will help NG cut down on human vulnerability and promote uniformity among the global employees.

4.3 Risk Management Framework

NatureGreen needs to adopt an official risk management system to ensure systematic detection, evaluation, and management of information security risks. *The NIST Cybersecurity Framework* (CSF) can be adjusted to meet the needs of NG because it is flexible and highly integrated in cloud and wireless infrastructures.



Figure 6: NIST Cybersecurity Framework (CSF)

Source: [23]

The framework provides sustained risk identification in five fundamental functions, which are: Identify, Protect, Detect, Respond, and Recover. The most important assets that should be prioritised during risk assessment include sensitive personal data, cloud systems and intellectual property repositories. The studies emphasise that unmanaged personal devices and a lack of cloud access control put the organisations at a high risk of exposure [23]. The Risk treatment decisions should be mitigated, transferred, accepted, or avoided depending on the risk appetite and the business goals of NG. Vulnerability assessment and auditing are important since they allow monitoring risks continuously, as the evaluation of the risks becomes outdated in the dynamic threat landscape quite soon [24]. Using a defined risk management life cycle will allow NG to be proactive in risk management instead of being reactive to security breaches.

4.4 Compliance, Legal and Ethical Considerations

Its international business also means that NG is exposed to various legal and regulatory rules regarding data protection and privacy.

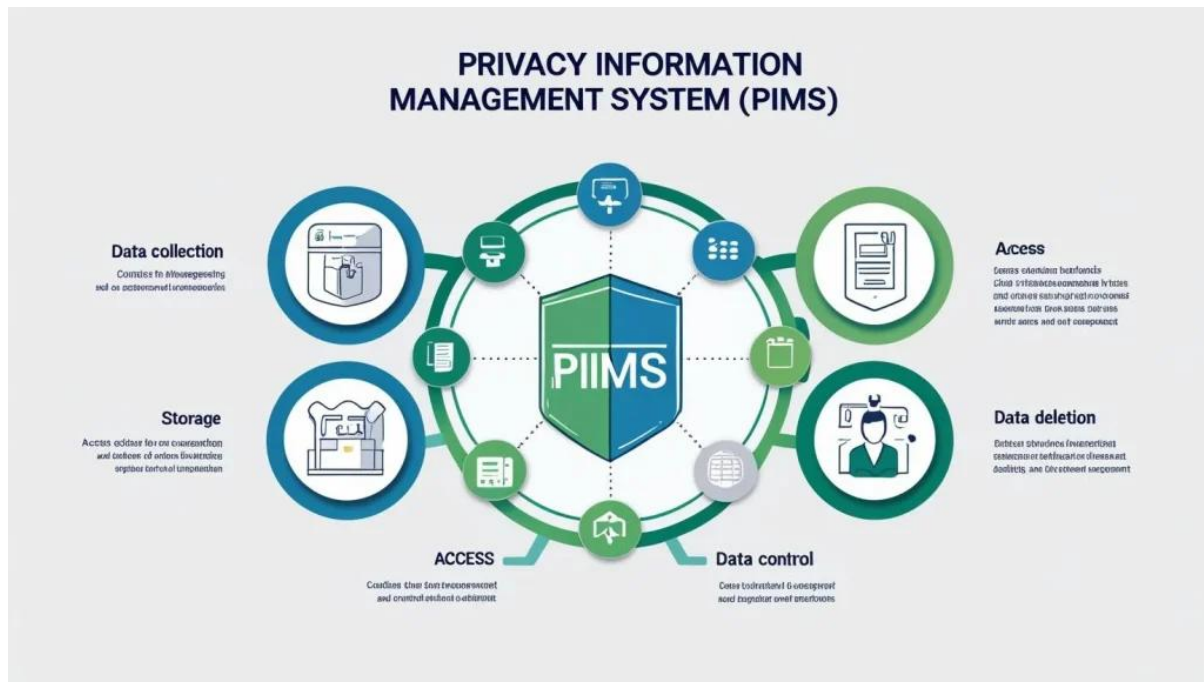


Figure 7: Privacy Information Management System (PIMS)

Source: [25]

By installing *ISO/IEC 27701 Privacy Information Management System (PIMS)*, the organisation will be able to expand its security governance to privacy compliance. This framework accommodates legal, open, and moral processing of individual information across borders. Non-adherence to data protection policies may lead to financial fines, loss of reputation and trust of the stakeholders. It has been empirically proven that robust compliance frameworks can help to enhance organisational credibility and minimise legal exposure [25]. In addition to legal requirements, NG is also required to consider ethical issues like proper utilisation of data, transparency, and fairness in surveillance of employees and clients. There is enhanced trust and long-term customer relationships with ethical security practices [26]. Due diligence should be done through regular compliance audits and documentation. The combination of legal and ethical factors in the security design will make the security approach of NG not only compliant but also socially responsible.

4.5 Security Management Models and Practices

To implement its security strategy, NG ought to use a layered security management strategy with reference to the *Defence-in-Depth security model*.

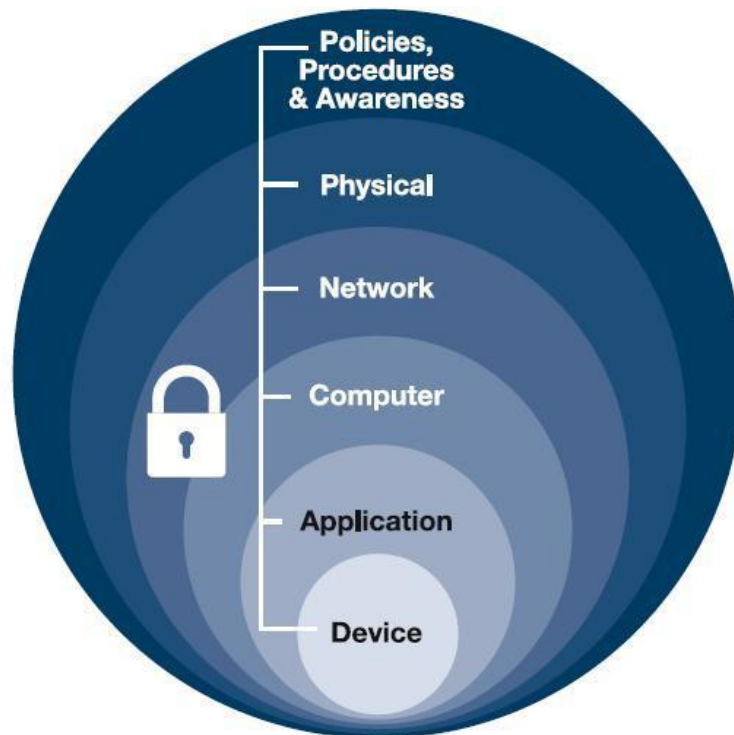


Figure 8: Defence-in-Depth security model

Source: [27]

This model will make sure that several complementary controls are implemented on the technical, administrative, and physical levels to minimise single points of failure. This can be very useful in cloud-based and wireless systems, and in such cases, perimeter-only security is not enough. The practices of security management are supposed to be identity and access management, sustained monitoring, incident management and frequent security testing. Studies suggest that organisations using layered security models have reduced impact of breaches on the organisation and recover more quickly [27]. Incident response plans should be well spelt out, and a simulation should be done about organisational preparedness. Post-incident reviews and updates to the policy should be incorporated to entrench continuous improvement to support adaptive security management [28]. Using systematic security management models, NG can remain resilient in its operations and still respond effectively to the changing threats of cybercrimes.

5. Security Controls and Protection Mechanisms

5.1 Technical Controls

Technical controls are system controls, which implement security policies, and ensure data integrity, confidentiality and availability. These comprise encryption, multi-factor authentication (MFA), firewalls, Intrusion Detection and Prevention Systems (IDS/IPS), identity and access management (IAM), and Security Information and Event Management (SIEM) tools to record and analyse them to identify anomalies [29]. Technical controls must be applied to organisations that have a high dependency on cloud services and wireless infrastructure to protect without human interference. Studies have indicated that combined technical protections will minimise the exposure to risk and better the reaction time to the threat, particularly against advanced attacks like ransomware and zero-day exploits.

5.2 Administrative and Physical Controls

Administrative controls are systematic procedures and policies which regulate human behaviour in security operations, such as access governance standards, incident response planning, security awareness training, and role-based procedures [30]. These controls establish responsibility, authority, and accountability to cybersecurity functions management. A scholarly article on the review of enterprise security policy models emphasises the significance of written policies in minimising the insider threat and strengthening employee adherence. Physical controls secure physical infrastructure and facilities, including data centres, CCTV surveillance, and other environmental protection (fire suppression) [31]. Physical controls are used together with administrative and technical controls to protect against physical attacks that may lead to the loss of digital assets, especially in a hybrid or cloud-connected environment.

5.3 Contingency and Business Continuity Planning

Business Continuity Management (BCM) and contingency planning is a way of making sure that an organisation is able to sustain the necessary operations both during and after disruptive events [32]. Implementing cyber risk planning in business continuity plans enhances resilience to unexpected outages and cyber events by defining the priorities in recovery, procedures of responding to the incident, and the alternative processes of running the company. Good continuity planning includes crisis communication, periodical testing, scenario planning, and backups to ensure continuity. The well-developed BCM structures enhance resilience in

operations and shorten recovery period after cyber disruptions, which is essential to organisations such as NG that have global operations.

6. Service Level Agreements (SLAs) and Vendor Management

Service Level Agreements (SLAs) are official treaties that outline the level of performance and security between an organisation and the service providers, especially cloud or managed security services. SecSLAs are performance guarantees with added security metrics such as confidentiality clauses, encryption rules, incident reporting schedules and compliance clauses according to the regulatory frameworks [33].

The cybersecurity SLAs emphasise that the inclusion of data confidentiality and access control as specific requirements in the contracts helps safeguard the organisational interests and brings about enhanced accountability in the outside vendors. The proper management of the vendor needs to be based on the constant monitoring of the security practices of the third parties, on the organised risk evaluation, on regular audits to make sure that the vendors comply with the terms proposed in the SecSLA. An extensive survey also focuses on the shift towards the concept of combining privacy and security performance metrics as the important elements of SLAs to guarantee the effective performance of service delivery in the cloud and outsourced setting [34]. Vendor management involves due diligence in selection, documented security expectations, periodic review and remedies that are enforced in case of non-compliance to create organisational security and continuity objectives.

7. Critical Discussion: Importance of Continuous Updates to Regulations and Standards

Dynamic Threat Landscape and Regulatory Evolution

The ongoing trends of cyber threats are changing fast due to the level of digital transformation, AI-powered attacks, and connected systems. Fixed standards and regulations become obsolete very quickly, exposing the organisations to emerging vulnerabilities. The studies show that modern cybersecurity rules contribute to a higher level of resilience and adherence to the current threat models, which fosters greater legal and operational conformity [35]. The cybersecurity regulation study asserts that cybersecurity regulatory updates are relevant to resilience by incorporating security expectations into institutional structures to secure that

capacity of the society and organisations to react to cyber threats also changes with the complexity of technology.

Regulatory Examples and Impacts

Recent legislation, such as the EU's Cyber Resilience Act (CRA) introduces proactive security obligations for software products and embedded devices, mandating risk assessments, secure-by-design principles, and vulnerability reporting requirements. These regulations change the compliance environment as it entails manufacturers to integrate cybersecurity across the lifecycle of the product, revealing that continuous regulatory changes are necessary [36]. Constant renewals also indicate socioeconomic and legislative changes such as the NIS2 Directive of the EU, that provides a tougher incident reporting and security requirement on the operators of essential services, solidifying the connection between regulation and operational risk management [37].

Business and Operational Justifications

An organisational perspective, the current compliance frameworks strengthen the alignment of governance structures, as well as strategic security and thus risk mitigation, trust in stakeholders and competitive advantage [38]. Lacking new standards, organisations can become lagging behind new threats, face legal fines, and reputational losses, so continuous regulatory adaptation can be at the heart of successful cybersecurity governance.

8. Conclusion

A strong information security posture, through the presence of effective security controls, including technical, administrative, and physical, with the working continuity planning, will result in a strong information security posture in NatureGreen. External dependencies are also strengthened by SLAs and vendor management that represent enforceable security expectations. Constant regulatory changes are essential and allow organisations to adjust to the changes in the threats and legal conditions. It has been established that incorporating the existing standards and looking ahead of the future regulatory trends is the greatest way of enhancing organisational resilience and governance. Combined, reactive, research-based security strategy will provide NatureGreen with a chance to operate in a constantly evolving cybersecurity sphere with continuity, legal standing, and trust of stakeholders.

References

- [1] L. Alexandra, "DATA BREACHES IN CLOUD ENVIRONMENTS CAUSES, CONSEQUENCES, AND PREVENTION," *ResearchGate*, p. 9, Apr. 2025, Available: https://www.researchgate.net/publication/391270943_DATA_BREACHES_IN_CLOUD_ENVIRONMENTS_CAUSES_CONSEQUENCES_AND_PREVENTION
- [2] T. Sasi, A. H. Lashkari, R. Lu, P. Xiong, and S. Iqbal, "A Comprehensive Survey on IoT Attacks: Taxonomy, Detection Mechanisms and Challenges," *Journal of Information and Intelligence*, vol. 2, no. 6, 2023. doi:10.1016/j.jiixd.2023.12.001. Available: <https://www.sciencedirect.com/science/article/pii/S2949715923000793>
- [3] Fauzia A, "Cybersecurity Challenges in Cloud Computing: Ensuring Information Security for Connected Devices," *ResearchGate*, 2019. doi: 10.13140/RG.2.2.19705.99682. Available: https://www.researchgate.net/publication/386504217_Cybersecurity_Challenges_in_Cloud_Computing_Ensuring_Information_Security_for_Connected_Devices
- [4] U. Inayat, M. Farzan, S. Mahmood, M. Fahad Zia, S. Hussain, and F. Pallonetto, "Insider threat mitigation: Systematic literature review," *Ain Shams Engineering Journal*, vol. 15, no. 12, pp. 103068–103068, 2024. doi: 10.1016/j.asej.2024.103068. Available: <https://www.sciencedirect.com/science/article/pii/S209044792400443X>
- [5] S. Mushtaq and M. Shah, "Critical Factors and Practices in Mitigating Cybercrimes within E-Government Services: A Rapid Review on Optimising Public Service Management," *Information*, vol. 15, no. 10, pp. 619–619, 2024. Available: <https://www.mdpi.com/2078-2489/15/10/619>
- [6] A. Folorunso, I. Wada, B. Samuel, and V. Mohammed, "Security compliance and its implication for cybersecurity," *World Journal of Advanced Research and Reviews*, vol. 24, no. 01, pp. 2105–2121, 2024, doi: 10.30574/wjarr.2024.24.1.3170. Available: https://www.researchgate.net/publication/385525362_Security_compliance_and_its_implication_for_cybersecurity
- [7] Jin, "The Introduction of Information Technology Infrastructure Library (ITIL)," *Geek Culture*, 2023. Available: <https://medium.com/geekculture/the-introduction-of-information-technology-infrastructure-library-til-66c1baf1b92f>

- [8] S. Gangula, “A Comprehensive Review of ITIL Frameworks for Managing Large-Scale Retail Cloud Operations and Challenges,” *International Journal of Engineering and Architecture*, vol. 2, no. 2, pp. 18–34, 2025, doi: 10.58425/ijea.v2i2.433. Available: https://www.researchgate.net/publication/397363294_A_Comprehensive_Review_of_ITIL_Frameworks_for_Managing_Large-Scale_Retail_Cloud_Operations_and_Challenges
- [9] A. M. Momani, “The Role of IT Governance in Organizations: Best Practices for Enhancing Audit, Control, and Success,” *SSRN Electronic Journal*, 2025, doi: 10.2139/ssrn.5053120. Available: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5053120
- [10] International Organization for Standardization, “ISO/IEC 27001 standard – information security management systems,” *ISO*, 2022. Available: <https://www.iso.org/standard/27001>
- [11] N. Ramadhan and U. Rose, “Adapting ISO/ IEC 27001 Information Security Management Standard to SMEs,” 2022. Available: <https://www.diva-portal.org/smash/get/diva2:1670976/ATTACHMENT01.pdf>
- [12] J. Huergo, “NIST Releases Version 1.1 of its Popular Cybersecurity Framework,” *NIST*, Apr. 16, 2018. Available: <https://www.nist.gov/news-events/news/2018/04/nist-releases-version-1-1-its-popular-cybersecurity-framework>
- [13] N. Munir, “DEGREE PROJECT The Impact of ISO 27001 Compliance on Employees’ Information Security Awareness and Behaviors in Medium Sized Enterprises (MSEs) NOMAN MUNIR,” 2024. Available: <https://www.diva-portal.org/smash/get/diva2:1874341/FULLTEXT01.pdf>
- [14] W. D. Camara *et al.*, “DIGITAL NIST: An examination of the obstacles and opportunities in the digital transformation of NIST’s reference materials,” *Acta IMEKO*, vol. 12, no. 1, pp. 1–4, 2023, doi: 10.21014/actaimeko.v12i1.1403. Available: <https://www.imeko.org/publications/tc6-2022/IMEKO-TC6-2022-031.pdf>
- [15] I. A. Essien *et al.*, “Optimizing Cyber Risk Governance Using Global Frameworks: ISO, NIST, and COBIT Alignment,” *Journal of Frontiers in Multidisciplinary Research*, vol. 3, no. 1, pp. 618–629, 2022, doi: 10.54660/jfmr.2022.3.1.618-629. Available: https://www.researchgate.net/publication/395104534_Optimizing_Cyber_Risk_Governance_Using_Global_Frameworks_ISO_NIST_and_COBIT_Alignment

- [16] V.A.Vora, "Demystifying Zero Trust Security: The No-Trust Network Paradigm," *Journal of Computer Science and Technology Studies*, 7(3), pp.141-148, 2025, doi: 10.32996/jcsts.2025.7.3.15 Available: <https://www.sciencedirect.com/science/article/pii/S2949715923000793>
- [17] G.Ahn, J.Jang, S.Choi, D.Shin, "Research on Improving Cyber Resilience by Integrating the Zero Trust security model with the MITRE ATT&CK matrix," *IEEE Access*. 2024 Jun 21;12:89291-309. doi: 10.1109/ACCESS.2024.3417182 Available: <https://ieeexplore.ieee.org/abstract/document/10568117/>
- [18] Dr Khawaja Tahir Mehmood, Zia Ashraf, Raza Iqbal, Adnan Ahmed Rafique, Hassam Gul, and Muhammad Ali, "Cyber security Governance as a Pillar of Enterprise Risk Management: Designing a Compliance-Driven Framework for Operational Resilience, Policy Enforcement, and Regulatory Alignment," *Annual Methodological Archive Research Review*, vol. 3, no. 5, pp. 59–77, May 2025, doi: <https://doi.org/10.63075/0jv35d33>. Available: <https://doi.org/10.63075/0jv35d33>
- [19] A. Kanaan, A. Mtair AL-Hawamleh, M. Aloun, A. Alorfi, and M. Abdalwahab Alrawashdeh, "Fortifying Organizational Cyber Resilience: An Integrated Framework for Business Continuity and Growth amidst Escalating Threat Landscapes," *International Journal of Computing and Digital Systems*, vol. 17, no. 1, pp. 1–14, Jan. 2025, doi: <https://doi.org/10.12785/ijcds/1571023809>
- [20] D. Kosutic, "What are the 11 new security controls in ISO 27001:2022?," *advisera.com*, 2025. Available: <https://advisera.com/27001academy/explanation-of-11-new-iso-27001-2022-controls/>
- [21] F. Whitelaw, J. Riley, and N. Elmabit, "A Review of the Insider Threat, a Practitioner Perspective Within the U.K. Financial Services," *IEEE Access*, vol. 12, pp. 34752–34768, 2024, doi: <https://doi.org/10.1109/ACCESS.2024.3373265>. Available: <https://ieeexplore.ieee.org/abstract/document/10458945/>
- [22] Saadia Drissi, Meriyem Chergui, and Zakaria Khatar, "A Systematic Literature Review on Risk Assessment in Cloud Computing: Recent Research Advancements," *IEEE Access*, pp. 1–1, Jan. 2025, doi: <https://doi.org/10.1109/access.2025.3561123>. Available: <https://ieeexplore.ieee.org/document/10965667>

- [23] J. Huergo, "NIST Releases Version 1.1 of its Popular Cybersecurity Framework," *NIST*, Apr. 16, 2018. Available: <https://www.nist.gov/news-events/news/2018/04/nist-releases-version-1-1-its-popular-cybersecurity-framework>
- [24] A. Mallick and R. Nath, "Navigating the Cyber security Landscape: A Comprehensive Review of Cyber-Attacks, Emerging Trends, and Recent Developments," 2024. Available: <https://worldscientificnews.com/wp-content/uploads/2024/01/WSN-1901-2024-1-69-1.pdf>
- [25] R. Bergman, "Just Published: Global Standard for Privacy Information Management Systems (PIMS). Summary for Legal and Dispute Resolution Professionals," *Mediate.com*, Oct. 20, 2025. Available: <https://mediate.com/global-standard-for-pims/>
- [26] M. Celestin, S. Sujatha, and A. D. Kumar, "ANALYZING THE ROLE OF ETHICAL BUSINESS PRACTICES IN BUILDING CONSUMER TRUST AND LONG-TERM BRAND LOYALTY: LEVERAGING CORPORATE ETHICS AS A COMPETITIVE ADVANTAGE," *ANALYZING THE ROLE OF ETHICAL BUSINESS PRACTICES IN BUILDING CONSUMER TRUST AND LONG-TERM BRAND LOYALTY: LEVERAGING CORPORATE ETHICS AS A COMPETITIVE ADVANTAGE*, no. 2, pp. 1–9, Oct. 2024, doi: <https://doi.org/10.5281/zenodo.14010882>. Available: https://www.researchgate.net/publication/385363150_ANALYZING_THE_ROLE_OF_ETHICAL_BUSINESS_PRACTICES_IN_BUILDING_CONSUMER_TRUST_AND_LONG-TERM_BRAND_LOYALTY_LEVERAGING_CORPORATE_ETHICS_AS_A_COMPETITIVE_ADVANTAGE
- [27] "Defence in Depth," *Open Practice Library*, 2025. Available: <https://openpracticelibrary.com/practice/defence-in-depth/>
- [28] E. Manning, "Optimizing Incident Management Processes for Effective Cybersecurity Incident Response MSc Research Project," 2023. Available: <https://norma.ncirl.ie/7296/1/ericamanning.pdf>
- [29] M. Sinan, M. Shahin, I. Gondal, "Implementing and integrating security controls: A practitioner's perspective", *Computers & Security*, 2025 May 10:104516. doi: 10.1109/ACCESS.2024.3417182. Available: <https://www.sciencedirect.com/science/article/pii/S0167404825002056>

- [30] YA.Marquis, “From theory to practice: Implementing effective role-based access control strategies to mitigate insider risks in diverse organizational contexts,” *Journal of Engineering Research and Reports*, 2024 Apr 10;26(5):138-54, doi: 10.9734/JERR/2024/v26i51141 Available: https://www.researchgate.net/profile/Yewande-Marquis/publication/379738680_From_Theory_to_Practice_Implementing_Effective_Role-Based_Access_Control_Strategies_to_Mitigate_Insider_Risks_in_Diverse_Organizational_Contexts/links/661ca76b66ba7e2359d97a45/From-Theory-to-Practice-Implementing-Effective-Role-Based-Access-Control-Strategies-to-Mitigate-Insider-Risks-in-Diverse-Organizational-Contexts.pdf
- [31] R.Damaševičius, N.Bacanin, S.Misra, “From sensors to safety: Internet of Emergency Services (IoES) for emergency response and disaster management,” *Journal of sensor and actuator networks* 2023 May 16;12(3):41, doi: 10.3390/jsan12030041. Available: <https://www.mdpi.com/2224-2708/12/3/41>
- [32] R.Steen, OJ.Haug, R.Patriarca, “Business continuity and resilience management: A conceptual framework,” *Journal of Contingencies and Crisis Management*, 2024 Mar;32(1):e12501, doi: 10.1111/1468-5973.12501 Available: <https://onlinelibrary.wiley.com/doi/abs/10.1111/1468-5973.12501>
- [33] Y.Nugraha, A. Martin, “Cybersecurity service level agreements: understanding government data confidentiality requirements,” *Journal of Cybersecurity*, 2022 Jan 1;8(1):tyac004. doi: 10.1093/cybsec/tyac004 Available: <https://academic.oup.com/cybersecurity/article-abstract/8/1/tyac004/6588067>
- [34] S. Nicolazzo, A. Nocera, W. Pedrycz, “Service level agreements and security sla: A comprehensive survey” arXiv:2405.00009. 2024 Jan 31, doi: [10.48550/arXiv.2405.00009](https://arxiv.org/abs/2405.00009) Available: <https://arxiv.org/abs/2405.00009>
- [35] R. Kelemen *ET AL.*, “Cybersecurity Regulations and Software Resilience: Strengthening Awareness and Societal Stability” *Social Sciences*. 2025 Sep 26;14(10):578. doi:[10.3390/socsci14100578](https://doi.org/10.3390/socsci14100578) Available: <https://www.mdpi.com/2076-0760/14/10/578>
- [36] F. Teichmann, “The cyber resilience act as a new paradigm for product security: a compliance roadma,” *International Cybersecurity Law Review*, 2025 Nov 28:1-7. doi:

10.1365/s43439-025-00162-4 Available: <https://link.springer.com/article/10.1365/s43439-025-00162-4>

[37] ISACA. “2023 Volume 5 Harmonizing Cybersecurity Practices.” ISACA, 2023. <https://www.isaca.org/resources/isaca-journal/issues/2023/volume-5/harmonizing-cybersecurity-practices>.

[38] K.Singh, S.Chatterjee, M.Mariani, SF. Wamba, “Cybersecurity resilience and innovation ecosystems for sustainable business excellence: Examining the dramatic changes in the macroeconomic business environment,” *Technovation*, 2025 May 1;143:103219. doi: [10.1016/j.technovation.2025.103219](https://doi.org/10.1016/j.technovation.2025.103219) Available: <https://www.sciencedirect.com/science/article/pii/S0166497225000513>