

Abstract

In this research paper, I analyze information security, governance, and compliance complexities at NatureGreen and present my experience in building an integrated security strategy. With 95% of the network of this global organization being wireless-based and fully cloud-based, the risk of information security is extremely high. In addition, the pressure of BYOD for employees and customers, the protection of personal information, and the protection of billions of dollars of intellectual property-all of these made me deeply realize the need to rebuild an effective and realistic security framework.

In the first phase of research, I performed a comparative analysis of internationally acclaimed security frameworks like ITIL, the ISO 27000 series, and the NIST Cybersecurity Framework. Such a review gave me insight into developing a sound security foundation that combined policy-based governance, risk management, security controls, and compliance. Based on the knowledge gained, I designed a custom-fit security architecture, keeping in mind the real needs and technological environment of NatureGreen, where clear security policies, BYOD management, data protection, access control, contingency planning, and SLA development were given prominence.

In one of the pivotal parts of the report, I critically explained why it is important to regularly update the security standards in line with modern technologies, evolving threats, and legal regulations. It's actually this consistent updating that gives an organization its long-term stability, credibility, and digital resilience. Most importantly, this report reflects my personal research, analysis, and strategic vision to formulate a well-organized and sustainable security roadmap for NatureGreen.

Introduction

In this globalized digital era, the Internet has become an integral part of our everyday life and business activities. While the number of Internet users is growing rapidly, so, too, does the possibility of cyber attacks [1],[3]. With billions of active users who can start their attacks anytime and from anywhere, information asset protection becomes of greater significance. In my opinion, information security is not just a technical issue; it is a critical element of the stability, credibility, and long-term survival of any organization. This research, as part of the ACCA7028 module, is not only an academic assignment for me; it is also a valuable opportunity to apply knowledge and skills in solving real-life problems in cybersecurity [2].

At the heart of this report is NatureGreen, a popular global health product retailer whose business success is directly dependent on their technology management. Though nearly 95% of its network is wireless and most of its services are cloudbased, the level of possible threats from all directions has grown massively. From social media to e-commerce sites, though the company's digital presence is very strong everywhere, its internal security infrastructure is extremely patchy. More particularly, the BYOD policy is already at the company's doorstep due to the pressure of a large workforce and international customer demands [3]. I realized that while adopting a BYOD policy increases efficiency and flexibility, it also poses serious risks to the organization's intellectual property, employees' personal information, and customers' sensitive data.

What is really disturbing is that such a big organization does not have an established information security policy. Consequently, they are lagging behind in every section of risk management, governance, access control, and compliance. This chaotic environment obliged me to design an integrated security approach that would match the technical realities and business needs of the organization [4].

To this end, I have first conducted in-depth research on internationally recognized security frameworks such as the ISO 27000 series, ITIL, and NIST Cybersecurity Framework. After analyzing each framework's structure, strengths, limitations, and applicability, I found that one uniform solution would not be useful for NatureGreen; instead, what is required is a multi-dimensional security framework tailored according to their needs. In this report, I present such a customized framework that combines BYOD policy, security governance, legal compliance, data protection, risk management, and contingency planning. I also discuss the importance of regular updating of security policies and international standards to keep pace with rapidly changing technologies and threats.

Literature Review

While analyzing the chaotic information security environment of NG, I realized that any effective design needs a strong theoretical foundation. It is not possible to think about any practical strategy without a clear understanding of the integrated framework of these three areas: information security, governance, and compliance. The aim of my literature review is to select the best solution for

NatureGreen through a critical analysis of internationally recognized frameworks, standards, and guidelines [1],[3].

1. Information Security Governance

The first thing that became clear after the start of the research was the fact that the main problem of NatureGreen is not only technical, but deeply related to governance. Information security of an organization is effective only when leadership, strategy, and policy work in harmony. Standard & Poor's, NIST, and ISACA-all studies say the same thing: Governance is the foundation of security.

In this scenario, the COBIT framework appeared especially useful to me. The COBIT 2019 Governance and Management Objectives clearly indicate how an organization should align its business objectives, risks, and information security investments [2]. This would be crucial for NatureGreen-security has never been one of the strategic priorities in their decision-making process. COBIT's RACI chart, role-based accountability, and alignment to enterprise goals may contribute much value to NatureGreen's volatile organizational structure.

2. ISO/IEC 27000 Series: An International Standard

The most important focus during my research was directed at the ISO/IEC 27000 series, since it represents the most complete and globally accepted standard for ISMS. Therefore, the framework of ISO 27001 is highly relevant for NatureGreens, given its vast array of challenges such as BYOD, cloud security, personal data protection, and international compliance [5].

Why the ISO series is useful for NatureGreen: It works on a risk-based principle, which is very effective in the high-risk environment of cloud and wireless networks. These include the 114 security controls of ISO 27002, an all-encompassing security framework that can be applied to BYOD policies, access control, incident management, and physical security [4],[5].

ISO 27017 (Cloud Security) and ISO 27018 (Protection of PII in Cloud) are directly relevant to NatureGreen's cloud-based operations. What stands out most in my analysis is that the ISO series helps the organization build a "security culture," which is presently entirely missing at NatureGreen.

3. NIST Cybersecurity Framework: A Practical Model for Risk Management

The NIST Cybersecurity Framework, especially the sections of the IPDRR model, have been very useful to me because NatureGreen's BYOD and cloud environments are most vulnerable to identification and protection.

Probably, one of the more notable features of the NIST CSF is that it's an outcome-based framework. Rather than a listing of controls, it articulates what actually should be achieved.

In my studies, I find that the flexibility of NIST combined with the strict structure of ISO 27001 produces a robust hybrid framework that is practical and cost-efficient for an organization such as NatureGreen.

4. Information Technology Infrastructure Library : A Service Management Perspective

While ISO and NIST provide the framework for security, ITIL has shown me how to put this into operation effectively. Given that NatureGreen delivers their IT services through cloud services, ITIL's Service Design, Change Management, and Incident Management practices are particularly useful to them.

I realized that ITIL would help NatureGreen ensure “security embedded in services”—that is, security is not an afterthought, but built in from the start [6].

5. CIS Controls: Rapid and effective implementation

The 18 priority controls within the CIS Controls brought a practical view to my literature review. An implementation of IG1 by NatureGreen, in terms of baseline security controls, would have drastically reduced their current vulnerabilities.

It means, specifically:

- Asset Management
- Secure Configuration
- Access Control
- Continuous Vulnerability Management
- These controls are extremely important in a BYOD environment.

6. Synthesis: The Need for a Hybrid Framework Throughout this literature review, I came to realize that one single framework could not solve multifaceted problems at NatureGreen. The most realistic path would be to create a Hybrid Security Framework: the principles of ISO 27001, the risk management of NIST, the operational strength of ITIL, and the rapid priority-based controls of CIS Controls [5],[7].

Case Analysis

When I first analyzed the NatureGreen case, it became clear to me that this was not just a technical problem; it was a deep governance and policy crisis. Although NG is a global company that relies heavily on modern technology, cloud infrastructure, and wireless networks, their security architecture is in complete disarray [8]. In this chapter, I analyze the company's current situation, vulnerabilities, and risks, along with their security challenges from a structured research perspective.

1. NatureGreen's Current IT Environment: Modern but Risky

Therefore, one of the biggest features of NatureGreen's IT infrastructure is that about 95% of their network is deployed wirelessly. This level of wireless reliance permits high-speed work execution but simultaneously places the corporation in a high-vulnerability position because any wireless network, by its design, is more vulnerable. The unauthorized access to, eavesdropping on, and rogue access points constantly expose the network to various attacks.

On the other hand, the company operates entirely on cloud services, which, while ensuring scalability and cost-efficiency, brings along new kinds of risks. Specifically:

- Where the data resides (Data Residency)
- Data sovereignty
- Poor understanding of shared responsibility model with the cloud provider
- These are further complicating NG's security.

2. Lack of governance and policies: The gap at the heart of the problem

What comes out most clearly from my analysis is that there is no established security policy in NG. This is a huge omission in operations for an international organization like it [8,9].

The serious problems that arise from the lack of policies are:

- No clear guidelines on access control
- No incident response plan
- No data classification
- No Acceptable Use or BYOD policy

Because of this, employees are confused about what they can and can't do, and the data of the organization is in an unsafe state.

3. BYOD: Bring Your Own Device - risks outweigh the benefits.

The pressure of having employees and customers access systems from personal devices creates a major threat for NG. Three of the most important risks I identified in the analysis are:

1. Untested devices: It is very difficult to check on the installation of updates, antivirus, or security controls on personal devices.
2. Data leakage: If the device is lost or stolen, sensitive NG data could be leaked.
3. Data mixing: With personal and corporate data on the same device, segregation becomes impossible.

This is why BYOD is a high-risk zone unless governed by strict policy and MDM controls.

4. Intellectual Property Risk: NG's most valuable assets are at risk.

NatureGreen's products, formulae, research data, and IP are worth billions of dollars. Because of the current chaos in security:

Competitors may steal trade secrets.

Careless insiders may leak IP.

Any breach could permanently damage their global brand.

First and foremost, I think NG should implement a Zero-Trust architecture and strict access control in order to protect their IP.

5. Legal Compliance and Regulatory Risks

NG serves international customers; hence, it will be subject to several regional laws, including GDPR. But without a compliance framework, it faces:

- Huge financial penalties
- Lawsuits
- Brand damage
- These are risks that have been created.

6. Requirements Analysis: My Identified Essential Needs for NG

Based on my analysis, NatureGreen's essential needs are:

- Formal Security Governance Structure
- BYOD and Access Control Policy
- Cloud Security & Vendor Management Guideline
- Incident Response and Business Continuity Planning
- Compliance Framework (GDPR-aligned) Regular Audit and Vulnerability Assessment
Employee Security Awareness Program

Proposed Security Framework

While analyzing the present state of NatureGreen, I distinctly found that though the organization is technologically advanced, its security governance policies, risk management, and compliance activities are totally detached and disorderly [10]. For a global organization in which 95% of its networks are wireless, cloud-based infrastructure is used, and billions of customers use their platform daily, it is almost impossible to survive without a strong security framework. Keeping that reality in mind, an integrated, scalable, and future-ready security framework for NatureGreen has been devised.

I have built this framework upon seven key pillars, organized by combining best practices from ISO 27001, ISO 27005, the NIST Cybersecurity Framework, ITIL v4, and Zero Trust Architecture.

1. Security Governance and Leadership Framework

The first condition for NatureGreen's security progress is to establish a coherent governance framework. In this context, I have realized that when leadership is committed to security, only then can an organization be secure, risk-aware, and compliant on a long-term basis [10].

1.1 Information Security Governance & Compliance (ISGC) Committee

I believe a high-level ISGC committee should be established at NatureGreen.

The committee will comprise the following:

1. CEO/COO representative
2. CISO - to be appointed
3. IT Director
4. Legal Head
5. HR Director
6. Data Protection Officer (DPO)

Responsibilities:

1. Security strategy approval
2. Risk appetite determination
3. Budget allocation
4. Final approval of high-risk decisions
5. Compliance assurance for GDPR, ISO 27001, HIPAA, etc.

1.2 Creation of the position of Chief Information Security Officer - CISO

I believe that a highly-trained CISO is critical in managing security for an organization with a global span. He will lead everything from security strategy to technical implementation.

1.3 Three-Layer Governance Model (Board–Management–Operational)

I have proposed a three-layer governance model that applies to NatureGreen:

Board Level: Strategic decisions

Management Level: Policy and team management

LSI -Operational Level: day-to-day security implementation

This structure will provide the organization with a more agile, integrated, and accountable security framework.

2. Compliance & Ethical Data Handling

NatureGreen operates internationally, so compliance with various laws becomes a basic requirement. I have, therefore, put extra emphasis on building a strong compliance framework.

2.1 GDPR Compliance as an Integral Requirement

Since NatureGreen works extensively in Europe, I want to put GDPR at the heart of the security policy.

1. My proposed framework includes
2. Data Minimization
3. DPIA (Data Protection Impact Assessment)
4. Consent Management
5. Right to Erasure
6. 72-hour Breach Notification

2.2 Inclusion of other international laws

I will seek alignment with CCPA, APPI, and other regional laws that may apply [12].

2.3 Policy of Ethical Handling of Data

Besides following the rule of law, I believe that NatureGreen should develop an ethical data usage policy to gain the trust of customers.

3. Core Security Policy Development

One major weakness in NatureGreen is the policy vacuum. I have designed three basic policies that should provide a sound basis for organizational security.

3.1 BYOD Policy (Bring Your Own Device Policy)

The riskiest area for NatureGreen is BYOD. I propose:

1. Compulsory MDM/MAM
2. Device encryption
3. Remote corporate data wipe only
4. Strong authentication
5. Corporate-personal data separation

This will ensure that the security of the organization is tightened while employee independence is not hampered.

3.2 Data Classification & Handling Policy

I have proposed a four-tier security hierarchy:

1. Public
2. Internal
3. Confidential
4. Secret (IP protection layer)

Information at the Secret layer will be accessed on a need-to-know basis only. Each layer will have different rules of encryption, handling, and disposal.

3.3 Zero Trust Access Policy

Because of the wireless networks and dependency on clouds, I have made the Zero Trust Model compulsory.

Policy:

1. Never Trust
2. Re-verify every request
3. Least Privilege Access
4. Device posture check

4. Risk Management Framework

I have developed a cyclic risk management process based on ISO 27005 for NatureGreen.

4.1 Risk Identification

Risk assessment, every 6 months.

Key risks:

1. BYOD malware
2. Cloud misconfigurations
3. Wireless intrusion
4. Ransomware
5. IP theft
6. Insider threats

4.2 Risk Analysis (Likelihood × Impact)

Each risk will be scored, and a risk register will be developed.

4.3 Risk Treatment Options

1. Avoid
2. Mitigate
3. Transfer

4. Accept
5. The mitigation is obligatory in cases of high risk.

4.4 Risk Monitoring

Risk will be reassessed quarterly.

Technical Protection Controls

NatureGreen bases its cybersecurity on a defense-in-depth principle.

5.1 Network Security Controls

Next-Generation Firewall

IDS/IPS

Network Segmentation: Guest, Corporate, Server, IoT VLAN

WPA3-based Wireless Security

5.2 Data Security Controls

1. AES-256 Encryption at Rest
2. TLS 1.3 Encryption in Transit
3. DLP Solutions
4. TDE database

5.3 Endpoint Security

1. EDR deployment
2. Patch automation
3. Device Compliance Enforcement

5.4 Cloud Security Controls

1. CASB for access control
2. CSPM for configuration scanning
3. Data residency and sovereignty control
4. Shadow IT Monitoring

5.5 Identity & Access Management

1. MFA everywhere
2. SSO implementation
3. Privileged Access Management

4. Continuous authentication
5. Business Continuity & Disaster Recovery

6.1 Business Continuity Plan (BCP)

I have determined RTO and RPO through BIA.

Priority Weight:

1. E-commerce services
2. Customer information
3. Financial systems
4. Supply chain

6.2 Disaster Recovery Plan (DRP)

1. 3-2-1 Backup Model
2. Cloud-based Geo-Redundant DR
3. Biannual DR Drill

6.3 Incident Response Plan (IRP)

Incident Response Team will be:

1. IR Manager
2. Technical Analyst
3. Legal & Compliance Officer
4. Communication Lead

Five-phase IR:

1. Detection
2. Containment
3. Eradication
4. Recovery
5. Lessons Learned
6. Security Awareness & Training

Organizational security entirely depends on the awareness of people. I therefore propose a structured training model:

7.1 Required Training

1. Orientation Security Training
2. Annual Refresher Course
3. Advanced Role-Based Training

7.2 Continuous Awareness Strategy

1. Monthly security newsletter
2. Bi-weekly phishing simulation
3. Security posters
4. Gamified Security Quiz

7.3 Success Metrics

Phishing click rate Training completion rate Human-error-based incident reduction

Critical Discussion

While designing the security framework for NatureGreen, I came to realize that information security is basically a battleground where nothing stands still. In my mind, periodic revisions of Security Standards & Regulations are not the best practice but an essential condition to make an organization sustainable and secure [5], [9].

First, the rapid changes in technology have amply taught me that new risks simply cannot be solved with old standards. When I analyzed NatureGreen's environment where 95% of services are cloud and wireless I realized that legacy frameworks such as ISO 27001 would not be able to meet their needs. Modern technologies like IoT, AI-driven systems, and hybrid cloud architecture are growing at a rapid pace, and newly updated guidelines are surely needed for their secure management.

Secondly, the changing Cyber Threat Landscape is consistently pushing for new security rules. Attacks like WannaCry or SolarWinds are proof to me that attackers are strategically ahead; thus, our frameworks must also be constantly enhanced. New standards normally integrate lessons learnt from such attacks, therefore minimizing the chances of damage to the organization [3],[6].

Third, NatureGreen is obliged to be legally compliant, as it is an internationally operating company. I have noticed that changes and updates of the law directly influence the policies and security controls of the organization. If the standards are not updated, the organization will face legal risks, including financial penalties and reputational damage.

Yet, small organizations cannot afford frequent and costly updates. I thus believe that there is a need for a risk-based and scalable update model that will be compatible with the different capabilities of various organizations.

Conclusion

In this research, I have analyzed NatureGreen for existing security vulnerabilities and proposed a realistic, risk-aware, and international standard-based security framework. The company's reliance on the cloud, wireless infrastructure, and pressures of BYOD make it clear to me that the core problem isn't with the technology but with governance, policy, and awareness.

The framework I created includes six pillars: Zero Trust, Data Classification, BYOD Policy, Risk Management, Legal Compliance, and Cyber Awareness. These are designed in order to align with the organization's technology environment, the behavior of employees, and the organizational realities.

Implementation of such a framework should be done in a phase-by-phase manner, whereby the company can quickly address the most vulnerable areas and build up a mature security culture gradually. I strongly believe that information security is not about technology but a holistic combination of leadership, processes, policies, and people awareness. If NatureGreen embraces this holistic approach, then they will be able to establish themselves as a secure, compliant, and trusted organization.

References

1. (2012). [Rev. of *IT governance; an international guide to data security and ISO27001/ISO27002, 5th ed*]. *Reference and Research Book News*, 27(3).
2. (2015). [Rev. of *IT Governance: An International Guide to Data Security and ISO27001/ISO27002, 6th Edition*]. *ProtoView*, 2(40).
3. IBM: Cost of a Data Breach Report. (2021). *Computer Fraud & Security*, 2021(8), 4–4. [https://doi.org/10.1016/S1361-3723\(21\)00082-8](https://doi.org/10.1016/S1361-3723(21)00082-8)
4. Upton, J. (2022). The Human Factor in Data Security Breaches. *Pharmaceutical Executive*, 42(3), 12–12.
5. Meltzer, E. (2022). Digitized, Connected and Exposed. *Security Technology & Design*, 32(5), 26–29.
6. Kutty, P. (2022). Data Breaches In Healthcare Can Put Lives At Risk. *Business World (India)*.
7. Gurinaviciute, J. (2021). Is the Construction Industry the Next Big Cybercrime Target? *Contractor*, 66(5), 69.
8. von Solms, R., & van Niekerk, J. (2013). From information security to cyber security. *Computers & Security*, 38, 97–102. <https://doi.org/10.1016/j.cose.2013.04.004>
9. Skinner, S. S., Von Solms, R., van Niekerk, J., & Delport, P. M. J. (2025). Cultivating Cybersecurity Awareness Among Seafarers. *Procedia Computer Science*, 263, 242–249. <https://doi.org/10.1016/j.procs.2025.07.030>

10. Van Niekerk, J. F., & Von Solms, R. (2010). Information security culture: A management perspective. *Computers & Security*, 29(4), 476–486.
<https://doi.org/10.1016/j.cose.2009.10.005>
11. Leung, L. (2007). What's in ITIL Version 3? U.K.'s Office of Government Commerce latest guidelines for efficient IT service delivery. *Network World*.
12. Henderson, L. (2019). Compliance Disruptors: Big pharma compliance leaders discuss the strategic move to principles-based policies at their companies and the impact of other emerging forces influencing industry compliance practice, including data analytics and security and training approaches adaptable to new workplace dynamics. *Pharmaceutical Executive*, 39(7), 12.