**ISMS REPORT FOR SOLARIS INTERNATIONAL LTD, UK**

BSc (Hons) Cyber Security and Digital Forensic

Security Management in Practice

UFCFRM-15-3

2022/23

**Name:** Hamza Wakili

Table of Contents

[Introduction 1](#_Toc139282079)

[Context 1](#_Toc139282080)

[Assumptions 3](#_Toc139282081)

[Justification for ISMS Implementation 3](#_Toc139282082)

[Risk Assessment 4](#_Toc139282083)

[Risk Identification 5](#_Toc139282084)

[Risk Evaluation 6](#_Toc139282085)

[Risk Treatment Plan 6](#_Toc139282086)

[References 11](#_Toc139282087)

[Appendix 12](#_Toc139282088)

**List of Tables and Figure**

[Table 1: Key assets of Solaris International 5](#_Toc137818464)

[Table 2: Key threats, likelihood and impact 6](#_Toc137818465)

[Table 3: Risk treatment plan 8](#_Toc137818466)

[Figure 1: Organogram of Solaris International 2](#_Toc139282486)

## Introduction

In the current digital landscape, the significance of safeguarding sensitive information within business organisations cannot be overstated (Khan, 2023). These organisations possess a vast amount of valuable data, ranging from customer details to financial records and intellectual property. The protection of such information is paramount for upholding trust, competitiveness, and compliance with regulatory requirements. It is imperative to establish and maintain effective security measures, such as encryption, firewalls, and access controls, to mitigate cyber threats and prevent unauthorized access (Jamal et al., 2021). Research conducted by Li and Liu (2021) emphasizes the severe consequences that can result from a breach, including substantial financial losses, damage to reputation, and legal liabilities. Therefore, business organisations must prioritize the implementation of robust data protection strategies, regular training for employees, and ongoing risk assessments to ensure the safeguarding of sensitive information and to retain the trust of stakeholders.

The ISO standard used in this report is ISO/IEC 27005:2018, which specifically addresses risk management in information security. ISO27005 is an internationally recognized standard developed by the International Organisation for Standardization (ISO) and the International Electrotechnical Commission (IEC). It provides a globally accepted framework and guidelines for information security risk management. By utilizing ISO27005, this report aligns the proposed organisation's risk management practices with international best practices.

## Context

Solaris International, a leading economic management company based in UK, is comprised of a diverse workforce of skilled professionals dedicated to driving the organisation's success. The company employs software developers, system administrators, cybersecurity experts, project managers, and support staff. These individuals work collaboratively within their respective departments and report to department heads who oversee their teams. The department heads, in turn, report to the Chief Technology Officer (CTO), who is responsible for aligning technology strategies with the company's overall objectives.

Within Solaris International, security is a top priority and is managed meticulously. The company has a dedicated cybersecurity team responsible for implementing and maintaining robust security measures. This team conducts regular risk assessments, monitors the network for potential threats, and promptly addresses vulnerabilities. They work closely with the IT department to ensure that systems and software are up to date with the latest security patches and configurations.

Solaris International's employees interact with various external stakeholders, including clients, partners, and regulatory bodies. Client interactions involve understanding specific software requirements, providing demonstrations, and addressing technical inquiries or concerns. The sales and marketing teams play a vital role in building and nurturing client relationships, ensuring that client expectations are met and exceeded.

External interactions differ from internal ones in terms of formality and objectives. While internal interactions focus on collaboration and knowledge sharing among team members, external interactions prioritize exceptional customer service, strategic alliances, and compliance with industry regulations.

Assumptions within Solaris International include the availability of sufficient resources to invest in technology, security infrastructure, employee training, and research and development. The organisation assumes a clear hierarchical structure with defined reporting lines, roles, and responsibilities. Processes are assumed to be Ill-documented, efficient, and regularly reviewed for continuous improvement.

A diagram of a company

Description automatically generated with low confidence

Figure 1: Organogram of Solaris International

The Roles and Responsibilities of the Management are explained in Appendix A

## Assumptions

|  |  |
| --- | --- |
| Resources | Solaris International assumes access to adequate financial resources to support technological advancements, security infrastructure, training programs, and research and development initiatives. |
| Hierarchy | The company assumes a hierarchical structure where department heads oversee their teams, who report to the CTO. The CTO is responsible for aligning technology strategies with the company's overall objectives. |
| Responsibilities | Clear roles and responsibilities are assigned within Solaris International to ensure accountability and efficient workflow. Employees are expected to fulfill their duties and contribute to the organisation's collective success. |
| Processes | Solaris International assumes the existence of documented and Ill-defined processes for various operations, including software development, cybersecurity, project management, and client interactions. These processes are regularly reviewed and refined to optimize efficiency and quality. |

## Justification for ISMS Implementation

Information security incidents have become increasingly prevalent in recent years, exposing organisations to significant risks, and highlighting the need for robust information security measures (OECD, 2020). Real-world examples, such as the high-profile Equifax data breach in 2017 and the widespread WannaCry ransomware attack in the same year, serve as stark reminders of the severe consequences that can arise from inadequate information security practices.

The Equifax data breach compromised the personal information of approximately 147 million individuals, leading to severe reputational damage, legal repercussions, and substantial financial losses for the company (OECD, 2020). The incident was attributed to a combination of lacking security controls and vulnerabilities within the organisation's systems, which allow cybercriminals to exploit weaknesses and gain unauthorized access to sensitive data.

Similarly, the WannaCry ransomware attack had a global impact, affecting organisations across various sectors, including healthcare institutions and government agencies (OECD, 2020). Exploiting a vulnerability in outdated software, the attack rapidly spread and encrypted critical files, demanding ransom payments for their release. Organisations with inadequate security practices and ineffective patch management Ire particularly vulnerable to this attack.

These real-world incidents serve as compelling evidence of the need for an Information Security Management System (ISMS) within our organisation. By implementing an ISMS, this report can establish a systematic approach to managing and securing the organisations information assets, safeguarding the confidentiality, integrity, and availability of critical data. This report adopted ISO/IEC 27005:2018 (ISO27005), the adoption of this ISO standard in this report is well-founded because it holds the position of an internationally acknowledged standard. It encompasses a thorough risk management approach, a structured methodology for assessing risks, integration with an Information Security Management System (ISMS), a focus on continuous improvement, and the opportunity for external validation. By adhering to ISO27005, this report establishes a strong basis for proficiently managing risks in information security and showcase the organisational dedication to protecting the organisation’s assets.

## Risk Assessment

This section discusses the Risk Identification by identifying the key assets of the organisation, the report will also evaluate the risk based on the key assets and the impact the contribute, finally the Risk Treatment will be discussed to mitigate the identified risk:

Risk assessment will deal with:

* Asset Identification: This includes tangible assets like hardware and infrastructure, as well as intangible assets like data, software, and intellectual property.
* Threat Identification: This includes external threats to the organisation’s key assets such as malicious attacks, social engineering as well as internal threats like human error or unauthorized access.
* Vulnerability Assessment: This includes technical evaluations, configuration analysis, or security control evaluation that may be used to find potential weak points.
* Risk Analysis: The risk assessment process involves analysing and evaluating the potential impact and likelihood of a threat exploiting a vulnerability. This helps in understanding the level of risk associated with each identified risk scenario.
* Risk Treatment: This includes selecting and implementing security controls, developing mitigation strategies, creating incident response plans, transferring risks through insurance, or accepting residual risks.

### Risk Identification

This section of the report will analyse the risk based on the organisation's major assets and the impact they have before discussing risk treatment to lessen the detected risk.

|  |  |
| --- | --- |
| Category | Key Assets |
| Information Assets | - Customer data (personal and financial information) |
|  | - Intellectual property (software code, patents, trade secrets) |
| - Employee data (personal and HR information) |
| - Business data (financial records, contracts, marketing plans) |
| Technology Assets | - IT infrastructure (servers, network devices, databases) |
|  | - Software applications (custom-developed and third-party) |
| - End-user devices (computers, mobile devices) |
| - Cloud services and data storage |
| Human Assets | - Employees (with varying access privileges) |
|  | - System administrators and IT staff |
| - External vendors and contractors |

Table 1: Key assets of Solaris International

### Risk Evaluation

Based on the asset inventory, a risk evaluation is conducted using the ISO27005 risk management methodology. This report assessed the likelihood and potential impact of various threats and vulnerabilities, considering both internal and external factors. The risk analysis identified the following key risks:

|  |  |  |  |
| --- | --- | --- | --- |
| S/N | Threat | Likelihood | Impact |
|  | Unauthorized Access to Customer Data | Moderate | High |
|  | Malware and Ransomware Attacks | High | High |
|  | Insider Threats and Data Leakage | Moderate | Moderate |
|  | Physical Security Breaches | Low | High |
|  | Inadequate Patch Management | Moderate | Moderate |
|  | Third-Party Security Incidents | Moderate | High |
|  | Social Engineering and Phishing Attacks | High | Moderate |

Table 2: Key threats, likelihood and impact

### Risk Treatment Plan

To mitigate the identified risks, this report proposes the following risk treatment plan, aligning with the control objectives outlined in ISO27001:

|  |  |  |
| --- | --- | --- |
| Identified Risk | Control Objectives | Risk Treatment Plan |
| Unauthorized Access to Customer Data | Access Control (A.9) | 1. Implement strong authentication measures like multi-factor authentication (MFA) for employees accessing customer data systems. |
|  | Information Security Incident Management (A.16) | 2. Develop an incident response plan specific to customer data access incidents, including defined roles and responsibilities within the incident response team. |
| Malware and Ransomware Attacks | Malware Prevention (A.12) | 1. Implement and regularly update antivirus and anti-malware solutions on all systems used by employees, particularly those involved in software development and system administration. |
|  | Backup (A.14) | 2. Establish a robust backup and recovery system for critical systems, ensuring regular backups are taken and securely stored off-site. Regularly test restoration procedures to verify data integrity. |
| Insider Threats and Data Leakage | Human Resources Security (A.7) | 1. Conduct thorough background checks for all employees, particularly those in positions involving access to sensitive data. Provide security awareness training to employees, emphasizing data protection and confidentiality. |
|  | Data Protection and Privacy (A.18) | 2. Implement data classification and access controls to limit data access based on job roles and responsibilities. Monitor and audit data access activities to detect and prevent unauthorized data leakage. |
| Physical Security Breaches | Physical and Environmental Security (A.11) | 1. Implement access controls such as electronic access cards and CCTV surveillance on Solaris International's premises. Conduct regular security audits to identify and address physical security vulnerabilities. |
|  | Information Security Incident Management (A.16) | 2. Develop and regularly test physical security incident response procedures. Educate employees about the importance of physical security and their role in reporting any suspicious activities. |
| Inadequate Patch Management | Information Systems Acquisition, Development, and Maintenance (A.14) | 1. Establish a patch management process that includes the software development team, system administrators, and IT support staff. Ensure patches are promptly evaluated, tested, and deployed to minimize vulnerabilities. |
|  | Change Management (A.12) | 2. Integrate patch management procedures into the change management process to ensure that patch deployments are controlled, documented, and do not disrupt business operations. |
| Third-Party Security Incidents | Supplier Relationships (A.15) | 1. Implement a comprehensive third-party risk management program, including due diligence assessments, contractual obligations regarding security, and periodic security audits of third-party vendors. |
|  | Information Security Incident Management (A.16) | 2. Define incident response procedures that involve third-party vendors and establish communication channels for reporting and addressing security incidents collaboratively. |
| Social Engineering and Phishing Attacks | Security Awareness and Training (A.7) | 1. Conduct regular security awareness and training sessions for all employees, focusing on recognizing, mitigating social engineering, and phishing risks. |
|  | Email and Ib Filtering (A.13) | 2. Implement robust email and Ib filtering solutions to block malicious content and reduce the risk of employees falling victim to phishing attacks. Regularly update filters to adapt to emerging threats. |

Table 3: Risk treatment plan

Implementing an ISMS is an ongoing process that requires continual monitoring and improvement. To achieve this, this report proposes the following steps:

1. Establish an Information Security Steering Committee comprising representatives from different departments to oversee the implementation and management of the ISMS.
2. Conduct regular risk assessments to identify emerging threats and vulnerabilities, ensuring that the risk treatment plan remains effective.
3. Implement a robust incident response plan to detect, respond, and recover from security incidents promptly, minimizing their impact on the organisation.
4. Regularly review and update information security policies, procedures, and guidelines based on changes in the threat landscape and evolving business requirements.
5. Conduct periodic audits and compliance assessments to evaluate the effectiveness of the ISMS and identify areas for improvement.

**Monitoring and Communication**

Solaris International aims to implement an effective Information Security Management System (ISMS) by establishing a robust monitoring and communication framework. Key components include:

1. Security Incident Monitoring: A Security Operations Centre (SOC) will be set up to monitor security events in real-time using advanced SIEM tools. Suspicious activity triggers immediate investigation and response.
2. Vulnerability Management: Ongoing vulnerability assessments, penetration testing, and patch management processes will be implemented to identify and address weaknesses in systems and applications.
3. Security Metrics and Reporting: Key performance indicators and security metrics will be defined to evaluate the effectiveness of the ISMS. Regular reports will provide visibility into the organisation's security posture.
4. Security Awareness Training: A comprehensive security awareness training program will educate employees on current threats, best practices, and their responsibilities in safeguarding information.
5. Incident Response and Communication: A well-defined incident response plan will outline roles, communication channels, and escalation procedures. Clear and timely communication will be maintained with stakeholders.
6. Continuous Improvement: Regular audits and assessments will be conducted to evaluate the ISMS and identify areas for improvement. Lessons learned from incidents and feedback will drive enhancements.

By implementing a comprehensive monitoring and communication framework, Solaris International can adopt a proactive stance in detecting, responding to, and mitigating information security risks. This proactive approach ensures the continuous effectiveness of the Information Security Management System (ISMS) and fosters the development of a resilient security posture. By effectively safeguarding sensitive data, Solaris International can uphold the trust of its stakeholders and maintain a strong reputation in the industry.

**Critical Reflection and Recommendations**

Establishing an ISMS for this task provided valuable insights into the importance of proactive information security measures. However, certain limitations were encountered during the process. These include:

1. Limited resources: Implementing an ISMS requires careful consideration of the organisation's resources, including budget, personnel, and time constraints. Solaris International must ensure that sufficient resources are allocated to support the implementation and ongoing management of the ISMS. Adequate budgetary provisions should be made to invest in necessary security technologies, conduct regular assessments, and address any identified vulnerabilities. Additionally, personnel with the required expertise and knowledge should be assigned to oversee the ISMS and ensure its effective operation. It is crucial to strike a balance between resource allocation and the level of security required to mitigate risks effectively.
2. Organisational culture: Building a strong security culture within Solaris International is pivotal for the success of the ISMS. A culture of security awareness should be fostered, where every employee understands their role in protecting sensitive information and preventing security incidents. Regular training and education programs should be conducted to enhance employees' knowledge of security practices, such as recognising phishing attempts, adhering to password policies, and reporting suspicious activities. By empowering employees to act as the first line of defence, Solaris International can significantly enhance its overall security posture.
3. Evolving threat landscape: The threat landscape is dynamic and continuously evolving. New attack vectors, vulnerabilities, and hacking techniques emerge regularly, making it crucial for Solaris International to stay abreast of the latest developments. The ISMS must be adaptable and flexible to address emerging threats effectively. This entails conducting regular risk assessments, staying informed about emerging trends and best practices, and promptly updating security controls and measures. By actively monitoring the threat landscape, Solaris International can proactively identify and address potential vulnerabilities, reducing the risk of security incidents.

To address these limitations, I recommend the following:

1. Acquisition of additional resources: Solaris International should proactively seek the acquisition of supplementary resources to ensure the successful implementation and continual management of the ISMS. This may involve securing a dedicated budget to invest in advanced security technologies, recruiting specialized personnel proficient in information security, and allocating sufficient time and effort to execute the ISMS efficiently. By presenting a compelling case that highlights the potential risks and benefits associated with adequate resource allocation, Solaris International can bolster its capacity to effectively mitigate information security risks and safeguard sensitive data.
2. Cultivation of a security-conscious culture: Cultivating a robust security-conscious culture within Solaris International is pivotal to the efficacy of the ISMS. Regular sessions should be conducted to raise awareness among employees about the significance of information security, prevalent threats, and best practices for protecting sensitive data. Recognizing and rewarding employees who demonstrate security-conscious behaviour can serve as a powerful incentive to foster a culture of vigilance. Moreover, establishing well-defined channels through which employees can report security incidents and potential vulnerabilities, and ensuring that such reports are promptly acknowledged and addressed, nurtures a sense of accountability among employees and fortifies the overall security posture.
3. Vigilance regarding emerging threats: The threat landscape is characterized by its continuous evolution, with new vulnerabilities and attack vectors surfacing regularly. To effectively combat these shifting threats, Solaris International should forge partnerships with external security organisations, such as industry-specific information sharing networks and providers of threat intelligence. Active participation in pertinent industry conferences, forums, and workshops also affords invaluable insights into emerging threats and best practices for mitigating them. By remaining attuned to the latest trends and emerging threats, Solaris International can adapt the ISMS and implement requisite security measures to effectively counteract these risks.

Thank you for considering this report regarding the proposed ISMS implementation.

## References

ISO 80585:2022, Data quality management — Principles and guidance. International Organisation for Standardization, Geneva, Switzerland, 2022.

Jamal, A. A., Majid, A. M., Konev, A., Kosachenko, T., & Shelupanov, A. (2023). A review on security analysis of cyber physical systems using Machine learning. Materials Today: Proceedings, 80(Part 3), 2302-2306. https://doi.org/10.1016/j.matpr.2021.06.320.

Khan, M. J. (2023). Securing network infrastructure with cyber security. World Journal of Advanced Research and Reviews, 17(02), 803–813. https://doi.org/10.30574/wjarr.2023.17.2.0308

Li, Y., & Liu, Q. (2021). A comprehensive review study of cyber-attacks and cyber security: Emerging trends and recent developments. Energy Reports, 7, 8176-8186. https://doi.org/10.1016/j.egyr.2021.08.126

OECD (2020), Encouraging Clarity in Cyber Insurance Coverage: The Role of Public Policy and Regulation, [www.oecd.org/finance/insurance/Encouraging-Clarity-in-Cyber-Insurance-Coverage.pdf](http://www.oecd.org/finance/insurance/Encouraging-Clarity-in-Cyber-Insurance-Coverage.pdf)

## Appendix

Explanation of the Organisational Structure:

* CEO: The Chief Executive Officer is responsible for the overall strategic direction and management of the company.
* CTO: The Chief Technology Officer oversees the company's technology initiatives, including software development, infrastructure, and quality assurance.
* CFO: The Chief Financial Officer manages the company's financial activities, including budgeting, financial reporting, and risk management.
* HR: The Human Resources department handles recruitment, employee relations, training, and other HR-related functions.
* Development: This department is responsible for software development projects, including frontend and backend development teams.
* Finance: The Finance department manages financial operations, such as accounting, budgeting, and financial analysis.
* Quality Assurance: The Quality Assurance team ensures the quality and reliability of software products through testing and quality control processes.
* Infrastructure Team: This team manages the company's IT infrastructure, including servers, network devices, and databases.
* Procurement Team: The Procurement team handles vendor management and procurement of necessary resources and services.
* Vendors: This category represents external vendors and contractors who provide specialized services to the company.