

Research on Data Security, Governance and Compliance of NatureGarden

CONTENTS

I	Introduction	2
II	Survey of security frameworks	2
II-A	Information Technology Infrastructure Library (ITIL)	2
II-B	ISO/IEC 27000, 27001 and 27002 for Information Security Management	3
II-C	Control Objectives for Information and related Technology (COBIT)	4
II-D	Payment Card Industry Data Security Standard (PCI DSS)	4
III	Main Problems in current NatureGarden Data Security Management	5
III-A	Lack of security interest, lack of security awareness training and hardware	5
III-B	Lack of management directives	5
III-C	Reformulating Data Security Policy Enhancement Measures	5
III-D	Challenges in NatureGarden's Software intensive systems (SIS) Service Management	5
III-E	Identify the level of information assets for classified and hierarchical protection	6
IV	Optimization Scheme of NatureGarden Data Security Management	6
IV-A	Strategic Initiatives for Strengthening Information Security	6
IV-B	Key Pillars for Advancing Organizational Information Security	6
IV-C	Implementing a Holistic Approach to Service Quality and Information Security	7
IV-D	Refining SLAs for Enhanced Business Alignment and Transparency	7
IV-E	Strategic Framework for Information Asset Protection and Risk Mitigation	8
V	Information Security in a Digitally-Integrated World	8
V-A	The Societal Imperative for Robust Cybersecurity	8
V-B	The Business Mandate for Adaptive Security Measures	9
VI	Conclusion	9
	References	9

Abstract

In the modern business landscape, organizations are increasingly dependent on information technology, presenting numerous challenges in information security. Drawing from an analysis of relevant literature, this paper investigates NatureGarden's data security, governance, and compliance frameworks, evaluating established standards like ITIL, ISO/IEC 27000, COBIT, and PCI DSS. It identifies key challenges in NatureGarden's current security posture, including a deficiency in security awareness and management directives. Strategic responses involve formulating tailored security policies and risk management procedures. The paper proposes an optimization scheme for NatureGarden's security management, emphasizing the necessity of regular updates to SLAs and security practices to keep pace with technological advances and maintain robust cybersecurity in line with global standards. As a result, an information security management system has been established that aligns with the company's business objectives while adhering to international standards.

I. INTRODUCTION

The criticality of information technology (IT) security in both academic research and practical application is well recognized. It is reasonable to anticipate that its significance will only escalate in public and organizational domains. The ubiquity of internet connectivity and the widespread deployment of software services necessitate robust security measures to safeguard private and corporate assets, amidst intensifying legal and regulatory pressures.

Within IT management, charged with the creation and maintenance of secure IT infrastructures, IT security has emerged as a paramount concern and a significant challenge. The imperative for robust protection of IT resources is amplified by several factors: (1) The increasing digital transformation of company assets, including mission-critical data, proprietary knowledge, and business processes. (2) The growing reliance on IT for a myriad of tasks and processes, elevates IT security as a vital safeguard for not only operational integrity but also for preserving a company's reputation and market competitiveness. (3) The broadening scope of inter-organizational business transactions, necessitates that the integrity of supplier and customer assets is contingent upon the security of a company's information systems.

In the dynamic landscape of modern network services, internet-based companies like NatureGarden are encountering unprecedented challenges in internal management, particularly in safeguarding information security. The diversification of service products has not only expanded the horizons of possibility but has also complexified the boundaries of information security, extending it from the network's infrastructure to the intricacies of application layers.

This expansion demands a more sophisticated approach to managing service resources, overseeing service processes, and adeptly addressing security risks. Information security, therefore, is no longer confined to a set of technical tasks; it has evolved into a multifaceted issue that requires a blend of acute awareness and meticulous management.

To navigate this complex domain, NatureGarden must refine its security management capabilities by enhancing security measures, utilizing an effective information security management model for guidance, and establishing risk control as the cornerstone of its process. This paper aims to provide a roadmap for NatureGarden to build an information security system that not only adheres to the company's strategic needs and regulatory demands but also supports its swift development and innovation in the face of evolving cyber threats.

II. SURVEY OF SECURITY FRAMEWORKS

A. Information Technology Infrastructure Library (ITIL)

Information Technology Infrastructure Library (ITIL), is recognized as a 'best practice' framework specifically designed for Information Technology (IT) service management. It can be flexibly applied across various business environments. This framework introduces a systematic approach to managing IT services within organizations.

Originally developed in the late 1980s [1] by the Central Computer and Telecommunications Agency (CCTA) in the UK, as shown in Table I, ITIL has undergone several revisions and developments over

the years. The evolution of ITIL can be traced through its various versions, each reflecting advancements and changes in the field of IT service management. The latest iteration, ITIL v4, introduces four key dimensions, marking a significant evolution from ITIL v3. The previous version, ITIL v3, was structured around five core dimensions: service strategy, service design, service transition, service operation, and continual service improvement. These dimensions collectively provided a comprehensive framework for delivering and managing efficient IT services.

TABLE I
ITIL FRAMEWORK HISTORY

Framework	Years	No of Volumes Incorporated in the framework
ITIL	1989-1995	31
ITIL v2	2000-2004	7
ITIL v3	2007-2018	5
ITIL v4	2019-now	4

The following is an explanation of the five components in ITIL v3:

(1) Service Strategy: This foundational element emphasizes the strategic approach to ITSM, treating it not merely as an operational task but as a vital strategic asset for the organization. It sets the overarching direction for managing and delivering services that align with the business's long-term objectives.

(2) Service Design: This component is concerned with the translation of the organization's service strategy into actionable plans. It involves the crafting of IT services that can fulfill the strategic objectives set forth by both IT and business stakeholders. It also identifies and incorporates necessary service assets, such as server resources and human capital, to bring these services to fruition. The design phase also addresses service performance, potential improvements, and service continuity considerations.

(3) Service Transition: This stage provides guidelines for IT organizations to implement and transition new or modified services from the design phase to live environments. It encompasses the testing and validation of services in operational settings predetermined by the organization, ensuring that they are ready for deployment.

(4) Service Operation: As the name suggests, this component encapsulates the day-to-day operations involved in managing IT services. It ensures that services are delivered effectively and efficiently, maintaining the value and performance expected by users and the business alike.

(5) Continual Service Improvement (CSI): CSI is dedicated to the ongoing enhancement of service quality and the management processes supporting them. It employs quality management principles and methodologies to perpetually refine the efficiency and effectiveness of services and processes, even if current service levels meet customer and business satisfaction. Recognizing that business requirements are ever-evolving, CSI aims to foster a culture of continuous development and adaptation within the organization.

Each of these components is integral to the ITIL lifecycle, with specific focal points addressed within each stage to maintain the framework's integrity and utility.

B. ISO/IEC 27000, 27001 and 27002 for Information Security Management

As the importance of information technology continues to grow, so does the urgency for effective information security measures. Establishing a systematic approach to information security management has become a paramount initiative within IT management. Ever since the public became aware of privacy breaches, security lapses, fraudulent accounting practices, and assaults on IT infrastructures, there has been a marked recognition by organizations of their duty to protect both physical and informational assets. Security standards serve as a strategic guide or framework to devise and uphold a robust Information Security Management System (ISMS). The ISO/IEC 27000 series, including standards 27001 and 27002, are internationally recognized benchmarks that are gaining widespread acceptance. Often described as

the global ‘lingua franca’ for information security [2], these standards enable organizations to have their ISMS independently certified, offering their clientele verifiable proof of their security protocols.

Various research efforts have been dedicated to juxtaposing security ontologies, employing specific methodologies to discern key parameters such as applied concepts, the nature of the ontology, methodologies employed, language, and related software development dimensions [3], [4]. In examining ontologies derived from the ISO/IEC 27000 security standards, we delineated five comparative criteria rooted in an extensive review of the literature [3]–[5]:

- Alignment with the ISO 27k standard, including the integration of supplemental security standards and established best practices [3].
- The methodology deployed, alongside the process of evaluating and validating the ontology [4].
- The absence of pivotal security concepts [5].

TABLE II
COMPARISON CRITERIA BETWEEN ONTOLOGIES BASED ON ISO/IEC 27000 SERIES SECURITY STANDARDS

Ontologies references	ISO/IEC 27000 series	Missing security concepts	Integration of other standards	Methodology of design	Validation
Fenz et al. [6]	ISO/IEC 27001	Vulnerability, Risk	-	-	✓
Parkin et al. [7]	ISO/IEC 27002	Security Attribute, Risk	-	✓	✓
Fenz and Ekelhart [8]	ISO/IEC 27001	Risk	✓	-	✓
Milisovic and Goeken [5]	ISO/IEC 27002	-	-	✓	✓
Ramanuskaite et al. [9]	ISO/IEC 27001	Security Attribute, Risk	✓	-	✓
Agrawal [10]	ISO/IEC 27005	-	-	✓	✓

Table II presents our comparative analysis of the aforementioned security ontologies, leveraging the identified criteria to elucidate their respective advantages and constraints.

C. Control Objectives for Information and related Technology (COBIT)

COBIT, established by the Information Systems Audit and Control Association (ISACA), represents a compendium of best practices for IT governance. Its primary purpose is to bridge the prevalent chasm between business exigencies and technological solutions, providing technology auditors, senior executives, and technology practitioners with a structured approach to managing technological risks, thereby safeguarding the integrity of information systems.

The framework is underpinned by five core principles: Strategic Alignment, Value Delivery, Resource Management, Risk Management, and Performance Measurement. Additionally, COBIT encompasses 34 IT processes aimed at augmenting the efficacy of internal controls, particularly concerning the reliability of financial reporting.

D. Payment Card Industry Data Security Standard (PCI DSS)

The Payment Card Industry Data Security Standard (PCI DSS) encompasses a comprehensive suite of stipulations aimed at enhancing the security of payment account data. It sets forth an information security benchmark for entities that handle cardholder information from prominent credit card companies such as American Express, MasterCard Worldwide, and Visa Inc. The process of achieving PCI compliance is tripartite, involving evaluation, reform, and reporting [11].

The PCI DSS specifies 12 principal requirements for control measures, categorized under themes such as network security, cardholder data protection, vulnerability management software, access control measures, network monitoring, and testing, as well as the formulation of an information security policy. Each requirement is further delineated into more detailed sub-requirements [12].

III. MAIN PROBLEMS IN CURRENT NATUREGARDEN DATA SECURITY MANAGEMENT

A. *Lack of security interest, lack of security awareness training and hardware*

- (1) Lack of a Formal Security Policy: NatureGarden lacks an established policy for managing its network security, which is fundamental for protecting data and intellectual property.
- (2) Insufficient Security Awareness: There is an absence of formal security awareness programs, which are essential for educating staff on recognizing and reporting security threats.
- (3) Inadequate Role Definition: The company has not clearly defined roles and responsibilities associated with security, leading to potential gaps in security enforcement.
- (4) Ineffective Risk Management: Current security measures may not adequately address the risks associated with integrating personal devices into the corporate network.

B. *Lack of management directives*

- (1) Insufficient Management Involvement: NatureGarden's security initiatives suffer from a lack of management directives, which are crucial for the success of any security awareness program.
- (2) Deficient Leadership: The absence of a dedicated leader with the requisite certifications and knowledge hinders the effective implementation of security measures.
- (3) Lack of Continuous Monitoring: There is a gap in the ongoing assessment and adjustment of security practices to address emerging threats and changes in the IT landscape.
- (4) Inadequate Enforcement Mechanisms: The company has not established sufficient mechanisms to enforce compliance with security policies among employees.
- (5) Insufficient Accountability Measures: Currently, there are no clear metrics or processes for holding individuals accountable for security lapses.

C. *Reformulating Data Security Policy Enhancement Measures*

- (1) Lack of Specific Security Policy: NatureGarden has not developed a security policy that aligns with its distinct security necessities, which is critical for effective security management.
- (2) Non-adherence to Standards: The company's security management documentation inadequately reflects current national policies and industry standards.
- (3) Fragmented Security Management Structure: There is an absence of a cohesive top-down security management architecture that includes strategy, systems, processes, and records.
- (4) Vague Information Security Strategy: NatureGarden's information security management lacks a clear strategic direction, resulting in ambiguous security protocols and practices.

D. *Challenges in NatureGarden's Software intensive systems (SIS) Service Management*

- (1) Focus on Effort Over Outcomes: NatureGarden's Service Level Agreement (SLA) predominantly emphasizes the efforts of service providers, such as response times, without ensuring alignment with the company's business goals and the effectiveness of services delivered.
- (2) Vague Service Metrics: Service level metrics, such as network availability, lack specificity in NatureGarden's context, creating ambiguity about their impact on the company's operations.
- (3) Incomplete Service Agreements: Current SLAs may not fully address critical services like security control or disaster recovery, crucial for NatureGarden's extensive online presence and data protection needs.
- (4) Inadequate Cost Management: NatureGarden's approach to cost management for SIS services appears to be opaque, often leading to fixed pricing that does not correlate with individual service requirements or customer value.

E. Identify the level of information assets for classified and hierarchical protection

(2) Vulnerability to Cyber Threats: Sensitive data across various information assets are exposed to risks such as hacking and data breaches, due to undefined security strategies.

(4) Lack of Intellectual Property Protection: Intellectual property, critical to the company's value, is inadequately protected due to the absence of specific security policies.

A. Strategic Initiatives for Strengthening Information Security

(2) **Security Awareness Training:** Development of a comprehensive security awareness program tailored to different roles within the organization, ensuring all staff are informed and vigilant.

(4) Enhanced Risk Management: Adopting a tiered approach to risk management that encompasses technical, organizational, and human factors, particularly focusing on the integration of personal devices.

(1) Enhanced Management Participation: Encourage active management engagement and support for the security awareness program throughout the NFC lifecycle.

(3) Establishment of Accountability Metrics: Create responsibility assessment metrics that allow the operational team to make joint decisions and enable continuous improvement.

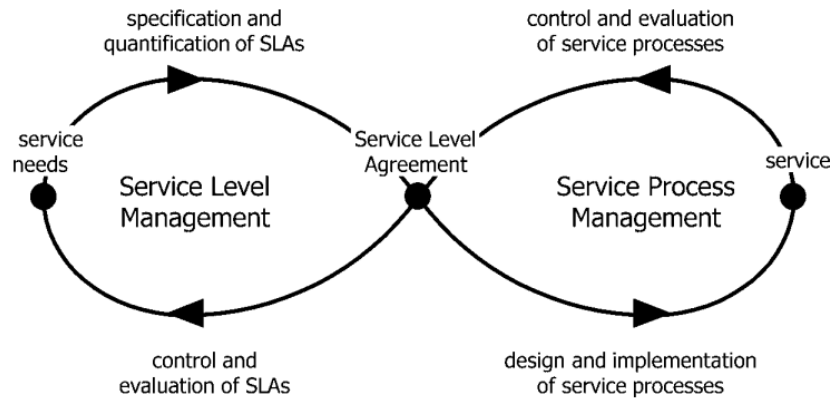


Fig. 2. The Service Management Lemniscate.

(4) Proactive Governance Team: Form a governance team that actively monitors and measures the progress of security implementations and reacts promptly to any issues.

(5) Regular Review and Adaptation: Implement a system of regular reviews and adapt security procedures and policies to align with global operational standards and address any identified obstacles.

(6) Security Compliance Enforcement: Develop a method to enforce security awareness programs and incorporate security metrics to gauge the performance of management and staff.

As shown in Fig 1, illustrates the complete model with the ten internal and external influences as well as the broad categories of Information Security Governance and the Organization Information Security Office. The complete model shows each of the identified categories.

C. Implementing a Holistic Approach to Service Quality and Information Security

Service quality is defined in the literature as meeting or surpassing customer expectations, yet a persistent gap often exists between customer needs and service delivery. To address this, the Service Management Lemniscate model has been introduced, promoting an iterative and continual process of service design, implementation, and improvement, as shown in Fig. 2.

(1) Development of a Tailored Security Policy: Craft a security policy and strategy that aligns with NatureGarden's particular security requirements.

(2) Conformity with Regulatory Standards: Update and improve security management documentation to conform with national policies and industry standards.

(3) Integrated Security Management System: Establish an integrated security management system with a clear hierarchy that encapsulates strategy, management systems, operational procedures, and records based on internal security management needs.

(4) Clear Strategic Security Direction: Introduce an explicit information security management policy and strategy at the organizational level to foster a culture of comprehensive security awareness and foundational security principles.

(5) Defining Security Approach and Tactics: Clarify the company's security approach by formulating a distinct information security management strategy, thus guiding the workforce in standardized operational procedures.

D. Refining SLAs for Enhanced Business Alignment and Transparency

(1) Outcome-Oriented SLAs: Refine NatureGarden's SLAs to guarantee outcomes that directly support the company's objectives, such as enhancing online customer experience or ensuring e-commerce platform stability.

(2) Clarified Service Definitions: Define service availability and other metrics in terms that reflect NatureGarden's operational needs, such as peak traffic management for their e-commerce portal.

(3) Holistic Service Specifications: Expand SLAs to thoroughly cover essential services like cybersecurity measures, considering NatureGarden’s global customer base and the value of its intellectual property.

(4) Transparent Cost Attribution: Develop a more granular cost management strategy that aligns with the specifics of NatureGarden’s service consumption, enabling a clearer understanding of price-performance ratios for each service.

TABLE III
NATUREGARDEN CLASSIFICATION OF INFORMATION ASSETS

Secrecy Level	Description	Example	Influence Level
Top Secret Information	There are only a few specific employees in the company, and it is of great commercial value. Unauthorized use or leakage will significantly affect the company’s benefit and sustainable development.	Overall corporate strategy, undisclosed financial statements, intellectual property, etc.	Significant
Confidential Information	Difficult for outsiders to understand and has commercial value. Unauthorized use or leakage can greatly impact the company’s operations and employee interests.	Business plans, information about high net worth customers, sensitive business information, etc.	Serious
Internal Disclosure	Information not to be made public by the company. Unauthorized use or leakage can have adverse effects on the company or employees.	Internal memos, address books, meeting minutes, etc.	Limited
External Disclosure	Information that has been publicly disclosed by the company and can be obtained freely. Leakage does not threaten the company or employees.	Published financial reports, information on the official website, etc.	None

E. Strategic Framework for Information Asset Protection and Risk Mitigation

(1) Asset Identification and Classification: Establish a clear process for identifying and classifying information assets based on their level of sensitivity and value to the organization.

(2) Robust Cybersecurity Measures: Implement comprehensive cybersecurity protocols to protect against unauthorized access and data breaches, particularly for sensitive data.

(3) Secure Device Policy: Develop and enforce policies for the secure use of personal devices within the company’s network to minimize the risk of data leakage.

(4) Intellectual Property Safeguards: Create specialized security measures for protecting the company’s intellectual property, ensuring confidentiality, and mitigating potential financial losses.

As presented in Table III, in alignment with the principles of information asset categorization, and taking into account the unique business model of NatureGarden, the company’s information assets have been methodically classified. A selection of these classifications is depicted in tabular form.

V. INFORMATION SECURITY IN A DIGITALLY-INTEGRATED WORLD

A. The Societal Imperative for Robust Cybersecurity

The exponential growth of the Internet has led to its integration into virtually all societal functions, resulting in the circulation of massive amounts of data, including sensitive information, across cyberspace. This trend has significant implications for national security and societal stability, underscoring the importance of continuously updating information security regulations and standards. Aligning these regulations with the evolving technological environment and corporate objectives is crucial for maintaining comprehensive network security controls, which in turn supports the broader objectives of national security and the prosperity of the economy and public welfare.

B. The Business Mandate for Adaptive Security Measures

For companies like NatureGarden, which operates in the internet services sector, the advent of cloud computing and related technologies represents a paradigm shift that demands an agile and informed approach to information security. The protection of personal data and the integrity of vast informational datasets are critical concerns with far-reaching societal and corporate ramifications. Timely updates to information security management regulations and standards are vital to prevent obsolescence due to rapidly evolving industry and policy landscapes. Internet companies must proactively seek and implement strategic solutions to these emerging security challenges, ensuring the continuation of their business trajectory amidst potential risks. Embracing updated regulations and standards for information security management in the current technological context will guide companies in refining their security strategies, compliance measures, and overall system-centric security frameworks, enhancing the management of cloud service security.

VI. CONCLUSION

This paper has examined the Information Technology Infrastructure Library (ITIL) and the ISO 27000 framework to propose a restructured information security system for NatureGarden, tailored for cloud computing services. By addressing these deficiencies with the proposed improvements, NatureGarden can enhance its security posture and ensure the sustained protection of its assets and client information. As the Internet evolves, propelled by advancements in cloud computing, mobile technologies, and big data, it promises a more diverse developmental landscape and a plethora of services enriching all aspects of social life.

In pursuit of overarching network security, it is critical to engage in continuous refinement within the information security domain, guided by international security policies and leveraging cutting-edge security management standards. Internet service providers, pivotal to the network service ecosystem, must swiftly acclimate to technological and business developments to enhance the Internet service experience. Concurrently, they are tasked with the formidable challenge of mitigating the evolving network security risks.

The discourse presented in this paper underscores the importance of regularly updating legal frameworks and standards to bolster network security management amidst emerging information technologies. The findings aim to empower NatureGarden with the capability to proactively identify new business security risks and enforce efficacious security controls, thereby fortifying its position in the ever-changing digital landscape.

REFERENCES

- [1] F. Cervone, "Itil: a framework for managing digital library services," *OCLC Systems & Services: International digital library perspectives*, vol. 24, no. 2, pp. 87–90, 2008.
- [2] E. Humphreys, "Information security management system standards," *Datenschutz und Datensicherheit-DuD*, vol. 35, pp. 7–11, 2011.
- [3] C. Blanco, J. Lasheras, E. Fernández-Medina, R. Valencia-García, and A. Toval, "Basis for an integrated security ontology according to a systematic review of existing proposals," *Computer Standards & Interfaces*, vol. 33, no. 4, pp. 372–388, 2011.
- [4] V. Singh and S. Pandey, "A comparative study of cloud security ontologies," in *Proceedings of 3rd International Conference on Reliability, Infocom Technologies and Optimization*. IEEE, 2014, pp. 1–6.
- [5] D. Milicevic and M. Goeken, "Ontology-based evaluation of iso 27001," in *Software Services for e-World: 10th IFIP WG 6.11 Conference on e-Business, e-Services, and e-Society, I3E 2010, Buenos Aires, Argentina, November 3-5, 2010. Proceedings 10*, 2010, pp. 93–102.
- [6] S. Fenz, G. Goluch, A. Ekelhart, B. Riedl, and E. Weippl, "Information security fortification by ontological mapping of the iso/iec 27001 standard," in *13th Pacific Rim International Symposium on Dependable Computing (PRDC 2007)*. IEEE, 2007, pp. 381–388.
- [7] S. E. Parkin, A. van Moorsel, and R. Coles, "An information security ontology incorporating human-behavioural implications," in *Proceedings of the 2nd International Conference on Security of Information and Networks*, 2009, pp. 46–55.
- [8] S. Fenz and A. Ekelhart, "Formalizing information security knowledge," in *Proceedings of the 4th international Symposium on information, Computer, and Communications Security*, 2009, pp. 183–194.
- [9] S. Ramanauskaitė, D. Olifer, N. Goranin, and A. Čenys, "Security ontology for adaptive mapping of security standards," *International Journal of Computers, Communications & Control (IJCCC)*, vol. 8, no. 6, pp. 813–825, 2013.
- [10] V. Agrawal, "Towards the ontology of iso/iec 27005: 2011 risk management standard," in *HAISA*, 2016, pp. 101–111.
- [11] S. Yulianto, C. Lim, and B. Soewito, "Information security maturity model: A best practice driven approach to pci dss compliance," in *2016 IEEE Region 10 Symposium (TENSYP)*. IEEE, 2016, pp. 65–70.

- [12] A. Ukidve, D. Smantha, and M. Tadvaka, "Analysis of payment card industry data security standard [pci dss] compliance by confluence of cobit 5 framework," *International Journal of Engineering Research and Applications*, vol. 7, no. 01, pp. 42–48, 2017.