



Prifysgol Cymru
Y Drindod Dewi Sant
University of Wales
Trinity Saint David

Data Security, Governance and Compliance

ACCA7028 Assessment Report

Student Name: Muhammad Waleed

Student ID: 2430361

Program: MSc Cybersecurity & Digital Forensics

Submission To: Dr Dipo Dunsin

Abstract

This report explores the information security challenges faced by NatureGreen (NG), a global health and wellness company. NG depends heavily on wireless networking for around 95% of its operations and makes extensive use of cloud services. In the absence of formal security policies and controls, employee data, customer information, and valuable intellectual property are exposed to significant risk.

The report reviews recognised security frameworks and models, including ITIL, ISO/IEC 27001, NIST-Cybersecurity Framework and COBIT, in order to identify good practice for data protection and risk management. Drawing on this research, a tailored security approach is proposed for NatureGreen(NG) that covers governance, compliance, risk management, protection mechanisms, incident response and business continuity.

The findings show that aligning with established security frameworks not only helps to protect sensitive information but also supports wider business objectives such as trust, resilience and regulatory compliance. The report also emphasises the importance of regularly updating security standards to reflect new technologies, emerging threats and evolving legal requirements.

Table of Contents

1. Introduction.....	1
1.1 Overview of NatureGreen (NG).....	1
1.2 Business Challenges and Security Concern	1
1.3 Aim and Objectives of the Report	1
1.4 Scope and Structure.....	1
2. Literature Review – Security Frameworks and Models.....	2
2.1 Overview of Information Security Governance	2
2.2 ISO/IEC 27000 Family (ISO 27001, 27002, 27005).....	2
2.3 NIST Cybersecurity Framework (CSF).....	3
2.5 Comparative Analysis of Frameworks.....	4
3. Analysis of NatureGreen’s Current Environment	5
3.1 ICT Infrastructure: Cloud, Wireless, and BYOD.....	5
3.2 Key Assets and Identified Risks.....	6
3.3 Gaps in Governance, Policy, and Compliance.....	6
4. Proposed Information Security Governance Approach for NG	6
4.1 Governance Structure and Strategic Planning	6
4.2 Security Policy Framework (BYOD, Wireless, Cloud, Data Protection).....	7
4.4 Compliance, Laws, and Ethical Considerations	8
4.5 Contingency Planning and Service Level Agreements (SLAs)	8
5. Discussion and Critical Analysis.....	8
5.1 Importance of Regularly Updating Security Regulations and Standards.....	8
5.2 Benefits and Challenges of Implementing Frameworks.....	9
5.3 Continuous Improvement and Monitoring	9
6. Conclusion and Recommendations	10
References	10

1. Introduction

1.1 Overview of NatureGreen (NG)

NatureGreen (NG) is a global company that promotes healthy living through a wide range of health and wellness products. It operates in multiple regions and has a strong online and social media presence to reach customers and promote its brand. To support its day-to-day activities, NG relies heavily on digital technologies, including cloud-based services and a largely wireless network infrastructure used by staff and customers.

1.2 Business Challenges and Security Concern

Although NG is technologically advanced, its rapid growth has created major security challenges. Around 95% of its network traffic is wireless, and the organisation allows staff and sometimes customers to access services using personal devices (BYOD). At the same time, NG holds sensitive employee records, customer data and valuable intellectual property. Without formal policies, clear governance or defined controls, these assets face increased risks such as data breaches, unauthorised access, disruption and regulatory non-compliance. Consequently, NG must adopt a well-structured, long-term information security strategy that is aligned with recognised standards, including ISO/IEC 27001 and the NIST Cybersecurity Framework [1][4][6].

1.3 Aim and Objectives of the Report

The aim of this report is to explore how recognised security frameworks and models can be used to improve NatureGreen's information security governance and compliance. The main objectives are to:

- review relevant security frameworks and models, including ISO/IEC 27001, the NIST Cybersecurity Framework, COBIT and ITIL;
- identify how these frameworks can help address NG's specific challenges around wireless networks, cloud services and BYOD;
- propose a tailored security approach for NG that strengthens governance, compliance, risk management and data protection;
- highlight the role of ongoing improvement and regular updates to security practices.

1.4 Scope and Structure

The scope of this report is limited to information security governance, risk management and compliance for NatureGreen's digital environment, with a focus on cloud services, wireless

networking and BYOD. Technical implementation details are discussed only at a high level where relevant to governance and policy.

The report is structured as follows: Section 2 reviews key security frameworks and models and explains their relevance to NG. Section 3 analyses NG's current environment and outlines a recommended security governance and compliance approach. Section 4 provides a critical discussion of the need to keep security regulations and standards up to date. Section 5 concludes the report and presents the main recommendations.

2. Literature Review – Security Frameworks and Models

2.1 Overview of Information Security Governance

Information security governance is the set of responsibilities and practices that ensure information security supports the organisation's overall goals. It focuses on direction, control and accountability, rather than just day-to-day technical controls. Good governance makes sure that security is not treated as a purely technical issue but as a business risk that needs leadership attention.

Key elements of security governance include clear roles and responsibilities, defined policies and standards, risk management processes, monitoring and reporting, and alignment with legal and regulatory requirements. For a company like NatureGreen, security governance provides a structured way to protect sensitive data, support trust with customers and partners, and ensure that investment in security is linked to business priorities, as reflected in standards such as ISO/IEC 27001 and related guidance [1][2].

2.2 ISO/IEC 27000 Family (ISO 27001, 27002, 27005)

The ISO/IEC 27000 family is a well-known set of standards that deal with managing information security. Together, they provide an organised approach for setting up, operating, maintaining, and continually improving an Information Security Management System (ISMS) [1][2].

- **ISO/IEC 27001** defines what an ISMS must include. It describes the management activities needed to recognise risks, choose appropriate controls, and track how well those controls are working. It is also the benchmark used when organisations seek formal certification [1].
- **ISO/IEC 27002** serves as a detailed guideline for information security controls. It lists a wide range of control measures covering areas such as access control, cryptography, physical and operational security, supplier management, and incident handling [2].
- **ISO/IEC 27005** concentrates on risk management in the context of information security. It explains how to identify assets, threats, and vulnerabilities, evaluate the resulting risks, and choose suitable risk-treatment options that support compliance with ISO/IEC 27001 [3].

For NatureGreen, the ISO 27000 family offers a structured and internationally accepted way to manage security. It would help NG define policies, identify risks related to wireless networks, cloud services and BYOD, and implement controls in a consistent and auditable manner [1][3].

2.3 NIST Cybersecurity Framework (CSF)

The NIST Cybersecurity Framework (CSF) provides a flexible, risk-based approach to managing cyber security [4]. It is organised around five core functions: **Identify, Protect, Detect, Respond and Recover**, which describe high-level outcomes that organisations should aim to achieve.

- **Identify** focuses on understanding assets, business environment, governance and risk.
- **Protect** covers safeguards such as access control, awareness training and data security.
- **Detect** deals with monitoring and discovering anomalous events or potential incidents.
- **Respond** covers incident handling, communication and mitigation activities.
- **Recover** focuses on restoring services and improving resilience after an incident [4].

The NIST CSF is designed to be adaptable to different sectors and sizes of organisation and can be mapped to other standards such as ISO/IEC 27001 [4]. For NatureGreen, the framework can provide a clear, high-level roadmap for improving cyber security, particularly around identifying critical assets, protecting cloud and wireless environments, and preparing for detection and response to incidents.

2.4 Information Technology Infrastructure Library (ITIL)

ITIL is a widely adopted framework for managing IT services across their lifecycle. Although it is not a security-specific standard, it includes many practices that support information security, especially in areas such as change management, incident management and service continuity [5].

In ITIL 4, security is treated as an integral aspect of service value rather than a separate activity. Security requirements are considered when designing, transitioning and operating services. For example, change management processes can ensure that security risks are assessed before new systems or configurations are introduced, and incident management can be aligned with security incident handling to provide clear escalation paths and communication channels [5].

For NatureGreen, ITIL can help ensure that security is built into everyday IT processes. When combined with security-focused frameworks like ISO/IEC 27001 and the NIST CSF, ITIL supports consistent implementation of controls, better handling of security incidents and improved coordination between IT operations and security governance.

2.5 Comparative Analysis of Frameworks

Each framework brings different strengths, and they are often used together rather than in isolation. ISO/IEC 27001, 27002 and 27005 provide a formal, certifiable structure for an ISMS, with a strong focus on risk management and documented controls [1]–[3]. This is valuable for demonstrating compliance and maturity, especially in a global organisation. The NIST CSF offers a clear, high-level model that is easy to communicate to management, using its five core functions as a straightforward way to discuss current capabilities and target improvements [4]. ITIL, meanwhile, supports the operational side, ensuring that security is embedded in IT service delivery, change management and incident response [5].

For NatureGreen, ISO/IEC 27001 can form the backbone of security governance and policy, NIST CSF can provide a practical lens for assessing current and target security posture, and ITIL can ensure that security processes are integrated into day-to-day IT operations. Used together, these frameworks can help NG move from an informal, reactive approach to a more structured, proactive and business-aligned security model.

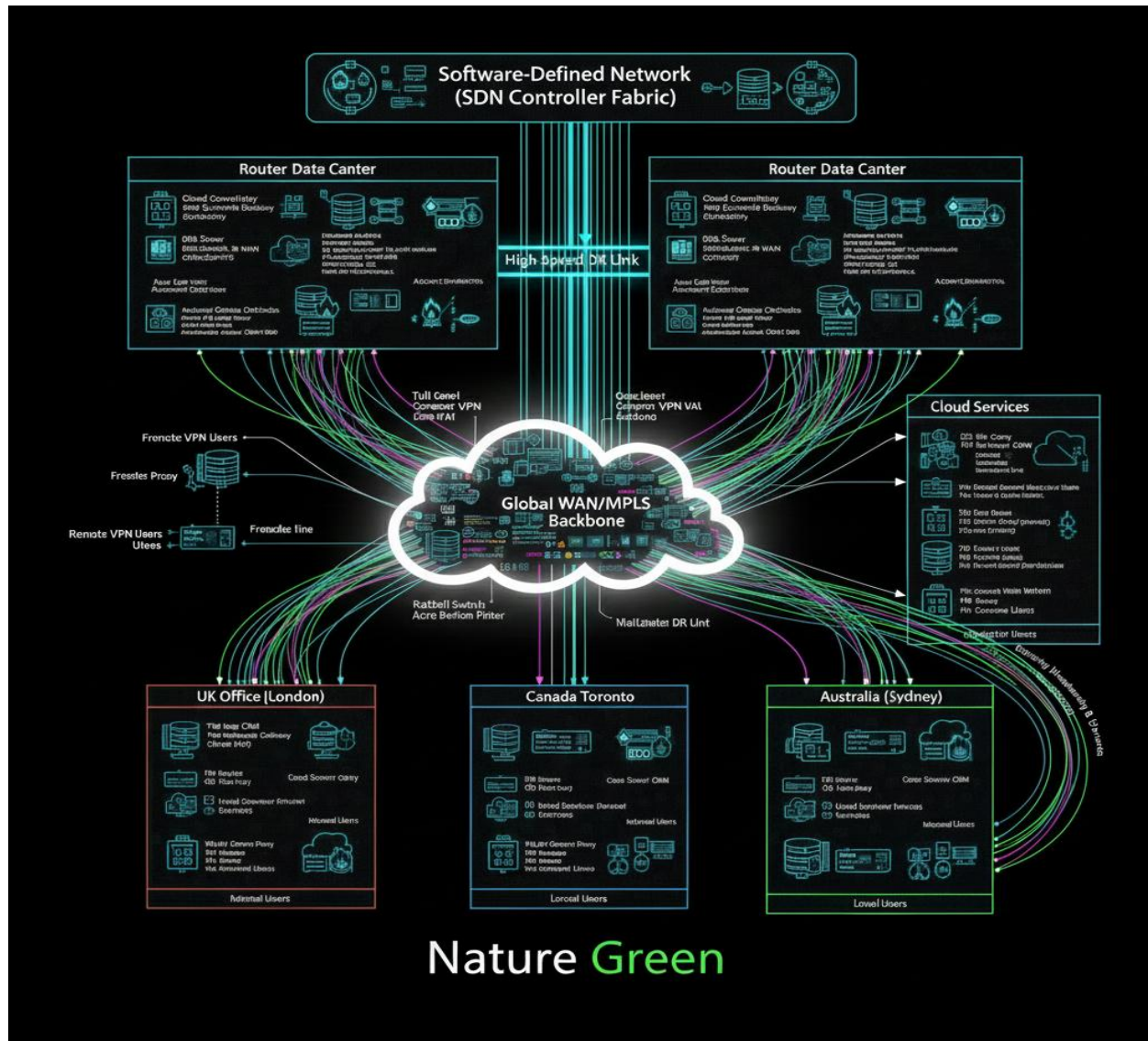


Figure 1

3. Analysis of NatureGreen's Current Environment

3.1 ICT Infrastructure: Cloud, Wireless, and BYOD

NatureGreen relies heavily on digital services, with about 95% of internal traffic running over Wi-Fi as staff use laptops, tablets and phones to access corporate systems. This gives flexibility but also expands the attack surface if wireless settings, access control or encryption are weak. NG also depends on cloud services for email, storage, collaboration and customer platforms, where misconfiguration or poor identity management can still cause data exposure or disruption without a structured framework such as ISO/IEC 27001 or the NIST Cybersecurity Framework [1], [4]. In addition, widespread BYOD means personal devices connect to company resources;

without mobile device management, strong authentication and network segmentation, it is difficult to ensure only trusted, up-to-date devices reach sensitive services [1], [3], [4].

3.2 Key Assets and Identified Risks

To understand NG's security posture, it is useful to identify its key information assets and the main risks they face. Important assets include customer data (personal and contact details, purchase history and possible health-related preferences), employee data (HR, payroll and internal records), intellectual property (product formulas, research and marketing plans), operational systems and cloud services (ordering, logistics, support, finance), and NG's reputation and online presence.

These assets are exposed to threats such as unauthorised access, accidental disclosure, phishing and credential theft, which can lead to privacy breaches, regulatory penalties and financial loss. Intellectual property is at risk from insider threats, compromised accounts and insecure cloud storage, while wireless and BYOD use increase the chances of device compromise, eavesdropping and rogue access points. Because NG depends heavily on cloud and online services, outages or denial-of-service attacks could also disrupt operations. Without a structured risk management process such as that described in ISO/IEC 27005, these risks may not be identified, assessed or treated in a consistent way [3].

3.3 Gaps in Governance, Policy, and Compliance

The scenario shows that NG has no established security policy and that "everything is in disarray", indicating major gaps in information security governance. There is no formal Information Security Management System (ISMS), no defined roles such as a security officer or governance board, and no documented processes for managing security risk in line with recognised standards [1][2][4]. At policy level, NG lacks clear rules for BYOD, wireless access, passwords, data classification, acceptable use and third-party cloud services, as well as formal procedures for incident response, business continuity and disaster recovery, which are key parts of ISO/IEC 27001, NIST CSF and ITIL [1][4][5].

Without structured governance, NG cannot easily show compliance with data protection and privacy laws, and supplier relationships are not managed from a security perspective. As a result, risks are handled in an ad-hoc way. NG needs to adopt a recognised governance framework, define policies, clarify responsibilities and embed security into daily processes.

4. Proposed Information Security Governance Approach for NG

4.1 Governance Structure and Strategic Planning

NatureGreen (NG) needs a formal information security governance structure instead of its current informal approach. An Information Security Steering Committee, reporting to senior management and including key functions such as IT, legal, HR and operations, should set

priorities, approve policies and review major risks [1][4]. A Chief Information Security Officer (CISO) should lead the implementation of an ISO/IEC 27001-based Information Security Management System (ISMS) and coordinate risk assessments, training, incidents and compliance [1]. Security planning should be linked to business goals such as protecting intellectual property, customer trust, BYOD and cloud usage, using ISO/IEC 27001's continuous improvement cycle and the NIST Cybersecurity Framework's "Identify–Protect–Detect–Respond–Recover" structure as a guide [1][4].

4.2 Security Policy Framework (BYOD, Wireless, Cloud, Data Protection)

NG should introduce a formal security policy framework, approved by management and clearly communicated to all staff. A top-level information security policy should be supported by focused sub-policies, using ISO/IEC 27002 as a guide for topics and controls [2]. Key policies for NG include:

- **BYOD Policy** – which personal devices are allowed, minimum security settings (PIN/biometric, encryption, updates) and rules for separating personal and company data.
- **Wireless Security Policy** – secure Wi-Fi configuration, strong encryption, separation of guest and corporate networks, and regular reviews for misconfigurations or rogue access points.
- **Cloud Usage Policy** – how cloud services are approved and monitored, including identity and access management, data location, backup, logging, encryption and restrictions on "shadow IT".
- **Data Protection and Classification Policy** – how information is classified (e.g. public, internal, confidential) and handled, including storage, sharing, retention and disposal of customer, employee and IP data, in line with legal requirements.

These policies should be backed by procedures, staff awareness training and technical controls such as endpoint protection, access management and secure network configuration [1][2][4].

4.3 Risk Management and Protection Mechanisms

NG needs a clear risk management process to understand and control threats, following ISO/IEC 27005 to identify assets, threats and vulnerabilities, assess likelihood and impact, and choose appropriate controls, especially for wireless, BYOD, cloud and third-party services [3].

To treat these risks, NG should use a mix of measures mapped to ISO/IEC 27002 and the "Protect" and "Detect" functions in NIST CSF [2][4], including: strong access and identity management, network segmentation and secure Wi-Fi, endpoint protection on corporate and personal devices, logging and monitoring of key systems, and regular security awareness training.

4.4 Compliance, Laws, and Ethical Considerations

NG operates internationally and must meet data protection and privacy laws in all regions where it works. Its governance model should therefore include a compliance role that works with the security team to interpret legal and contractual requirements and turn them into policies, controls and supplier SLAs, in line with ISO/IEC 27001 [1]. At the same time, NG should go beyond minimum legal duties by handling data in a transparent and fair way, clearly informing staff and customers how their information is used and protected, and promoting a culture where everyone shares responsibility for safeguarding information.

4.5 Contingency Planning and Service Level Agreements (SLAs)

Given NG's reliance on wireless networking, cloud services and online channels, contingency planning is essential. The governance framework should include documented **incident response**, **business continuity** and **disaster recovery** plans, aligned with ISO/IEC 27001, the NIST Cybersecurity Framework and ITIL service continuity guidance [1][4][5]. Incident response plans should define how incidents are detected, escalated, handled and reviewed. Business continuity and disaster recovery plans should identify critical processes and systems, set recovery objectives, and ensure that data is backed up, tested and recoverable if primary services fail.

These plans must be supported by clear **Service Level Agreements (SLAs)** with cloud, network and other key suppliers. SLAs should specify availability targets, support times, security and data protection obligations, and responsibilities during incidents, including conditions for reporting, audit and termination. Aligning SLAs with NG's risk appetite and continuity requirements helps ensure that external providers do not weaken its overall security governance.

5. Discussion and Critical Analysis

5.1 Importance of Regularly Updating Security Regulations and Standards

Cyber security is not static. New attack methods, technologies and business models appear constantly, so regulations and standards that never change quickly become outdated. Studies show that organisations are increasingly adopting and updating formal frameworks because of the growth in cyber-attacks and regulatory expectations [6][8][11]. For a company like NatureGreen, which relies heavily on wireless networking, cloud services and BYOD, depending on old standards or informal practices would leave major risks unmanaged.

International standards are revised to reflect new threats and technologies. Recent updates to ISO/IEC 27001 and the NIST Cybersecurity Framework give more attention to cloud security, governance and integration with wider risk management [1][4][6]. Using current versions helps organisations follow good practice and stay aligned with what regulators and auditors expect.

For NatureGreen, regularly reviewing and updating its policies and controls against these standards is therefore essential. Treating security frameworks as living documents supports compliance, resilience and long-term trust [6][8][11].

5.2 Benefits and Challenges of Implementing Frameworks

Implementing security frameworks such as ISO/IEC 27001, NIST CSF, COBIT and ITIL can reduce security incidents, improve visibility of risks and support better decisions [4][6]. They give a common language for security and governance, helping technical staff and business leaders communicate about priorities. Using recognised standards also saves time and cost by reducing ad-hoc approaches and duplication of effort [6][16].

From a compliance point of view, frameworks support alignment with data protection laws and sector rules. Organisations that combine ISO/IEC 27001 with NIST CSF often find it easier to show control effectiveness to auditors and regulators [6][8]. COBIT and ITIL help link security to wider IT governance and service management, so controls are built into everyday processes rather than treated as one-off tasks [5][15].

However, frameworks can be demanding to implement and maintain, especially for organisations with limited staff or complex legacy systems [11][16]. For NatureGreen, the key is to use frameworks in a pragmatic, risk-based way: starting with the most relevant controls, aligning them with NG's key risks and increasing maturity gradually instead of trying to implement everything at once.

5.3 Continuous Improvement and Monitoring

A key principle in modern security frameworks is that security management should be continually improved, not applied once and left unchanged. ISO/IEC 27001 builds this into the Plan–Do–Check–Act (PDCA) cycle, which requires organisations to review their ISMS regularly, assess performance, fix non-conformities and update controls as threats and business needs change [1][7].

Continuous improvement depends on monitoring and measurement. Frameworks emphasise internal audits, management reviews, clear metrics and periodic risk reassessments to keep the security programme aligned with reality [1][3][16]. For NatureGreen, this means tracking indicators such as incident numbers, policy compliance, training completion and patching timelines, and using these results to guide decisions rather than relying on assumptions.

NIST CSF 2.0 and related guidance also stress that cybersecurity should be part of wider risk and performance management, not a separate silo [4][6]. For NatureGreen, adopting this continuous improvement mindset would help ensure that its governance model, policies and controls remain effective as the company grows, enters new markets and adopts new technologies, and that its security posture stays aligned with current threats and business objectives [1][4][6].

6. Conclusion and Recommendations

This report has examined the security challenges faced by NatureGreen (NG), a global health and wellness company that relies heavily on wireless networking, cloud services and bring-your-own-device (BYOD). The analysis showed that, although NG benefits from modern technology, the lack of formal governance, clear policies and structured risk management leaves customer data, employee information and intellectual property at unnecessary risk.

The literature review highlighted that frameworks such as the ISO/IEC 27000 family, the NIST Cybersecurity Framework and ITIL provide a solid basis for effective information security governance. Using these, a tailored approach was proposed for NG covering governance structure, policy development, risk management, compliance, ethics and contingency planning. The discussion stressed that these frameworks must be updated and reviewed regularly to keep pace with changing threats, technologies and regulatory demands.

Key recommendations include: establishing a steering committee and security lead; implementing an ISO 27001-based ISMS supported by NIST CSF; introducing and enforcing policies for BYOD, wireless, cloud and data protection; strengthening risk management and technical controls; formalising compliance and supplier SLAs; enhancing incident response and continuity planning; and adopting continuous improvement through regular reviews and metrics.

References

- [1] ISO/IEC, *ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection — Information security management systems — Requirements*, International Organization for Standardization, 2022. [ISO+1](#)
- [2] ISO/IEC, *ISO/IEC 27002:2022 Information security, cybersecurity and privacy protection — Information security controls*, International Organization for Standardization, 2022. [ISO+1](#)
- [3] ISO/IEC, *ISO/IEC 27005:2018 Information security, cybersecurity and privacy protection — Information security risk management*, International Organization for Standardization, 2018. [ISO+1](#)
- [4] National Institute of Standards and Technology, *Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1*, NIST, Gaithersburg, MD, USA, Apr. 2018. [NIST Publications+2NIST+2](#)
- [5] AXELOS, *ITIL Foundation: ITIL 4 Edition*, London, UK: The Stationery Office, 2019.
- [6] H. Taherdoost, “Understanding Cybersecurity Frameworks and Information Security Standards,” *Electronics*, vol. 11, no. 14, p. 2181, 2022. [MDPI](#)
- [7] S. Vacca, *Information Security Management Based on ISO 27001*, Morgan Kaufmann, 2015. [ACM Digital Library](#)

- [8] B. Reuben-Owoh and A. Dehghantanha, “A Systematic Review of Voluntary Cybersecurity Standards and Frameworks,” 2025. [Portsmouth Research Portal](#)
- [9] I. Tikanmäki, “The Role of Standards in Enhancing Cybersecurity and Business Continuity,” *International Journal of Intelligence and Security Informatics*, 2024. [ISI](#)
- [10] “PDCA: An Implementation Guide to ISO 27001:2022,” Citation Group, 2024. [Citation Group](#)
- [11] T. R. McIntosh, “From COBIT to ISO 42001: Evaluating Cybersecurity Governance, Risk and Compliance Frameworks,” *Computers & Security*, 2024. [ScienceDirect](#)
- [12] “The CISO’s Guide to the Top Cybersecurity Frameworks,” AttackIQ White Paper, 2020. [AttackIQ](#)
- [13] NIST, *The NIST Cybersecurity Framework (CSF) 2.0*, NIST CSWP 29, 2024. [NIST Publications](#)
- [14] C. Luidold *et al.*, “Cybersecurity Policy Framework Requirements for the European Health Data Space,” *Frontiers in Digital Health*, 2024. [PMC](#)
- [15] “What is COBIT? Framework, Principles & Benefits,” The Knowledge Academy, 2025. [The Knowledge Academy](#)
- [16] BSI Group, “Integrating ISO/IEC 27001 to Increase Efficiency, Eliminate Redundancy, and Demonstrate Effectiveness,” White Paper, 2013. [BSI](#)
- [17] M. Liu *et al.*, “Toward Effective Cybersecurity Management: A Hierarchical Framework,” *Cybersecurity*, vol. 11, no. 1, 2025. [OUP Academic](#)
- [18] “Understanding IT Frameworks: Types and Importance,” Cflow, 2025. [Cflow](#)
- [19] “Continual Improvement – ISMS Online,” ISMS.online, 2024. [ISMS.online](#)
- [20] “Top 4 Cybersecurity Frameworks,” IT Governance USA, 2024. [IT Governance USA](#)
- [21] “Evaluating the Impact of Risk Management Frameworks on IT Audits: A Comparative Analysis of COSO, COBIT, ISO/IEC 27001 and NIST CSF,” 2025. [ResearchGate](#)
- [22] “ISO/IEC 27001 Compliance Guide: Your Path to Compliance,” Protecht Group, 2025. [Protecht Group](#)
- [23] NIST, “The NIST Cybersecurity Framework (CSF) 2.0 Overview,” 2024. [NIST Publications](#)
- [24] “PDCA and ISO 27001: Continuous Improvement in the ISMS,” Consultants Like Us, 2024. [ISO 27001 Consultants](#)
- [25] “What is ISO 27001? Key Information at a Glance,” DataGuard, 2024. [dataguard.com](#)

[26] “Achieving Regulatory Compliance with ISO 27001 and NIST Frameworks: The Process and Challenges,” 2025. [ResearchGate](#)

[28] “Integrating ISO 27001 and ISO 9001 into a Single Management System,” Evalian, 2024. [evalian.co.uk](#)