



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

**Applied Computing Department - Wales Institute of
Science and Art**

ASSESSMENT

on

**“Data Security, Governance and Compliance”
(ACCA7028)**

NAME: SNEHA SINDHE

STUDENT ID: 2304464

TABLE OF CONTENTS

ABSTRACT	3
CHAPTER 1: INTRODUCTION	4
CHAPTER 2: SECURITY FRAMEWORKS AND MODELS	6
2.1 NIST Cybersecurity Framework:	6
2.2 Information Technology Infrastructure Library (ITIL)	8
2.3 International Organization for Standardization - ISO 27000	11
CHAPTER 3: DESIGN AND IMPLEMENTATION	16
3.1: Integrated Strategy for the Security, Governance, and Compliance of NatureGarden's Information System	16
CHAPTER 4: ANALYSIS	20
4.1: Importance of New or Updated Regulations and Standards	20
REFERENCE	23

LIST OF TABLES

Table 3.1: Framework Integration	16
Table 3.2: Risk Management	17
Table 3.3: Security Policies	17
Table 3.4: Contingency Planning	18
Table 3.5: Governance and Compliance	18
Table 3.6: Protection Mechanism	19
Table 3.7: Service Level Agreement	19

LIST OF FIGURES

Figure 2.1: NIST Core Functions	7
Figure 2.2: ITIL Framework	9
Figure 2.3: ITIL Service Lifecycle Stages	10
Figure 2.4: Summary of recommendations of ontologies based on ISO 27000	12
Figure 2.5: ISO 27001 Meta Model	13
Figure 2.6: Overview of ISO 27005	14

ABSTRACT

This report emphasizes the importance of adaptability in the ever-changing technology and security landscape. It emphasizes how important it is to be adaptive when dealing with new hazards, how changing legal frameworks affect, and how cutting-edge technologies and security precautions are used. Following the most recent standards shows customers that one is dedicated to security and promotes confidence. Organizations must stay up to date with regulatory regulations because non-compliance can have negative effects on their reputation and legal consequences. The study argues that while static techniques lose efficiency over time, cybersecurity strategies should adopt an approach that moves towards continuous improvement. Frequent updates encourage organizations to examine and evaluate their security postures, learn from past errors, and incorporate user feedback into small improvements. Cybersecurity is an evolving procedure that requires constant improvement. It also emphasizes the need to cultivate a forward-thinking mindset crucial for the constant commitment to strong and efficient cybersecurity measures and to strengthen security against new threats.

CHAPTER 1

INTRODUCTION

An era of extraordinary connection has arrived with the widespread adoption of the Internet, transforming how companies perform and communicate with their stakeholders. A global establishment in healthy living items, NatureGarden (NG), is positioned at the center of creativity and market leadership. An increasing number of experts are required to secure information assets due to the growing threat of cyberattacks brought on by the world's increasing reliance on the Internet. With billions of users, there is an increasing demand for IT specialists. But there are many obstacles in the way of achieving greatness, especially when it comes to data security, governance, and compliance.

- **The Internet's widespread nature and NG's Digital Footprint:** As NG grows its digital reach worldwide, it is essential to use cloud services to provide IT solutions. The company's network is thought to be 95% wireless, demonstrating its dedication to cutting-edge technology infrastructure. The widespread use of digital technology, however beneficial, also creates risks that necessitate a careful and comprehensive approach to information security.
- **The Urgent Need for Personal Device Integration:** NG is under increasing pressure to accept personal device usage within its network due to the expectations of a dynamic workforce and a worldwide client base. This change has far-reaching effects on interactions between employees and customers. However, this increased flexibility also means that accessibility and security must be carefully balanced, which emphasizes the importance of having a clear security policy.
- **The Risks -Data and Intellectual Property Protection:** Due to NG's extensive operations, sensitive customer and employee data must be managed. Safeguarding this information is not only legally necessary but also morally and ethically required. Furthermore, NG's billion-dollar intellectual property is what drives its innovation and distinguishes it in the market. The necessity of

protecting these digital assets is made more urgent by the lack of a formal security policy.

- **Information Security Disorder:** Even if information security is given priority, NG is in a chaotic state. The lack of a formalized security policy exposes the business to risks from a wide range of sources, including governmental agencies, organized crime groups, and individual hackers. The identification of this vulnerability highlights the urgent requirement for an all-encompassing and customized security architecture.
- **The Mandate for the Ideal Combination of Skills and Experiences:** Information Technology (IT) workers must have the ideal combination of skills and experiences due to the complexity of today's cybersecurity threats.

Due to the worldwide reach of the Internet, threats can originate from anywhere in the globe, necessitating the need for a sophisticated skill set to proactively protect NG's information assets. With these difficulties and requirements in mind, this evaluation sets out to provide a customized strategy that combines the best security frameworks and models available. To Strengthen the company's digital defenses and ensure compliance with governance and compliance requirements, we want to develop a comprehensive strategy that takes into consideration the particular requirements and subtleties of NG's Operations.

CHAPTER 2

SECURITY FRAMEWORKS AND MODELS

Documents with standards, best practices, and guidelines for risk management in cybersecurity are called cybersecurity frameworks. Their goal is to reduce an organization's susceptibility to cyber-attacks. Although the phrase might suggest hardware, it offers structure and backing for the security procedures and initiatives of an organization [1].

2.1 NIST Cybersecurity Framework:

These kinds of attacks are what the NIST Framework is intended to defend against in organizations. The Framework was created initially to assist infrastructure-related U.S. organizations in organizing their cybersecurity efforts in a methodical and up-to-date manner, but according to NIST, it “has since proven flexible enough to be adopted voluntarily by large and small companies and organizations across all industry sectors, as well as by federal, state, and local governments” [2].

Agency heads are required to manage their cybersecurity risk using the Framework and to submit a risk management report to the Director of the Office of Management and Budget (OMB) and the Secretary of Homeland Security. The Framework has been substantially improved and clarified in its revised version, but it still has all of its original features, making it simple for both new and current users to apply. The CSF is still very much focused on ensuring that the cybersecurity measures that are adopted are cost-effective and adequate for the degree of risk involved [2].

Describing the NIST Cybersecurity Framework Core Functions from Figure 2.1:

- **Identifying vital Assets and Intellectual Property:** Within NG's extensive activities, a careful identification of vital assets and intellectual property is required as the first pillar of the NIST Cybersecurity Framework. This stage necessitates a thorough inventory of both digital and physical assets,

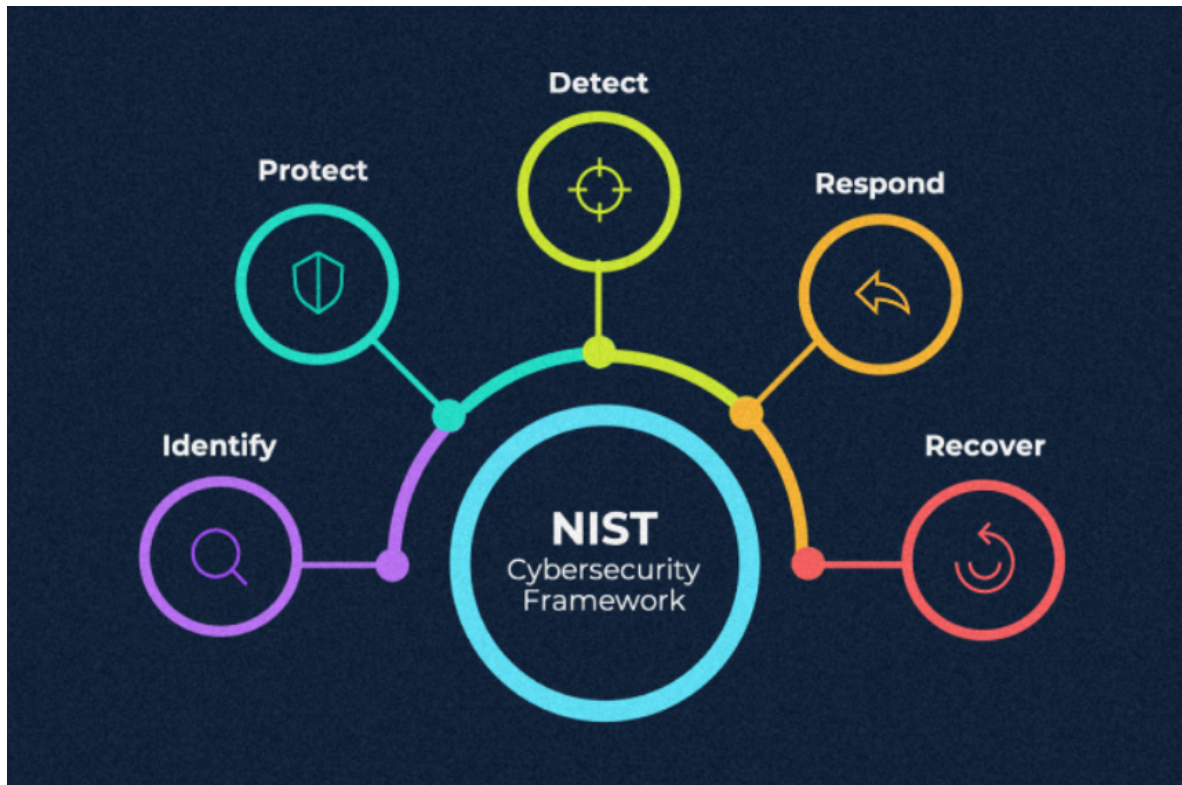


Figure 2.1: NIST Core Functions

classifying them according to how important they are to the main operations of the business. NG's innovation and competitiveness in the market are based on its critical intellectual property, which needs to be properly defined.

- **Putting Data Protection Measures in Place, Particularly for Wireless Networks:** After the identification of key assets and intellectual property, the framework requires the adoption of strong protective measures. With wireless networks accounting for an estimated 95% of the network in NG, data security during transit becomes critical. This entails the deployment of encryption technologies, secure setups, and access controls to limit the hazards involved with wireless communication. The goal is to establish a safe space where private information is protected from prying eyes and kept secret [3].
- **Using Sophisticated Detection Techniques to Identify Dangers Quickly:** The "Detect" function of the NIST framework concentrates on proactive threat identification. For NG, this translated towards cutting-edge detection methods capable of recognizing irregularities and potential threats in real time. Behavioral analytics, anomaly detection algorithms, and sophisticated

intrusion detection systems become essential elements. The objective is to minimize potential harm and downtime by quickly detecting and mitigating security problems.

- **Creating a Rapid Response Plan:** The "Response" function is essential in the case of a security incident. When a security breach is discovered, NG needs to have a fast-reaction strategy in place that outlines the procedures and predetermined actions that must be followed. This calls for communication plans to update stakeholders in addition to technical actions like isolating impacted systems. The goal is to quickly contain the issue to stop it from getting worse and affecting operations.
- **Creating a Sturdy Recovery Plan:** The last function, "Recover," is creating and putting into action a sturdy recovery plan. Procedures for repairing impacted systems, confirming their integrity, and starting up regular operations must be outlined by NG. To improve resilience against similar disasters in the future, this also includes data restoration, system changes, and post-incident analysis. The recovery plan ought to be all-inclusive, covering the operational and technological facets of the recovery procedure [4].

2.2 Information Technology Infrastructure Library (ITIL)

The Office of Government Commerce (OGC) in the UK created the Information Technology Infrastructure Library (ITIL), a framework that describes best practices in information and communication technology (ICT) service management. ITIL makes the unproven claim that it raises customer happiness and service quality. Using a service culture as a foundation, service management concentrates on creating service offerings and delivery methods that satisfy client needs [5].

ITIL, or Information Technology Infrastructure Library, is a widely adopted set of practices for IT service management (ITSM). It offers businesses a thorough framework to make sure that IT services are delivered effectively and efficiently and are in line with business goals. The framework is shown in Figure 2.2.

Essential NG Integration Steps:

Service Strategy: It's critical to match corporate goals with security measures. NG makes sure that security considerations are a crucial component of service planning at the service strategy phase. To do this, it is necessary to comprehend risk tolerance, company objectives, and compliance needs to customize the security plan.

Service Design: NG designs IT services with security requirements integrated into the framework during this step. The availability, confidentiality, and integrity of data are emphasized. To build a secure foundation, access management, encryption techniques, and security controls are integrated throughout the service design process [6].



Figure 2.2: ITIL Framework

Service Transition: NG makes sure that security measures are smoothly integrated into the service transition phase to prevent vulnerabilities during modifications and updates. This entails validating setups, subjecting security measures to rigorous testing, and making sure that any modifications don't pose new security threats. Keeping your posture stable during changes is the aim.

Service Operation: To ensure a safe operating environment, it is essential to set up strong procedures for service operation. NG is centered on problem management, incident response, and ongoing monitoring. This entails proactive problem-solving to stop security breaches, timely incident response, and real-time monitoring of security occurrences.

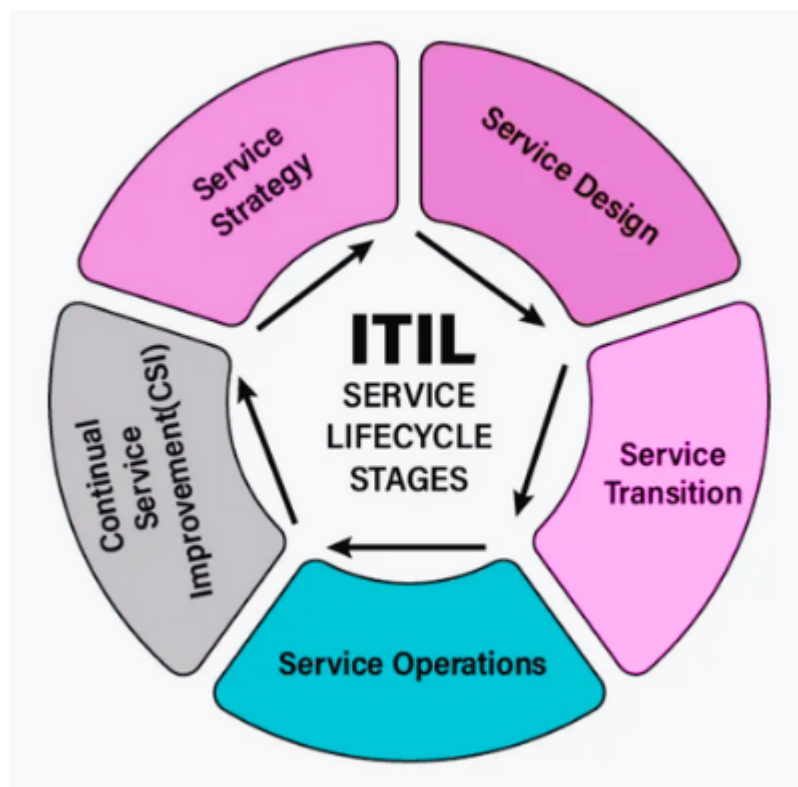


Figure 2.3: ITIL Service Lifecycle Stages

Continual Service Improvement: A key component of ITIL is the continual improvement of service or CSI. NG continuously evaluates and enhances its security protocols in response to user input, incidents, and new threats. This continuous procedure ensures that the security policy remains flexible and connected with the developing threat scenario and business requirements as shown in Figure 2.3 [7].

2.3 International Organization for Standardization - ISO 27000

The International Organisation for Standardization (ISO) and the International Electro-technical Commission (IEC) created the ISO/IEC 27000 family of security standards to serve as a foundation for information security management systems (ISMS). The series includes recommendations, best practices, and requirements for businesses looking to create, implement, manage, and enhance their ISMS over time. The ISO 27001, ISO 27002, and ISO 27005 standards are part of the ISO 27000 series and differ in terms of their depth, breadth, and granularity [8][10].

- The first member of the ISO/IEC standards family, ISO 27001 offers a framework for creating, implementing, running, overseeing, assessing, and enhancing ISMS. It divides the criteria for information security into eleven categories, each of which has numerous subcategories.
- A code of practice for information security management is presented by ISO 27002, which lists hundreds of implementable procedures.
- The Information Security Management System (ISMS) standard, ISO 27005, builds on the concepts, models, procedures, and terminology specified by ISO 27001 to guide Information Security Risk Management (ISRM) in an organization. It facilitates implementation by using the viewpoint of risk management.

Introduction and Vocabulary for ISO/IEC 27000:

As a fundamental standard, ISO/IEC 27000 offers vocabulary and concepts that are utilized throughout the ISO/IEC 27000 series. It creates a common vocabulary that businesses using information security management can use as shown in Figure 2.4 [10][11].

Information Security Management System (ISMS) - ISO/IEC 27001:

The fundamental standard in the series, ISO/IEC 27001, outlines the conditions for creating, putting into practice, preserving, and continuously enhancing an ISMS. This standard offers a methodical, risk-based approach to sensitive information management as shown in Figure 2.5 [10][12].

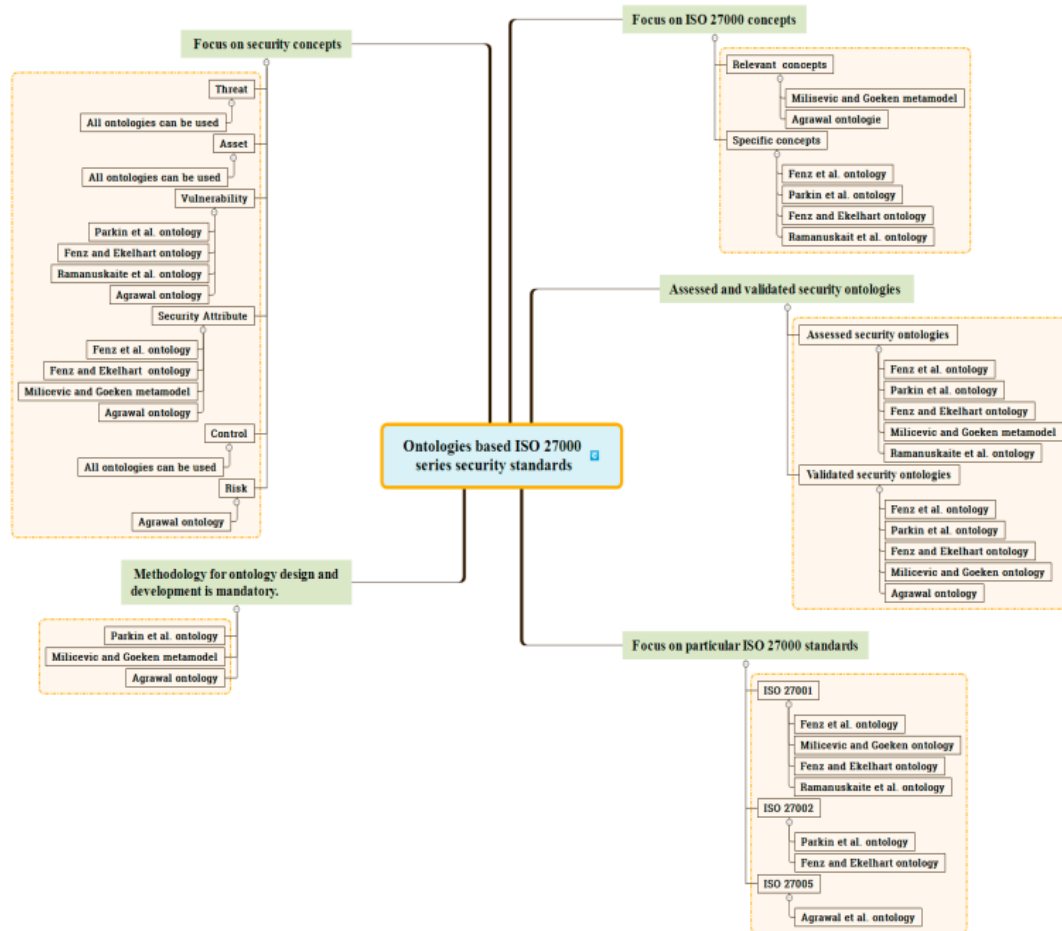


Figure 2.4: Summary of recommendations of ontologies based on ISO 27000

The Code of Practice for Information Security Controls, ISO/IEC 27002:

A comprehensive collection of information security best practices and controls is provided by ISO/IEC 27002. It helps companies tailor their information security controls according to their unique risk profile and environment by offering guidance on choosing and putting into practice the measures found in Annex A of ISO/IEC 27001 [10].

Guidance for Implementing an Information Security Management System, ISO/IEC 27003:

The requirements of ISO/IEC 27001 are the basis for the practical guidelines provided by ISO/IEC 27003. It provides information about the planning, designing, implementing, monitoring, and improving stages of an ISMS

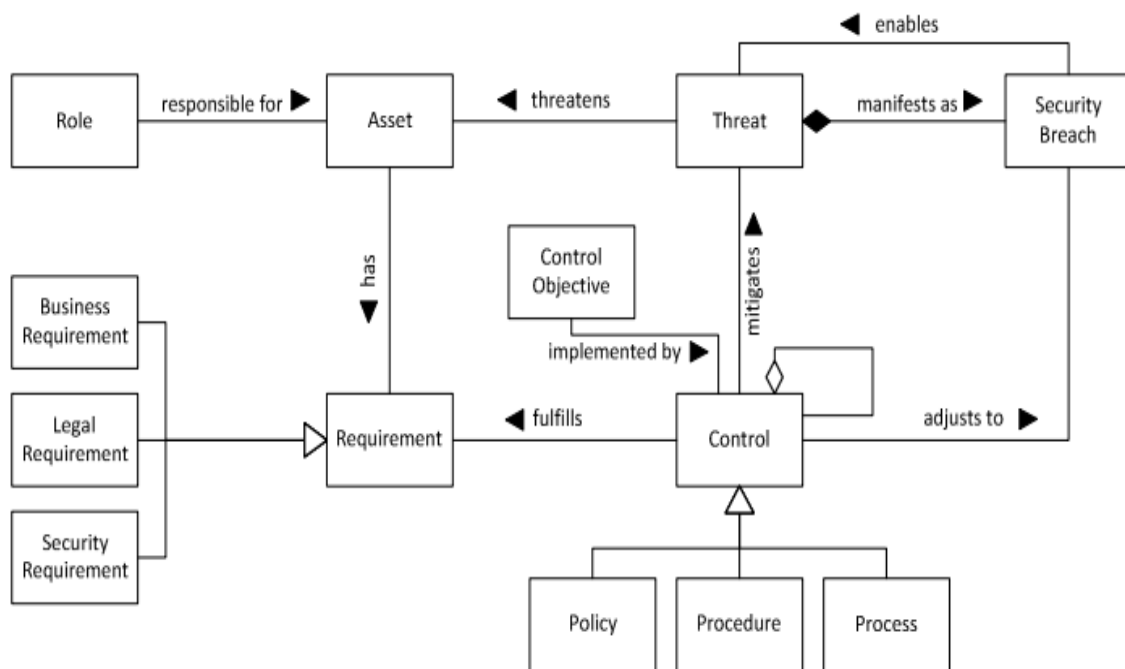


Figure 2.5: ISO 27001 Meta Model

Information Security Management Measurement (ISO/IEC 27004):

Information security measurement is the main topic of ISO/IEC 27004, which aids organizations in establishing a methodical strategy for tracking and evaluating the effectiveness of their ISMS. It offers direction on creating measurements and indicators to evaluate how well security policies are working.

Information Security Risk Management, ISO/IEC 27005:

Organizations can identify, assess, and manage information security risks with the help of ISO/IEC 27005, which offers standards for the process. It conforms with ISO/IEC 27001's risk management methodology as shown in Figure 2.6 [9].

The implementation process involves several key steps:

Recognizing the Requirements: Organizations begin by establishing an in-depth knowledge of the ISO/IEC 27000 standards, primarily ISO/IEC 27001, which serves as the basis for ISMS implementation.

Performing an Evaluation of Risk (ISO/IEC 27005): A risk assessment is undertaken to detect and evaluate information security vulnerabilities. This serves as the cornerstone for creating an efficient ISMS [13].

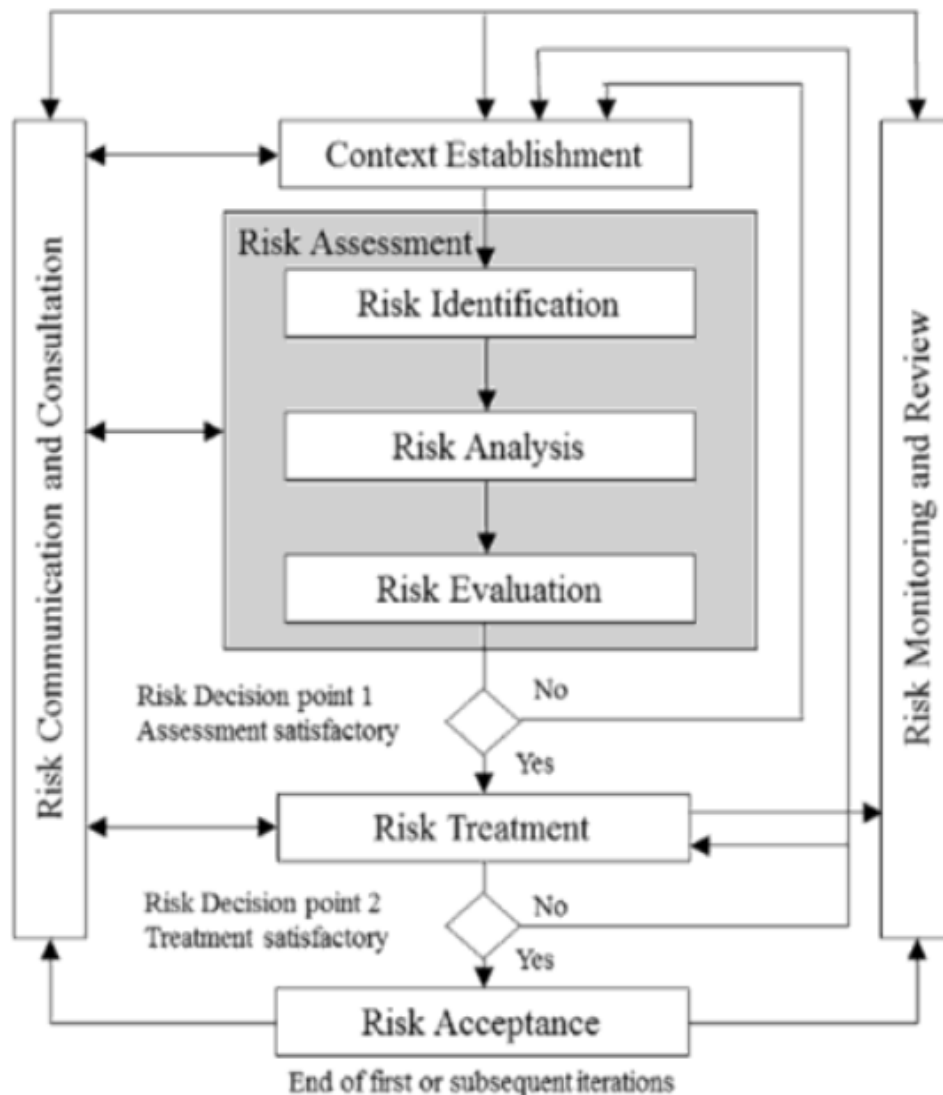


Figure 2.6: Overview of ISO 27005

The process of creating an ISMS (ISO/IEC 27001 and 27002): Organizations create and implement an ISMS in compliance with ISO/IEC 27001 standards according to the risk assessment. Guidance on the selection and implementation of particular security controls can be found in ISO/IEC 27002.

Control Implementation (ISO/IEC 27001 and 27002): Information security is improved and risks are mitigated by implementing controls that were found in the risk assessment and chosen from ISO/IEC 27002.

Observation and Quantification (ISO/IEC 27004): Organisations use metrics and indicators created in compliance with ISO/IEC 27004 to establish systems for tracking and measuring the effectiveness of the ISMS.

Constant Enhancement: Organizations continuously evaluate and enhance their ISMS through an iterative process that takes into account changes in the risk environment, monitoring data, and security event lessons learned [13].

CHAPTER 3

DESIGN AND IMPLEMENTATION

3.1 Integrated Strategy for the Security, Governance, and Compliance of NatureGarden's Information System

A comprehensive solution is necessary to meet the particular issues that NatureGarden (NG) faces in guaranteeing information system security, governance, and compliance. The main elements of a customized framework for NG are shown in the following design:

1. Framework Integration:

Approach: Use a combination of security management frameworks, including ITIL, ISO/IEC 27001, and the NIST Cybersecurity Framework.

Implementation: Create a combined approach that supports organizational objectives and makes the most of each framework's advantages.

Framework	Focus Areas
NIST Cybersecurity Framework	Identify, Protect, Detect, Respond, and Recover functions tailored to NG's context.
ISO/IEC 27001 and 27002	Establish an Information Security Management System (ISMS) and implement detailed security controls.
ITIL	Integrate IT service management practices with a focus on security in service strategy, design, and operation.

Table 3.1: Framework Integration

2. Risk Management:

Approach: To detect, evaluate, and reduce risks to information assets, put in place a risk management procedure.

Implementation: Create a risk database, carry out routine risk assessments, and include risk management in decision-making procedures.

Risk Management Components	Description
Risk Assessment	Identify and assess risks to information assets, prioritizing them based on potential impact.
Risk Treatment	Develop and implement risk treatment plans, incorporating security controls and mitigation strategies.

Table 3.2: Risk Management

3. Security Policies:

Approach: Create detailed security policies that address incident response, data protection, access controls, and other areas.

Implementation: Make sure policies comply with regulations, hold frequent training sessions, and establish an easily accessible policy repository.

Security Policy Components	Description
Access Control	Restrict access based on roles and responsibilities, implementing multi-factor authentication.
Data Protection	Employ encryption and secure data storage mechanisms to safeguard sensitive information.
Incident Response	Establish a well-defined incident response plan, ensuring swift detection and mitigation of security incidents.

Table 3.3: Security Policies

4. Contingency Planning:

Approach: Build an effective backup plan to guarantee that operations continue even in the event of unforeseen circumstances.

Implementation: Make sure the plan is in line with risk assessments, update it regularly, and do simulated exercises.

Contingency Planning Components	Description
Business Continuity Planning	Develop strategies to ensure continuous business operations in the event of a disruption or incident.
Disaster Recovery Planning	Establish procedures to recover and restore critical systems and data after a disaster.

Table 3.4: Contingency Planning

5. Governance and Compliance:

Approach: To verify compliance with relevant regulations and industry standards, undertake assessments of legal and ethical compliance regularly.

Implementation: Create a calendar for compliance, carry out recurring audits, and keep a database of relevant laws and guidelines.

Governance and Compliance Components	Description
Regular Compliance Audits	Conduct regular audits to ensure adherence to regulatory requirements and industry standards.
Board-level Involvement	Engage senior management and the board in strategic planning for security, emphasizing governance.

Table 3.5: Governance and Compliance

6. Protection Mechanism:

Approach: Establish in place many layers of security, such as firewalls, access controls, and encryption.

Implementation: To modify defense tactics, periodically update security tools, carry out penetration tests, and keep an eye out for new threats.

Protection Mechanism Components	Description
Advanced Threat Detection	Utilize advanced threat detection tools to identify and respond to evolving cybersecurity threats.
Endpoint Security	Implement robust endpoint security measures to secure end-user devices accessing NG's network.

Table 3.6: Protection Mechanism

7. Service Level Agreement:

Approach: Develop SLAs with security metrics, making sure that outside services adhere to NG's security requirements.

Implementation: Create a feedback loop for ongoing improvement, audit service providers' security, and review SLAs regularly.

SLA Components	Description
Security Incident Response	Outline response times, communication protocols, and responsibilities in case of a security incident.
Data Handling Procedures	Define procedures for handling and protecting customer and staff data, ensuring compliance with privacy regulations.

Table 3.7: Service Level Agreement

CHAPTER 4

ANALYSIS

4.1: Importance of New or Updated Regulations and Standards

New cyber threats are always emerging, and the threat landscape is always changing. To combat these dangers and allow organizations to implement the newest security measures, legislation, and standards must be updated regularly. As technology develops, new attack channels and vulnerabilities are introduced, and new regulations assist organizations in navigating these complexities. Over time, changes in law and regulation also occur, and periodic updates guarantee adherence to the most recent standards. To improve overall cybersecurity resilience, new guidelines take into account the evolving industry best practices.

International cooperation is crucial, and updated standards offer a shared vocabulary and structure for international cooperation. These standards make it easier to share information, work together to respond to cyber threats, and create a cohesive front in global cybersecurity. It is imperative to be flexible in response to new dangers, as evolving laws direct the application of cutting-edge technologies and security measures. Following the most recent standards demonstrates a dedication to security and confidence among stakeholders, while non-compliance carries dangers to one's reputation and legal standing.

Static approaches grow antiquated and less effective over time, therefore continuous development is essential. Regular updates help companies create a culture of continuous development by motivating them to review their security postures, draw lessons from previous mistakes, and incorporate user feedback into their cybersecurity plans for continuous improvement.

Factors Underlying Continual Updates:

- **Changing Threat Environment:** To handle new and growing cyber threats and make sure that organizations are strong against different attack vectors, new and updated rules and standards are required.
- **Technological Advancements:** Due to the quick speed of technological innovation, laws, and standards must be updated frequently to take new technology into account and protect against related risks.
- **Connectivity and Globalisation:** Because company operations are conducted globally, new laws and standards serve to standardize procedures, enabling a reliable and uniform approach to information security across borders.
- **Legal and Ethical Considerations:** To guarantee that organizations operate by the law and maintain ethical standards, guidelines must be updated in response to changes in laws and ethical standards.
- **Industry-Specific Issues:** Various sectors have different issues. New rules provide guidance that is specifically designed for industry-specific hazards and compliance needs.

The Importance of Regular Updates:

- **Adapting to Evolving Risks:** Frequent upgrades lessen the chance of security failures and data breaches by allowing organizations to actively manage new threats.
- **Enhanced Resilience:** Conforming with the most recent rules makes an organization stronger, making it better equipped to handle and bounce back from security incidents.
- **Maintaining Relevance:** Maintaining policies guarantees that guidelines stay applicable despite evolving business procedures, technological advancements, and security environments.

- **Better Compliance:** Frequent updates lessen the chance of legal ramifications by enhancing an organization's capacity to uphold compliance with changing legal and regulatory standards.
- **Global Consistency:** In today's interconnected world, modern regulations promote global consistency by promoting cross-border collaboration and information sharing.

REFERENCE

- [1]R. Azmi, W. Tibben, and K. T. Win, “Review of cybersecurity frameworks: context and shared concepts,” *Journal of Cyber Policy*, vol. 3, no. 2, pp. 258–283, May 2018, doi: <https://doi.org/10.1080/23738871.2018.1520271>.
- [2]J. Huergo, “NIST Releases Version 1.1 of its Popular Cybersecurity Framework,” *NIST*, Apr. 16, 2018, <https://www.nist.gov/news-events/news/2018/04/nist-releases-version-11-its-popular-cybersecurity-framework>
- [3]A. Calder, “NIST Cybersecurity Framework: A pocket guide,” *JSTOR Books EBA Collection*, 2018. <https://www-jstor-org.ezproxy.uwtsd.ac.uk/stable/j.ctv4cbhfx>
- [4]J. Costanzo, “What is the NIST CyberSecurity Framework?,” *11:11 Systems*, Sep. 20, 2022. <https://1111systems.com/blog/what-is-the-nist-cybersecurity-framework/>
- [5]Nandini, “ITIL Processes List and ITIL Service Lifecycle Stages,” *Sprintzeal.com*, Sep. 30, 2023. <https://www.sprintzeal.com/blog/itil-processes>
- [6]B. Potgieter, D. B. C. Potgieter, and D. C. Lew, “Evidence that use of the ITIL framework is effective,” *Evidence that use of the ITIL framework is effective*, 2005, Available: <https://citeseerx.ist.psu.edu/document?repid=rep1&type=pdf&doi=593a6632fbdd20f32ead8474819d8947d32faf7f>
- [7]M. Gervalla, N. Preniqi, and P. Kopacek, “IT Infrastructure Library (ITIL) framework approach to IT Governance,” *IFAC-PapersOnLine*, vol. 51, no. 30, pp. 181–185, 2018, doi: <https://doi.org/10.1016/j.ifacol.2018.11.283>.
- [8]I. Meriah and L. B. Arfa Rabai, “Comparative Study of Ontologies Based ISO 27000 Series Security Standards,” *Procedia Computer Science*, vol. 160, pp. 85–92, Nov. 2019, doi: <https://doi.org/10.1016/j.procs.2019.09.447>.
- [9]V. Agrawal, *Towards the Ontology of ISO/IEC 27005: 2011 Risk Management Standard*.

Lulu.com,2016.Available:https://www.google.co.uk/books/edition/Proceedings_of_the_Tenth_International_S/zRqqDAAAQBAJ?hl=en&gbpv=1&dq=Agrawal

[10]G. Disterer, “ISO/IEC 27000, 27001 and 27002 for Information Security Management,” *Journal of Information Security*, vol. 04, no. 02, pp. 92–100, May 2013, doi: <https://doi.org/10.4236/jis.2013.42011>.

[11]C. Gikas, “A General Comparison of FISMA, HIPAA, ISO 27000 and PCI-DSS Standards,” *Information Security Journal: A Global Perspective*, vol. 19, no. 3, pp. 132–141, Jun. 2010, doi: <https://doi.org/10.1080/19393551003657019>.

[12]D. Milicevic and M. Goeken, “Ontology-Based Evaluation of ISO 27001,” *IFIP advances in information and communication technology*, pp. 93–102, Jan. 2010, doi: https://doi.org/10.1007/978-3-642-16283-1_13.

[13]S. Fenz, “Ontology-based generation of IT-security metrics,” *ACM Symposium on Applied Computing*, Mar. 2010, doi: <https://doi.org/10.1145/1774088.1774478>.