

DATA SECURITY GOVERNANCE AND COMPLIANCE

Module Title:

Data Security Governance and Compliance

Module Code:

ACCA7028

Assessment Type:

Coursework

Case Study:

NatureGreen (NG)

Title of Report:

Design and Analysis of a Custom Data Security Governance and Compliance Framework (NG-DSGCF) for NatureGreen

Student Name: *Rishabh Choudhary*

Student ID: *2434332*

Programme: *MSc Cybersecurity and Digital Forensics*

University: *University of Wales Trinity Saint David, London*

Lecturer / Module Leader: *Dr. Dipo Dunsin*

Submission Date: *19 Dec. 25*

Contents

1 Introduction	1
2 SCENARIO ANALYSIS	2
2.1 Assets & Data	2
2.2 Threats	2
2.3 Governance and Risk Gap Analysis.....	2
3 FRAMEWORK REVIEW AND SELECTION	3
3.1 The NIST Risk Management Framework and Cybersecurity Framework	3
3.2 ISO/IEC	4
3.3 COBIT	4
3.4 ITIL.....	4
3.5 Discussion on Regulatory Updates	5
4 Custom Framework Design: NG-DSG	5
4.1 Framework Overview.....	5
4.2 Step 1 - Scenario Analysis.....	6
4.3 Step 2 – Identification of Assets, Data, and Threats.....	6
4.4 Step 3 – Governance and Risk Gap Analysis	7
4.5 Step 4 – Selection of Framework Models	7
4.6 Step 5 - Synthesis of Custom Framework	7
4.7 Implementation Road.....	8
4.8 Additional Diagrams and Flowcharts	9
5 Discussion.....	13
5.1 Why Framework Integration Matters	13
5.2. Importance of Continuous Improvement	13
5.3 Addressing BYOD	13
5.4 Limitations and Future Work	13
6 Conclusion	14
References	15

Abstract

NatureGreen (NG) is a worldwide business organisation with a specialisation in healthy living products, spreading its roots via primarily wireless networking and cloud infrastructure. Although this organisation has an extensive presence on the web, it still lacks formally defined and implemented information security policies and governance. Furthermore, due to its stringent need for ensuring Bring-Your-Own-Device (BYOD) connectivity facilities for employees as well as customers, there is intensified vulnerability to security threats and issues regarding data protection. The NatureGreen scenario is examined in this study to determine primary weaknesses, vulnerabilities, and threats that impact the confidentiality, integrity, and availability of an organisation's resources and assets. Subsequently, a custom-designed Data Security Governance and Compliance Framework (NG-DSGCF) construct is employed, taking into account specific security, governance, and compliance needs of NG within the scope of this study. In this respect, a targeted synthesis of primary models and best practices from pre-existing, standard frameworks of NIST, ISO/IEC 27000, COBIT 2019, and ITIL 4 is introduced for a holistic, efficient, and effective management of specific information security risks and associated web-based regulatory aspects.

1 Introduction

The rising trend in cloud computing, wireless networks, and web services has greatly amplified the efficiency and interconnectedness of organisations. At the same time, the use of cloud computing, wireless networks, and web services has amplified the challenges posed by security, governance, and compliance. This is due to the increased threats associated with organizations in highly connected environments, including security threats, breaches, and compliance issues that can result from the absence of proper security management.

NatureGreen (NG), a world-leading brand for healthy living products, is mainly operating in a cloud-based and wireless environment with strong online and social networking activities. It is also facing challenges as an organisation to provision Bring Your Own Device (BYOD) connectivity for employees as well as customers. The absence of an effective information security governance structure makes it difficult for NG to mitigate cyber threats.

This paper explores the security needs and governance gaps of NG using a structured analysis of various industry standards and best practices drawn from the likes of NIST, ISO/IEC 27000 standards, COBIT 2019, and ITIL 4. Based on various models mentioned in these standards and best practices, a tailored version of the Data Security Governance and Compliance Framework for NatureGreen (NG-DSGCF) has also been proposed.

2 SCENARIO ANALYSIS

2.1 Assets & Data

The most critical resources and competencies owned by NG are customer and employee personal information, intellectual properties, financial information, product research, and cloud-based facilities used in logistics and marketing and sales activities. The company's reputation in relation to its brands is an intangible asset that should be protected. Since it is a global company, NG must adhere to regulations on data protection, such as GDPR in dealing with European customers.

2.2 Threats

There are risks posed using the network by employees and clients through their own devices. BYOD makes the security controls in the devices unpredictable, where factors such as malware and the lack of security in the Wi-Fi network and the method of authentication on the device may pose a threat to the organisational network [1]. A review on the risk management processes involved in BYOD asserts that ISO/IEC 27000 risk analysis establishes risks and their corresponding vulnerabilities linked to organisational assets and limits the risks through the application of controls [1]. In the context of the NC, the following risks, in addition to the one mentioned above, are posed by the framework:

- Attacks on wireless networks, namely eavesdropping, rogue access points, and denial of service to the existing 95% wireless infrastructure.
- Cloud vulnerabilities: misconfiguration, insecure APIs, and loss of data because of unencrypted cloud storage.
- Social-engineering and phishing: targeting employees through their presence on social sites.
- Insider threats: abuse of privileged access.
- Non-compliance with regulations: lack of protection of personal data may cause legal consequences.

2.3 Governance and Risk Gap Analysis

“The current state of NG is that it lacks policy, roles, or processes for risk management. This is reinforced by the OSFI Technology/Cyber Risk

Management Guideline, which asserts that there is “no one-size-fits-all approach” – organizations need “a risk-based mindset proportionates” to their size, activities, or risk profile [2]. NG requires focus on accountability/governance, having a strong “technology environment,” as well as ensuring the “confidentiality, integrity, or availability” of assets, which are lacking [2]. This leaves a gap in the governance structure.”

3 FRAMEWORK REVIEW AND SELECTION

The pertinent frameworks and the reason for using certain models to develop the NG-DSGCF are discussed in this part.

3.1 The NIST Risk Management Framework and Cybersecurity Framework

The National Institute of Standards and Technology in the United States has offered widely used cyber security standards. The NIST Risk Management Framework offers a comprehensive, flexible, and measurable and repeatable process involving seven steps through which an organization should follow to manage information security and privacy risk [3]

1. preparing the organization
2. Categorizing
3. selecting controls
4. implementing controls
5. assessing controls
6. Authorizing systems
7. monitoring controls.

The NIST Cybersecurity Framework, or CSF, supports the RMF by breaking down five essential activities: Identify, Protect, Detect, Respond and Recover, which form a universal vocabulary to address cyber risks [4]. The five activities allow organisations to evaluate their security posture, establish target profiles, and focus efforts to improve them.

The CSF also focuses on continuous improvement. According to CG Compliance: "Continuous improvement ensures the continuous evolution of cybersecurity to keep pace with new cyber threats. This feature of a CSF is

very essential in the context of NG because new threats as well as new technologies are emerging rapidly.”

3.2 ISO/IEC

The ISO/IEC 27000 series have established international standards for Information Security Management Systems. ISO/IEC 27001 is a global most popular standard related to information security management systems and their requirements [5]. Other relevant standards include ISO/IEC 27002, dealing with information security controls, and ISO/IEC 27005, focusing on information security risk management. All these standards make it possible for organizations to handle information security issues related to their resources, as well as financial information, intellectual property, employees' information, and information entrusted by third parties [5]. The ISO standards apply a Plan–Do–Check–Act (PDCA) model, allowing for ongoing improvement in ISMS.

3.3 COBIT

COBIT, or Control Objectives for Information Technologies, is an enterprise IT governance guidance developed by ISACA. The essence of COBIT 2019 defines enhance governance and the COBIT principles that describe the framework's overall structure, with The Governance and Management Objectives publication describing in depth the COBIT core model and 40 governance and management objectives with defined objectives and their processes attributed to enterprise and alignment goals [6]. For NG, governance, and management objectives in COBIT are used to shape management roles, metrics, and enterprise and IT business alignments.

3.4 ITIL

ITIL (Information Technology Infrastructure Library) is a best practice guidance on IT service management (ITSM). ITIL 4 is an upgrade on its predecessors, offering a new digital operating model to assist organisations in their digital transformation journey [7]. ITIL 4 combines best practices from Agile, DevOps, and digital transformation; it moved from a prescriptive to a flexible way of working. The main points include four dimensions (organizations and people, information and technology, partners and suppliers, value streams, and processes), seven guiding principles, as well as a service value system that focuses on continual improvements. ITIL’s service value chain includes plan, improve, engage, design and transition,

obtain/build, and deliver/support in assisting an integrated way of delivering their services [7].

3.5 Discussion on Regulatory Updates

Cybersecurity Frameworks also need to be updated with the latest risks, technologies, and ever-changing regulations. The OSFI guideline states that the technologies and cyber risk domains are constantly evolving and cut across other risk domains as well [2]. The importance of continuous improvement in the NIST CSF and the statement from CG Compliance about the need for a change in the measures taken at the organizational level to keep up with the latest risks establish the need for periodic modifications in the frameworks [4]. New regulations like GDPR, CCPA, or the latest standards for Artificial Intelligence governance also emerge over time and impose a set of compliances on the organizations to be adhered to.

4 Custom Framework Design: NG-DSG

4.1 Framework Overview

The NGDSGCF combines models chosen from NIST, ISO 27000, COBIT 2019, and ITIL 4 to meet the customized needs of NG by basing a tailored framework on these models. This framework is based on a high-level approach to methodology and is represented in *Figure 1* below.

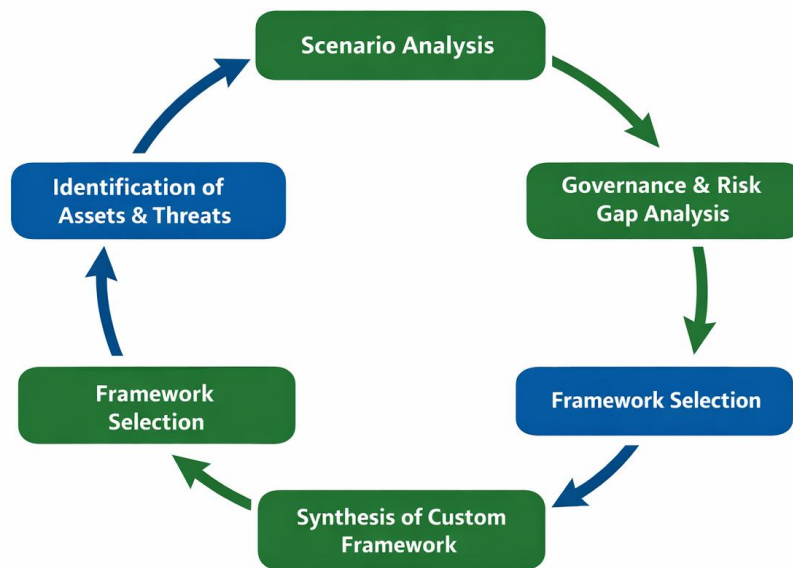


Figure 1 – NG-DSGCF process

Figure 1 depicts a circular workflow starting with scenario analysis. This design reflects the principle of continuous improvement; after the synthesis of the custom framework, the organisation should revisit the scenario as new threats and requirements emerge.

4.2 Step 1 - Scenario Analysis

The model starts by evaluating the operating context of NG, business goals, regulatory requirements, and stakeholders' expectations. This phase requires the formation of a security governance committee consisting of company executives, technology managers, lawyers, as well as risk managers. The committee determines security program scope, lists security program objectives, as well as identifies stakeholders.

4.3 Step 2 – Identification of Assets, Data, and Threats

A list of assets (data, hardware, software, and human) is created. Confidentiality, integrity, and availability needs are specified for every asset. Based on threat intelligence feeds, security alerts, and thorough BYOD reviews a threat catalog is developed [1]. Vulnerabilities are identified through vulnerability scans and penetration testing. This step generates an asset threat matrix and initial risk register.

4.4 Step 3 – Governance and Risk Gap Analysis

Based on the governance factors defined in COBIT and the clauses mentioned in ISO/IEC 27001, the existing policies, processes, and controls are compared with the requirements. The lack of policies is noted, and the maturity assessments are conducted. The framework applied by the OSFI on the aspects of accountability and governance is applied to define the roles to be followed [2]. The risk attitude and tolerance thresholds are determined. The results of the gap analysis provide the road map for the development of policies, organizational changes, and allocation of resources.

4.5 Step 4 – Selection of Framework Models

The NG-DSGCF picks and customizes models using established frameworks:

1. Risk Management: Implement the seven-step risk management process proposed by NIST RMF, along with the risk assessment approach by ISO/IEC 27005 [3]. NG selects security controls using NIST SP 800-53 Release 5.2 and ISO/IEC 27002. Focus is on controls like AC-18: Wireless Access, SC-13: Cryptographic Protection, cloud security, and BYOD.
2. Governance: The goals of COBIT 2019 governance and management should be used to identify roles, responsibilities, decision rights, and performance measures, with goals such as EDM03 – risk optimization ensured, APO12 – risk managed, and DSS05 – security services managed. This is to ensure security processes meet business requirements [6].
3. Service Management: Integrate ITIL 4 practices in the areas of incident management, change control, and continual improvement. The service value system and the principles help create value and satisfy the customer [7].
4. Compliance: Support ISO/IEC 27701 (Privacy Information Management) and GDPR standards. Data classification and privacy impact assessments should also be implemented.

4.6 Step 5 - Synthesis of Custom Framework

NG combines the components into a unified framework:

Governance Layer: A security charter is formed by the Board and the executive team. The CISO maintains accountability to the Board. The Board is guided by the COBIT framework of security governance. The

ISO/IEC 27001 framework is used to define the information security policy and scope. The OSFI accountability framework supports this [2].

Risk management layer: The NIST RMF processes are conducted iteratively. Systems are categorized according to impact levels; controls are identified and implemented based on NIST SP 800-53 and ISO/IEC 27002 standards. Control evaluations are carried out; system authorizations are issued by senior management leaders. Continuous monitoring comprises vulnerability scanning, Security Information and Event Management (SIEM), and system audits conducted periodically. CG Compliance highly stresses that in the CSF processes (Identify, Protect, Detect, Respond, Recover), a universal language is achieved through continuous improvement processes [4].

Service management layer: ITIL best practices address issues related to authorizing and recording system modifications, managing incidents effectively, and delivering service requests. The service value chain enables collaboration between IT and business teams; service metrics include mean time to detect, mean time to respond, and service availability.

Control Implementation: Controls are implemented at different technical, organizational, and physical levels. These include multi-factor authentication, network segmentation, encryption of data at rest and in transit, endpoint protection, security awareness training, enforcement of the BYOD policy, and logging and monitoring.

Compliance & Audit: Internal and external audits are carried out to check adherence to regulations. Privacy impact assessments are used to guarantee that personal information is processed in a legal manner. Plans are made to fill gaps in areas that do not comply.

4.7 Implementation Road

Implementation of the Framework is staggered:

1. Preparation (months 1–2): Form the governance committee and develop the scope and objectives. Perform awareness sessions to gain acceptance.

2. Risk Assessment (Months 3-5): Asset inventory, Threat/Vulnerability identification, Development of Risk Register. Categorize data and assign them to their respective owners.
3. Policy Development (months 4-6): Write information security policy, BYOD policy, acceptable use policy, incident response plan, and data retention policy. The policies should be aligned with ISO/IEC 27001 clauses.
4. Control Implementation (6-12 months): Deployment of technical controls (such as network segmentation and endpoint protection) and identity and access management (IAM) tools, along with cloud security posture management (CSPM) and security awareness training.
5. Assessment and Certification (months 9-14): Perform self-audits, fix any detected issues, and obtain certification (for example, ISO/IEC 27001 certification) if desired. Follow NIST RMF actions 4-6
6. Continuous Monitoring (Ongoing): SIEM implementation, vulnerability management, continuous control monitoring/process performance metrics. Continuous management reviews – updating the framework as threats and regulations evolve.

4.8 Additional Diagrams and Flowcharts

For further explanation, this section offers additional diagrams of pivotal processes and interactions in the NG-DSGCF.

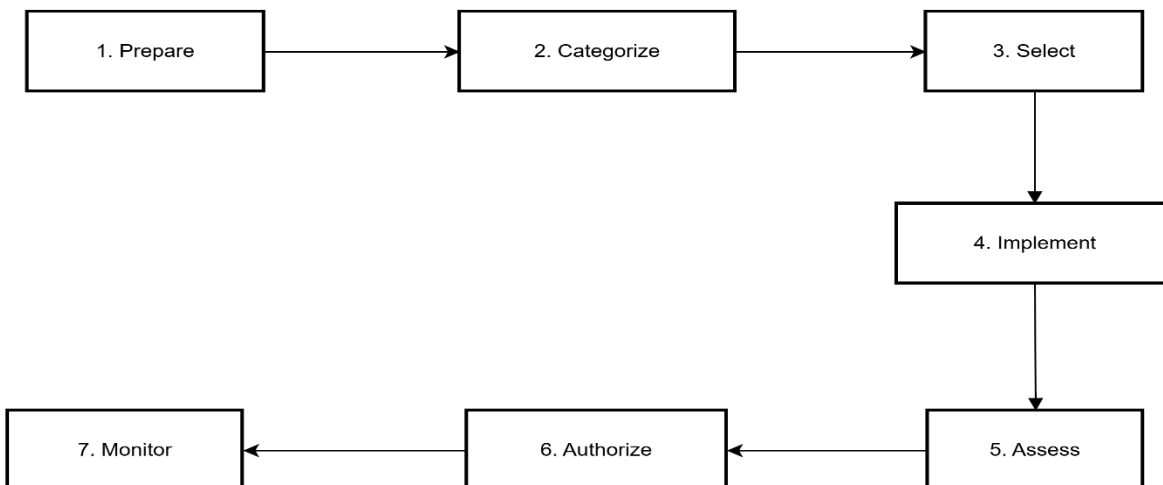


Figure 2 – NIST RMF Seven-Step Process.

The above flowchart represents the seven steps involved in the NIST Risk Management Framework, which include Prepare, Categorize, Select, Implement, Assess, Authorize, and Monitor. Every step in the flowchart leads to the other, highlighting the fact that the risk management process should be cyclical, involving steps such as preparing, selecting, and monitoring. For NG, the above process makes sure that the information systems are protected during their design, authorization, and subsequent maintenance [\[3\]](#).

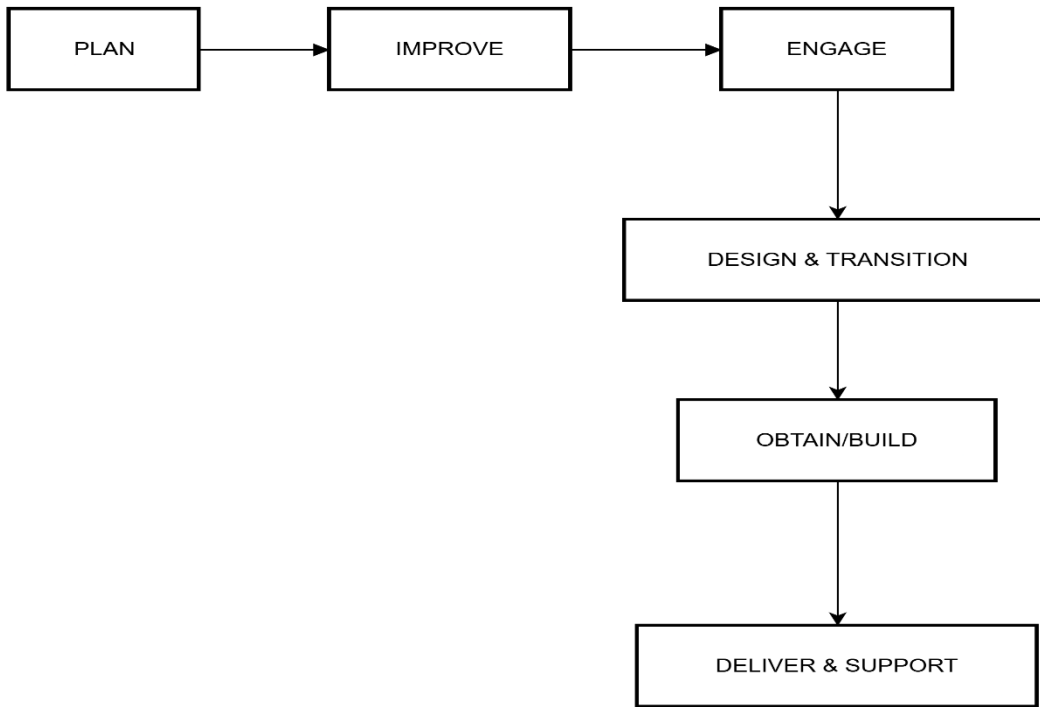


Figure 3 – ITIL 4 Service Value Chain

The ITIL service value chain comprises six activities—*Plan*, *Improve*, *Engage*, *Design & Transition*, *Obtain/Build* and *Deliver & Support*. These activities form a continuous loop that transforms demand into value. The diagram below shows the sequential nature of the value chain; in practice, the activities may be performed in different orders or concurrently. NG should leverage this model to coordinate IT service delivery and ensure alignment with business outcomes [7].

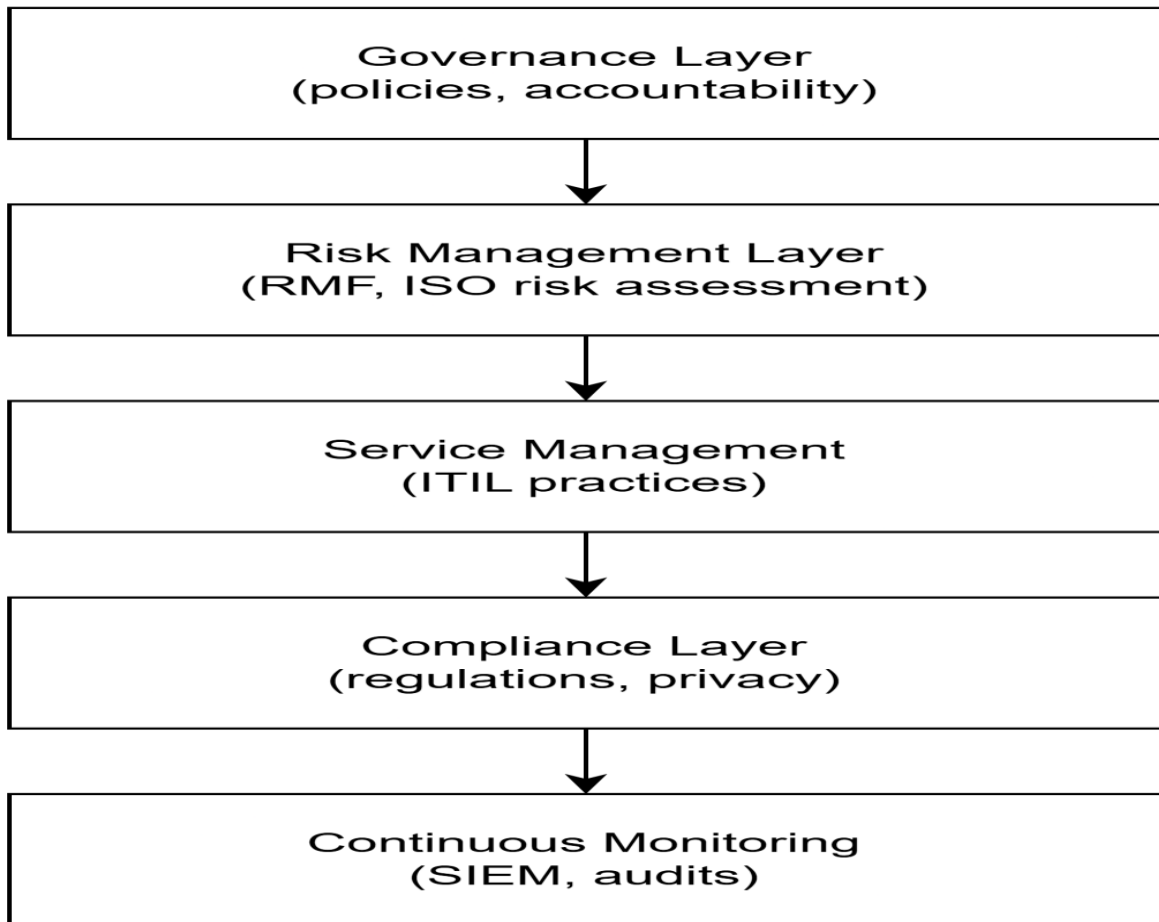


Figure 4 – NG-DSGCF Layered Framework

According to this figure, governance forms the top level and is responsible for defining policy. The risk management level implements both NIST RMF risk assessment and ISO risk assessment. The service level manages IT IL for change, incident, and service requests. The final level on the bottom is responsible for supporting all levels with continuous auditing. The bottom arrows show how information flows to all levels for purposes of continuous improvement [2], [4].

5 Discussion

5.1 Why Framework Integration Matters

The strength of combining various frameworks is to utilize their complementary capabilities. The NIST RMF offers a systematic risk management method and extensive controls catalog. The ISO/IEC 27001 gives emphasis to management systems and international best practices. The COBIT framework concentrates on governance, alignment, and performance. The ITIL framework offers operational effectiveness and service value. The blending effect offsets any weakness in individual frameworks and helps develop a comprehensive program for NG.

5.2. Importance of Continuous Improvement

Cyber threats rapidly evolve. The regulatory environment keeps changing. Hence, the role of continuous improvement is paramount. The key processes in the CSF and the PDCA Wheel embedded in the ISO/IEC 27001 standard facilitate reviews and improvements. CG Compliance emphasizes that sharing lessons learned and improving processes means that controls become effective against new risks continuously [4]. OSFI argues that the cybervariables and overall technology risks are constantly changing [2]. Hence, NG must assess risks and make new controls and training on a constant basis.

5.3 Addressing BYOD

BYOD adds unpredictability and widens the threat landscape. For the systematic review on managing risks associated with BYOD, one finds that risks are primarily of a technical nature (such as Malware), but that risk controls must be both organisational and technical in coverage [1]. Under these conditions, it becomes necessary for the NG to adopt BYOD policy. This policy should mandate registration, with necessary security software, encryption, and adherence to company policy. This work can be facilitated with MDM or ensure segmentation through containerization. Lastly, employee training is necessary regarding secure practices and privacy issues.

5.4 Limitations and Future Work

The proposed framework also demands investment. Small and medium-sized businesses might not have the ability to undertake all the measures; however,

focusing on high-risk areas and MSPs could help overcome such issues. Future developments might include the integration of emerging frameworks such as Zero Trust Architecture and the evaluation of the framework's efficacy through pilot projects.

6 Conclusion

NG finds itself operating within a high-risk environment, as it has a broad wireless and cloud infrastructure, as well as BYOD policy requirements. The lack of policies and governance infrastructure leaves NG vulnerable to cyber-attacks and legal actions. By combining various models including those from NIST, ISO/IEC 27000, COBIT 2019, and ITIL 4, the proposed framework for NG-DSGCF enables a structured framework that covers governance, risk management, control implementation, and service management. Through continuous improvement and upgrading, this framework ensures resilience to stay above any challenges that it may face after implementation and contribute to NG safeguarding its resources, meeting legal requirements, and securing services to both employees and clients.

References

[1]

C. G. Compliance, “Understanding the NIST Cybersecurity Framework: Importance and Implementation for Organizations.” CG Compliance, 2025. [Online]. Available: <https://info.cgcompliance.com/blog/understanding-the-nist-cybersecurity-framework-importance-and-implementation-for-organizations>

[2]

A. Anand, “ITIL 4 Explained: Framework, Practices and Key Changes.” ITSM.tools, 2025. [Online]. Available: <https://itsm.tools/itil-4-explained/>

[3]

and T. National Institute of Standards, “Risk Management Framework (RMF).” in Computer Security Resource Center. NIST, Gaithersburg, MD, USA, 2025. [Online]. Available: <https://csrc.nist.gov/projects/risk-management>

[4]

F. I. Office of the Superintendent of, “Technology and Cyber Risk Management,” Government of Canada, Ottawa, Canada, 2022. [Online]. Available: <https://www.osfi-bsif.gc.ca/en/guidance/guidance-library/technology-cyber-risk-management>

[5]

M. Staffans, “Bring Your Own Device Risk Management: A Systematic Review of Threats, Vulnerabilities and Mitigation Strategies,” University of Borås, Borås, Sweden, 2024.

[6]

ControlCase, “What is ISO/IEC 27001? A detailed, simple, and straightforward guide.” ControlCase, 2025. [Online]. Available: <https://www.controlcase.com/what-is-iso-27001/>

[7]

ISACA, “COBIT 2019 Framework: Governance and Management Objectives,” ISACA, Schaumburg, IL, USA, 2019. [Online]. Available: <https://www.isaca.org/resources/cobit>