

Data Security, Governance and Compliance Report - Mateusz Jadasz

by Mateusz Jadasz

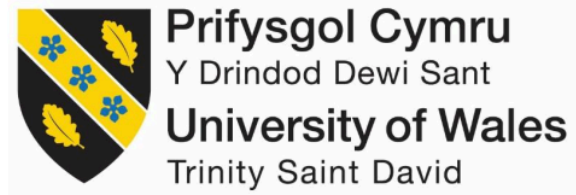
Submission date: 29-Dec-2024 01:28PM (UTC+0000)

Submission ID: 246925245

File name: 17845_Mateusz_Jadasz_Data_Security_Governance_and_Compliance_Report_-_Mateusz_Jadasz_634839_596355898.docx (150.42K)

Word count: 3194

Character count: 20636



NATUREGARDEN DATA SECURITY PRINCIPLES AND PRACTICES

by

Mateusz Jadasz

MSc Software Engineering and Artificial Intelligence

Data Security, Governance and Compliance

ACCA7028

Carlene Campbell

December 2024

TABLE OF CONTENTS

Table of Tables	3
Table of Figures	3
Abstract	4
Introduction.....	4
Problem Statement	4
Research and Security Frameworks.....	5
ISO/IEC 27001	5
NIST Cybersecurity Framework	5
COBIT	6
ITIL	7
CIS Controls.....	7
NatureGarden Solution.....	8
Compliance with Laws and Ethics.....	8
Governance and Strategic Planning for Security	8
Security Policies	8
Risk Management	8
Security Management Models and Practices	8
Contingency Planning	9
Protection Mechanisms	9
Service Level Agreement	9
Security Implementation Plan	9
Security Governance Model	9
Regulations and Standards	10
Adapting to Evolving Threats.....	10
Addressing Technological Advances	10
Legal and Ethical Compliance	10
Boosting Stakeholder Confidence.....	10
Encouraging Innovation.....	10
Critique of Constant Updates	10
Conclusion	10
References	12

TABLE OF TABLES

Table 1: Security Implementation Plan.....	9
--	---

TABLE OF FIGURES

Figure 1: Security Governance Model	9
---	---

ABSTRACT

This report explores the implementation and benefits of prominent cybersecurity frameworks such as CIS Controls, ITIL, ISO/IEC 27001, and the NIST Cybersecurity Framework in the context of NatureGarden's problem. By analysing key components and practices of these frameworks, the report highlights how they help organizations strengthen their cybersecurity posture, align IT operations with business objectives, and ensure regulatory compliance. Furthermore, through the analysis of each framework, this report holds the solution to NatureGarden's problem of allowing customers and employees access to their resources and network through personal devices. The report concludes by underscoring the necessity staying up to date with regulations and standards as well as the importance of integrating the frameworks into organizational strategies to build a secure and resilient IT environment in the face of evolving cyber threats.

INTRODUCTION

In the modern, digitally driven and dependant world, the significance of robust information security cannot be overstated. As a leader in the healthy living products sector with an extensive global presence, NatureGarden heavily relies on cloud-based IT services and wireless networks to support its staff and serve its vast amounts of clients. However, due to the demand to allow both employees and customers to use personal devices to access company resources, NatureGarden faces great challenges in safeguarding billions in sensitive data and intellectual property.

By exploring various security frameworks and models, this report aims to address NatureGarden's pressing data security, governance, and compliance needs. It will identify existing challenges in NatureGarden's security infrastructure and examine relevant frameworks, such as ISO/IEC 27001, NIST Cybersecurity Framework, and COBIT, to establish a foundation for best practices.

Furthermore, this report will also explore the importance of staying up to date with regulations and standards in an ever-changing and evolving threat landscape, ensuring NatureGarden can adapt to technological advancements, maintain legal compliance, and reinforce stakeholder confidence.

PROBLEM STATEMENT

NatureGarden is a globally recognized brand. They specialise in the sales of products that help maintain healthy living, however they face significant challenges related to the security of the data they possess. With almost 95% of their network relying on wireless infrastructure and an increasing demand to support access to the network and resources using personal devices, NatureGarden is exposed to a heightened risks of data breaches, intellectual property theft, and non-compliance with regulatory standards.

According to a journal article published in April 2024, a 2013 survey conducted by Clearswift in the UK, revealed that 42% of data breaches were orchestrated by outsiders, while 58% originated from insiders. This included third parties, as well as former and current employees [1]. With that in mind, it is very clear to see that anything and anyone could not only cause harm but can also be considered a vulnerability and thus it is imperative that NatureGarden does everything in their power to protect their assets, especially if they were to allow access to their network and resources through personal devices.

The absence of a formalized security policy worsens the vulnerabilities that may already be present, putting sensitive employee and client data, along with NatureGarden's intellectual assets, at risk. To ensure

operational resilience and to maintain trust, NatureGarden must implement a comprehensive information security framework that addresses governance, compliance, and risk management while safeguarding its technological infrastructure and global operations.

RESEARCH AND SECURITY FRAMEWORKS

In order for NatureGarden to facilitate the usage of personal devices for others to access their assets and network without compromising any aspect of the company and its data, it is important to assess the potential risks and threats as they necessitate a proactive and systematic approach to preventing them, or at the very least minimising the impact that a cyber-attack may have on the company. To do so, NatureGarden can enhance its information security by adopting established frameworks and models that provide structured approaches to managing and safeguarding data. One of the more obvious benefits of implementing a structured framework is that by following a framework's guidelines, NatureGarden can better protect their information assets against cyber threats and data breaches. Furthermore, a certification demonstrates a commitment to information security, enhancing trust among clients, partners, and other stakeholders.

ISO/IEC 27001

ISO/IEC 27001 is a widely recognized standard that provides a comprehensive framework for establishing, implementing, maintaining, and continually improving an information security management system. This standard enables organizations to systematically manage sensitive information, ensuring its confidentiality, integrity, and availability.

Some of the key components of this framework are:

- Risk Assessment and Treatment
- Leadership and Commitment
- Continual Improvement

This standard emphasizes a risk-based, systematic approach, requiring organizations to identify potential security risks, assessing them and implementing appropriate controls to mitigate them. Furthermore, the management's active involvement is crucial in establishing and maintaining an effective information security management system, ensuring alignment with the objectives of the organisation. The ISO/IEC 27001 also promotes an ongoing process of monitoring, reviewing, and enhancing the information security management system to adapt to evolving security threats and business needs. [2] [3] [4]

One benefit of this standard is that it provides regulatory compliance and adherence, as the ISO/IEC 27001 standard helps organizations meet legal and regulatory requirements related to information security, thereby avoiding potential penalties. This is especially important in NatureGarden's circumstances as they are a global firm. Another benefit is, it allows for an improved incident response as the ISO/IEC 27001 ensures that NatureGarden has a robust incident response plan, enabling swift and effective action during a security event.

NIST CYBERSECURITY FRAMEWORK

The NIST Cybersecurity Framework, developed by the National Institute of Standards and Technology, provides organizations with a structured approach to managing and mitigating cybersecurity risks. It is particularly beneficial for critical infrastructure sectors but is adaptable to various industries, such as that of NatureGarden.

Some of the key components of this framework are:

- Core Functions
- Implementation Tiers
- Profiles

At the core, the framework comprises of five functions: Identify, Protect, Detect, Respond, and Recover. These functions offer a high-level, strategic view of an organization's management of cybersecurity risk. The implementation tiers assist organizations like NatureGarden in understanding the degree to which their cybersecurity risk management practices exhibit the characteristics defined in the framework, for example if said practices are risk-informed, repeatable and adaptive. The framework profiles represent the alignment of the framework's core functions with the business requirements, risk tolerance, and resources of the organization. This alignment helps in identifying and prioritizing opportunities for improving NatureGarden's cybersecurity posture. [5]

One of the benefits of the NIST cybersecurity framework is that it addresses the entire lifecycle of cybersecurity, from risk identification to recovery, ensuring NatureGarden can adopt a holistic approach. Furthermore, it is scalable and applicable to organizations of all sizes and across a variety of industries, from small businesses to critical infrastructure sectors, this makes it perfect for a global organisation specialising in the healthy living products sector. Another benefit is that it facilitates regulatory compliance by aligning with many regulatory requirements such as GDPR, which would help NatureGarden demonstrate compliance.

COBIT

The Control Objectives for Information and Related Technologies, or COBIT, is a comprehensive framework developed by Information Systems Audit and Control Association for the governance and management of enterprise IT. It provides organizations with a set of best practices, tools, and guidance to ensure effective alignment between IT and business objectives.

Some of the key components of this framework are:

- Framework
- Process Descriptions
- Control Objectives
- Management Guidelines
- Maturity Models

The COBIT framework provides a comprehensive structure for IT governance by organizing objectives and aligning them with business requirements while promoting best practices across IT domains and processes. It also includes process descriptions that act as a standardized language within an organisation like NatureGarden, covering the planning, building, operation, and monitoring of IT processes. Additionally, control objectives offer a detailed set of requirements to ensure effective management and oversight of IT and business functions. Furthermore, management guidelines assist in clearly assigning responsibilities, setting performance metrics, aligning goals, and enhancing the integration of interrelated processes. Lastly, maturity models are used to evaluate the capability and development of each process, identifying and addressing any gaps. [6] [7] [8]

COBIT offers numerous benefits by providing a structured framework for IT governance and management. It ensures alignment between IT operations and business goals, enabling organizations to maximize value from their IT investments. Furthermore, the framework enhances risk management by identifying and addressing potential gaps in processes, promoting a proactive approach to security and compliance. COBIT also improves accountability and transparency within IT by establishing clear responsibilities and performance metrics.

Additionally, it facilitates better decision-making, optimizes resource utilization, and fosters integration across organizational processes, driving efficiency and strategic alignment.

ITIL

The information technology infrastructure library is a globally recognized framework for IT service management that provides best practices for delivering high-quality IT services aligned with business needs. ITIL offers a systematic approach to managing IT services across their lifecycle, emphasizing continuous improvement and customer satisfaction

Some of the key components of this framework are:

- Service Value System
- Guiding Principles
- Governance
- Service Value Chain
- Processes
- Continual Improvement

ITIL is a holistic framework that integrates key elements such as governance, practices, and continual improvement to deliver value, it ensures alignment between IT services and business goals. It also provides recommendations that lay a foundation for effective decision-making and behaviours, such as focusing on value, and progressing iteratively with feedback. Additionally, it establishes authority and accountability for policies and decision-making within an organization, and it is a flexible operating model consisting of six service value chain activities: Plan, Engage, Design and Transition, Obtain/Build, Deliver/Support, and Improve. Furthermore, it also consists of five processes: Service Strategy, Service Design, Service Transition, Service Operation, and Continual Service Improvement. The continual improvement process is a structured approach to identifying and implementing improvements in processes, services, and products to maintain alignment with organizational goals. [9] [10]

The ITIL framework provides numerous benefits, including improved service quality, better alignment of IT operations with business goals, and enhanced efficiency by optimizing processes and reducing redundancies. It helps organizations manage risks proactively, ensuring business continuity while fostering customer satisfaction through a customer-centric approach. ITIL supports compliance with international standards, facilitates continual improvement to adapt to changing needs, and fosters collaboration across teams with a common language. Additionally, it is scalable and flexible for organizations of any size, ensuring a higher return on IT investments by delivering cost-effective and reliable services.

CIS CONTROLS

The centre for internet security controls is a set of best practices designed to help organizations enhance their cybersecurity posture by focusing on key areas that effectively mitigate cyber threats. These controls are informed by real and past attack data and are regularly updated to address emerging threats.

Some of the key components of this framework are:

- Basic Controls
- Foundational Controls
- Organizational Controls

The CIS Controls consist of 18 prioritized guidelines designed to address key areas of cybersecurity. They are grouped into three Implementation Groups based on the organization's size, resources, and cybersecurity

maturity. The basic controls cover safeguards one through six. They are fundamental steps to establish a secure foundation, such as inventory and control of hardware/software, data protection, and vulnerability management. The foundational controls cover safeguards seven through sixteen and they are the best practices to build a robust cybersecurity infrastructure, including email and web browser protections, secure configuration for devices, account management, and malware defences. Finally, the organizational controls cover safeguards seventeen and eighteen and they focus on developing overarching policies and strategies, such as incident response and penetration testing, to strengthen organizational resilience. [11]

Implementing CIS Controls helps organizations enhance their cybersecurity posture by providing clear, prioritized, and actionable guidelines. These controls reduce the risk of cyberattacks by addressing the most critical vulnerabilities and focusing on real-world threats. They enable organizations to optimize resource allocation, and although they are particularly good for small and medium enterprises with limited budgets, they can be easily applied to global firms such as NatureGarden. CIS Controls also foster regulatory compliance, streamline incident response processes, and improve overall operational efficiency, thereby building trust among stakeholders and safeguarding sensitive data.

NATUREGARDEN SOLUTION

In order to provide access to the network and resources both to the employees and the customers, while meeting the needs of the company information system security, governance, and compliance, NatureGarden will need to implement the following approach to address the different the different areas of interest.

COMPLIANCE WITH LAWS AND ETHICS

- Implement ISO/IEC 27001 for information security management to ensure international compliance
- Adhere to the general data protection regulation for handling customer data
- Comply with local cybersecurity laws in regions of operation
- Develop an internal code of ethics to govern data usage and intellectual property

GOVERNANCE AND STRATEGIC PLANNING FOR SECURITY

- Establish a governance framework using COBIT to align IT objectives with business goals
- Form a security steering committee responsible for overseeing all security initiatives
- Develop a 3-year roadmap for security improvements with annual reviews

SECURITY POLICIES

- Define a bring your own device policy by implementing device enrolment and security configurations
- Establish an acceptable use policy to set clear guidelines for using company resources
- Develop a data protection policy to ensure confidentiality, integrity, and availability of sensitive data

RISK MANAGEMENT

- Conduct periodic risk assessments using the NIST framework
- Maintain a risk register to track identified risks and their mitigation strategies
- Apply centre for internet controls for prioritized implementation of security measures

SECURITY MANAGEMENT MODELS AND PRACTICES

- Use ITIL Practices to manage IT services and incidents efficiently
- Adopt a zero-trust security policy for better control over access to resources

- Implement identity and access management systems for user authentication and authorization

CONTINGENCY PLANNING

- Develop a business continuity plan and include disaster recovery procedures as well as alternate operational plans
- Establish an incident response plan to define roles, responsibilities, and actions during a breach
- Conduct regular tabletop exercises to test contingency plans

PROTECTION MECHANISMS

- Deploy enterprise-level encryption for sensitive data at rest and in transit
- Implement endpoint protection solutions to secure personal and corporate devices
- Use firewalls, intrusion detection/prevention systems, and network segmentation
- Establish a secure VPN for remote access

SERVICE LEVEL AGREEMENT

- Define clear service level agreements with cloud service providers, ensuring uptime guarantees, incident response times, and data recovery measures
- Conduct regular service level agreement reviews to align with evolving business needs

SECURITY IMPLEMENTATION PLAN

Phase	Key Activities	Timeline
Planning	Governance setup, risk assessment, policy development	0-6 months
Implementation	Deploy IAM, endpoint protection, and data encryption	6-18 months
Testing and Training	Simulate incidents, train staff on policies	18-24 months
Continuous Improvement	Annual reviews, updates to policies, risk reassessments	Ongoing

Table 1: Security Implementation Plan

SECURITY GOVERNANCE MODEL



Figure 1: Security Governance Model

REGULATIONS AND STANDARDS

ADAPTING TO EVOLVING THREATS

Cybersecurity threats are constantly evolving, with attackers employing new techniques. Regular updates to regulations ensure that organizations stay resilient against emerging risks, such as:

- Advanced Persistent Threats
- Ransomware and phishing schemes
- IoT vulnerabilities

ADDRESSING TECHNOLOGICAL ADVANCES

New technologies like cloud computing, AI, and blockchain introduce both opportunities and vulnerabilities. Updated standards reflect best practices for securely adopting these technologies.

LEGAL AND ETHICAL COMPLIANCE

As laws like GDPR evolve, organizations must adapt to avoid penalties and reputational damage. Staying updated ensures:

- Ethical handling of data
- Transparent practices with customers and regulators

BOOSTING STAKEHOLDER CONFIDENCE

Clients, employees, and partners are more likely to trust an organization that complies with current regulations and follows industry best practices. This can:

- Enhance brand reputation
- Improve customer retention

ENCOURAGING INNOVATION

Updated standards drive innovation by promoting new security practices. For example:

- Adoption of Zero Trust architectures
- Implementation of AI-driven threat detection

CRITIQUE OF CONSTANT UPDATES

While frequent updates are necessary, they pose challenges:

- Cost: Upgrading systems to meet new standards can be expensive.
- Complexity: Implementing changes across global operations may disrupt workflows.
- Training: Regular staff training is essential but time-consuming.

CONCLUSION

In conclusion, adopting robust security frameworks like COBIT, CIS Controls, ITIL, ISO/IEC 27001, and the NIST Cybersecurity Framework is critical for organizations to safeguard their assets, ensure compliance, and align IT practices with business objectives. Each framework offers unique benefits, from improving operational efficiency and risk management to fostering continual improvement and regulatory adherence. Implementing

these frameworks not only mitigates vulnerabilities but also enhances customer trust and organizational resilience. By tailoring these best practices to their specific needs, NatureGarden can build a secure, scalable, and sustainable IT environment to address the ever-evolving challenges of cybersecurity while allowing both customers and its employees to access NatureGarden's network and resources with minimal risk to the company. It is important to realise also that no company or network will ever be 100% secure, as there will always be a risk of a potential breach, however it is definitely possible to mitigate the chances of a data breach happening, or at the very least, minimising the impact of a data breach.

REFERENCES

- [1] D. Molitor, A. Saharia, V. Raghupathi and W. Raghupathi, "Exploring the Characteristics of Data Breaches: A Descriptive Analytic Study," *Journal of Information Security*, vol. 15, no. 2, pp. 168-195, 2024.
- [2] G. Culot, G. Nassimbeni, M. Podrecca and M. Sartor, "The ISO/IEC 27001 information security management standard: literature review and theory-based research agenda," *The TQM Journal*, vol. 33, no. 7, pp. 76-105, 2021.
- [3] E. Humphreys, *Implementing the ISO/IEC 27001 Information Security Management System Standard*, Artech House Publishers, 2007.
- [4] A. Calder, *ISO 27001/ISO 27002: A guide to information security management*, IT Governance Publishing, 2023.
- [5] National Institute of Standards and Technology, "The NIST Cybersecurity Framework (CSF) 2.0," U.S. Department of Commerce, Gaithersburg, Maryland, 2024.
- [6] C. Kidd, "What is COBIT? COBIT Explained," BMC, 6 December 2024. [Online]. Available: <https://www.bmc.com/blogs/cobit/#:~:text=COBIT%20components%20include%3A,Process%20descriptions..> [Accessed 11 December 2024].
- [7] Cyber Talents, "Understanding COBIT Framework: Definition, Components, and Benefits," Cyber Talents, [Online]. Available: <https://cybertalents.com/blog/understanding-cobit-framework-definition-components-and-benefits>. [Accessed 11 December 2024].
- [8] M. T. Edmead, "Using COBIT 2019 to Plan and Execute an Organization's Transformation Strategy," ISACA, 28 September 2020. [Online]. Available: <https://www.isaca.org/resources/news-and-trends/industry-news/2020/using-cobit-2019-to-plan-and-execute-an-organization-transformation-strategy>. [Accessed 11 December 2024].
- [9] C. Agutter, *ITIL Foundation Essentials ITIL 4 Edition: The ultimate revision guide*, IT Governance Publishing, 2020.
- [10] M. Marrone and L. Kolbe, "Impact of IT Service Management Frameworks on the IT Organization An Empirical Study on Benefits, Challenges, and Processes," *Business & Information Systems Engineering*, vol. 3, no. 1, pp. 5-18, 2011.
- [11] Center for Internet Security, "CIS Critical Security Controls Version 8.1," May 2021. [Online]. Available: <https://learn.cisecurity.org/cis-controls-download>. [Accessed 12 December 2024].

Data Security, Governance and Compliance Report - Mateusz Jadasz

GRADEMARK REPORT

FINAL GRADE

GENERAL COMMENTS

76/100

PAGE 1

PAGE 2

PAGE 3

PAGE 4

PAGE 5

PAGE 6

PAGE 7

PAGE 8

PAGE 9

PAGE 10

PAGE 11

PAGE 12

GRADING FORM: L7 DSGC (ACCA7028)

ENGAGEMENT WITH LITERATURE

Your work must include articles published by peer reviewed journals, conference proceedings, books, and related website (e.g. IEEE, ACM, Science direct). Information from website such as ehow, wiki, forums, etc. will not be accepted (15 marks)



You have provided a reference list, appropriate referencing. Also you have engaged with peer reviewed articles, which are credible sources but more updated ones could be used.

12

You are awarded marks based on:
awarded for:

- Diversity of sources and materials used
- Key concepts discussed
- Appropriate summaries of articles and level of critical appraisal of literature
- Application of appropriate referencing conventions

KNOWLEDGE AND UNDERSTANDING

Your work must demonstrate understanding of concepts and underlying principles. You should explain and analysis the chosen area in a meaningful way. (15 marks)



You have demonstrated specialised area of knowledge. Understanding of the concepts of the subject informed by current research. Critical

13

awareness of current problems and insights.

You are awarded marks based on:

- Depth of the research
- Strength of the statements
- Structure of the paper
- Quality of the report

COGNITIVE AND INTELLECTUAL

Your work must demonstrate critical analysis and evaluation of your approach for security framework and model. Your work must also justify your findings and provide evidences. (40 marks)



Sound critical evaluation/ critique of current research and methodologies, Proposes new hypotheses, where appropriate.

Marks are awarded based on:

critical analysis and evaluation of your approach for security framework and model.

How you justify your findings and provide evidences.

32

PRACTICAL SKILLS

Marks will be awarded based on the quality of and level of detail provided for the design approach; diagrams, table, charts and any other design methods utilise will enhance marks. (20 marks)



You have provided a relevant appropriate table and a security model diagrams. More tables and diagrams could be used to aid your own approach.

Marks are awarded based on the quality of and level of detail provided for the design approach;

12

diagrams, table, charts and any other design methods utilise will enhance marks.

TRANSFERABLE SKILLS FOR LIFE

This should be presented in an academic way and therefore must include an abstract, an introduction, a conclusion and a list of references. (10 marks)



A presentable work but could do with some formatting alignment. All acronyms to spell out first time used.

6.5