

Apply the principles and practices of Data security, Governance and Compliance based on a given scenario

Module:	Data Security, Governance and Compliance
ID number:	2300263
Programme:	MSc Software Engineering and AI
Name:	Yue Yu
Lecturer:	Assoc. Prof. Carlene Campbell

6/1/2024

Abstract

With globalisation, businesses are increasingly reliant on information technology, which has created new cybersecurity challenges. According to a report by BSI America, globalisation, specialisation and digital transformation are major threat factors to digital and physical supply chains. With the globalisation of the industry, organisations are directly affected by the cyber related risks they face^[1]. Cyber attacks are growing exponentially in organisations and societies across the globe, now occurring every two seconds. This trend poses a serious challenge for companies that rely heavily on the Internet and information technology, such as NatureGarden (NG).

NG is a global brand that sells healthy living products and its business model relies heavily on online services and social media. However, this also exposes the company to significant information security challenges such as securing customers' and employees' personal data, preventing intellectual property theft, and responding to cyberattacks. The risk of data leakage and unauthorised access is particularly acute where employees and customers are allowed to use their personal devices to access company network resources. For this reason, developing an effective information systems security strategy is critical to protecting NG's business interests and preserving its reputation in the marketplace.

This thesis will explore and design a comprehensive information system security programme to address these challenges faced by NG. By examining different security frameworks and models such as the Information Technology Infrastructure Library (ITIL) and the International Organisation for Standardisation (ISO) 27000 series, the aim is to come up with a bespoke security strategy that is suitable for NG.

Key Words: data, ITIL, ISO

Directory

1. Security Frameworks And Models.....	1
1.1 Information Technology Infrastructure Library (ITIL)	1
1.2 International Organisation For Standardisation (ISO) 27000 series	2
1.3 Comparative Analysis	4
2. Information Systems Security	6
2.1 Integrated Security Strategy and Governance	6
2.2 Risk Assessment And Management.....	6
2.3 Security Implementation And Emergency Response.....	7
3. Importance of Updating Regulations	9
3.1 Evolution of Technologies And Threats.....	9
3.2 Changes In Compliance.....	10
3.3 Case Studies	10
4.Conclusion.....	11
Reference	13

1. Security Frameworks And Models

1.1 Information Technology Infrastructure Library (ITIL)

The Information Technology Infrastructure Library (ITIL) is a comprehensive set of practices for IT service management (ITSM) that focuses on aligning IT services with the needs of business. It emerged in the 1980s, developed by the UK government, with the aim of providing a standardized approach to IT service management. This framework has undergone several revisions over the years, adapting to the changing IT landscape.

The most recent version, ITIL 4, introduced in 2019, marks a significant shift towards a more holistic, flexible, and adaptable approach. Unlike its predecessors, ITIL 4 emphasizes the importance of co-creating business value, focusing on continuous improvement and adapting to the digital era. It is designed to be more agile, flexible, and adaptable to various types of organizations and technology environments.

ITIL 4 is underpinned by a set of guiding principles that form the core of its framework. These principles include:

Focus on Value: Everything ITIL does is driven by the need to create value for the business and its customers.

Start Where You Are: It advises against unnecessary changes and suggests leveraging existing services and processes.

Progress Iteratively with Feedback: Emphasizes the importance of incremental improvements and learning from feedback.

Collaborate and Promote Visibility: Encourages teamwork and transparency across the organization.

Think and Work Holistically: Recognizes the interconnected nature of ITSM and the need for an integrated approach.

Keep It Simple and Practical: Advises simplifying processes and only doing what

is necessary.

Optimize and Automate: Promotes the use of technology to improve efficiency and effectiveness.

These guiding principles help organizations adopt a more comprehensive and integrated approach to ITSM, ensuring that IT processes and services are aligned with business objectives and are delivering maximum value. ITIL 4 also integrates concepts from other methodologies like Agile, DevOps, and Lean, reflecting the need for a more dynamic IT environment.

The framework structure of ITIL, depicted in diagrams like Figure 1, provides a visual representation of these principles and how they interact with various components of IT service management. This structure helps organizations understand how to implement ITIL practices effectively and how they can be adapted to suit individual business needs..



Figure 1 ITIL framework structure diagram

1.2 International Organisation For Standardisation (ISO) 27000 series

The ISO 27000 series, encompassing a range of international standards, is centered around information security management systems (ISMS). It is designed to assist organizations in establishing, implementing, maintaining, and continually enhancing their information security management. This series is critical for organizations aiming to safeguard their information assets, which include not only internal data like employee details and financial records but also sensitive information from customers and business

partners.

Key aspects of the ISO 27000 series include:

Systematic Risk Management: It emphasizes a structured approach to identifying, assessing, and managing information security risks. This process is essential for understanding the potential threats to an organization's information and devising effective strategies to mitigate them.

Compliance Guidance: The standards provide comprehensive guidance on meeting compliance requirements. This is particularly valuable for organizations that must adhere to various legal, regulatory, and contractual obligations concerning information security.

Information Security Governance: A strong focus is placed on governance, ensuring that information security is aligned with the overall strategic objectives of the organization and that there's accountability at all levels.

Continuous Improvement: The ISO 27000 series encourages organizations to adopt a mindset of continual improvement. This approach helps organizations stay ahead of evolving security threats and changing business environments.

Protection of Information Assets: The primary goal is to protect the organization's information assets. This includes everything from hardware and software to data and intellectual property.

Stakeholder Trust: By implementing these standards, organizations can enhance the confidence of customers, investors, and other stakeholders in their ability to manage information security risks.

Flexibility and Scalability: The standards are designed to be applicable to all types of organizations, regardless of their size, nature, or complexity.

Figure 2 typically illustrates the structure of the ISO 27000 series, showcasing the interrelation of various standards within this series and how they collectively contribute to a robust ISMS. This visual representation aids organizations in understanding the breadth of the ISO 27000 series and how its different components can be applied to establish a comprehensive and effective information security management system.

ISO 27000 Series of Standards



Figure 2 ISO 27000 series of standards

1.3 Comparative Analysis

ITIL and the ISO 27000 series, while distinct in their focus and approach, are complementary frameworks essential in the field of IT service management and information security^[2]. ITIL, with its roots in the 1980s and evolving over time to its latest iteration, ITIL 4, offers comprehensive guidance for managing and delivering IT services. It emphasizes aligning these services with business needs and covers various aspects such as strategy, design, transition, and operational execution. ITIL 4's guiding principles like focusing on value, starting from the current state, and progressing iteratively with feedback, highlight its adaptability and holistic approach.

In contrast, the ISO 27000 series, an international standard for information security management systems (ISMS), is centered around protecting information assets like employee data, financial information, and intellectual property. Its systematic approach to risk management, clear guidance on compliance, and emphasis on information security governance make it crucial for organizations looking to mitigate information security risks and enhance stakeholder trust. Its framework, adaptable to various organizational types, focuses on establishing, implementing, maintaining, and continually improving ISMS.

Organizations must consider their specific needs and objectives when selecting a

suitable framework. Some may benefit more from ITIL's specific guidance on IT service delivery, while others might find the ISO 27000 series' broad framework for information security more pertinent, especially regarding risk management and compliance. However, many organizations discover that a combination of both ITIL and ISO 27000 addresses their challenges in IT service management and information security more comprehensively. This synergistic use of both frameworks can lead to a more robust and effective management of IT services and security, leveraging ITIL's detailed processes and ISO 27000's strong emphasis on risk management and compliance. The integration of these frameworks provides a more holistic approach, ensuring not only the alignment of IT services with business strategies but also the protection and secure management of critical information assets.

Figure 3 compares ITIL and ISO 27000, often illustrating the similarities and differences in a structured format, making it easier for organisations to assess which framework (or a combination of the two) is best suited to their specific needs and objectives for managing IT services and information security. For decision makers, such comparisons are an important tool for aligning their IT strategies with business objectives and regulatory requirements.

Service Strategy (SS)	Service Design (SD)	Service Transition (ST)	Service Operation (SO)	Continual Service Improvement (CSI)
• Service management • Service life cycle • Service assets and value creation • Service provider types and structures • Strategy, markets and offerings • Financial management • Service portfolio management • Demand management • Organisational design, culture and development • Sourcing strategy • Service automation and interfaces • Strategy tools • Challenges and risks	• Balanced design • Requirements, drivers, activities and constraints • Service-oriented architecture • Business service management • SD models • Service catalogue management • Service level management • Capacity and availability • IT service continuity • Information security • Supplier management • Data and information management • Application management • Roles and tools • Business impact analysis • Challenges and risks • SD package • Service acceptance criteria • Documentation • Environmental issues • Process maturity framework	• Goals, principles, policies, context, roles and models • Planning and support • Change management • Service asset and configuration management • Release and deployment • Service validation and testing • Evaluation • Knowledge management • Managing communication and commitment • Stakeholder management • Configuration management system • Staged introduction • Challenges and risks • Asset types	• Balance in SO • Operational health • Communication • Documentation • Events, incidents and problems • Request fulfilment • Access management • Monitoring and control • Infrastructure and service management • Facilities and data centre management • Information and physical security • Service desk • Technical, IT operations and application management • Roles, responsibilities and organisational structures • Technology support to SO • Managing change, projects and risk • Challenges • Complementary guidance	• Goals, methods and techniques • Organisational change • Ownership • Drivers • Service level management • Service measurement • Knowledge management • Benchmarks • Models, standards and quality • CSI seven-step improvement process • Return on investment (ROI) and business issues • Roles • Authority matrix (RACI) • Support tools • Implementation • Governance • Communications • Challenges and risks • Innovation, correction and improvement • Best practices supporting CSI

Figure 3 Comparison of ITIL and ISO 27000

2. Information Systems Security

2.1 Integrated Security Strategy and Governance

Addressing NatureGarden's specific business needs began with the development of a comprehensive security strategy that took into account the characteristics of its global business, which relies on cloud services and wireless networks. This included assessing the security posture of the existing IT infrastructure, identifying critical assets, potential security vulnerabilities and areas for improvement. Of particular concern was protecting the security and integrity of customer data and transactional information.

To ensure information security and compliance, it is recommended that a centralised Information Security Management System (ISMS) be implemented, following the ISO 27000 standard. This involves the establishment of a cross-functional security management team responsible for overseeing and enforcing the information security policy. The governance structure should include an information security committee to monitor the implementation of the security policy and compliance with various international and regional data protection regulations.

Security policies should be developed to cover cyber security, physical security and employee security awareness education. Develop appropriate security guidelines and practices for mobile and remote work environments^[3]. The policy also needs to include detailed guidelines on data encryption, access control, password management, and how to securely handle and store sensitive data.

2.2 Risk Assessment And Management

Based on the NIST Cybersecurity Framework, it is critical to conduct regular risk assessment and management. This includes identifying and categorising potential risks such as cyberattacks, data breaches, and system failures, and then developing appropriate risk mitigation and response strategies. Risk management strategies should include risk mitigation measures, such as strengthening security measures at network

boundaries, implementing strict user access controls, etc.^[4]

At the heart of risk management is a comprehensive risk assessment framework that uses methods such as FAIR to quantify and prioritise risks. This involves regularly reviewing the effectiveness of existing security measures and developing mitigation strategies for identified high-risk areas, as shown in the risk assessment and management flowchart in Figure 4.

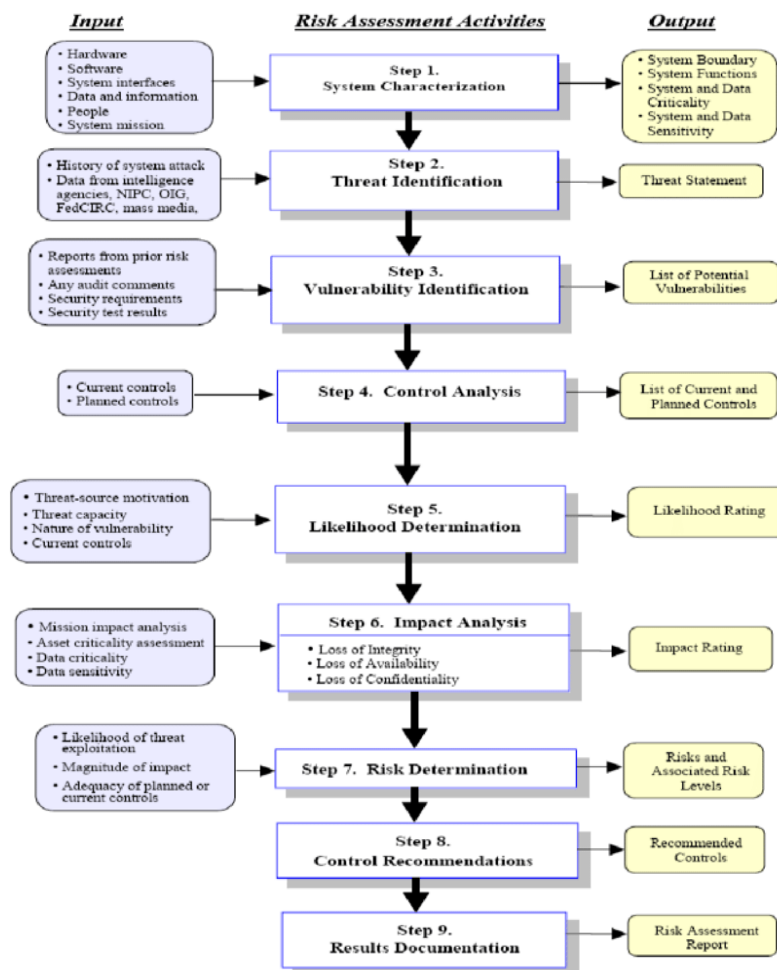


Figure 4 Risk assessment and management flowchart

2.3 Security Implementation And Emergency Response

Implementing robust security measures is paramount in safeguarding an organization's digital assets and infrastructure. Integrating specific security technologies such as firewalls, intrusion detection systems, data encryption, and multi-

factor authentication forms the cornerstone of a secure IT environment. These measures are essential in preventing unauthorized access, detecting potential breaches, securing sensitive data, and ensuring that only authenticated users have access to critical systems.

Adopting a hierarchical security control model is crucial for a comprehensive security strategy. This model should encompass technical controls, like the aforementioned security technologies, which provide a direct defense against threats. Additionally, administrative controls are necessary for defining and maintaining security policies, procedures, and standards, in line with the ISO 27000 series and NIST guidelines. These guidelines provide a structured framework for managing information security risks and ensuring compliance with legal and regulatory requirements. Physical controls, such as secure access to facilities and protection of physical equipment, further fortify the organization's defense against security incidents.

Incorporating a Security Information and Event Management (SIEM) system is vital for enhancing visibility and responsiveness to security events. A SIEM system collects and analyzes security-related data from various sources, enabling quick detection, analysis, and response to security incidents. This real-time monitoring is critical in identifying potential threats and mitigating risks promptly.

Developing and implementing a robust incident response plan is another critical component. This plan should outline a clear incident response process, designate responsible personnel and teams, and establish an effective communications strategy to handle security breaches efficiently. In the event of a security incident, a well-structured plan ensures that the organization can respond swiftly and effectively, minimizing potential damages.

Furthermore, a comprehensive data backup and disaster recovery plan is essential for the continuity and resilience of critical business functions. Regular backup exercises and disaster recovery drills ensure that the organization is prepared to quickly restore operations in the event of data loss or a catastrophic incident. These practices are crucial for maintaining business continuity, minimizing downtime, and protecting against data loss or corruption.

By integrating these layered security measures and adhering to established frameworks and guidelines, organizations can create a robust and resilient IT security posture, capable of defending against and responding to the evolving landscape of cyber threats.

3. Importance of Updating Regulations

3.1 Evolution of Technologies And Threats

The rapid advancement of technology, particularly in domains like cloud computing, big data, artificial intelligence (AI), and the Internet of Things (IoT), has ushered in a new era of security challenges. These technological innovations, while offering significant benefits, also introduce complex and evolving security threats.

Cloud computing, with its advantages in data storage and processing, brings specific concerns, especially in multi-tenant environments where data segregation is crucial. The risk of data breaches in such environments can be significant, necessitating advanced security protocols to protect sensitive information. Similarly, the emergence of big data has raised issues related to the storage, processing, and protection of large volumes of data, often including sensitive personal information.

The integration of AI in various systems adds another layer of complexity to security. AI systems, if not properly secured, can be manipulated or exploited, leading to potential risks in decision-making processes and data integrity. Furthermore, the proliferation of IoT devices, ranging from smart home gadgets to sophisticated industrial control systems, presents a vast attack surface. These devices, often lacking robust security measures, can be vulnerable to hacking, leading to privacy invasions and even large-scale disruptions in critical infrastructure.

In light of these technological advancements, it is imperative for security standards and regulations to evolve and keep pace with emerging threats. Regular updates and improvements in security standards are not just necessary; they are essential for safeguarding corporate assets and ensuring information security. This includes

developing more stringent protocols for cloud security, enhancing data protection measures in big data analytics, ensuring the ethical and secure use of AI, and reinforcing the security of IoT networks.

Organizations must be proactive in adapting to these changes, implementing robust security frameworks, and ensuring compliance with the latest standards and regulations. This continuous evolution in security practices is critical in building resilience against increasingly sophisticated cyber threats and maintaining the integrity and confidentiality of data in a rapidly changing digital landscape.

3.2 Changes In Compliance

As technologies and cyber threats evolve, so do laws and industry standards on data protection. The European Union's General Data Protection Regulation (GDPR) has revolutionized personal data protection, influencing how businesses globally handle data. In the U.S., the California Consumer Privacy Act (CCPA) has heightened data privacy standards, granting consumers more control over their personal information. These changes necessitate businesses to update their compliance strategies and procedures to align with new regulatory requirements. Adapting to these regulations is crucial not only to avoid legal risks and fines but also to maintain an organization's reputation and customer trust. In today's digital era, a commitment to data protection and transparency is key to building strong customer relationships and gaining a competitive advantage. Businesses must view these evolving standards as an opportunity to enhance data protection practices, thus ensuring compliance and preparing for future changes in the data privacy landscape.

3.3 Case Studies

In 2013, one of the most notable data breaches involved Target Corporation, affecting approximately 110 million retail customers. The breach was caused by a hacking incident and is considered one of the major data breaches in recent history.

In the case of Target Corporation's data breach, the main issue was the

vulnerability of their cyber security measures and systems. Hackers gained access by infiltrating their third-party vendor's system, and then used that access to get into Target's payment system, which resulted in a large amount of customer data.

Improvements that follow the security strategy proposed in this paper, particularly in the areas of risk management and third-party vendor security management, may yield different results. For example, implementing more stringent third-party vendor security assessment and monitoring to ensure that all partners comply with the company's security standards^[5]; strengthening internal network security controls, especially in access control to sensitive parts such as the payment system; and establishing a better incident response plan to act quickly when anomalies are detected may all have a positive impact on mitigating damages and protecting customer data^[6].

4. Conclusion

This paper presents an in-depth analysis and design of a comprehensive information system security program specifically tailored for NatureGarden, addressing its unique security challenges. The emphasis is on developing a security strategy that not only aligns with the company's specific business needs but also integrates effectively with its existing IT infrastructure. Drawing lessons from the Target Corporation data breach, the importance of regularly updating security protocols and implementing advanced security technologies in a timely manner is highlighted.

In the fast-evolving digital landscape, organizations like NatureGarden must continually revise and enhance their security policies and practices to safeguard against emerging threats. The proposed security program for NatureGarden includes conducting thorough risk assessments to identify potential vulnerabilities, incorporating state-of-the-art security solutions such as intrusion detection systems and encryption, and establishing robust security policies. Also crucial is the implementation of regular training programs to enhance employee awareness of security best practices.

The development of a comprehensive incident response plan ensures quick and effective action in the event of a security breach. Regular security audits are proposed

to evaluate and update existing security measures continually. This approach, which involves engaging all stakeholders in the security program, aims to create a culture of security awareness throughout the organization.

By adopting this comprehensive and flexible approach to security management, NatureGarden can ensure the protection of its corporate assets and customer data. This strategy addresses current security needs and lays a foundation for future adaptability and resilience in the face of new and evolving digital security challenges.

Reference

- [1] Cremer F, Sheehan B, Fortmann M, et al. Cyber risk and cybersecurity: a systematic review of data availability[J]. The Geneva Papers on risk and insurance-Issues and practice, 2022, 47(3): 698-736.
- [2] Densham B. Three cyber-security strategies to mitigate the impact of a data breach[J]. Network Security, 2015, 2015(1): 5-8.
- [3] Schlackl F, Link N, Hoehle H. Antecedents and consequences of data breaches: a systematic review[J]. Information & Management, 2022, 59(4): 103638.
- [4] Kuipers S, Schonheit M. Data breaches and effective crisis communication: a comparative analysis of corporate reputational crises[J]. Corporate Reputation Review, 2022, 25(3): 176-197.
- [5] Snider K L G, Shandler R, Zandani S, et al. Cyberattacks, cyber threats, and attitudes toward cybersecurity policies[J]. Journal of Cybersecurity, 2021, 7(1): tyab019.
- [6] Seh A H, Zarour M, Alenezi M, et al. Healthcare data breaches: insights and implications[C]//Healthcare. mDPI, 2020, 8(2): 133.