

Executive Summary

This research investigates the creation of a customised information security framework for NatureGarden (NG) by examining established models such as ITIL, ISO 27000, the NIST Cyber-Security Framework, and COBIT. The research attempts to aid NG in bolstering its IT defences by focusing on governance, risk management, policy adherence, identity and access management, infrastructure protection, business continuity, incident response, employee education, and audits. The conclusion emphasises the importance of continual regulatory updates and adherence to industry standards in order to ensure NG's resilience in the face of emerging cyber threats and to build an information security culture within the organisation.

Contents

Executive Summary	1
Introduction	3
Literature Review of Security Frameworks and Models	3
Information Technology Infrastructure Library	3
Description of the security framework.....	3
ISO 27000	6
Description of security framework:	6
NIST Cyber-Security Framework.....	8
Description.....	8
COBIT (Control Objectives for Information and Related Technologies)	11
Designing own security framework for NatureGarden.....	13
Conclusion.....	17
References.....	18

Introduction

In order for NatureGarden to continue expanding its global footprint, it is vital to have an information technology (IT) environment that is both secure and resilient. The organisation is faced with the challenging problem of allowing employees and customers to use their devices while also securing confidential information, preserving intellectual property, and ensuring that all applicable regulations are adhered to. Through the utilisation of information gleaned from previously established models and frameworks, the objective of this study is to present a structured approach to the process of developing a one-of-a-kind security framework for NG.

Literature Review of Security Frameworks and Models

Information Technology Infrastructure Library

Description of the security framework

According to the author, ITIL represents a widely adopted framework of best practices, which are designed to streamline and enhance technology service management. This framework was originally developed by the United Kingdom's Central Computer and Telecommunication Agency (CCTA) (Palilingan & Batmetan, 2018). The author provided that this framework evolved over the years to become a globally recognized and adaptable set of guidelines that can be followed to manage IT services within business organizations.

As a fundamental principle, ITIL emphasizes the significance of aligning information technology services with the operational requirements and strategic objectives of the business. The goal of the IT Infrastructure Library (ITIL) (Ahmad & Shamsudin, 2013) is to maximise the provision of information technology services by ensuring that these services not only meet but also exceed the expectations of the firm and the parties that are interested in the company. In order to assist the efficient planning, designing, implementing, running, and improving of information technology services, the framework is comprised of a variety of procedures, roles, and obligations that function together.

The Information Technology Infrastructure Library (ITIL) is not designed to be a security framework; nonetheless, it does provide a stable and well-organized base for IT service processes, and the practices and concepts that it entails provide some little assistance for information security. The IT Infrastructure Library (ITIL) advocates for aligning information technology services

with business goals, which are organically tied to risk management, data security, and system integrity systems. Organizations that include ITIL standards in their day-to-day operations naturally address a number of information security-related challenges, thereby setting the framework for an IT environment that is both safe and reliable.

The key aspect of this framework (Lopes, 2021) highlighted in the article is risk management, which is encouraged by ITIL. Further, this can be enabled by managing risks associated with IT services, and successful management will enhance the ability to protect against potential security threats. Further, another major aspect is incident management, in which swift and coordinated responses can be developed for security incidents. ITIL defines processes clearly for identifying, reporting, and resolving incidents, and it contributes to the information security posture of the business. ITIL, in its most fundamental sense, functions as a supplementary framework that, when included in the activities of an organization, cultivates a culture of service excellence while indirectly strengthening information security safeguards. ITIL is a useful asset for organisations that are looking to not only optimise their IT services but also provide a foundation for a safe and resilient IT environment. This alignment with industry best practices presents ITIL as a valuable asset.

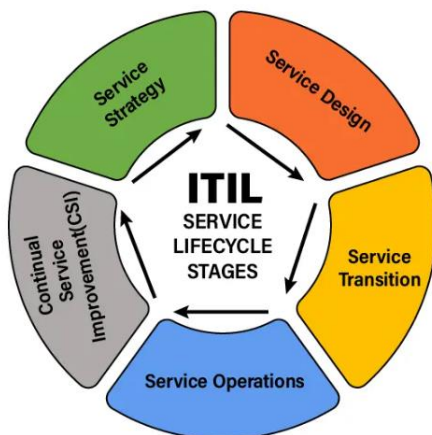


Figure 1: ITIL Framework

Key Components of ITIL:

1. Service Strategy: The Service Strategy phase of the ITIL lifecycle is the fundamental stage in which organisations determine their strategy approach to developing and delivering

information technology services. To do this, it is necessary to connect information technology services with the broader business objectives, recognise opportunities (Al-Ashmoery et al., 2021) in the market, and comprehend the requirements of customers. The Service Strategy outlines the ways in which information technology can assist to the accomplishment of organisational goals and determines the direction for the full service lifecycle. In the context of information security, the alignment of security measures with business objectives is an essential component of the Service Strategy phase. It is possible for organisations to guarantee that information security becomes an important component of the overall company strategy by incorporating security considerations into the process of strategic planning. Because of this alignment, a proactive approach to risk management is fostered, in which security measures are designed to meet the aims of the organisation while also addressing possible risks and weaknesses.

2. Service Design: The term "Service Design" refers to the process of meticulously designing information technology services that are both successful and efficient within an organisation. The development of service architectures, procedures, operational policies, and documentation are all included in its scope. In this phase, organizations outline how information technology services will meet the requirements of the business, taking into consideration a variety of factors, including scalability, availability, and performance. The incorporation of security needs into the design of information technology services and systems is an essential component of service design. This is relevant within the context of information security. Consequently, this guarantees that security issues are not an afterthought but rather are integrated without any disruption from the very beginning. The integration of security design principles, access restrictions, encryption methods, and data protection measures into the architecture of information technology services results in the establishment of a foundation that is both resilient and secure for the entirety of the service lifetime.

ISO 27000

Description of security framework:

According to the author, the ISO 27000 series consists international standards, which provide a systematic and comprehensive approach to information security management systems. The International Organisation has developed it for Standardization, in which the guidelines and practices are defined to establish, implement, maintain, and continually improve the existing security management structure of the business. According to the article, the author highlighted one of the key components, which serves as a core standard, in which requirements are outlined and helps to establish or maintain information systems. Risk management is one of the components, in which the requirements analysis is a major step that outlines the requirements needed to establish and maintain an ISMS (Meriah & Arfa Rabai, 2019). It will provide a risk-based framework, which allows businesses to identify, assess, and mitigate information security risks. Along with this, ISO27002 offers set of security controls and best practices through the implementation of security framework ISO27001 can be done. In this, a wide range of areas like access control, cryptography, physical security, and incident management are included.



Figure 2: ISO Series Standards

Key Components of ISO27000 framework

ISO 27001: Information Security Management System (ISMS) - Requirements

ISO 27001 is a standard that outlines the standards that must be met in order to establish, implement, maintain (Kitsios et al., 2023), and continuously improve an information security management system (ISMS) within the context of an organization's overall potential business risks. Additionally, it offers a risk-based approach to the management of information security.

Treatment and risk assessment are the two most important components.

- The policy and objectives of information security.
- In addition, control objectives and controls.
- Commitment and support from management.
- processes that are always being improved.

ISO 27002: Code of Practice for Information Security Controls

The International Organisation for Standardisation (ISO) 27002 offers a comprehensive collection of security controls and best practices that supplement the execution of ISO 27001. In addition to providing direction on the design (Disterer, 2013) and implementation of controls, it covers a wide variety of information security-related subjects.

Access control is one of the key components.

- Using cryptography.
- The protection of both the environment and the body.
- Security incident management and response.
- Both business continuity and disaster recovery are important.

ISO 27003: Information Security Management System Implementation Guidance

ISO 27003 provides practical assistance for implementing an ISMS that is based on the standards of ISO 27001. It offers a systematic approach to the establishment, installation, operation, monitoring, evaluation, and maintenance of an information security management system (ISMS), as well as the continued improvement of the system.

Planning for the installation of the ISMS is a key component.

- Specifications for the documentation.
- Evaluating and managing potential dangers.
- Observation and evaluation of activity.
- Audits and reviews conducted among employees.

ISO 27005: Information Security Risk Management

ISO 27005 is a standard that focuses exclusively on information security vulnerability management. It offers organisations recommendations for efficiently assessing and managing information security risks, so assisting them in making educated decisions regarding the treatment and acceptance of hazards.

Process of risk assessment is one of the key components.

- The process of identifying and managing risks.
- Assessing and treating potential dangers.
- A review and monitoring of the risks.
- Consultation and communication are involved.

NIST Cyber-Security Framework

Description

NIST cyber-security framework is defined as a set of voluntary standards, guidelines, and best practices, which are designed to help the business manage and improve the cyber-security risk management process. NIST developed this framework and offers a common language used to understand, manage and express cyber-security, which aligns according to the needs of business. NIST cyber-security framework is relevant to the infrastructure sectors and has been applicable across numerous industries. The author defined five key functions, namely identify, protect, detect, respond, and recovery, which are used to manage the important assets of the business.

Key Components of NIST Cyber-security Framework

Identify:

Description: This function entails gaining an awareness of the context in which the organisation operates, laying the groundwork for efficient cybersecurity management, and generating a comprehensive comprehension of the assets, risks, and vulnerabilities.

- Asset management is one of the key components.
- The environment of companies.
- Governance, risk, and compliance, respectively.
- An analysis of the risks.



Figure 3: NIST Cyber-security framework

Protect:

Description: The Protect function is concerned with the implementation of safeguards and controls in order to guarantee the supply of services related to critical infrastructure. Measures to control and safeguard against risks that have been identified are the primary emphasis of this (Moreira et al., 2021).

- Access control is one of the key components.

- Data protection and backup.
- Training and awareness are both important.
- Technology designed to protect.

Detect:

Description: The Detect function is responsible for determining whether or not a cybersecurity event has taken place. In addition to this, it involves the creation and implementation of capabilities that allow for the timely identification of anomalies, occurrences, and incidents.

- Anomalies and happenings are the most important components.
- Maintaining a constant watch.
- Detection processes.

Respond:

Description: The primary purpose of this function is to respond to a cybersecurity incident that has been discovered. Among these are the implementation of reaction plans, the coordination of communication, the reduction of the impact of incidents, and the acquisition of knowledge from the experience.

- Response planning is one of the key components.
- Communication and analysis are both important.
- Risk reduction.

Recover:

Description: The Recover function is responsible for restoring and sustaining key infrastructure services that have been disrupted as a result of a cybersecurity event. The process entails the creation and execution of recovery plans, the enhancement of resilience, and the acquisition of knowledge from incidents.

- Recoveries planning is one of the key components.
- Advancements made.
- It is communication.

- The act of coordinating.

COBIT (Control Objectives for Information and Related Technologies)

The framework stands for control objectives for information and related technologies, as discussed by the author, and has been developed by ISACA. In this framework, a set of guidelines and best practices are defined for the easy management of IT enterprise systems. It has been assigned to align IT activities with business goals, ensure risk management for business, and develop a framework for IT governance and control. One of the key principles of this framework is that it aligns information technology with business objectives and is able to satisfy the stakeholder needs. Furthermore, a holistic approach can be followed to manage IT governance (Ghildyal & Chang, 2017), which can cover the entire organisations. In this, the integration of numerous frameworks and standards can be done for seamless governance and to address every aspect of the business. Another major component described by the author is enabled, in which foundational rules and guidelines can be designed for the management. The structures of the business can be defined in order to support IT governance and encourage positive and ethical systems.

Components of COBIT

COBIT Processes:

Description: COBIT defines a set of processes that organizations can implement to achieve effective IT governance. These processes are organized into four domains: Plan and Organize, Acquire and Implement, Deliver and Support, and Monitor and Evaluate.

Key Components:

- Plan and Organize:
 - Establishing the context for IT governance and defining a strategic direction (Dairo et al., 2021) .
- Acquire and Implement:
 - Identifying solutions and acquiring, implementing, and maintaining them.
- Deliver and Support:

- Ensuring the delivery of IT services and providing support for ongoing operations.
- Monitor and Evaluate:
 - Monitoring performance, ensuring compliance, and evaluating the effectiveness of IT governance.



Figure 4: Components of COBIT

3. COBIT Maturity Models:

Description: COBIT includes maturity models that help organizations assess their current state of IT governance maturity (Rea-Guaman et al., 2017) and identify areas for improvement.

Maturity models are available for each COBIT process.

Key Components:

- Maturity Levels:
 - Level 0 - Nonexistent: Processes are not performed.
 - Level 1 - Initial: Processes are ad hoc and chaotic.

- Level 2 - Repeatable: Basic processes are established, but success depends on individual effort.
- Level 3 - Defined: Processes are documented and standardized.
- Level 4 - Managed: Processes are monitored and measured for performance (Al-Matari et al., 2021).
- Level 5 - Optimized: Continuous improvement is ingrained in the organization's culture.

Designing own security framework for NatureGarden

1. Governance and Risk Management as a Foundation

1.1 Structure of Governance

NatureGarden will develop an Information Security Steering Committee, which will be in charge of:

- Supervising the security framework's creation, implementation, and management.
- Approval of security policies, standards, and large-scale security efforts (Alraja et al., 2023).
- Assuring that information security and business objectives are in sync.

1.2 Risk Control

NatureGarden will undertake a comprehensive risk management strategy, which will include the following steps:

- Regular risk assessments are performed in order to detect and prioritise information security issues.
- Risk mitigation techniques are developed depending on the business impact and possibility.
- Continuous risk monitoring and reassessment as the business landscape changes.

2. Policy and Adherence

2.1 Security Procedures

NatureGarden will create and enforce a set of security policies that will include:

- Data security and privacy.
- User permissions and access control.
- Response and reporting of incidents (Ke & Yongzhen, 2021).
- Use of IT resources that is acceptable.

2.2 Regulatory Adherence

NatureGarden will implement a compliance programme to ensure:

- Compliance with applicable laws, regulations, and industry standards.
- Policies and procedures must be updated on a regular basis to remain compliant.
- Third-party audits are performed on a regular basis to ensure compliance.

3. Identity and Access Management

3.1 Security Policies

NatureGarden will put in place access control policies such as:

- The notion of least privilege applies to user access.
- User access privileges should be reviewed on a regular basis.
- For important systems, multi-factor authentication is used.

3.2 Identity Administration

NatureGarden will implement an identity management system in order to:

- Manage user identities and access rights more effectively.
- Processes for onboarding and offboarding should be automated.
- Ensure that user information is correct and up to date.

4. Infrastructure Protection

4.1 Network Safety

NatureGarden will protect the network by implementing the following measures:

- Strong firewalls and intrusion detection/prevention systems are required.
- During transmission, sensitive data is encrypted.
- Regular network monitoring for unusual activity.

4.2 Endpoint Protection

NatureGarden will keep endpoints secure by:

- Antivirus software is being deployed and updated on all devices.
- Device encryption is being used to protect data.
- Endpoint security configurations are enforced.

5. Business Continuity and Incident Response

5.1 Incident Response Strategy

NatureGarden will create an incident response strategy that includes the following elements:

- Procedures for identifying and responding to security events must be clearly defined.
- Plans for communicating with internal and external stakeholders.
- Sessions for post-incident reviews and lessons learnt.

5.2 Disaster Recovery and Business Continuity

NatureGarden will develop business continuity and catastrophe recovery plans, which will include:

- Clearly defined roles and responsibilities in the event of a disruption.
- Testing and updating continuity and recovery plans on a regular basis (Sahebjamnia et al., 2015).
- Strategies for keeping key services running during and after incidents.

6. Employee Education and Awareness

6.1 Security Awareness Training

NatureGarden will launch a security awareness campaign by:

- Organising frequent security best practices training sessions.
- Increasing public knowledge of phishing, social engineering, and other risks (Khando et al., 2021).
- Continuing education to keep personnel informed about changing threats.

6.2 Mechanisms for Reporting

NatureGarden will implement anonymous reporting mechanisms such as:

- Employees should be encouraged to report security events or concerns.
- Providing several reporting channels, such as a dedicated hotline or an internet portal.
- Creating a culture in which reporting is encouraged without fear of retaliation.

7. Inspection and auditing

7.1 Security Surveillance

NatureGarden will implement continuous security monitoring, which will include the following:

- Security information and event management (SIEM) tools are being deployed.
- Real-time log analysis and notifications for questionable activity.
- Monitoring findings informed incident response.

7.2 Audits and assessments on a regular basis

NatureGarden will do frequent audits and assessments, which will include:

- External penetration testing and vulnerability assessments are both performed.
- Internal audits are performed to assess the efficacy of security controls.
- Audit findings drive continuous improvement.
- Management of Third-Party Risks.

8.1 Vendor Security Evaluation

NatureGarden will adopt a vendor security evaluation methodology, which will include the following steps:

- Third-party security procedures and controls are being assessed.
- Vendors' adherence to security standards is regularly monitored.
- Collaboration with suppliers to identify and address security issues.

Conclusion

The dynamic nature of international business, in conjunction with the growing dependence on technology, highlights the paramount significance of strong information security frameworks. This paper intends to assist NatureGarden (NG) in creating a customised approach to information system security, governance, and compliance by thoroughly examining well-known frameworks like ITIL, ISO 27000, NIST Cyber-Security Framework, and COBIT. These frameworks offer insightful information about establishing security controls, coordinating IT services with business goals, and cultivating a continuous improvement culture. NG can create its own security strategy by utilising the advantages of each model and placing a strong emphasis on governance, risk management, policy adherence, identity and access control, infrastructure protection, business continuity, incident response, staff training, and routine inspections and audits. NG can strengthen its defences, safeguard confidential information, and lessen the impact of the constantly changing threat landscape by combining these elements into a coherent framework that promotes a safe and reliable IT environment. The report also highlights the need for ongoing updates to regulations and standards due to the dynamic nature of cyber threats. It also emphasises the importance of governance, strategic planning, risk management, security policies, contingency planning, protection mechanisms, and service level agreements in providing thorough and efficient information security. The report essentially functions as a strategic roadmap to help NG traverse the intricate world of information security, encouraging a proactive and flexible approach to protecting company data, intellectual property, and stakeholders' trust in a constantly changing digital environment.

References

- Ahmad, N. and Shamsudin, Z.M. (2013) 'Systematic approach to successful implementation of ITIL', *Procedia Computer Science*, 17, pp. 237–244. doi:10.1016/j.procs.2013.05.032.
- Al-Ashmoery, Y. *et al.* (2021) 'Impact of IT service management and ITIL framework on the businesses', *2021 International Conference of Modern Trends in Information and Communication Technology Industry (MTICTI)* [Preprint]. doi:10.1109/mticti53925.2021.9664763.
- Al-Matari, O.M.M. *et al.* (2021) 'Adopting security maturity model to the organizations' capability model', *Egyptian Informatics Journal*, 22(2), pp. 193–199. doi:10.1016/j.eij.2020.08.001.
- Alraja, M.N., Butt, U.J. and Abbod, M. (2023) 'Information security policies compliance in a global setting: An employee's perspective', *Computers & Security*, 129, p. 103208. doi:10.1016/j.cose.2023.103208.
- Dairo, M. *et al.* (2021) 'Benchmarking strategic alignment of business and IT strategies: Opportunities, risks, challenges and solutions', *International Journal of Information Technology*, 13(6), pp. 2191–2197. doi:10.1007/s41870-021-00815-7.
- Disterer, G. (2013) 'ISO/IEC 27000, 27001 and 27002 for information security management', *Journal of Information Security*, 04(02), pp. 92–100. doi:10.4236/jis.2013.42011.
- Ghildyal, A. and Chang, E. (2017) 'It governance, IT/business alignment and organization performance for public sectors', *Journal of Economics, Business and Management*, 5(6), pp. 255–260. doi:10.18178/joebm.2017.5.6.522.
- Ke, Z. and Yongzhen, L. (2021) 'Research on internet data security and privacy protection', *Journal of Physics: Conference Series*, 2005(1), p. 012004. doi:10.1088/1742-6596/2005/1/012004.
- Khando, K. *et al.* (2021) 'Enhancing employees information security awareness in private and public organisations: A systematic literature review', *Computers & Security*, 106, p. 102267. doi:10.1016/j.cose.2021.102267.
- Kitsios, F., Chatzidimitriou, E. and Kamariotou, M. (2023) 'The ISO/IEC 27001 information security management standard: How to extract value from data in the IT sector', *Sustainability*, 15(7), p. 5828. doi:10.3390/su15075828.
- Lopes, S.F. (2021) 'The importance of the ITIL framework in managing information and Communication Technology Services', *International Journal of Advanced Engineering Research and Science*, 8(5), pp. 292–296. doi:10.22161/ijaers.85.35.

- Meriah, I. and Arfa Rabai, L.B. (2019) 'Comparative study of ontologies based ISO 27000 Series Security Standards', *Procedia Computer Science*, 160, pp. 85–92. doi:10.1016/j.procs.2019.09.447.
- Moreira, F.R. *et al.* (2021) 'Evaluating the performance of NIST's framework cybersecurity controls through a constructivist multicriteria methodology', *IEEE Access*, 9, pp. 129605–129618. doi:10.1109/access.2021.3113178.
- Palilingan, V.R. and Batmetan, J.R. (2018) 'Incident management in academic information system using ITIL framework', *IOP Conference Series: Materials Science and Engineering*, 306, p. 012110. doi:10.1088/1757-899x/306/1/012110.
- Rea-Guaman, A.M. *et al.* (2017) 'Comparative study of cybersecurity capability maturity models', *Communications in Computer and Information Science*, pp. 100–113. doi:10.1007/978-3-319-67383-7_8.
- Sahebjamnia, N., Torabi, S.A. and Mansouri, S.A. (2015) 'Integrated Business Continuity and disaster recovery planning: Towards organizational resilience', *European Journal of Operational Research*, 242(1), pp. 261–273. doi:10.1016/j.ejor.2014.09.055.