



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

School of Applied Computing

ACCA7028

Report on ‘Implementing Security for NatureGarden’

By

2227183

Chisom Vanessa Nwankwo

MSC. Data Science and Analytics

TABLE OF CONTENTS

ABSTRACT.....	iii
CHAPTER ONE: INTRODUCTION.....	1
CHAPTER TWO: INFORMATION SECURITY FRAMEWORKS.....	2
2.1. NIST Cybersecurity Framework	2
2.2. PCI DSS	3
2.3. COBIT	3
2.4. ISO 27000 family	4
2.5. CIS CSC	6
2.6. ITIL	6
CHAPTER THREE: SECURITY APPROACH.....	8
CHAPTER FOUR: REFLECTION	12
4.1. Critique.....	12
4.2. Analysis.....	12
4.3. Discussion	13
CHAPTER FIVE: CONCLUSION.....	14
BIBLIOGRAPHY	15

ABSTRACT

The report provides a comprehensive overview of the security approach for NatureGarden (NG), a company with a global presence that presumably uses cloud services and has a predominantly wireless network. Given the company's requirements and the evolving cybersecurity landscape, the report explores various frameworks and models to enhance NG's information security. These include the NIST Cybersecurity Framework, PCI DSS, COBIT, the ISO 27000 family, CIS CSC, and ITIL. The approach is meticulously designed in stages, from understanding the business context to implementing continuous improvement processes. This report also reflects on the importance of constantly updating regulations and standards, discussing the balance between staying current and managing the complexity and cost of compliance.

CHAPTER ONE: INTRODUCTION

Information security frameworks and standards exist to establish the security of data and digital devices and to protect customers' and employees' data and the company's assets. It is impossible for any IT company to avoid attacks on their services or systems completely. Therefore, they need to be resilient. NatureGarden's security system can be considered resilient and dependable if its human resources, processes, and technology are considered, as effective security relies on these factors. The right technology is important for data and information security. This technology will also be managed by people who must follow a defined process. Resilience means that the company can withstand attacks. They should be able to reduce the time between detection and recovery. Hence, security education is important. According to [1], resilient systems should be able to:

- a. Monitor and log changes within the system.
- b. Respond to those changes.
- c. Anticipate threats.
- d. Learn from success and failures.

The aspect of security fundamental to any organisation is referred to as the CIA triad. It comprises three aspects, namely:

- a. Confidentiality: Information assets should only be provided to those who need access.
- b. Integrity: Information assets should be protected to prevent unauthorised data modification and loss.
- c. Availability: Information assets should be accessible to authorised personnel when needed.

This is because restricting access to data on a need-to-know basis is vital in securing data. However, the data can only be useful if it is accurate and is available when needed. Physical security of systems is also crucial to security, as firewalls and antivirus software are pointless if an external person can obtain data by looking over an employee's shoulder or even stealing the device.

CHAPTER TWO: INFORMATION SECURITY FRAMEWORKS

Information and Cybersecurity frameworks in existence capable of addressing the security issue at NatureGarden include:

2.1. NIST Cybersecurity Framework

This framework was developed by the National Institute of Standards and Technology, also known as NIST, to address cybersecurity issues. Its purpose is to aid organisations in managing and reducing cyber-attacks [2]. The NIST CSF provides a common language for understanding, managing, and expressing cybersecurity risk to internal and external stakeholders [3]. The framework comprises three components [4]: the core, profiles, and implementation. The core contains the cybersecurity activities or controls of the company, and the profiles component identifies the actions the company should take to be secure. The implementation component describes the level of sophistication of the company's risk management. The core component details five functions that specify how to organise cybersecurity activities [5]. They include:

- a. Identify: At this stage, the organisation should know their assets, both physical and digital, their roles and interconnections. This will enable them to understand security policies to implement and manage risks to their information systems.
- b. Protect: This function consists of the relevant policies and procedures to defend against attacks and threats. It also includes security education for the employees to ensure the organisation's protection.
- c. Detect: The company should also have relevant controls in place to detect security breaches and intrusions. This can be achieved using intrusion detection systems to discover abnormal activities within the system.
- d. Respond: In the event of security breaches, the organisation should also have plans and controls in place to withstand these breaches and recover. The necessary steps in the plan should be followed to address the issue as quickly as possible. A business recovery plan should also serve as a guide to restore corrupted or damaged services. The incident should be recorded to learn and improve security.

Companies such as Amazon, Microsoft, Intel, and JP Morgan Chase [5] have adopted this framework to improve the security of their information systems.

2.2. PCI DSS

The Payment Card Industry Data Security Standard (PCI DSS) [2] was developed and is administered by the founding payment brands of the PCI SSC, or Payment Card Industry Security Standards Council. The payment brands are American Express, JCB International, Mastercard, Discover Financial Services and Visa [6]. It is an industry-wide set of security standards followed by companies that maintain and transmit the credit card data of their clients, to protect against data breaches. Companies that use third parties to manage cardholder data must ensure that the third party complies with the standard. It does not apply if primary account numbers are not stored or transmitted [7]. The standard is applicable to any media on which credit card data may be held, such as hard drives, magnetic tapes, and even printed or handwritten receipts for credit and debit card transactions on which the full card number is visible. The PCI SSC is also responsible for defining qualifications for Qualified Security Assessors, Internal Security Assessors, PCI professionals, etc. They train, test, and certify quality assurance programs for the certifications. This standard consists of six control objectives [8] to maintain security, namely:

- a. Building and maintaining secure systems and networks.
- b. Protecting the data of cardholders.
- c. Maintaining programmes for vulnerability management.
- d. Implementing strong access control mechanisms.
- e. Regularly testing and monitoring networks.
- f. Maintaining information security policies.

2.3. COBIT

The Control Objectives for Information and Related Technology, or COBIT, is a data security framework developed by ISACA (Information Systems Audit and Control Association) in 2011 for IT management and governance [5], [9]. It is a framework for managing and governing enterprise IT and provides an end-to-end business perspective on the compliance and governance of enterprise IT. Its original focus was to overcome technical risks to organisations. This framework is commonly adopted to align IT strategies with the goals of the company and aid in risk management [10]. The principles of the framework include [11]:

- a. Meeting the needs of stakeholders
- b. End-to-end covering of the enterprise

- c. Application of an integrated framework.
- d. To enable a holistic approach.
- e. Separating management and governance.

The domains covered by COBIT include access control, configuration management, media protection, etc. It provides generic processes that represent the activities usually found in IT operations to provide a standard reference that business managers and IT personnel can understand.

2.4. ISO/IEC 27000 family

The ISO/IEC 27000 series is a family of frameworks comprising several information security policies to safeguard business and customer data. They were jointly introduced by the IEC (International Electrotechnical Commission) and ISO (International Organization for Standardization).

1. ISO 27014

This framework provides guidance on IT governance to align business objectives with the information security of the company, deliver values to key stakeholders and ensure security risks are adequately addressed [10]. The six principles applied by the governing body of the framework are:

- a. To establish information security across the organisation.
- b. To adopt a risk-based approach.
- c. To direct investment decisions.
- d. To ensure conformity with external and internal business requirements.
- e. To foster an environment that is security positive.
- f. To review performance about business outcomes.

The standard is also not rigid about by whom and when the principles should be implemented, as each organisation can choose their best approach.

2. ISO 27017

This set of security practices addresses information security in the cloud [12]. It enables cloud users to implement the right security controls and providers to support it. It also details seven cloud-specific controls such as:

- a. Shared responsibility in cloud-computing environments.
- b. Removal of the assets of customers using cloud services.
- c. Isolation in a virtual computing environment.
- d. Hardening of Virtual Machines.
- e. Operational security of the administrator.
- f. Cloud service monitoring.
- g. Aligning security management for physical and virtual networks.

3. ISO 27035

ISO 27035 offers guidance on the management of information security incidents. The standard consists of the principles for managing security incidents and a guide to prepare for responses to these incidents. The five phases for handling security incidents [12] are outlined below:

- a. Planning and Preparing
- b. Detecting and Reporting of security incidents or events.
- c. Assessing the events to determine if they qualify as security incidents.
- d. Responding to the security incidents.
- e. Reviewing actions to identify areas for improvement.

4. ISO/IEC 27001

This standard provides a systematic approach for organisation-wide information security management. It provides best practices for information security management systems also called ISMS, ensuring that sensitive data remains secure. This standard can be combined with other security systems or frameworks. It consists of 14 categories [4], to improve the information security of a company. Some of them include:

- a. Policies for information security.
- b. Information security organisation.
- c. Security of human resources.
- d. Management of assets.
- e. Cryptography.
- f. Communications security.

- g. Security of operations.
- h. Management of information security incidents, etc.

The standard's risk management ensures that risks are handled appropriately to give security confidence to stakeholders. This means that the measures implemented should be cost-effective and sufficiently reduce risks. An essential activity in ISO 27001-compliant systems is penetration testing to detect vulnerabilities in the system.

2.5. CIS CSC

The Centre for Internet Security Critical Security Controls is a set of best practices to protect against cyber-attacks and implement plans to prevent information security threats and attacks. The CIS CSC comprises 20 controls [11], which follow the Pareto principle, meaning that the first five controls mitigate about 85% of risks and are specially designed to protect important information infrastructure. They are:

- a. Inventory of both unauthorised and authorised devices.
- b. Inventory of both unauthorised and authorised software.
- c. Security configurations for both hardware and software.
- d. Continuous assessment of vulnerabilities and remediation.
- e. The controlled use of admin privileges.

2.6. ITIL

The Central Computer and Telecommunication Agency, or CCTA, developed the Information Technology Infrastructure Library [9], which defines codes of practice for information technology services management. It is a comprehensive, cost-effective, and efficient framework with which companies can design and implement security procedures. ITIL aims to achieve information security management through People, Technology, Partners, and Processes. The life cycle of its services is as follows:

- a. Service strategy, which involves achieving strategic goals.
- b. Service design, which involves providing guidance on IT services and practices design and policies to implement the design.
- c. Service transition, which involves guiding the development of capabilities for service transitions.

- d. Service operation, which involves guidance on effective IT delivery and support services
- e. Continual improvement of services, which involves guiding the provision of customer value.
- f. Service Management, which involves guidance on continuous service improvement.

In other words, ITIL is focused on the continuous assessment and improvement of the quality of information technology services. The framework uses four processes: Plan, Implement, Evaluate, Maintain and Control [9], to ensure that information is protected at every stage in a business process.

CHAPTER THREE: SECURITY APPROACH

Based on the needs of NatureGarden, an approach that considers and manages the company's assets is necessary. It should also encompass the aspects of the CIA triad. The approach outlined in steps is as follows:

Step 1: Establish the Foundation

- **1.1 Understand the Business Context:** Gain a thorough understanding of NG's operations, objectives, and the nature of its data and services. Conduct a SWOT (strengths, weakness, opportunities, threats) analysis.
- **1.2 Identify Legal and Regulatory Requirements:** Determine the legal, regulatory, and contractual obligations NG must comply with and track them using compliance management tools like Compliance 360 or NAVEX Global

Step 2: Select and Tailor the Frameworks

- **2.1 Choose Relevant Frameworks:** Use governance and risk management software like RSA Archer to integrate frameworks like NIST CSF, PCI DSS, COBIT, ISO/IEC 27000 series, and CIS CSC.
- **2.2 Tailor Frameworks to NG:** Customise the selected frameworks to fit NG's specific context. A mix of these frameworks can be utilised, depending on the company's detailed requirements. This will involve using custom checklists and policy templates, for instance, Templafy or Process sheet.

Step 3: Risk Assessment and Asset Management

- **3.1 Identify Assets:** Create a catalogue of NG's physical and digital assets, especially those involved in wireless and cloud services. Asset management tools like SolarWinds can create a catalogue of physical and digital assets.
- **3.2 Conduct Risk Assessment:** Perform a risk assessment to identify and prioritise potential threats and vulnerabilities using tools like Qualys or RiskLens.

Step 4: Protection and Defence

- **4.1 Develop Security Policies:** Create comprehensive policies covering device usage, data, and intellectual property protection. Tools like PolicyTech can be used to manage these policies.
- **4.2 Implement Protection Measures:** Establish security measures like encryption, access controls, and secure network configurations. Deploy antivirus and network security tools like Cisco Firewalls.
- **4.3 Secure Personal Devices:** Deploy tools and policies for securely managing personal devices. Also, for employees to have secure remote access to the company's resources, policies should be developed to control the use of devices off-premises. Remote wiping of an employee's lost device should also be possible. Use Mobile Device Management (MDM) solutions like VMware AirWatch or Microsoft Intune.

Step 5: Detection and Response

- **5.1 Establish Detection Mechanisms:** Implement systems to monitor and detect security incidents, especially in wireless and cloud environments. Implement SIEM (Security Information and Event Management) tools like Splunk or IBM QRadar for monitoring and detection.
- **5.2 Develop an Incident Response Plan:** Create a detailed plan outlining the steps to take in response to a security incident. Utilise incident management software like ServiceNow Incident Management.

Step 6: Governance and Compliance

- **6.1 Integrate Governance Frameworks:** Apply COBIT principles to align IT and business strategies and ensure proper governance.
- **6.2 Ensure Compliance:** Regularly audit against the chosen standards and legal requirements to ensure ongoing compliance. Use compliance software like Compliancy Group or ZenGRC.

Step 7: Training and Awareness

- **7.1 Employee Training:** Conduct regular security training and awareness programs for all employees, focusing on NG's specific risks; a security-positive culture should be cultivated. This training should cover several attacks, such as phishing, social engineering, vishing, catfishing, shoulder surfing, eavesdropping, etc.
- **7.2 Customer Education:** Provide guidance and information to customers on how to securely interact with NG's services.

Step 8: Continuous Improvement

- **8.1 Monitor and Review:** Continuously monitor the security environment and regularly review the effectiveness of the implemented measures. Use continuous monitoring tools like Datadog or New Relic and regular review platforms like ReviewSnap.
- **8.2 Update and Adapt:** Regularly update the security measures and policies in response to new threats, technologies, and business changes. Implement change management software like ServiceNow Change Management to manage updates.

Step 9: Documentation and Communication

- **9.1 Document Policies and Procedures:** Document all security policies, procedures, and guidelines.
- **9.2 Develop a Communication Plan:** Ensure all staff and relevant stakeholders are informed about security policies, incidents, and updates.

The security areas covered by this approach are:

- a. Asset management.
- b. Information security policies.
- c. Physical and environmental security.
- d. Identity and access control.
- e. Malware protection.
- f. Configuration and patch management.
- g. Encryption.

- h. System Security.
- i. Network and communications security.
- j. Security competence and training.
- k. Staff awareness training.
- l. Comprehensive risk management programme.
- m. Threat and vulnerability intelligence.
- n. Security monitoring.
- o. Incident response management.
- p. ICT continuity management.
- q. Business continuity management.
- r. Formal information security management programme.
- s. Continual improvement process.
- t. Governance structure and processes.
- u. Internal audit.
- v. External certification/validation.

By following these steps, NG can build a comprehensive and adaptive IT framework that secures its data and resources, aligns with its business objectives, and ensures compliance with industry standards and regulations.

CHAPTER FOUR: REFLECTION

Constantly updating regulations and standards is beneficial in various sectors, including technology, healthcare, environment, and finance. The following are reasons why it is considered good practice:

4.1. Critique

a. Over-Regulation and Complexity:

- i. **Critique:** Constant updates can lead to over-regulation, creating a complex web of standards organisations need help navigating. This can be particularly burdensome for small businesses and startups with limited resources.
- ii. **Counterpoint:** While complexity is a valid concern, the alternative — outdated or inadequate regulations — could lead to more significant risks, including safety issues, environmental damage, or unfair market practices.

b. Cost and Compliance:

- i. **Critique:** Regular updates require organisations to spend significant time and resources to stay compliant, which might divert attention from innovation and growth.
- ii. **Counterpoint:** The cost of non-compliance and the potential harm from outdated practices often outweigh the expenses associated with updating and adhering to new standards.

4.2. Analysis

a. Safety and Well-being:

- i. **Analysis:** Updated regulations are crucial for protecting public health and safety. As new risks emerge, regulations need to evolve to mitigate these threats effectively.
- ii. **Example:** In healthcare, updated drug approval and medical device standards ensure that patients receive safe and effective treatments.

b. Technological Advancements:

- i. **Analysis:** Rapid technological changes, especially in areas like AI, cybersecurity, and biotechnology, necessitate regular updates to regulations to address new challenges and ethical considerations.
- ii. **Example:** Data protection laws have been updated in many regions to address privacy concerns arising from data collection and analysis technology advancements.

c. **Environmental Protection:**

- i. **Analysis:** As our understanding of environmental impacts deepens, regulations must evolve to incorporate new scientific findings and mitigate ecosystem harm.
- ii. **Example:** Emissions and waste management regulations have been updated in response to new insights into their effects on climate change and pollution.

d. **Economic and Market Stability:**

- i. **Analysis:** Updated regulations help maintain fair competition, prevent market abuse, and ensure economic stability.
- ii. **Example:** Financial regulations have been updated post-economic crises to prevent future collapses and protect consumers and investors.

4.3. Discussion

a. **Balancing Act:**

- i. **Discussion:** The challenge lies in balancing the need for updated regulations with the potential for over-regulation. Ensuring that updates are necessary, evidence-based, and provide clear benefits is crucial.
- ii. **Consideration:** Regulatory impact assessments can help determine the potential effects of regulation changes and ensure that they are justified and beneficial.

b. **Inclusivity and Flexibility:**

- i. **Discussion:** Regulations should be developed with input from a wide range of stakeholders, including industry experts, public interest groups, and the public, to ensure they are comprehensive and equitable.
- ii. **Consideration:** Flexible regulations that provide guidelines rather than prescriptive rules can adapt more easily to different scenarios and innovations.

c. **Global Considerations:**

- i. **Discussion:** In an increasingly interconnected world, regulations in one region can have global implications. International cooperation and standards are vital for dealing with issues like climate change, internet governance, and trade.
- ii. **Consideration:** Harmonizing regulations across borders can reduce compliance costs and complexity, facilitating international cooperation and trade.

CHAPTER FIVE: CONCLUSION

The study concludes that for NatureGarden, implementing a structured, multi-layered security approach is critical for protecting its data, resources, and reputation. The suggested frameworks and models should be tailored to address the unique challenges of NG's reliance on cloud services and a wireless network. By systematically following the outlined steps, NG can enhance its resilience against cyber threats, ensure compliance with international standards, and maintain its position as a trusted leader in the market. There should be an emphasis on regularly updating regulations and standards to mitigate emerging risks and harness new opportunities, advocating for a balanced, inclusive, and flexible approach to regulation to ensure safety, fairness, and sustainability in a rapidly evolving digital world.

BIBLIOGRAPHY

- [1] Costel Ciuchi, “Developing a Comprehensive Model for Digital Lifelong Learning Using Cyber Resilience Framework,” *International Conference on Cybersecurity and Cybercrime*, vol. 9, pp. 105–112, Apr. 2022, doi: <https://doi.org/10.19107/cybercon.2022.14>.
- [2] D. Gould, “Organizational Resilience Approaches to Cyber Security,” *International Journal of Smart Education and Urban Society*, vol. 9, no. 4, pp. 53–62, Oct. 2018, doi: <https://doi.org/10.4018/ijseus.2018100105>.
- [3] A. Calder, “Chapter Title: AIMS OF THE FRAMEWORK Book Title: NIST Cybersecurity Framework Book Subtitle: A pocket guide,” IT Governance Publishing, 2018. Accessed: Dec. 28, 2023. [Online]. Available: <https://www.jstor.org/stable/j.ctv4cbhfx.5>
- [4] A. Calder, “Chapter Title: BASELINE,” in *The Cyber Security Handbook – Prepare for, respond to and recover from cyber attacks*, IT Governance Publishing, 2020, pp. 321–327.
- [5] K. Elangovan, “Security Framework for Supply-Chain Management,” in *Handbook of Research on Interdisciplinary Approaches to Decision Making for Sustainable Supply Chains*, A. A. Awasthi and K. Grzybowska, Eds., IGI Global, 2020, pp. 533–555. doi: <https://doi.org/10.4018/978-1-5225-9570-0.ch025>.
- [6] A. Calder and G. Williams, “WHAT IS THE PAYMENT CARD INDUSTRY DATA SECURITY STANDARD (PCI DSS),” in *PCI DSS: A pocket guide, sixth edition*, 6th ed. IT Governance Publishing, 2019, pp. 10–12. doi: <https://doi.org/10.2307/j.ctvndv9hz>.
- [7] A. Calder and G. Williams, “IT Governance Publishing Chapter Title: WHAT IS THE SCOPE OF THE PCI DSS? Book Title: PCI DSS: A pocket guide, sixth edition,” : IT Governance Publishing, 2019.
- [8] A. Calder and G. Williams, “PCI DSS – THE STANDARD,” in *PCI DSS: A pocket guide, sixth edition*, IT Governance Publishing, 2019, pp. 33–35. Accessed: Dec. 28, 2023. [Online]. Available: <https://doi.org/10.2307/j.ctvndv9hz.13>
- [9] T. C. Herath, H. S. B. Herath, and D. Cullum, “An Information Security Performance Measurement Tool for Senior Managers: Balanced Scorecard Integration for Security Governance and Control Frameworks,” *Information Systems Frontiers*, vol. 25, pp. 681–721, Feb. 2022, doi: <https://doi.org/10.1007/s10796-022-10246-9>.

- [10] A. Calder, “EMBEDDED,” in *The Cyber Security Handbook – Prepare for, Respond to and Recover from Cyber Attacks*, IT Governance Publishing, 2020, pp. 33–35. Accessed: Dec. 28, 2023. [Online]. Available: <https://doi.org/10.2307/j.ctv19shhms>
- [11] A. Calder, “FRAMEWORK CORE,” in *NIST Cybersecurity Framework: A Pocket Guide*, IT Governance Publishing, 2018, pp. 23–44. Accessed: Dec. 28, 2023. [Online]. Available: <https://doi.org/10.2307/j.ctv4cbhfx.6>
- [12] A. Calder, “EXTENDED,” in *The Cyber Security Handbook – Prepare for, respond to and recover from cyber attacks*, IT Governance Publishing, 2020, pp. 328–336. Accessed: Dec. 28, 2023. [Online]. Available: <https://doi.org/10.2307/j.ctv19shhms.32>
- [13] A. Calder, “FRAMEWORK IMPLEMENTATION TIERS,” in *NIST Cybersecurity Framework: A Pocket Guide*, IT Governance Publishing, 2018, pp. 49–54. Accessed: Dec. 28, 2023. [Online]. Available: <https://doi.org/10.2307/j.ctv4cbhfx.8>
- [14] A. Calder, “ALIGNMENT WITH OTHER FRAMEWORKS,” in *NIST Cybersecurity Framework*, IT Governance Publishing, 2018, pp. 63–68. Accessed: Dec. 28, 2023. [Online]. Available: <https://doi.org/10.2307/j.ctv4cbhfx.10>
- [15] H. Taherdoost, “Understanding Cybersecurity Frameworks and Information Security Standards—A Review and Comprehensive Overview,” *Electronics*, vol. 11, no. 14, p. 2181, 2022, doi: <https://doi.org/10.3390/electronics11142181>.
- [16] A. Calder and G. Williams, “COMPLIANCE AND COMPLIANCE PROGRAMMES,” in *PCI DSS: A Pocket Guide, Sixth Edition*, IT Governance Publishing, 2019, pp. 17–19. Accessed: Dec. 28, 2023. [Online]. Available: <https://doi.org/10.2307/j.ctvndv9hz.9>
- [17] A. Calder and G. Williams, “THE PCI DSS AND ISO/IEC 27001,” in *PCI DSS: A Pocket Guide, Sixth Edition*, IT Governance Publishing, 2019, p. 50. Accessed: Dec. 28, 2023. [Online]. Available: <https://doi.org/10.2307/j.ctvndv9hz.17>
- [18] A. Calder, “INFORMATION AND CYBER SECURITY,” in *The Cyber Security Handbook – Prepare for, respond to and recover from cyber attacks*, IT Governance Publishing, 2020, pp. 15–16. Accessed: Dec. 28, 2023. [Online]. Available: <https://doi.org/10.2307/j.ctv19shhms.5>
- [19] L. Ladu and Minique Vrins, “Supportive Regulations and Standards to Encourage a Level Playing Field for the Bio-based Economy,” *International journal of standardization research*, vol. 17, no. 1, pp. 58–73, Jan. 2019, doi: <https://doi.org/10.4018/ijsr.2019010104>.

- [20] C. Latoz, L. Larkin, and K. Huynh-Ba, “Stability considerations for drug-device combination products-21 CFR part 4 update,” *AAPS Open*, vol. 9, no. 1, May 2023, doi: <https://doi.org/10.1186/s41120-023-00078-5>.
- [21] J. Seaman, “An Introduction to the PCI DSS Controls Framework,” *Apress eBooks*, pp. 231–284, Jan. 2020, doi: https://doi.org/10.1007/978-1-4842-5808-8_9.
- [22] J. Seaman, “The Evolution of PCI DSS,” *Apress eBooks*, pp. 29–60, Jan. 2020, doi: https://doi.org/10.1007/978-1-4842-5808-8_2.
- [23] “NIST Cybersecurity Framework 2.0 Concept Paper: Potential Significant Updates to the Cybersecurity Framework Note to Reviewers,” 2023. Available: https://www.nist.gov/system/files/documents/2023/01/19/CSF_2.0_Concept_Paper_01-18-23.pdf
- [24] “Updating the NIST Cybersecurity Framework – Journey To CSF 2.0 | NIST,” *NIST*, May 26, 2022. <https://www.nist.gov/cyberframework/updating-nist-cybersecurity-framework-journey-csf-20> (accessed Dec. 28, 2023).
- [25] Rias Kumalasari Devi, Dana Indra Sensuse, Kautsarina Kautsarina, and Ryan Randy Suryono, “Information Security Risk Assessment (ISRA): A Systematic Literature Review,” *Journal of Information Systems Engineering and Business Intelligence*, vol. 8, no. 2, pp. 207–217, Oct. 2022, doi: <https://doi.org/10.20473/jisebi.8.2.207-217>.
- [26] Y. You, J. Oh, S. Kim, and K. Lee, “Advanced approach to information security management system utilizing maturity models in critical infrastructure,” *KSII Transactions on Internet and Information Systems*, vol. 12, no. 10, pp. 4995–5014, Oct. 2018, Accessed: Dec. 28, 2023. [Online]. Available: <https://itiis.org/digital-library/manuscript/2155>