# Security Management Plan

# Pharm Universe

# 2021

A. D. DISSANAYAKA

Table of contents



A. D. DISSANAYAKA

A. D. DISSANAYAKA

## Approval History

| Version: | Reviewed By: | Approved By: | Approver's Position: | Date Approved: | Next Review Date: |
|---|---|---|---|---|---|
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |

## Revision History

| Version | Date | Author | Description |
|---|---|---|---|
| 1 | 10/12/2021 | A. D. DISSANAYAKA | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |

A. D. DISSANAYAKA

# Glossary:

| Abbreviations | |
|---|---|
| **Abbreviation** | **Expansion** |
| SMP | Security Management Plan |
| FDA | Food and Drug Administration |
| DoS | Denial of Service |
| DDoS | Distributed Denial-of-Service |
| ICT | Information and Communication Technology |
| IPS | Intrusion Prevention System |
| SDS | Software-Defined Security |
| WWW | World Wide Web |
| FTP | File Transfer Protocol |
| DNS | Domain Name Server |
| LAN | Local Area Network |
| ISMS | Information Security Management System |
| CVSS | Common Vulnerability Scoring System |
| VPN | Virtual Private Network |
| NPV | Net Present Value |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |

A. D. DISSANAYAKA

# 1 Introduction

## 1.1 Background

In this 21st century, information security plays an enormous role due to the critical and rapidly evolving world and this information security management is now becoming a crucial factor for an organization to rely on standards. So there is no doubt, that computer and information security is a great concern for almost every organization, which is equally important in both the private and public sectors.

Pharm Universe is an international pharmaceutical company, that has obtained venture capital, hired several other researchers, patented the formula, and established its viability in clinical tests and got the approval of the US Food and Drug Administration for this particular drug, only by prescription. They are concerned about ensuring the privacy of important data such as drug formulas, because any leak could have serious consequences for the operation of the company. Acquiring competitors' drug formulas before products go to market is a huge advantage for competitors because it significantly decreases the time and resources needed in the costly research process. Having any of these formula stolen is a worst-case scenario for a pharmaceutical company. The company's revenues from a new product are likely to be curtailed.

The international standard ISO/IEC 27001:2013 'Information Security Management Systems' and its complementary standard ISO/IEC 27002:2013 'Codes of Practice for Information Security Management' form the basis of the controls required to ensure risks to information and systems are identified and effectively managed. ISO/IEC 27001:2013 covers all kinds of organisations and specifies the necessities for creating, employing, operating, revising, continuing, and improving an information security management system in the context of risks followed by the organisation's commercial, technical, and regulatory environment.[1]

This document describes how Pharm Universe manages information security which is according to the leading industry practice and specifies additional application of controls, policies, procedures, plans, roles, responsibilities, practices, structures, and resources that are used to protect and preserve the information assets of the company.

## 1.2 Purpose

This Policy delivers a framework for the management of information assets and their security throughout the organization. In this document, it underpins the policies, procedures, standards and guidance for the security of electronically stored data (drug formulars, employee data, etc), a phased-in approach to develop, implement and monitor an Information Security Management System within the Pharm Universe organisation and how to evaluate and defend the organisation against the following identified risks.

- Research is the division where information security is critical as the most crucial information assets (e.g. Drug formula etc) are stored inside this research division. Due to the low-level security of research division, it would expose to any unauthorised access to the drug formula and other critical information and would cause loss of competitive advantage.
- Leakage of information regarding the research can happen through disgruntled employees who leave behind the research team at a very short time to join competitors. This would lead to an outsider exploits their access to steal, modify or delete information.

A.D. DISSANAYAKA

- The research team is using cloud services and using these external resources for data storage is not secure. If any external user accesses this cloud service, all the critical information is exposed.
- The company benefits from a very low level of information security and is mainly based on firewall protection. With this kind of security system, it would easily come up with some malwares, virus, worms or even DOS/DDOS attacks and would take through some Identity theft, exfiltration/theft of sensitive information, data corruption, ICT service outages.
- Analysis, protection, and penetration tests were performed ostensibly only before the auditors' control, and the lack of knowledge related to the company's standards and security policies within the management members. This would make advantage to any insider to exploit their access to steal, modify or delete information.

## 1.3 Readership

This document, while basic in nature, delivers the background information to realise the development of information security policies. The intended audience for this document includes the chief executive officer, company managers, information security officers, vice presidents, information security professionals, risk analysts, security policy and compliance analysts.

A. D. DISSANAYAKA

# 2 Solution Overview

**The problem:**

The Pharm Universe heavily depend on its intellectual properties to be successful within the industry of pharmaceuticals. The organization is at a risk of intellectual property theft for various reasons such as;

- The existing security controls are mostly firewalls and intrusion prevention systems (IPSs) which is very minimal and not suitable for the long run.
- The research division use cloud storage to store important date, which is criticized for its security.
- Vulnerability analysis and penetration testing have only been conducted at the time of the audit checks.
- As most of the employees are scientists they prefer a free exchange of data, convincing them to use secure methods can be difficult as it would slow their work process.
- The wait and see approach could leads to irreversible situations especially when working with non – patent products or formulas.

**The solution:**

The organization must adopt an 'information – centric' structure which enable to implement a good information security policy. The employees from top to bottom needs to be educated about the best practices of information security.

- In the first year we will be focusing to enhance the existing security controls while gradually adding essential and cost-effective controls over the course of time.
- An organization wide memo to be circulated among the employees regarding the basic practices of security.
- The research division which is the most vital division of the company will need to undergo with appropriate changes with the preview of the senior management as it is identified as a major data leak point.
- Frequent brainstorming sessions will be conducted with the management to understand the business requirements thus implementing effective controls.
- In the first stages of the implementation monthly meetings will be held to discuss the current status and issues with the process.

A. D. DISSANAYAKA

**The outcome:**

We aim to achieve a win-win situation for all the stakeholders including employees, the management and board members.

The main goal is to minimize/ avoid intellectual property theft while maintaining a safe and stress-free working environment. This will not only enable the company to maximize the profitability but also enhance the job satisfaction for employees as well.

Adding these controls will create formal and secure communication channels for the scientist whilst providing additional security for the information.

A. D. DISSANAYAKA

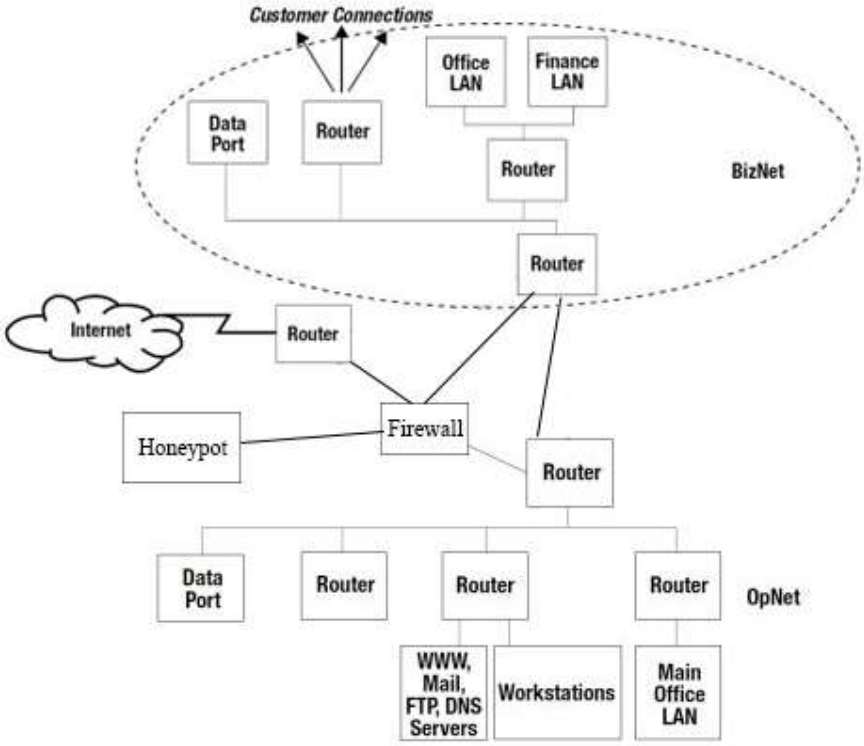
## 2.1 Security control overview

To improve the security architecture of Pharm Universe, there are several controls that can be implemented. Some of the key controls are;

- **Honeypots -** Additional programs or levels that act as trap servers or systems that put up to collect information about any intruder attempting to access the Pharm Universe system. Therefore, they are divulging their significant threats.
- **Cloud protection and software-defined security (SDS) –** since the Pharm Universe scientists use the cloud to save important work, there is a host to deliver protection especially aimed at safeguarding cloud-based assets.
- **Kerberos protocol** - Using symmetric key encryption methodology to verify different network services for individual users. It facilitates the use of tickets to allow users to communicate via non-secure channels.
- **A centralized user access control system** - Must be implemented in the TACACS or DIAMETER and RADIUS rows.
- **Packet Sniffers, Vulnerability Scanners and OS Detection Tools** – Some of the necessary tools that are easy to employ and deliver an enhanced monitoring solution to augment the Pharm Universe security. Observing of firewall logs and system logs is an crucial factor of enhanced security.

A. D. DISSANAYAKA

## 2.2 Secure architecture scope



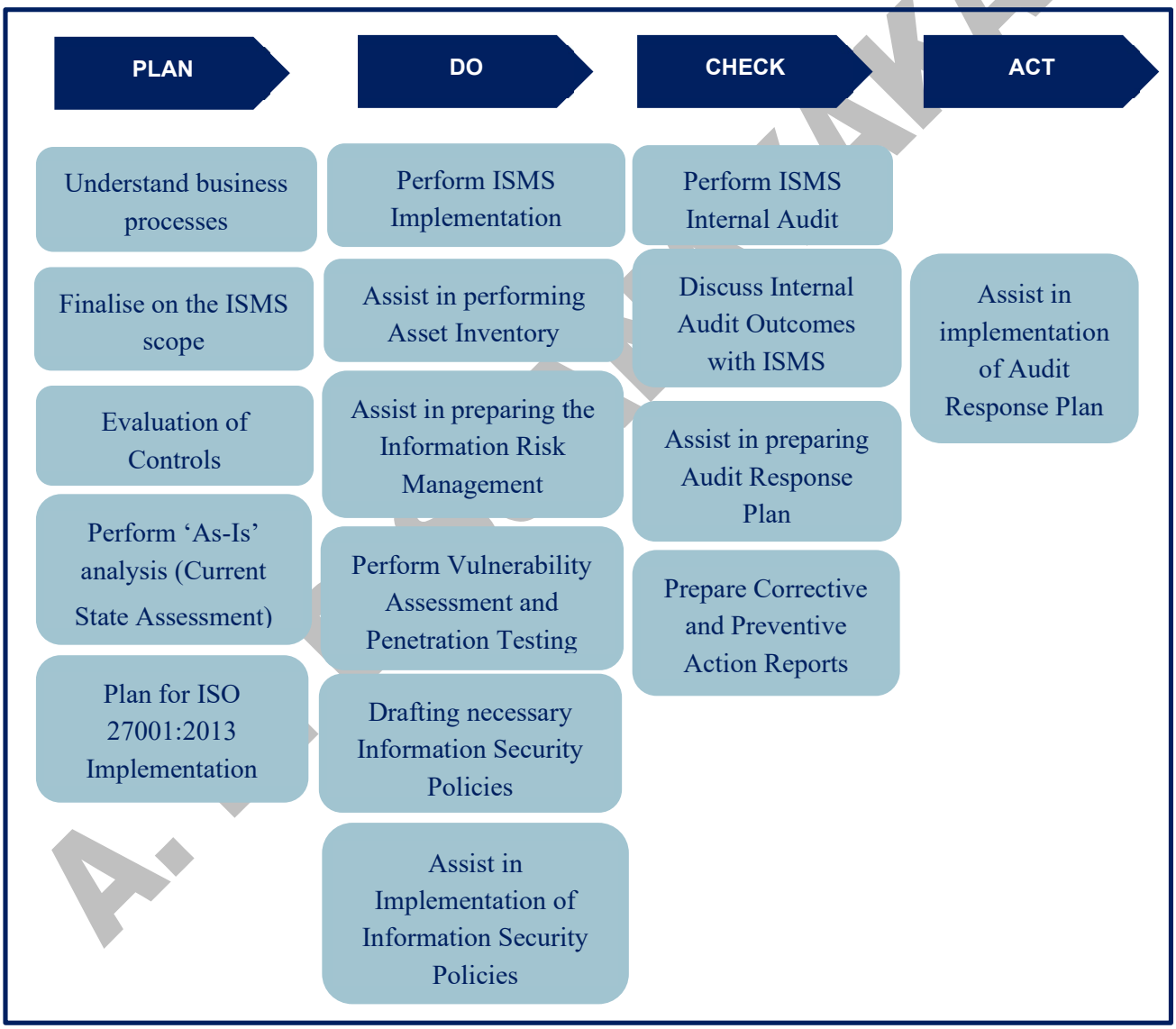

e.g. Figure 2.2 Updated network diagram with honeypots

A. D. DISSA KA

# 3 Scope

## 3.1 Assurance Approach

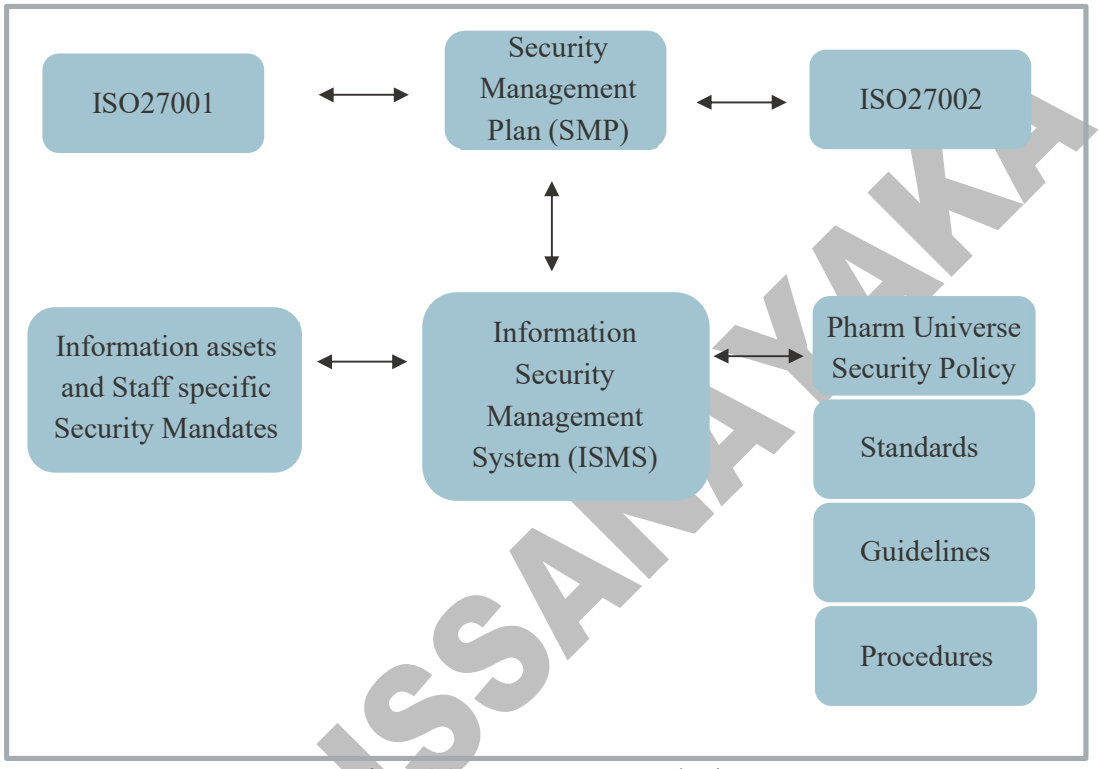
- Pharm Universe information security team will improve the information security management system continually in line with a PLAN-DO-CHECK-ACT framework, to improve process embedded within the company ISMS [2].
- The Plan, Do, Check and Act framework is cyclic and must be continuously done for a long run and with the consistent backing of the management. It is recommended that the ISMS be based on this framework safeguards that the appropriate components are employed, assessed, scrutinized, and enhanced on a continuous basis [3].




e.g. Figure 3.1 Assurance approach diagram

## 3.2 Assurance Frameworks

This addresses the requirements of Pharm Universe that are needed to meet the specific information security, governance, and assurance requirements of the company and how these additional requirements are to be added to the Pharm Universe ISMS. The position of the SMP in the complete ISMS framework and security policy document is shown in the figure below. As the SMP is the top-level manuscript, it refers out to other documents rather than duplicating their content.




e.g. Figure 3.2 Assurance Framework Diagram

A. D. DISSANAYAKA

## 3.3 Scope of Security Services

The Information Security Management System (ISMS) applies to the provision of trusted and managed information security services to the information assets, the staff, and the customers of Pharm Universe.

This Policy and the Framework applies to:

- Everyone within the organisation (eg: staff), who accesses the organisation information assets or technology.
- Technologies or services utilized to access or process organisation information assets.
- Information assets will be handled in relation to any organisation's function, including by, for, or with, external parties.
- Information assets that are stored by the organisation and an external service provider on behalf of the organisation.
- Information that is transferred from and/or to the organisation for a functional reason.
- Third party, public, administrator, or any other information that the organisation is storing, modifying, or using on behalf of another party.
- Internal and/or external activities that are used to process, transfer or store organisation information.

A. D. DISSANAYAKA

# 4 Information Security Management System

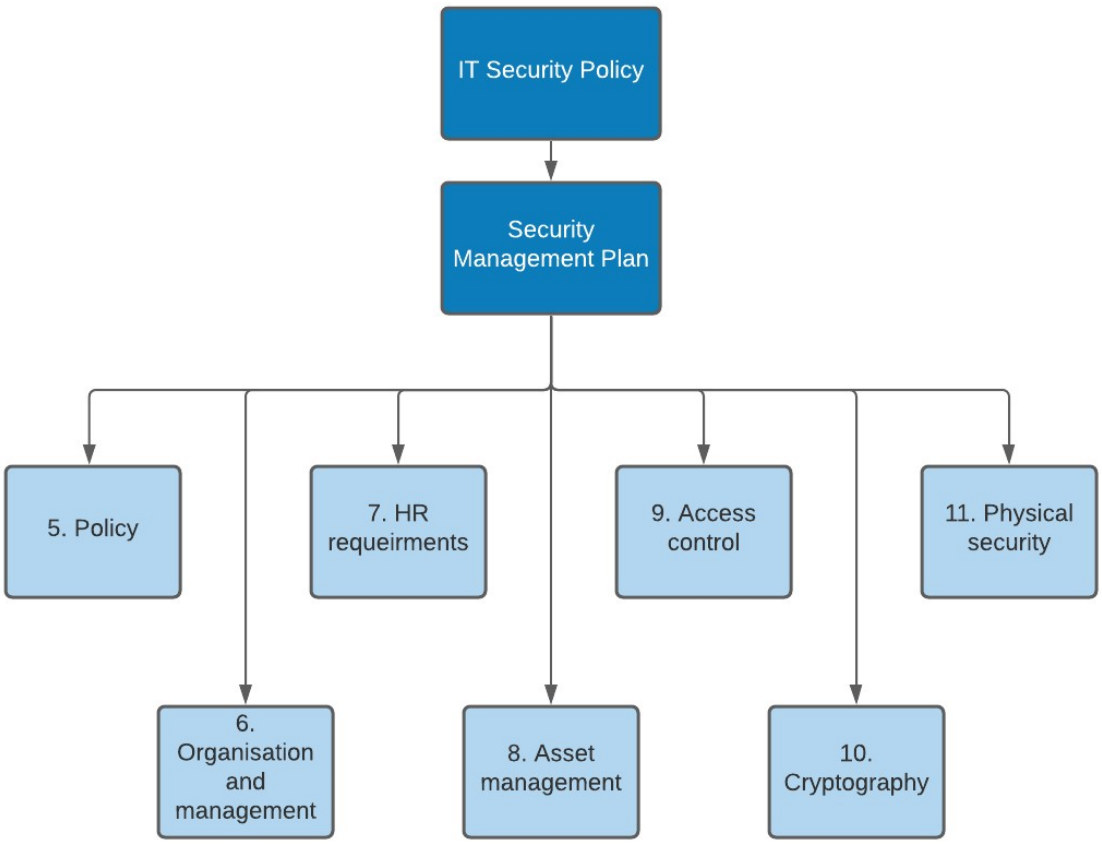
The ISMS contributes for implementing, protecting, and maintaining confidentiality, integrity, and availability of the respective business processes and the information assets in line with best practices recommended in ISO/IEC 27001 as well as ISO/IEC 27002. It is an organizational approach to information security [4]. The business objectives laid out by organisation management and the IT objectives derived from the organisation objectives serve as the foundation for defining the information security objectives and the subsequent controls.

The main objective of this ISMS is to ensure,

- Information is only accessible to authorized parties inside or outside the company.
- Business requirements for confidentiality, integrity and availability of information assets will be achieved and maintained throughout the process, according to the ISO/IEC 27001:2013 standard (Business continuity plans will be established, maintained, and tested).
- All personnel will be trained on information security and will be informed that compliance with the policy is mandatory (Making the staff aware of their responsibilities, roles and accountability).
- All breaches of information security and presumed weaknesses will be explored and assessed.
- Confirm whether the organisation's information assets and systems are appropriate for security (Procedures that exist to support the policy, including virus control measures, passwords, and continuity plans).
- The Information Security Manager is accountable for maintaining the policy and delivering support and advice during its implementation.
- All managers are directly responsible for implementing the policy and ensuring the staff compliance in their individual departments.
- This policy must be approved by the company management and will be reviewed by the management review team annually.

These signify the additional controls expected to complete the ISO27001 Statement of Applicability.

A. D. DISSANAYAKA




e.g. Figure 4.1 ISO/IEC 27001:2013 control coverage

A. D. DISSA

### 4.1.1 Certification delivery schedule


e.g. Figure 4.1.1 Certification delivery schedule diagram

A. D. DIS

### 4.1.2 Risk Management

Pharm Universe will employ an approach to risk management based on a combination of qualitative and quantitative processes that follow the framework defined in the ISO/IEC Information Security Risk Management standard and that meets the requirements of the organisation Information Security Risk Management Framework.

The risk assessment process includes the following steps:

- Periodical workshops involving relevant managers, team leaders, and specialists will be undertaken to define or confirm the list of information assets which should be protected under the ISMS and recognizing the owner and the categorization of each asset.
- Evaluation of the threat, likelihood and the business impact based on the identified information
- assets to ensure that the risk assessment indicates the realistic view of the business.
- Population and maintenance of an Information Security Risk Register regularly by the Pharm Universe Information Security Team.
- Based on the existing controls and residual risk, either accept the risk or agree on a treatment action (i.e. avoid, mitigate or transfer), which will be added to the Risk Treatment Plan. All risk actions taken by the information asset owner must be reviewed by the Pharm Universe Information Security Team.
- The Risk Treatment Plan will be re-evaluated on an on-going basis by the Pharm Universe Information Security Team.

The Pharm Universe information security team will determine:

- The appropriate approach to line up the organisation's risk processes to ensure coherent definitions (impact, likelihood).
- The severity at which risks are escalated to the organisation.
- Who will own risks within the organisation and the criteria for acceptance of residual risk.

For Risk assessment purposes, all the critical information assets of the Pharm Universe should be identified and documented.

Critical Information assets of pharm Universe organisation were identified as follows.

1. Drug formula
2. Cloud data storage

According to the risk assessment process, following risks were identified as the key risks for the critical information assets of the Pharm Universe.

1. Research is the division where information security is critical as the most crucial information assets (eg: Drug formula etc) are stored inside this research division. Due to the low-level security of research division, it would expose to any unauthorised access to the drug formula and other critical information and would cause loss of competitive advantage.

A. D. DISSANAYAKA

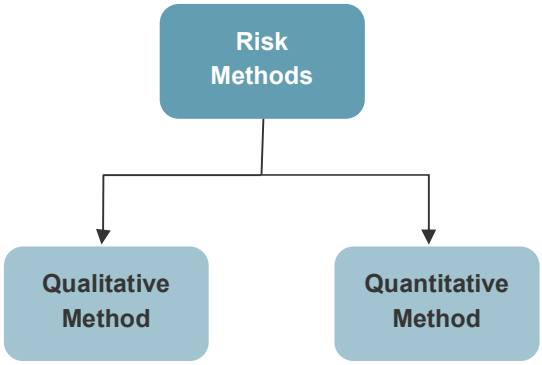
2. Leakage of information regarding the research can happen through disgruntled employees who leave behind the research team at a very short time to join competitors. This would lead to an outsider exploits their access to steal, modify or delete information.
3. The research team is using cloud services and using these external resources for data storage is not secure. If any external user accesses this cloud service, all the critical information is exposed.
4. The company benefits from a very low level of information security and is mainly based on firewall protection. With this kind of security system, it would easily come up with some malwares, virus, worms or even DOS/DDOS attacks and would take through some Identity theft, exfiltration/theft of sensitive information, data corruption, ICT service outages.
5. Analysis, protection, and penetration tests were performed ostensibly only before the auditors' control, and the lack of knowledge related to the company's standards and security policies within the management members. This would make advantage to any insider to exploit their access to steal, modify or delete information.

These identified risks can be prioritised using the threat responses based on the vulnerabilities for which exploits are currently taking place or the ones that organisation can expect activity in the near future, based on predictive probability analysis.

Using Common Vulnerability Scoring System (CVSS), it is easy to access threats, identify impacts, and identify existing countermeasures and apply threat intelligence in a reliable way.

A. D. DISSANAYAKA

There are two current base methodologies that are used to determine the level of risk.




e.g. Figure 4.1.2 Risk method

### *1. Qualitative Method*

The qualitative risk analysis is a process of evaluating the impact of the identified risks within an organisation. Using this process, the priorities of vulnerabilities are determined to solve the risks based on the impact they could have on the organisation. The definite characteristic of the qualitative method is the use of various subjective indexes such as ordinary hierarchy values: low-medium-high, vital-critical-important etc.

| Impact of Loss | LOW | MEDIUM | HIGH |
|---|---|---|---|
| **Confidentiality**<br><br>Ensuring that information is accessible only to those authorized to have access | The unauthorized disclosure of information could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals | The unauthorized disclosure of information could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals. | The unauthorized disclosure of information could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals. |
| **Integrity**<br><br>Safeguarding the accuracy and completeness of information and processing methods | The unauthorized modification or destruction of information could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals. | The unauthorized modification or destruction of information could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals. | The unauthorized modification or destruction of information could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals. |
| **Availability**<br><br>Ensuring that authorized users have access to information and associated assets when required | The disruption of access to or use of information or an information system could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals. | The disruption of access to or use of information or an information system could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals. | The disruption of access to or use of information or an information system could be expected to have a severe or catastrophic adverse effect on organizational operations, |

A.D. DISSANAYAKA

| | | | |
|---|---|---|---|
| | | | organizational assets, or individuals. |

e.g. Impact levels

| RISK ASSESSMENT | | | | | |
|---|---|---|---|---|---|
| **Asset** | **Known or suspected threats** | **Known or suspected vulnerabilities** | **CIA Profile** | **Replacement value** | **Risk Value** |
| **Cloud Data Storage** | **Hacking -** Disclosure (Gives advantage to third party) | Internet connectivity; inadequate firewall protection | C : High<br>I : High<br>A : High | High | High |
| **Drug Formula** | **Unauthorised access by insiders -** Disclosure (Gives advantage to competitor); company might lose business | Lack of physical security to research division | C : High<br>I : High<br>A : High | High | High |
| | **Vulnerable to malware exploits –** Sensitive data loss | Lack of penetrations tests and audits | C : Medium<br>I : High<br>A : High | High | High |

Table 4.1.2.1 Qualitative Risk Assessment

A. D. DISSANAYAKA

### *2. Quantitative Method*

Through the quantitative risk analysis method, can obtain some numerical results that express an approximate probability of each risk factor and its outcomes on the objectives of the organisation, but also the risks at the individual vulnerability level. The process uses several different mathematical techniques to assess risks and make the determination based on the financial loss if the risk occurs within a specific period.

**Asset Valuation Matrix**

*Hypothesis*

- Confidentiality, Integrity and Availability of information will have minimum valuation as 1.
- The value of levels for Confidentiality, Integrity and Availability are taken as follows:

| | |
|---|---|
| **Low** | **1** |
| **Medium** | **2** |
| **High** | **3** |

e.g. Confidentiality, Integrity and Availability levels

- Asset value is determined by sum of all (attribute * its level).

**Severity and Threat Vulnerability Matrix**

*Hypothesis:*

- The value of levels for severity of threat and vulnerability are taken as follows:

| | |
|---|---|
| **Low** | **1** |
| **Medium** | **2** |
| **High** | **3** |

e.g. Threat and vulnerability levels

- The severity value matrix will be; **mathematical Asset Value * Severity of Threat Value * Severity of Vulnerability Value**.

**Risk Impact Matrix**

*Hypothesis:*

- While determining the risk impact matrix probability values are taken as follows:

| **Probability** | | |
|---|---|---|
| **Value** | **Likelihood** | **Explanation** |
| 1 | Never happened | Not happened in last 3 years |
| 2 | Rare | Once in Year |
| 3 | Periodic | Once in a Quarter |
| 4 | Regular | Once in a fortnight |
| 5 | Frequent | Once in a week |

e.g. Probability levels

The probability of occurrence is required to understand the frequency at which such failures occur.

Risk Impact is calculated as per following formula:

**Risk Impact = Asset Value * Severity Of threat * Severity of Vulnerability * Probability**

| RISK ASSESSMENT | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| **Asset** | **Known or suspected threats** | **Known or suspected vulnerabilities** | **Primary concerns (C/I/A)** | **Possibility of occurrence** | **Impact level** | **Raw risk level** | **Incident undetectability** | **Detected risk level** |
| **Cloud data storage** | Data or system corruption | Lack of network security | I + A | 4 | 4 | 16 | 3 | 48 |
| | Virus, worm, trojan or other malware | Lack of awareness of the threats | C + I + A | 3 | 5 | 15 | 4 | 60 |
| **Drug Formula** | Sensitive data leakage among competitors | Former employee of research team | C | 5 | 5 | 25 | 3 | 75 |

Table 4.1.2.1 Quantitative Risk Assessment

DISSANAYAKA

### 4.1.3 Continual Improvement

As a part of the provision of service, a process will be defined to continually improve the suitability, adequacy, and effectiveness of the ISMS for the duration of the commercial agreement.

### 4.1.4 Effectiveness measures

| Risk | Impact | Raw probability | Raw impact | Raw risk rating | Treatment | Treatment cost | Treated probability | Treated impact | Residual risk rating |
|---|---|---|---|---|---|---|---|---|---|
| Low security level of research division | Unauthorised access to critical information | 95% | 100% | 95% | **Controllable** - encryptions, physical security, access control policies | £500 | **15%** | **75%** | 11% |
| Former Employees in research team are joining with competitors | An outsider exploits their access to steal, modify or delete information | 60% | 85% | 51% | **Controllable** – Access control policies, change of passwords | £0 | **5%** | **70%** | 4% |
| External Cloud Storage | Unauthorised external user access to critical information | 65% | 100% | 65% | **Controllable** - Encryptions, Virtual Private Network (VPN), backups | £100 | **3%** | **80%** | 2% |
| Low level of Network Security – malware, virus | Identity theft, exfiltration/theft of sensitive information, data corruption, ICT service outages | 72% | 90% | 65% | **Controllable** – Anti malware product, Updating systems, software firewall systems | £600 | **5%** | **15%** | 1% |
| Lack of knowledge on security policies within management members. | An insider exploits their access to steal, modify or delete information | 45% | 96% | 43% | **Avoidable** – share knowledge, workshops to guide employees through new security breaches | £0 | **2%** | **10%** | 0% |

Table 4.1.4 Risk Treatment Plan

A. D. DISSANAYAKA

**Calculation of cost benefit analysis**

The mathematical model used to calculate cost benefit analysis;

$$\textbf{Net Present Value (NPV)} = \sum \textit{Present Value of expected benefits} - \sum \textit{Present Value of expected costs}$$

***Assumptions:***

**The expected revenue of the company's latest IP is US $500 million and if this information falls into a hand of a competitor before the launch, the company will lose at least 50% of the revenue which is US $ 250 million. This can be avoided by implementing an information security policy and by educating the employees with proper trainings on best information security practices, but this will take more time and additional resources.**

**The estimated salary for the information security team is US $30 million and estimated cost for additional resources to conduct trainings and to increase the awareness of the employees is US $120 million.**

| | | | | | |
|---|---|---|---|---|---|
| **Cost Benefit Analysis** | = | ***Expected Benefits*** | - | ***Expected Costs*** |
| | = | US $500M | - | (US $30M + US $120M) |
| | = | **US $350M** | | |

***If the company decided to go with the new information security policy the cost will be US $150 million but if they decide not to go with it the cost will be at least US $150 million. Additionally, implementing information security policy and best practices will also be beneficial for future projects as well.***

## 4.2 Security Testing

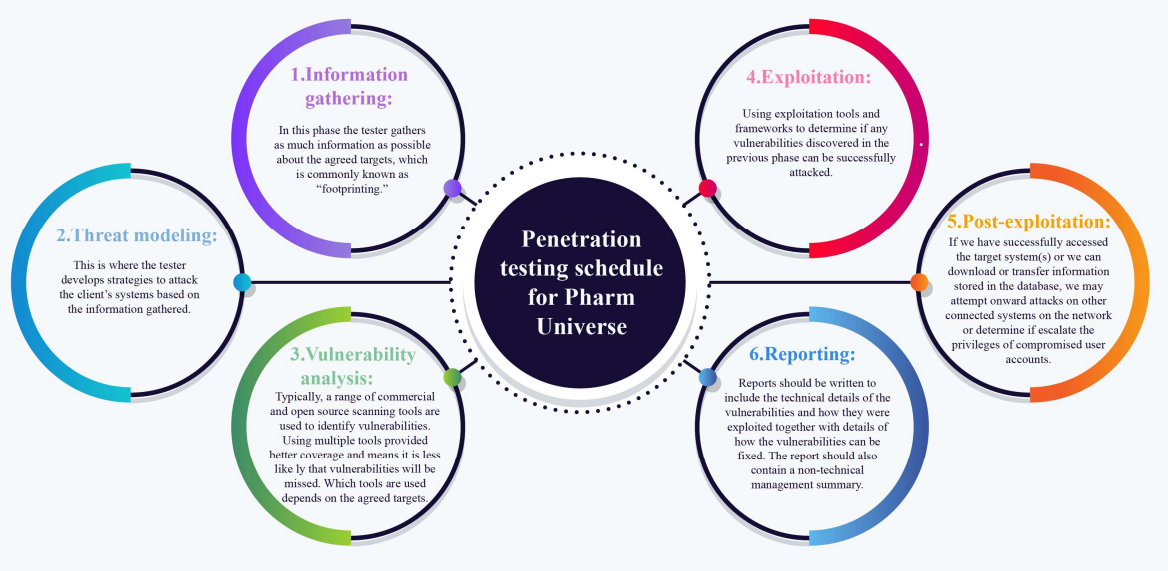
Penetration testing is a vital component of any ISO 27001 Information Security Management System (ISMS), from initial development to ongoing maintenance and continual improvement at three points [5]:

1. **As part of the risk assessment process** – A penetration test to discover the vulnerabilities in any web applications, Internet-facing IP addresses, other applications, and internal devices, and link them to identifiable threats.
2. **As part of the risk treatment process** – A penetration test to ensure that controls work as designed.
3. **As part of the continual improvement process** – A penetration test to ensure that the controls continue to work and new threats and vulnerabilities are detected and fixed.

### 4.2.1 Scheduled penetration testing

Penetration testing is a crucial to achieving and maintaining a robust Information Security Management System (ISMS) that is compliant with ISO/IEC 27001 [6**].** Objective A.12.6.1 of ISO 27001 states that information about technical security vulnerabilities should be obtained in a timely fashion and appropriate measures taken to address the associated risks.

A. D. DISSANAYAKA




e.g. Figure 4.2.1 Penetration testing schedule for Pharm Universe

### 4.2.2 Specific testing - considerations

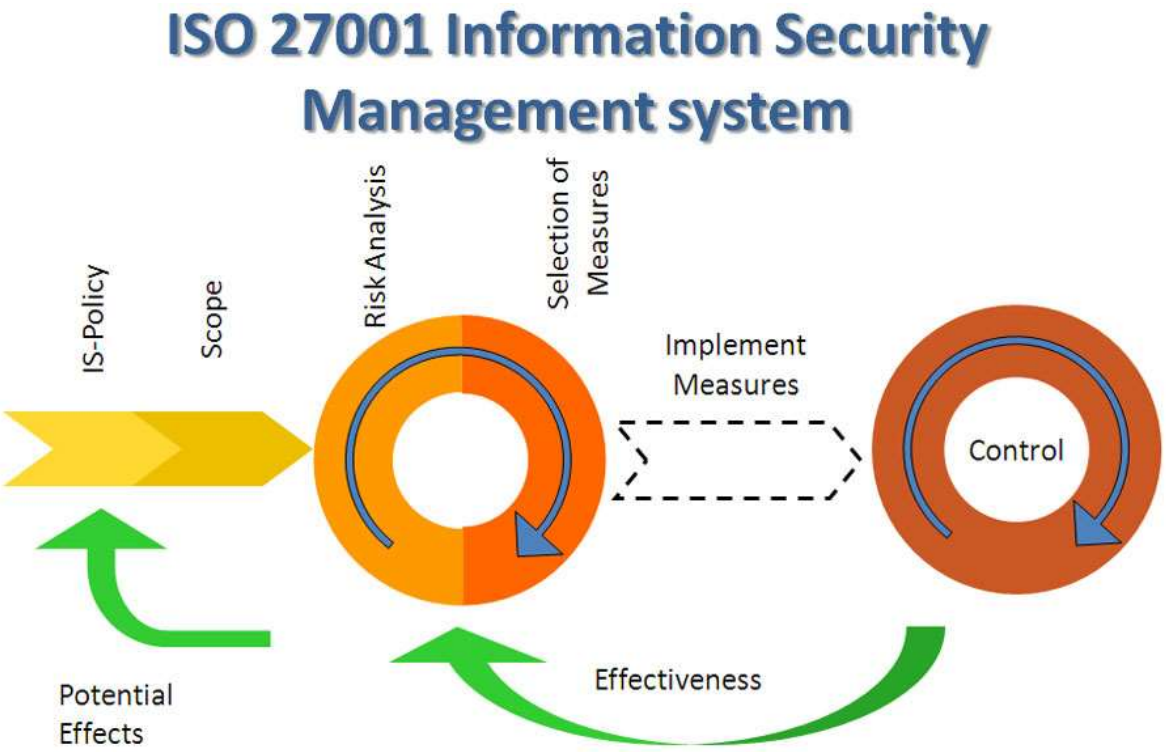
- **External tests** - Aiming on the internet, including IP addresses, web applications and other such services.
- **On-site tests** - Aiming on the devices, including wireless devices that make up the network, applications and operating systems that run on them.

A. D. DISSANAYA

# 5 Information Security Policies

The Information Security Policy describes the Pharm Universe organisation's approach to information security as well as approved mandatory information security controls based on the Statement of Applicability.

All approved amendments to the policy will be communicated to all affected personnel.




e.g. Information Security policy is structured in accordance with ISO/IEC 27001:2013[8].

A. D. D.

## 5.1 Policies and Standards

| A.5.1 Management direction for information security | | |
|---|---|---|
| **Objective**: To provide management direction and support for information security in accordance with business requirements and relevant laws and regulations | | |
| **Sec.** | **Control#** | **Description** |
| A.5.1.1 | Policies for information security document | The Pharm Universe security policy will take precedence. |
| A.5.1.2 | Review of the policies for information security | The policies for information security will be reviewed at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness. (Review in line with annual Security Management Plan) |

A. D. DISSANAYAKA

# 6 Organisation of Information Security

## 6.1 Operational Model

| **A.6.1 Internal organization** | | |
|---|---|---|
| **Objective**: To establish a management framework to initiate and control the implementation and operation of information security within the organization | | |
| **Sec.** | **Control#** | **Description** |
| A.6.1.1 | Policies for Information security roles and responsibilities | All information security responsibilities will be defined and allocated. The programme team will define an organisation chart which will clearly identify all security roles |
| A.6.1.2 | Segregation of duties | Conflicting duties and areas of responsibility will be segregated to reduce opportunities for unauthorised or unintentional modification or misuse of the organisation's assets. Clear segregation of duties will be maintained between development and other IT support staff as necessary. |
| A.6.1.3 | Contact with authorities | Appropriate contact with relevant authorities will be maintained. |
| A.6.1.4 | Contact with special interest groups | Appropriate contact with special interest groups or other specialist security forums and professional associations will be maintained. |
| A.6.1.5 | Information security in project management | Information security will be addressed in project management, regardless of the type of the project. |

A. D. DISSANAYAKA

## 6.2 Teleworking

| A.6.2 Mobile devices and teleworking | | |
|---|---|---|
| **Objective**: To ensure the security of teleworking and use of mobile devices | | |
| **Sec.** | **Control#** | **Description** |
| A.6.2.1 | Mobile device policy | A policy and supporting security measures will be adopted to manage the risks introduced by using mobile devices. |
| A.6.2.2 | Teleworking | Not applicable- no provision of service from teleworking sides. |

A. D. DISSANAYAKA

# 7 Personnel Security

## 7.1 Prior to joining

| **A.7.1 Prior to employment** | | |
|---|---|---|
| **Objective**: To ensure that employees and contractors understand the responsibilities and are suitable for the roles for which they are considered. | | |
| **Sec.** | **Control#** | **Description** |
| A.7.1.1 | Screening | Background verification checks on all candidates for employment will be carried out in accordance with relevant laws, regulations and ethics and will be proportional to the business requirements, the classification of the information to be accessed and the perceived risks. |
| A.7.1.2 | Terms and conditions of employment | The contractual agreements with employees and contractors will state their and the organisation's responsibilities for information security. |

A. D. DISSANAYAKA

## 7.2 During employment

| A.7.2 During employment | | |
|---|---|---|
| **Objective**: To ensure that employees and contractors are aware of and fulfil their information security responsibilities. | | |
| **Sec.** | **Control#** | **Description** |
| A.7.2.1 | Management responsibilities | Management will require all employees and contractors to apply information security in accordance with the established policies and procedures of the organisation. |
| A.7.2.2 | Information security awareness, education, and training | All employees of the organisation and where relevant contractors will receive appropriate awareness education and training and regular updates in organisational policies and procedures, as relevant for their job function. |

A. D. DISSANAYAKA

## 7.3 Termination and Change of Employment

| A.7.3 Termination and change of employment | | |
|---|---|---|
| **Objective**: To protect the organization's interests as part of the process of changing or terminating employment. | | |
| **Sec.** | **Control#** | **Description** |
| A.7.3.1 | Termination or change of employment responsibilities | Information security responsibilities and duties that remain valid after termination or change of employment will be defined and communicated to the employee or contractor. |

A. D. DISSANAYAKA

# 8 Asset Management

## 8.1 Responsibility for assets

| **A.8.1 Responsibility for assets** | | |
|---|---|---|
| **Objective**: To identify organizational assets and define appropriate protection responsibilities. | | |
| **Sec.** | **Control#** | **Description** |
| A.8.1.1 | Inventory of assets | Information, other assets associated with information and information processing facilities will be identified and an inventory of these assets will be drawn up and maintained |
| A.8.1.2 | Ownership of assets | Assets maintained in the inventory shall be owned |
| A.8.1.3 | Acceptable use of assets | Rules for the acceptable use of information and of assets associated with information and information processing facilities will be identified, documented and implemented. |
| A.8.1.4 | Return of assets | All employees and external party users will return all of the organisational assets in the possession upon termination of their employment, contract or agreement. |

A. D. DISSANAYAKA

## 8.2 Information classification

| A.8.2 Information classification | | |
|---|---|---|
| **Objective**: To ensure that information receives an appropriate level of protection in accordance with its importance to the organisation. | | |
| **Sec.** | **Control#** | **Description** |
| A.8.2.1 | Classification of information | Information will be classified in terms of legal requirements, value, criticality and sensitivity to unauthorised disclosure or modification. |
| A.8.2.2 | Labelling of information | An appropriate set of procedures for information labelling shall be developed and implemented in accordance with the Information classification scheme adopted by the organisation. |
| A.8.2.3 | Handling of assets | Procedures for handling assets will be developed and implemented in accordance with the information classification scheme adopted by the organisation. |

### 8.2.1 Classification of information

| Type | Description |
|---|---|
| **A** | OFFICIAL - The majority of information that is created or processed by the public sector. |
| **B** | SECRET - Very sensitive information that justifies heightened protective measures to defend against determined and highly capable threat actors. |
| **C** | TOP SECRET - most sensitive information requiring the highest levels of protection from the most serious threats [7]. |

The following table identifies further the types of data associated with each of the sub-sets identified in the previous table (if required):

| Information | Government Security Classification | Type | Notes |
|---|---|---|---|
| e.g. Personal information as defined by the Data Protection Act (DPA) | OFFICIAL | B | Protection of personal information |
| e.g. Sensitive personal information as defined by the Data Protection Act (DPA) | OFFICIAL SENSITIVE | A | Protection of sensitive personal information. Note the more sensitive information may be marked Official-Sensitive |
| e.g. Legal privilege information | OFFICIAL SENSITIVE | A or B | Treat as sensitive personal information |
| e.g. Witness information | OFFICIAL SENSITIVE | A | Specifically sensitive as compromise may cause personal injury. Note the more sensitive information may be marked Official-Sensitive |

## 8.3 Media handling

| A.8.3 Media handling |
|---|

A.D. ISSANAYAKA

| **Objective**: To prevent unauthorized disclosure, modification, removal or destruction of information stored on media. | | |
|---|---|---|
| **Sec.** | **Control#** | **Description** |
| A.8.3.1 | Management of removable media | Procedures will be implemented for the management of removable media in accordance with the classification scheme adopted by the organisation |
| A.8.3.2 | Disposal of media | Media will be disposed of security when no longer required using formal procedures. |
| A.8.3.3 | Physical media transfer | Media containing information shall be protected against unauthorised access, misuse, of corruption during transportation. |

A. D. DISSANAYAKA

# 9 Access Control

## 9.1 Business requirements of access control

| **A.9.1 Business requirements of access control** | | |
|---|---|---|
| **Objective**: To limit access to information and information processing facilities. | | |
| **Sec.** | **Control#** | **Description** |
| A.9.1.1 | Access control policy | An access control policy will be established, documented, and reviewed based on business and information security requirements. |
| A.9.1.2 | Access to networks and network services | Users will only be provided with access to the network and network services that they have been specifically authorised to use. |

## 9.2 User access management

| **A.9.2 User access management** | | |
|---|---|---|
| **Objective**: To ensure authorized user access and to prevent unauthorized access to systems and services. | | |
| **Sec.** | **Control#** | **Description** |
| A.9.2.1 | User registration and de-registration | A formal user registration and de-registration process will be implemented to enable assignment of access rights. |
| A.9.2.2 | User access provisioning | A formal user access provisioning process will be implemented to assign or revoke access rights for all user types to all systems and services. |
| A.9.2.3 | Management of privileged access rights | The allocation and use of privileged access rights will be restricted and controlled. |
| A.9.2.4 | Management of secret authentication information users | The allocation of secret authentication information will be controlled through a formal management process. |
| A.9.2.5 | Review of user access rights | Asset owners will review users access rights at regular intervals. |
| A.9.2.6 | Removal or adjustment of access rights | The access rights of employees and external party users to information and information processing facilities will be removed upon termination of their employment contract or agreement or adjusted upon change. |

## 9.3 User responsibilities

| **A.9.3 User responsibilities** | | |
|---|---|---|
| **Objective**: To make users accountable for safeguarding their authentication information. | | |
| **Sec.** | **Control#** | **Description** |
| A.9.3.1 | Use of secret authentication information. | Users will be required to follow the organisation's practices in the use of secret authentication information. |

## 9.4 System and application access control

| **A.9.4 System and application access control** |
|---|
| **Objective**: To prevent unauthorized access to systems and applications |

A. D. DISSANAYAKA

| Sec. | Control# | Description |
|---|---|---|
| A.9.4.1 | Information access restriction | Access to information and application system functions will be restricted in accordance with the access control policy. |
| A.9.4.2 | Secure log-on procedures | Where required by the access control policy, access to systems and applications will be controlled by a secure log-on procedure. |
| A.9.4.3 | Password management systems | Password management systems will be interactive and will ensure quality passwords. |
| A.9.4.4 | Use of privileged utility programs | The use of utility programs that might be capable of overriding system and application controls will be restricted and tightly controlled. |
| A.9.4.5 | Access control to program source code | Access to program source code will be restricted. |

A. D. DISSANAYAKA

# 10 Cryptography

## 10.1 Encryption of Data in Transit

| **A.10.1 Cryptographic controls** | | |
|---|---|---|
| **Objective**: To make sure proper and effective use of cryptography to safeguard the confidentiality, authenticity and/or integrity of data. | | |
| **Sec.** | **Control#** | **Description** |
| A.10.1.1 | Policy on the use of cryptographic controls | A policy on the employment of cryptographic controls for protection of information will be developed and implemented. |
| A.10.1.2 | Key management | A policy on the utilisation and lifetime of cryptographic keys shall be developed and employed through their whole life cycle. |

A. D. DISSANAYAKA

# 11 Physical & Environmental Security

## 11.1 Secure Areas

| **A.11.1 Secure areas** | | |
|---|---|---|
| **Objective**: To prevent unauthorized physical access, damage, and interference to the organization's information and information processing facilities. | | |
| **Sec.** | **Control#** | **Description** |
| A.11.1.1 | Physical security perimeter | Security perimeters will be defined and used to protect areas that contain other sensitive or critical information and information processing facilities. |
| A.11.1.2 | Physical entry controls | Secure areas will be protected by appropriate entry controls to ensure that only authorised personnel are allowed access. |
| A.11.1.3 | Securing offices, rooms, and facilities | Physical security for offices, rooms, and facilities will be designed and applied. |
| A.11.1.4 | Protecting against external and environmental threats | Physical protection against natural disasters, malicious attacks or accidents will be designed and applied. |
| A.11.1.5 | Working in secure areas | Procedures for working in secure areas will be designed and applied. |
| A.11.1.6 | Delivery and loading areas | Access points such as delivery and loading areas, and other points where unauthorised persons could enter the premises will be controlled and if possible, isolated from information processing facilities to avoid unauthorised access. |

A. D. DISSANAYAKA

## 11.2 Equipment Security

| A.11.2 Equipment | | |
|---|---|---|
| **Objective:** To prevent loss, damage, theft or compromise of assets and interruption to the organization's operations. | | |
| **Sec.** | **Control#** | **Description** |
| A.11.2.1 | Equipment siting and protection | Equipment will be s and protected to reduce the risks from environmental threats and hazards and opportunities for unauthorised access. |
| A.11.2.2 | Supporting utilities | Equipment will be protected from power failures and other disruptions caused by failures in supporting utilities. |
| A.11.2.3 | Cabling security | Power and telecommunications cabling carrying data or supporting information services will be protected from interception, interference, or damage. |
| A.11.2.4 | Equipment maintenance | Equipment will be correctly maintained to ensure its continued availability and integrity. |
| A.11.2.5 | Removal of assets | Equipment, information, or software will not be taken off-site without prior authorisation. |
| A.11.2.6 | Security of equipment and assets off-premises | Security will be applied to off-site assets taking into account the different risks of working outside the organisation's premises. |

A. D. DISSANAYAKA

# 12. Key Barriers

- The management is ignoring the wrong practices in the company and hesitant to make changes to implement good practices.
- Senior management is not educated about the necessity nor the basic practices of the information security and convincing them is difficult especially with the “wait and see” aptitude.
- The management did not even aware about the company’s existing security policy let along the current status of the information security of the company.
- The key personals, the company relays highly to be successful, the scientists of the research team are already under pressure to produce new products, forcing them to change their usual practices appease to be very difficult.
- Implementing the security controls cost additional resource even though the funding for the information security is not regulated and already threatened which could leads to uncertainties and negativity with in the security team.
- Companywide trainings need to be conducted to educate all the employees and managers to effectively protect the information by employing best practices, this require additional resource but the likelihood of approving the funds by the management is uncertain.
- Since the security team has only three members, even with the correct number of findings it will take a huge amount of time to implement the controls and conduct trainings.

A. D. DISSANAYAKA

# 13 References


[1] Queensland Government Chief Information Office, “Implementing an ISMS Participant Guide,” Queensland Government, Australia, 2017.

[2] The Data Crew, “ISMS Information Security Policy,” The Data Crew, Manchester, 2016.

[3] V. K. Puthuseeri, “ISMS Implementation Guide,” Vinod Kumar Puthuseeri, 2006.

[4] P. Biswas, “ISO 27001:2013 Information Security Management System,” *Overview of an Information Security Management System,* 20 07 2019.

[5] itgovernance, “ISO 27001 Penetration Testing,” *How does penetration testing fit into my ISO 27001 project?,* 2020.

[6] Redscan Cyber Security Limited, “Identify and address vulnerabilities in line with ISO 27001 requirements,” *What is an ISO 27001 penetration test?,* 2021.

[7] Cabinet Office, “Government Security Classifications,” London, 2018.

[8] “Information Security World”.*Information Security Management System(ISO 27001.*


A. D. DISSANAYAKA