Security Management Plan

Pharm Universe

2022

Table of contents

Approval History

Version:	Reviewed By:	Approved By:	Approver's Position:	Date Approved:	Next Review Date:
SMP Draft	Chief Scientist Research	CEO	CEO	08/12/2022	15/12/2022
SMP Draft	Research Manager	Manager	Manager	22/12/2022	27/12/2022

Glossary:

Abbreviations	
Abbreviation	**Expansion**
SMP	Security Management Plan
ISMS	Information Security Management System
IP	Intellectual Property
PDCA	Planning, doing, checking and acting
R & D	Research and Development
FDA	Food and Drug Administration
SLE	Single loss Expectancy
ARO	Annual Rate of Occurrence
CISO	Chief Information Security Officer
GIS	Geographic Information System

1 Introduction

Pharmaceutical firm Pharm Universe implements the ISO 27001 information security standard when producing and supplying medications to consumers. The common security model, ISO 27001, elaborates on information about security management challenges. An efficient information system for organising the difficult activities of renowned pharmaceutical businesses is the standard system of ISO 27001. The present papers seek to showcase Pharm Universe's security management strategy and its methods for reducing the risks of security problems.

1.1 Background

An international pharmaceutical business with roughly 9000 workers is called Pharm Universe. The corporation, which has its headquarters in London, UK, also has modest offices there as well as in Hanover, Germany; Barcelona, Spain; Singapore; Hong Kong; and St. Louis, Missouri, USA. A new medication mix created by Pharm Universe will significantly reduce the danger of blood clots in the lungs and other body areas. Another concoction being developed by Pharm Universe greatly increases people's resistance to bacterial illnesses like pneumonia, a feat that medical science has long regarded as impossible. Additionally, research has begun on a drug that will aid older patients who are suffering from memory loss. Having access to competitor pharmaceutical formulations before they are made available on the market is a huge advantage since it saves time and money on the expensive and time-consuming research process. Industrial espionage in the pharmaceutical industry is possible. On the other hand, the pharmaceutical industry's worst-case scenario is having a formula stolen. There will be a significant financial loss as well as damage to the pharmaceutical industry's image.

1.2 Purpose

The following is the goal of this document, the Security Management Plan (SMP):

• Create the optimum state of information security practice by identifying and fusing a collection of information security attributes with business requirements.

• Establish the parameters and scope of the Pharm Universe Information Security Management System (ISMS).

• Tasks and obligations that are documented within the Pharm Universe ISMS.

• Establish an "information-centric security framework" with the main emphasis on low-cost risk mitigation measures and dangers related to IP production, handling, and storage.

• To educate, train, and make management and staff aware of environmental security issues.

• In line with ISO/IEC 27001 and other recommended standards, manage assets and regulate access.

1.3 Readership

The report's target audience is Pharm Universe's management and staff. Employees will be the audience who learns about the plan's implementation since they are the ones who leak the most information to the public. They will understand that if they act inappropriately, the organisation will reprimand them as a result.

2 Solution Overview

2.1 Security control overview

1) System and application access control (ISO/IEC 27001, A.9.4)

One of the controls listed in Annex A.9.4, which talks about the business needs for access control, is this one. This Annex A.9 control's goal is to restrict access to information and information processing infrastructure. It ensures that only authorised users are permitted access to a service, preventing unauthorised users from utilising it.

Establishing, documenting, and routinely assessing an access control policy with corresponding business and information security requirements is a necessity, according to control A.9.4.1 in particular. Asset owners should establish appropriate access controls, access rights, and user role restrictions to safeguard their assets, with the volume of information and the rigour of controls reflecting the dangers to information security that are related to it.

For Pharma Universe, it is crucial to take into account access restrictions' utility and justification.

The business needs that access restrictions for users and service providers must satisfy should be clearly stated [4].

2) Policy on the use of Cryptographic Controls (ISO/IEC 27001, A.10.1)

This control is a component of Annex A.10.1, cryptography, a term for secure information and communication methods that utilise mathematical ideas and a collection of rule-based computations known as algorithms to transform communications into forms that are challenging to read. It makes communication between sender and receiver safer since it prevents outsiders from hacking into it and reading the contents.

By assisting us in understanding and identifying risks and opportunities to focus on, this risk control might speed up the encryption process for our organisation. When faulty or missing keys are discovered, a risk assessment is helpful in navigating such risks and boosting information security during ISO 27001 implementation [5].

3) Controls against malware (ISO/IEC 27001, A.12.2.1)

Operation Security is the process of preventing leaks, loss, and damage to priceless information assets. This control is a Part of Annex A.12 operation security. Guidelines for the secure administration and monitoring of our information processing operations are provided in this Annex A.12. To avoid the loss or unauthorised transmission of vital information and to guarantee its confidentiality and integrity, proper alignment with Annex A.12 is necessary.

This control in particular discusses the defensive measures that must be put in place to guarantee the detection of malware attacks, protection from them, and recovery from them [6].

4) Technical vulnerability management (ISO/IEC 27001, A.12.6)

This control is a part of Annex A.12. Information on technological vulnerabilities of information systems used should be obtained promptly, the exposure of the organization to such vulnerabilities should be assessed and appropriate measures are taken to address the risk involved under this control [7].

5) Network Security Management (ISO/IEC 27001, A.13.1)

This control is a part of Annex A.13 Communications Security, which protects information and information systems from unauthorized access or modifications. A system's effectiveness is measured by how well it accomplishes its objectives while still preserving the ability to produce useful output.

The purpose of this Annex, especially this control, is to discuss securing data in networks and the information processing facilities that allow them. The management of network security and the preservation of data availability and integrity are two of the most crucial issues to concentrate on in this section [8].

6) Management of information security incidents, events, and weaknesses (ISO/IEC 27001, A.16.1)

Information security incidents might include any behaviour that jeopardises the safety of information technology operations or contravenes approved responsible usage guidelines. The standards for addressing information security events are outlined in Annex A.16, which includes this control.
This control's major goal is to make sure that our company always takes a sensible strategy to handling and disclosing information security incidents, such as breaches, unauthorized disclosure, data loss, or destruction, among other things [9].

2.2 Secure architecture scope

The management's usage of an ISO 27001 system and a security management system make up Pharm Universe's secure architecture scope. It has to do with protecting the company's sensitive data. Due to the increased possibility of information and chemical formulae utilised by businesses being leaked, the medical sectors are at risk. To prevent the GIS-based information and technological information utilised by pharmacies and clinical enterprises from leaking, the corporation creates an emergency evacuation strategy.

3 Scope

3.1 Assurance Approach

Take into mind the following aspects:

- Security policies and procedures are formed, considered by the environment, and communicated to all workers who may be affected.
- The highest levels of leadership support and are dedicated to information security.
- That information security policy and procedures are spelt out, regularly revised, and altered.
- The company risk profile is considered while developing the information security risk management plan, which is standardised and properly communicated.

3.2 Assurance Frameworks

The PDCA Model applied to ISMS procedures, which is the set of standards that facilitate the application of ISO/IEC 27001, is part of the Framework for Pharm Universe, which controls all risks and threats.

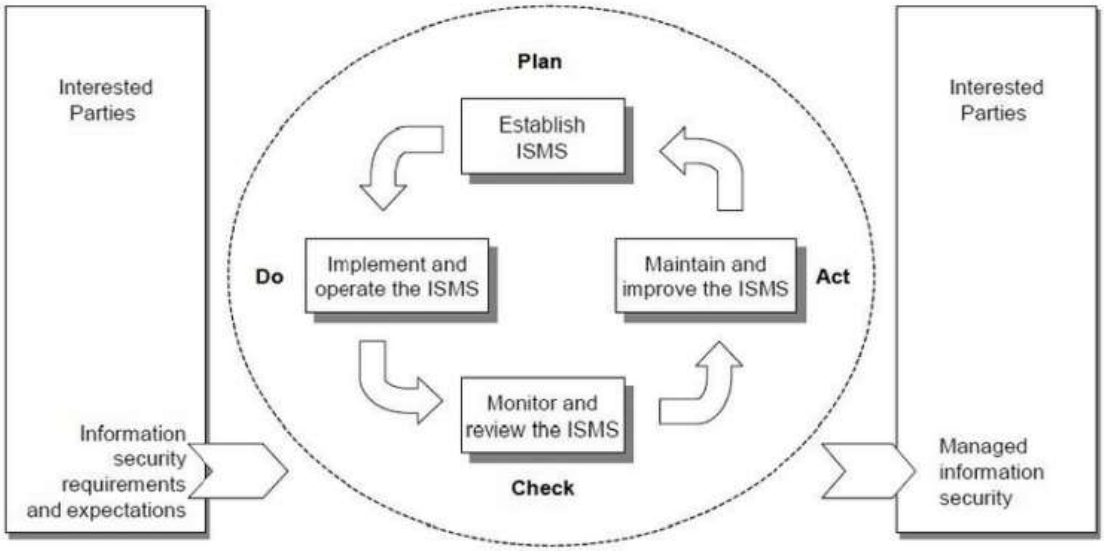

Figure 1: ISO 27001 Framework

3.3 Scope of Security Services

The following is a list of crucial security services to maintain the safety of the pharm universe:

- Confidentiality
- Data Integrity
- Authentication
- Authorization
- Non-repudiation or Key Management

3.4 Security Services Out of Scope

However, Pharm Universe excludes several vital security services from its coverage:

- Security Operation Centre (SOC)
- Threat Intelligence

4 Information Security Management System

Figure 4.1 ISO/IEC 27001:2013 control coverage [10]

4.1.1 Certification delivery schedule

A customised ISMS framework may help organisations with ISO 27001 certification maintain the CIA - Confidentiality, Integrity, and Availability - of corporate information.

• Better security measures, such as information protection and limited access, to thwart data abuse and theft and protect the assets of the firm.

• Making it easier for information to be recovered and for IT services to continue in line with corporate objectives.

• Assists in preparing a company for security lapses and online assaults.

• Organizations may run more effectively by conforming to contractual and legal requirements by adhering to defined rules, policies, and processes.

• ISMS aid organisations in building greater levels of trust in competitive marketplaces by assisting businesses in delivering trustworthy and secure services.

4.1.2 Risk Management

The risk management strategies include details on formulating rules for the pharmaceutical company's information security. Effective risk management strategies lower the likelihood of company data being hacked. As a result, Pharm Universe employs the risk management technique to deal with security-related difficulties.

4.1.3 Continual Improvement

The performance of the security system is always being improved, and the risk of data leaking is decreased. Additionally, the use of information and technology systems reduces the risks and

challenges related to data vulnerability. Pharm Universe is continually being processed to ensure security management.

4.1.4 Effectiveness measures

Companies employ effective measures including securing internal data and information as well as putting in place efficient procedures. Utilizing these techniques aids in lowering the threats to the security procedures of businesses like Pharm Universe. Additionally, Pharm Universe workers are not involved in creating policies to recognise the significance of information security policies. Maintaining the Pharm Universe's moral and legal bounds involves taking effective action.

4.2 Security Testing

4.2.1 Scheduled penetration testing

Penetration Testing Schedule												
Penetration Testing	Jan'21	Feb'21	Mar'21	Apr'21	May'21	Jun'21	Jul'21	Aug'21	Sept'21	Oct'21	Nov'21	Dec'21
All Database of Pharm Universe												
Cloud Services												
Applications												
Interal and External Network												

Figure 4.2.1 Penetration testing schedule for Pharm Universe

5 Information Security Policies

Due to the security dangers that the Pharm Universe faces, the organisation has adopted security management measures. The business employs efficient security management practices based on the international standard ISO 27001 By outlining the duties and obligations of each member of the management system, ISO 27001 defines the norms of efficient legal rules for the management of data and information (Stoica et al., 2020). As a result, Pharm Universe, a manufacturer of pharmaceuticals, developed several supporting rules relating to data protection and the production of legal certifications. Corporations use employee and IP databases to safeguard stored data and information and defend it from hackers and criminal organisations.

5.1 Policies and Standards

Control Description

Sec.	Obj.	Control#		Description
1	Policies for information security	ISO/IEC 27001, A.5.1.1		Pharm Universe rules have to be clear and precise. Combining all levels of policy into one document might not be the greatest approach. In this case, the top-level information security policy may easily refer to more specific policies.
2	Review of the policies for information security	ISO/IEC 27001, A.5.1.2		This control is essential to the continual upkeep, assessment, and revision of the ISMS. The information security policy should be updated as needed to maintain it current and represent how the pharm universe will effectively manage its risks during this maintenance operation, which should identify all changes that have an impact on the ISMS.

Policies For Pharm Universe

• Pharmacies are required to abide by legal specifications for a safety monitoring system that issues an audible, visual, or electronic alarm when an assault is discovered. The security system must have a backup plan in place in case the safety system is tampered with or rendered inoperable to maintain alertness and continued functioning.

• A monthly training and awareness programme explaining new dangers and attack vectors to the pharmaceutical industry will be organised. Any policy modification must be communicated to workers in advance.

• All employees and, if appropriate, contractors of the firm are required to get sufficient awareness education and training, as well as regular updates on the policies and practices of the organisation, as applicable to their job function.

• Those obligations and tasks that continue to apply after termination or change of employment must be established, communicated to the employee or third party, and enforced.

• Employees who have broken information security must face a proper and well-communicated disciplinary process.

• The operational categorization structure of the company must be followed in the design and implementation of asset management procedures.

• The organisation is in danger from the loss of data availability and confidentiality on removable media. Media assets such as backup tapes, discs, USB sticks, removable hard drives, CDs, DVDs, and printed materials must be managed through controls. By the categorization of the data stored on the media, procedures should be developed and put into place to ensure that approved media are used, maintained, and transported in a safe and controlled manner.

• When classifying information, legal constraints, value, criticality, and sensitivity to unauthorised disclosure or change must all be taken into account.

6 Organisation of Information Security

6.1 Operational Model

Figure 6.1 Operational Model of Pharm Universe

6.1.1 Roles and Responsibilities

Chief Executive Officer:

• Speaking on behalf of the business in communications with shareholders, regulatory bodies, and the general public.

• Overseeing the creation of the company's short- and long-term strategies.

• establishing and carrying out the organization's or company's vision and objective.

• Evaluating the performance of other senior executives inside the organisation, such as directors, vice presidents, and presidents.

• Retaining a full awareness of, among other things, the competitive market landscape, prospects for expansion, and industry innovations.

• Ensuring that all of the organization's operations uphold a high standard of social responsibility.

• Evaluating and monitoring the company's risks and taking steps to reduce them.

• Setting strategic goals and making sure they are quantifiable and measurable.

Chief Information Officer:

• Pick the right technologies and use them to your advantage to maximise strategic gains and streamline internal processes.

• Arrange for the installation of new systems and give IT professionals and other staff members guidance.

• Ensure top functioning of the organization's technology infrastructure.

• You are in charge of managing and organising IT-related tasks.

• Monitor technology advancements to see whether the company could gain a competitive edge.

• Assess the costs, advantages, and risks associated with information technology in order to offer management advice and suggestions.

The IT security team:

• Put up obstacles to prevent unwanted access to computer systems.

• Identify system flaws by keeping an eye out for peculiar activity.

• Conduct audits and analyse the current level of network security.

• Implement improvements as needed, and notify users of system security status by delivering performance reports regularly.

Department of Research:

• Create fresh solutions to the world's main issues.

• Respect for and comprehension of their colleagues' main points.

• Show loyalty to the business since they are a valuable asset.

• Create and develop novel medications that are beneficial to the human race.

6.1.2 Segregation of Duties

ISO/IEC 27001 Control References					Control Description
Sec. 5.1	Obj.	Control# 5.2.3			Control Description
1	Segregation of duties	ISO/IEC 27001, A.6.1.2			Role separation is a frequent company guideline that lowers the possibility of purposeful misuse and human error. There could be a few dishonest personnel in the pharmacy industry, even though most are usually honest. Equally honest people could be compelled to take actions that are inconsistent with who they are. A certain proportion of people risk getting worse at controlling their behaviour over time.

6.2 Teleworking

ISO/IEC 27001 Control References					Control Description
Sec.	Obj.	Control#			Description
1	Teleworking	ISO/IEC 27001, A.6.2.2			The user's home typically lacks the same level of physical protection, and they commonly allow family members and guests access to their office. Teleworking shouldn't be implemented until the pharm universe has created the necessary policies and procedures, put in place physical controls to secure the workspace, and sufficiently increased teleworking employees' awareness of the need to control physical and logical access to the information processing facilities used for teleworking activities. This is done to reduce the risks associated with it.

7 Personnel Security

ISO/IEC 27001 Control References					Control Description
Sec.	Obj.	Control#			Description
1	Screening	ISO/IEC 27001, A.7.1.1			Background checks must be carried out on all possible workers (strictly inside the research division) by all laws, regulations, and ethical standards. They must also be proportionate to the demands of the business, the type of data to be accessed, and any potential risks.
2	Terms and conditions of employment	ISO/IEC 27001, A.7.1.2			Employees and consumers of cloud services must be aware of their obligations under security and regulatory requirements for information protection, categorization, and usage of information processing facilities, as well as the repercussions of breaking such conditions.

7.1 Prior to joining

The employee must present their identity card and other personal security details before beginning work for the medical company. To reduce the dangers associated with data security and keep corporate operations operating smoothly, personal safety is crucial. As a result, the information supplied before joining a company is vital to the effectiveness of corporate operations. The information provided before joining is crucial to summarise for personal data protection to maintain the business data safe. As a result, organisations can quickly analyse the bid data and preserve the information by a business firm's requirements.

7.2 During employment

Personal information must be supplied throughout the hiring process to combat the concerns of data vulnerability. Having reliable staff improves a company's operational effectiveness (Sanyal et al., 2018). As a result, trust and staff productivity are crucial for Pharm Universe's data security. Additionally, cooperation among team members and employee behaviour support and encourage the security and appropriateness for business use of company information as well as data gathered from employee personal security.

7.2.1 Management Responsibilities

The roles and obligations of each employee at the pharmaceutical firm must be stated. Because it is important to be aware of each employee's duties when they are employed by the company. Pharmacists have a crucial part in society since they are involved in so many different jobs, such as checking the drug and their formulas. The operational model must thus outline the duties of each employee. It is necessary to distinguish the tasks and responsibilities of each employee, including pharmacists.

7.2.2 Security Training

Basic Security Awareness: Pharm Universe will provide all employees and third-party users with a minimal degree of security awareness training. Training will include the organization's security strategy, objectives, and structure as well as how workers are expected to function within it. It is necessary to present and describe the pertinent stages. Staff members should have easy access to the training materials, which should include policies and procedures, and notices of updates should be sent out if there are changes—ideally, just to those who would be affected. Updates to awareness and consistent action should be made as needed.

Technical Security Training: In addition to the fundamentals, employees with unique security responsibilities (and not just those in security-related professions) should get the requisite specialised training. A training programme should be created for everyone based on the specific knowledge and skills required for their position. Employees' total security knowledge may be considerably increased by attending relevant conferences and well-selected, often free activities. The person's training record should include information on all training and attendance at relevant events. All parties involved—employees, agency personnel, and third parties—should get the necessary training. Check to see if training providers employ staff that are suitably competent and if the curriculum is clear and suitable for the organization's goals.

7.3 Termination and Change of Employment

When an employee or pharmacist quits their position, the employer is required to give a crucial document proving that they did not engage in bad data management. The legal handling of employee personal information at the moment of termination is therefore crucial. It is crucial for Pharm Universe's commercial operations that the management and executives of the company give efficient management strategies to be done on employee personal data protection and implement the ISO 27001 standard. Ethics are crucial to uphold, thus if terminations like this occur, the organisation must adopt a successful model to keep the employee's personal information.

8 Asset Management

8.1 Responsibility for assets

ISO/IEC 27001 Control References					Control Description
Sec.	Obj.	Control#			Description
1	Inventory of assets	ISO/IEC 27001, A.8.1.1			Physical assets must be inventoried to meet accounting standards. Such an inventory should be kept by Pharm Universe for both this and information security purposes. For information security reasons, an inventory should also cover the organization's information assets. If they are appropriately coupled, this might be in the same system or a distinct one (for example, to identify which databases hold which data).
2	Ownership of assets	ISO/IEC 27001, A.8.1.2			The most important concept in terms of asset responsibility and protection is assigning asset ownership. The designation of an asset owner is necessary for all significant assets as well as assets with particular specifications (such as an employee database). This asset's owner is in charge of managing the asset's security. This involves classifying the asset, aiding risk assessments by giving data on the asset's commercial worth and significance to the organization's operations, ensuring the item is protected appropriately throughout daily usage and maintaining security classifications and control arrangements.
3	Acceptable use of assets	ISO/IEC 27001, A.8.1.3			In the world of pharmacy, guidelines for the appropriate use of information and resources related to information and information processing facilities must be identified, documented, and put into practice.
4	Return of assets	ISO/IEC 27001, A.8.1.4			All personnel, including users from outside the organisation, are required to return all items they have in their possession upon termination of employment, a contract, or an agreement.

8.1.1 Inventory of Assets

Serial #	Assets	Control #
1	Manufacturing Infrastructure	1-6
2	Database	1-6

8.1.2 Ownership of assets

The principal owner of the assets is the company's owner. Therefore, the CEO of Pharm Universe is the sole owner of all assets, including the security system and other IT-related resources.

8.1.3 Acceptable Use of Assets

Assets are utilised by providing each department inside the organisation with accurate budgets and parts.

8.2 Information classification

ISO/IEC 27001 Control References					Control Description
Sec.	Obj.	Control#			Description
1	Classification of information	ISO/IEC 27001, A.8.2.1			When classifying information, it is important to take legal constraints, value, criticality, and sensitivity to unauthorised disclosure or alteration into account.
2	Labelling of information	ISO/IEC 27001, A.8.2.2			A suitable set of information labelling processes must be developed and put into place in line with the organization's choice of information classification approach.
3	Handling of assets	ISO/IEC 27001, A.8.2.3			Asset management processes must be created and put into place in accordance with the operational categorization structure of the company.

8.3 Media handling

ISO/IEC 27001 Control References					Control Description
Sec.	Obj.	Control#			Description
1	Management of removable media	ISO/IEC 27001, A.8.3.1			The organisation is put in peril when data saved on removable media lose availability and confidentiality. Controls must be used in order to manage media objects such as printed media, backup tapes, discs, USB sticks, detachable hard drives, CDs, and DVDs. To ensure that authorised media are used, maintained, and transported in a safe and regulated manner that is consistent with the categorization of the data held on the media, procedures should be created and put into practice.
2	Disposal of media	ISO/IEC 27001, A.8.3.2			Some people consider something that is no longer required to be worthless. However, if it provides information, it could be useful and interesting to others. Serious breaches of confidentiality occur when seemingly useless drives, discs, cassettes, paper files, and printers are discarded without thought for their destruction.
3	Physical media transfer	ISO/IEC 27001, A.8.3.3			Risks linked with media transit include theft, unauthorised access, and misuse. The availability, confidentiality, and integrity of the data or programme stored on the medium are therefore compromised. To choose the best transit mode and controls (such as personal delivery by reputable couriers, safe parcel delivery, and post with confirmed delivery), a risk assessment should be used.

9 Access Control

9.1 Business requirements of access control

ISO/IEC 27001 Control References					Control Description
Sec.	Obj.	Control#			Description
1	Access control policy	ISO/IEC 27001, A.9.1.1			Business needs should be taken into account when assigning user access rights, which should then be expressly stated in the access control policy and authorised and reviewed on a regular basis by asset owners. Access that isn't necessary for carrying out the duties of the function should be restricted. This tactic is known as "least privilege."
2	Access to networks and network services	ISO/IEC 27001, A.9.1.2			Business networks, which can provide a few specific services, can benefit thousands of users involved in a variety of activities. Each customer could only need a small number of these services (such as email, shopping apps, and the intranet). Users should only have access to networks and network services that they are formally authorised to use, according to the access control policy.

9.2 User access management

ISO/IEC 27001 Control References					Control Description
Sec.	Obj.	Control#			Description
1	User registration and deregistration				A record of every information system, network, or service that a user has a business requirement to connect to should be preserved for each user, who should be formally recognised and given a unique identification by the organisation. Lack of registration control may result in a data breach, unauthorised change, and/or loss.
2	User access Provisioning				The organisation is more susceptible to misuse leading to breaches of confidentiality, data integrity, and availability when access privileges are distributed improperly. The necessary information system, network, service, or application(s), as well as the access requirements, should be listed on a user registration form.
3	Management of privileged access rights				It is regularly found that the allocation and usage of unnecessary privileges significantly increase the vulnerability of systems that have been infiltrated. Data unavailability, integrity loss owing to data modification, and confidentiality loss due to exposure are all frequent results.
4	Management of secret authentication information of users				User identification and authentication work hand in hand with access control, user registration, and privilege assignment. Passwords, which are still a common but not exclusive means of user authentication, are routinely used to do this.
5	Review of user access rights				Always base access permissions decisions on the requirements of the business. It should be cancelled after the need for access ceases to exist.

9.3 User responsibilities

ISO/IEC 27001 Control References					Control Description
Sec.	Obj.	Control#			Description
1	Use of secret authentication information	ISO/IEC 27001, A.9.3.1			Regarding the usage of private authentication data, users are required to abide by the organization's regulations.

9.4 System and application access control

ISO/IEC 27001 Control References					Control Description
Sec.	Obj.	Control#			Description
1	Information access restriction	ISO/IEC 27001, A.9.4.1			The owner of the information held in each application should establish the access rights and guidelines for that application in accordance with business requirements and the access control policy.
2	Secure logon procedures	ISO/IEC 27001, A.9.4.2			For authorised users, a log-on process should be straightforward, but it shouldn't divulge unnecessary details about the operating system, service, or application the user is seeking to access.

10 Cryptography

10.1 Encryption of Data in Transit

To reduce security risks at the organisation, Pharma Universe only accepts encrypted data. The protected features and codes can reduce any attacks on the information while the files are moved from one location to another.

The security measures that will be put in place to achieve data-in-transit for different Pharm Universe solutions are listed in the following table:

Solution Component	Encryption Methodology	Key Management Process	Compliancy Level
Configured VPN in firewall.	IPsec	Securely locked on VPN gateway devices	GDPR
Access Control	TLS 1.2	Digital certificates	GDPR
Database Security	RSA Algorithm	Asymmetric	ISO 27001
SIEM	AES Encryption	Symmetric	ISO 27001

10.2 Encryption of Data at Rest

The data can be protected and the data at rest will be encrypted with the use of specific keys and certificates with codes that are only accessible to Pharma Universe owners.

Solution Component	Encryption Methodology	Key Management Process	Compliancy Level
Database Security	RSA Algorithm	Asymmetric	ISO 27001
SIEM	AES Encryption	Symmetric	ISO 27001

10.3 Certificate and Key Management

Cryptographic keys are used to ensure the creation, dissemination, updates, any backup plan, and storage of the company's data. Utilizing specific keys and certificates by themselves also guarantees dealing with compromised keys in a secure and safe manner.

11 Physical & Environmental Security

11.1 Secure Areas

Limited knowledge and locations where the file cannot be created by any unauthorised access. The auditor can assist with the security aspects of Pharma Universe.

11.2 Equipment Security

Computers such as laptops, desktops, and other ICT tools can be used to keep confidential information only accessible to authorised key holders.

12 Operations Security

12.1 Operational procedures and responsibilities

ISO/IEC 27001 Control References					Control Description
Sec.	Obj.	Control#			Description
1	Documented operating procedures	ISO/IEC 27001, A.12.1.1			The organisation should make sure that there is adequate documentation available to support routine duties at work, such as media handling, computer room and mail handling management, backup, equipment maintenance, mobile working, and computer start-up and shutdown processes.
2	Change management	ISO/IEC 27001, A.12.1.2			Information security-related changes to the organisation, operational procedures, information processing infrastructure and systems must be closely monitored.
3	Capacity Management	ISO/IEC 27001, A.12.1.3			The production, test, and operational environments must be segregated to reduce the risk of unauthorised access or alterations to the organisational context.
4	Separation of development, test and operational environments	ISO/IEC 27001, A.12.1.4			The production, test, and operational environments must be segregated to reduce the risk of unauthorised access or alterations to the organisational context.

12.2 Protection from malware

ISO/IEC 27001 Control References					Control Description
Sec.	Obj.	Control#			Description
1	Controls against malware	ISO/IEC 27001, A.12.2.1			On a weak system, malware is very simple to instal, but it may be expensive and hard to eradicate. Anti-malware software usually misses relatively new infections, for example, so protection can only go so far. Nevertheless, it is crucial to apply and implement this control carefully. The only solution to this issue is IPS.

12.3 Backup

ISO/IEC 27001 Control References					Control Description
Sec.	Obj.	Control#			Description
1	Information Backup	ISO/IEC 27001, A.12.3.1			Every business is vulnerable to failing discs or tapes, as well as other problems that might cause data loss or software damage. To guarantee the integrity and accessibility of all crucial data and software, regular copies of other media should be made. The regularity will depend on how vital the data are. In certain systems, real-time backup—writing the duplicate concurrently with the original—is acceptable. Additional copying techniques, whether automatic or user-initiated, should be used if this is not practical.

12.4 Logging and monitoring

ISO/IEC 27001 Control References					Control Description
Sec.	Obj.	Control#			Description
1	Event logging	ISO/IEC 27001, A.12.4.1			Monitoring all relevant data might produce a large volume of data that has to be analysed rapidly. Automated methods and the right tools are crucial for separating genuinely significant events from the background noise of logging data. For instance, SIEM.
2	Protection of log information	ISO/IEC 27001, A.12.4.2			The logging equipment and data need to be secured against tampering and unauthorised access.
3	Clock synchronization	ISO/IEC 27001, A.12.4.4			All critical information processing systems must have their clocks synchronised to a single reference time source inside an organisation or security area.

12.5 Control of operational software

ISO/IEC 27001 Control References					Control Description
Sec.	Obj.	Control#			Description
1	Installation of software on operational systems	ISO/IEC 27001, A.12.5.1			Operating systems may be infected by unauthorised software, and unauthorised modifications to operational software may result in the loss of system and data integrity. Controls are necessary to reduce the risk of system failure, the admission of any unauthorised software, and the possibility of fraud.

12.6 Technical vulnerability management

ISO/IEC 27001 Control References					Control Description
Sec.	Obj.	Control#			Description
1	Management of technical vulnerabilities	ISO/IEC 27001, A.12.6.1			The organisation should have mechanisms in place to promptly identify and implement appropriate actions as well as to quickly discover any technological vulnerabilities in its information systems. There are several tools for vulnerability scanning that should be employed. Manual penetration testing could be necessary for systems that are extremely sensitive or crucial.
2	Restrictions on software installation	ISO/IEC 27001, A.12.6.2			Now that some user groups have more access, they can instal or modify the software that is necessary for their jobs. The usage of these rights has to be strictly restricted, with appropriate uses being tracked and documented.

12.7 Information systems audit considerations

ISO/IEC 27001 Control References					Control Description
Sec.	Obj.	Control#			Description
1	Information systems audit controls	ISO/IEC 27001, A.12.7.1			To minimise interference with business operations, audit requirements and activities requiring operational system verification must be adequately planned and agreed upon.

13 Network controls

13.1.1 Security of network services

Pharm Universe may implement security elements at multiple management levels in addition to outsourcing. Simply said, in order to maintain safe and current networks, organisations must include all forms of security measures in their network service agreements.

13.2 Information transfer

13.2.1 Agreements on information transfer

ISO 27001 can help with the creation of the identification standards' criteria. Technical controls must be utilised in conjunction with more formal transfer policy processes. To guarantee ongoing, total, and effective security protection, each of these must be operated, monitored, and reviewed.

13.2.2 Electronic messaging

End-to-end encryption can minimise any additional costs for the workforce when used with electronic messaging. In order to prevent unauthorised access, every electronic message must be protected, to put it another way.

13.2.3 Confidentiality or non-disclosure agreements

At Pharm Universe, no data may be moved without also changing the system's security. Non-disclosure agreements and confidentiality provisions must encompass any information that has to be safeguarded in full, according to organisations.

14 System Acquisition, Development and Maintenance

14.1 Security requirements of information systems

Pharma Universe can consider Data Protection Privacy Impact Assessments (DPIA) for security.

14.1.1 Information security requirements analysis and specification

Utilizing the National Cyber Security Centre will enhance Pharm Universe's security measures (NCSC).

While developing new systems or making modifications to existing ones, it's also critical to understand what the business needs are for security controls. Risk analyses can be helpful here.

14.1.2 Securing application services on public networks

It is essential to comprehend the different risk levels involved and the unique business needs for information protection, especially for services that have been provided through a public network like the internet. Accessibility, confidentiality, and integrity must all be considered, though. By carrying out the GDPR's requirements for encryption, especially for usage on public networks.

14.1.3 Protecting applications services transactions

Regulations and certification for ISO 27001 safeguard applications, especially when they make use of electronic signatures, encryption, and security protocols.

14.2 Security in development and support processes

14.2.1 Secure development policy

By creating software, Pharma Universe may have a secure infrastructure and reliable technology.

14.2.2 System change control procedures

Planning and specifications can be carried out using formal protocols.

14.2.3 Technical review of applications after operating platform changes

Including the efficient execution of processes and audit testing for additional software updates.

14.2.4 Restrictions on changes to software packages

Reduce the number of risk analysis and security control features.

14.2.5 Secure systems engineering principles

Utilize the engineering principles in ISO 270001.

14.2.6 Secure development environment

When proposals are required, taking no formal approval into account.

14.2.7 Outsourced development

When proposals are required, taking no formal approval into account.

14.2.8 System security testing

Develop trial-and-error testing tactics.

14.2.9 System Acceptance Testing

Think about software updates and modifications.

14.3 Test data

Think about software updates and modifications.

15 Supplier Relationships

15.1 Information security in supplier relationships

For information security management systems, establish an ISO 270001 certification. Also take into account the ISO-compliant supplier contract terms.

16 Information Security Incident Management

ISO/IEC 27001 Control References					Control Description
Sec.	Obj.	Control#			Description
1	Responsibilities and procedures	ISO/IEC 27001, A.16.1.1			Management responsibilities and processes must be established in order to respond to information security events in a prompt, efficient, and organised manner.
2	Reporting information security events	ISO/IEC 27001, A.16.1.2			Incidents involving information security must be notified as soon as is practical using efficient management channels.
3	Reporting security weaknesses	ISO/IEC 27001, A.16.1.3			Employees and outside parties are required to identify and report any information security issues in the organization's information systems and services.
4	Assessment of and decision on information security events	ISO/IEC 27001, A.16.1.4			It is necessary to assess information security occurrences to see if they qualify as information security incidents.
5	Response to information security incidents	ISO/IEC 27001, A.16.1.5			Information security incidents must be addressed in accordance with established processes.
6	Learning from information security incidents	ISO/IEC 27001, A.16.1.6			To reduce the likelihood of and the effect of future information security events, knowledge gleaned from analysing and resolving them will be applied.
7	Collection of evidence	ISO/IEC 27001, A.16.1.7			The organisation has to develop and put into action strategies for locating, gathering, acquiring, and keeping data that can be used as evidence.

16.1.1 Responsibilities and procedures

There will be a security incident handling governance framework which will put overall process control in the hands of Pharma Universe Operational Security Team.
Below is a table illustrating the identified roles and responsibilities in the process:

Role	Who	Description
IT Security Team	Pharm Universe	The group is in charge of upholding the network's security protocols throughout all of the organization's departments, as well as securing and keeping track of all devices and important resources. Moreover, gathering and managing all network logs.
Management	Pharm Universe	The manager's job is to assist the team and issue the necessary permissions quickly so that the situation may be handled.
System and Network Team	Pharm Universe	Any delays or unexpected or suspicious findings must be reported promptly to the IT security team. The team is also responsible for providing a detailed report on the network and the environment's important systems.
Application Team	Pharm Universe	The group is in charge of creating and maintaining the essential application for the pharmaceutical industry using the correct coding technique.

17 Business Continuity

17.1 Information security continuity

17.1.1 Planning information security continuity

Preparing for a core team meeting to review Pharma Universe's security measures.

17.1.2 Implementing information security continuity

Taking into account the continuity of security level and making sure any escalation trigger points.

17.1.3 Verify, review and evaluate information security continuity

At Pharm Universe, periodic reviews are an appropriate way to reduce security concerns while utilising cutting-edge technology.

17.1.4 Resilience

The software can be changed or deleted to eliminate any undesired features or additions.

18 Compliance

18.1 Compliance with legal and contractual requirements

ISO/IEC 27001 Control References					Control Description
Sec.	Obj.	Control#			Description
1	Identification of applicable legislation and contractual requirements	ISO/IEC 27001, A.18.1.1			All applicable legal, legislative, regulatory, and contractual requirements, as well as the company's strategy for satisfying these requirements, must be openly acknowledged, documented, and kept up to date for each information system and the organisation.
2	Intellectual property rights	ISO/IEC 27001, A.18.1.2			If organisations do not abide by the guidelines, they run the danger of exceeding the copyright usage restrictions. There is a significant possibility of legal action being taken against the company and specific workers when software is used on more computers than is allowed under its licence.
3	Protection of Records	ISO/IEC 27001, A.18.1.3			A few examples of crucial records and documents that must be preserved and protected from loss, confidentiality breaches, or change are accounting records, database records, transaction logs, audit logs, and operational procedures.
4	Privacy and protection of personally identifiable information	ISO/IEC 27001, A.18.1.4			As required by current law and regulation, the privacy and protection of personally identifiable information must be protected when applicable.
5	Regulation of cryptographic controls	ISO/IEC 27001, A.18.1.5			Analyzing the time and resources needed to comply with legal and regulatory requirements and guidelines for the usage of cryptographic controls is essential. When considering whether to impose cryptographic restrictions, the findings of these assessments should be taken into account.

18.1.1 Identification of applicable legislation and contractual requirements

Regulations	Who needs to comply	Security Areas Cover	Compliance Requirement
HIPAA	US healthcare organisations and partners	Creating, storing, and transmitting electronic protected health information	All major "Best Practice Security" areas
Sarbanes Oxley (SOX) & Acctg Standards COSO, COBIT®, SAS	US public companies	Defined to secure the public against corporate fraud and misrepresentation.	All major "Best Practice Security" Areas
PCI DSS (Also Covered by Breach Laws)	Merchants who take credit cards	Privacy of Customer Financial Data	Varies by size of merchant, requires Best Practices plus 3rd Party Quality Risk Assessments
GLBA - Federal Law 106 - 102 FDIC/FFIEC	US financial institutions	A Financial Services Act - Privacy of Personal Info. Safety	"Best Practices", Security Two-Factor Authentication, ensure

Guidelines FACT U.S. Patriot Act (2001)		of Internet based Products & Services Fair and Accurate Credit Transactions Anti – Terrorism	Accuracy & Safety Identity Verification
Breach Laws in 31 US States Including California SB 1386	Any company storing, or accessing private consumer data	Consumer Privacy - Security Breach Acts	All major "Best Practices Security" areas
EU General Data Protection Regulation (GDPR) and Privacy Regulations	Any EU organisation holding personal data	Personal data	All major best practice areas

18.2 Information security reviews

ISO/IEC 27001 Control References					Control Description
Sec.	Obj.	Control#			Description
1	Independent review of information security	ISO/IEC 27001, A.18.2.1			The organization's strategy for managing information security and its execution (i.e., control goals, controls, policies, processes, and procedures for information security) must be independently evaluated on a regular basis or if significant changes take place.
2	Compliance with security policies and standards	ISO/IEC 27001, A.18.2.2			Managers must routinely assess how well information processing practises and other duties related to their roles and responsibilities adhere to pertinent security policies, standards, and other security requirements.
3	Technical compliance review	ISO/IEC 27001, A.18.2.3			To make sure that they adhere to the organization's information security policies and standards, information systems must undergo frequent audits.

APPENDIX 1 - Assets

1) **Manufacturing Infrastructure:** Pharma Universe focuses on making high-quality of products by manufacturing them precisely. The company has a range of uniquely identifiable products as it continuously invents ways to improvise on the previous product range. This means the manufacturing infrastructure is of the utmost importance as they use precise techniques which helps them produce the exact same quality every time and they also have a unique mechanism which helps them create new product ranges. This asset directly affects quality. They rely heavily on the manufacturing process in order to retain their customers. The manufacturing infrastructure can include:-
    a. Agitators
    b. Centrifuges
    c. Granulators
    d. Homogenisers
    e. All components monitored under SCADA systems

2) **Database:** Data is one of the most critical assets of twenty first century. Data can help this organisation to set prices, control demand and supply, when to do clinical trials. Our focus is on the internal database that can be information related to the company's systems and functions within. Database can contain information about:-
    a. Drug Formula
    b. Clinical Trial Data
    c. Medical Records
    d. Research and Development
    e. Employees
    f. Supply-chain
    g. Client

APPENDIX 2 – Risks

Risk ID	Risk Factor	CVSS Rating	Risk
001	Hacking	**9.8**	**H**
002	Ransomware	**7.8**	**H**
003	Denial of Service (DoS)	**7.5**	**H**
004	Insider Threat	**7.0**	**H**
005	Drug Formula Leak	**6.5**	**M**

Table 1: CVSS ratings of risks

1) Hacking

Accessing IT systems from outside of an organisation still presents a lucrative target for hackers. A corporation like Pharma Universe faces a serious risk from network hacking. Hackers have historically tried to access the business's internal systems and move within the network to see what services are being used. Once they get an initial foothold, they may manipulate the process to take advantage of the weaknesses and interfere with the production units. The supply chain might be disrupted and the entire production facility could go offline as a result.

CVSS Base Score: 9.0
Impact Subscore: 6.0
Exploitability Subscore: 2.3

Figure 1: CVSS score [1]

2) Ransomware

This particular kind of malware tries to encrypt data and then demands a ransom in exchange for the release of an unlock code. Visiting unsafe websites or opening infected emails are the two main ways that ransomware spreads. In 2021, ransomware affected 55% of industrial and production firms [2]. So, Pharma Universe has a significant chance of contracting ransomware. Due to this danger, the manufacturing unit and other organisational activities may be impacted, which might damage the company's reputation with the general public.

CVSS Base Score: 7.8
Impact Subscore: 5.9
Exploitability Subscore: 1.8

Figure 2: CVSS score [1]

3) Distributed Denial of Service (DDoS)

A denial-of-service (DoS) attack aims to overburden the resources of a target system, render it inoperable, and prevent people from accessing it. In a DDoS attack, a large number of compromised computers or other devices are used in a coordinated attack against the target system.

DDoS assaults are frequently combined with other online threats. These assaults may begin with a denial of service to distract security personnel and cause confusion while carrying out more covert actions to steal data or do other harm. Research by Cloudflare [3] found that the number of DDoS assaults increased by 641% QoQ during Q4'21.

Pharma universe is vulnerable to such attacks, in which a perpetrator may attempt to disrupt organisation activities by flooding the network or may trick security employees by simulating a DDoS in order to acquire additional sensitive data from the server.

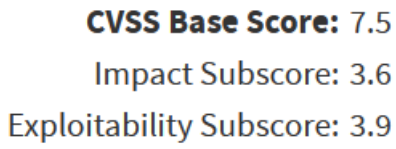

Figure 3: CVSS Rating [1]

4) Insider Threat

If our company employs personnel (full-time or contract workers), there is a chance that they might inadvertently or purposefully leak data. It is impossible to overestimate the harm that may be caused by a document leak.

If not handled properly, this might pose the biggest threat to Pharma Universe since anybody who interacts with clients or scientists and researchers from the R&D team could leak secrets. The firm may lose its position in the market if the specifics of the purchase or the secret medicine formula are made public.

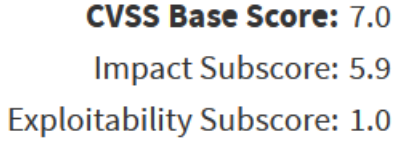

Figure 4: CVSS Rating [1]

5) Drug Formula Leak

For a pharmaceutical company, its drug design and the drug formulas are its precious assets. There can be various types of research going on related to disease and the most effective drug against it. The organization might lose its race against the invention of a new product if someone else replicates it. Hence, this can be one of the most potential risks that a

pharmaceutical firm can encounter. This can result in the loss of investors if the secret information is out in public and unable to take first mover's advantage.

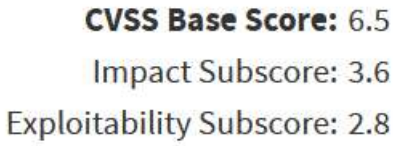

Figure 5: CVSS Rating [1]

Category	High Risk Asset Character	Manufacturing Infrastructure	Database
Confidentiality	Persistently contains Level 1 data	No	Yes
Integrity	Breach of data integrity could result in severe legal or financial risk to the company	Yes	Yes
	Breach of data integrity causes significant impact on critical company business processes	Yes	Yes
	Breach in system integrity could expose data that could result in putting the Company in severe legal or financial risk	No	Yes
	Breach in system integrity could put Priority 1 or Priority 2 assets at high risk of inappropriate data exposure, lack of integrity or availability	Yes	Yes
Availability	Service interruption puts the company at some legal or financial risk	Yes	Yes
	Loss of data puts the company at significant legal or financial risk	Yes	Yes
	Service interruption causes significant impact on critical company business processes	Yes	No
	Loss of data causes significant impact on critical company business processes	Yes	Yes
	A significant amount of university resources are required to	Yes	Yes

Table 2: Asset risk level

APPENDIX 3 – Controls

Using this outstanding foundation, the internationally renowned ISO/IEC 27001 standard assists enterprises in managing and safeguarding their information assets so that they stay safe and secure. It benefits an organisation to continuously assess and improve how they accomplish this, both for the now and for the future.

It is crucial to protect sensitive economic information and personal data. An organisation may put into practice a solid strategy for managing information security (infosec) and developing resilience with the aid of ISO/IEC 27001. The ISO 27001 accreditation may assist firms in formalising operations, enhancing info-sec procedures, and fostering stakeholder and customer trust.

The 114 controls in the ISO 27001 checklist are broken down into 14 categories. The ISO 27001 Annex A lists these controls.

1) System and application access control (ISO/IEC 27001, A.9.4)

   One of the controls listed in Annex A.9.4, which talks about the business needs for access control, is this one. This Annex A.9 control's goal is to restrict access to information and information processing infrastructure. It ensures that only authorised users are permitted access to a service, preventing unauthorised users from utilising it.

   Establishing, documenting, and routinely assessing an access control policy with corresponding business and information security requirements is a necessity, according to control A.9.4.1 in particular. Asset owners should establish appropriate access controls, access rights, and user role restrictions to safeguard their assets, with the volume of information and the rigour of controls reflecting the dangers to information security that are related to it.

   For Pharma Universe, it is crucial to take into account access restrictions' utility and justification.

   The business needs that access restrictions for users and service providers must satisfy should be clearly stated [4].

2) Policy on the use of Cryptographic Controls (ISO/IEC 27001, A.10.1)

   This control is a component of Annex A.10.1, cryptography, a term for secure information and communication methods that utilise mathematical ideas and a collection of rule-based computations known as algorithms to transform communications into forms that are challenging to read. It makes communication between sender and receiver safer since it prevents outsiders from hacking into it and reading the contents.

   By assisting us in understanding and identifying risks and opportunities to focus on, this risk control might speed up the encryption process for our organisation. When faulty or missing keys are discovered, a risk assessment is helpful in navigating such risks and boosting information security during ISO 27001 implementation [5].

3) Controls against malware (ISO/IEC 27001, A.12.2.1)

   Operation Security is the process of preventing leaks, loss, and damage to priceless information assets. This control is a Part of Annex A.12 operation security. Guidelines for the secure administration and monitoring of our information processing operations are provided in this Annex A.12. To avoid the loss or unauthorised transmission of vital information and to guarantee its confidentiality and integrity, proper alignment with Annex A.12 is necessary.

   This control in particular discusses the defensive measures that must be put in place to guarantee the detection of malware attacks, protection from them, and recovery from them [6].

4) Technical vulnerability management (ISO/IEC 27001, A.12.6)

This control is a part of Annex A.12. Information on technological vulnerabilities of information systems used should be obtained promptly, the exposure of the organization to such vulnerabilities should be assessed and appropriate measures are taken to address the risk involved under this control [7].

5) Network Security Management (ISO/IEC 27001, A.13.1)

This control is a part of Annex A.13 Communications Security, which protects information and information systems from unauthorized access or modifications. A system's effectiveness is measured by how well it accomplishes its objectives while still preserving the ability to produce useful output.

The purpose of this Annex, especially this control, is to discuss securing data in networks and the information processing facilities that allow them. The management of network security and the preservation of data availability and integrity are two of the most crucial issues to concentrate on in this section [8].

6) Management of information security incidents, events, and weaknesses (ISO/IEC 27001, A.16.1)

Information security incidents might include any behaviour that jeopardises the safety of information technology operations or contravenes approved responsible usage guidelines. The standards for addressing information security events are outlined in Annex A.16, which includes this control.

This control's major goal is to make sure that our company always takes a sensible strategy to handling and disclosing information security incidents, such as breaches, unauthorized disclosure, data loss, or destruction, among other things [9].

APPENDIX 4 – Estimated Effectiveness

1) **Qualitative analysis for System and application access control (ISO/IEC 27001, A.9.4)**

		Impact		
		Low	**Medium**	**High**
Probability	**Low**	Low Risk	Low Risk	Medium Risk
	Medium	Low Risk	Medium Risk	High Risk
	High	Medium Risk	High Risk	High Risk

Implementations of PCLs and DCLs:

ISO 27001 COST BENEFIT ANALYSIS

COMPANY NAME	Pharm Universe	DATE CONDUCTED	12/12/2022
ISO STANDARD	ISO 27001	COMPLETED BY	CISO

QUANTITATIVE ANALYSIS	YEAR 1	YEAR 2	YEAR 3	YEAR 4	TOTAL
NON-RECURRING COSTS					
Implementation Support costs (see Tab A)	£ 1,250,000.00				£ 1,250,000.00
Employee hours costs (see Tab B)	£ 1,852,400.00				£ 1,852,400.00
Certification Body costs (if applicable - see Tab C)	£ -				£ -
Certificate of Attestation costs	£ -				£ -
TOTAL NON-RECURRING COSTS	£ 3,102,400.00	£ -	£ -	£ -	£ 3,102,400.00
RECURRING COSTS (ANNUAL)					
Management System maintenance costs (see Tab D)		£ 59,874,200.00			£ 59,874,200.00
Additional employee hours costs (see Tab B)		£ 55,875,520.00			£ 55,875,520.00
Certification Body costs (if applicable - see Tab C)		£ -			£ -
TOTAL RECURRING COSTS	£ -	£ 115,749,720.00	£ -	£ -	£ 115,749,720.00
TOTAL COSTS	£ 3,102,400.00	£ 115,749,720.00	£ -	£ -	£ 118,852,120.00

Residual Risk:

- DNS attack
- Spoofed DNS risk
- ARP Spoofing attack

2) **Quantitative analysis for Controls against malware (ISO/IEC 27001, A.12.2.1)**

Several considerations for the quantitative analysis of the pharmaceutical industry:

• Pharm Universe has operating reserves of around $20 million and produced sales of over $500 million in 2012.

• The goal for this year is to increase market share to 10%. By the end of last year, the pharm universe market share has increased sales volume in dollars.

Annual loss Expectancy: Over time, money loss is anticipated.

For instance

Likelihood/frequency	Impact/consequence
Less than once per year	Up to $100
Every year	Up to $1,000
Every month	Up to $10,000
Every week	Up to $100,000
Every day	Up to $1,000,000
Every hour	More than $1,000,000

Single loss Expectancy: Money expected to be loss if incident occur 1 time.

Annual Rate of Occurrence: How many times in 1 year interval the incident is expected to Occur.

Estimated Value of Database is USD 5 Million (SLE)

4/12= 0.3 (ARO)

4 = Number of incidents in 1 year

12= Number of months in 1 year

ALE = SLE × ARO

ALE= USD 5 million * 0.3

ALE= 15 million

Pharm Universe can expect USD 15 million loss every year if the formula gets revealed or leaked due to any hack.

Cost Benefit Analysis

ISO 27001 COST BENEFIT ANALYSIS

COMPANY NAME	Pharm Universe	DATE CONDUCTED	12/12/2022
ISO STANDARD	ISO 27001	COMPLETED BY	CISO

QUANTITATIVE ANALYSIS	YEAR 1	YEAR 2	YEAR 3	YEAR 4	TOTAL
NON-RECURRING COSTS					
Implementation Support costs (see Tab A)	€ 2,500,000.00				€ 2,500,000.00
Employee hours costs (see Tab B)	€ 40,000.00				€ 40,000.00
Certification Body costs (if applicable - see Tab C)	€ -				€ -
Certificate of Attestation costs	€ -				€ -
TOTAL NON-RECURRING COSTS	€ 2,540,000.00	€ -	€ -	€ -	€ 2,540,000.00
RECURRING COSTS (ANNUAL)					
Management System maintenance costs (see Tab D)		€ 12,000.00			€ 12,000.00
Additional employee hours costs (see Tab B)		€ 100,000.00			€ 100,000.00
Certification Body costs (if applicable - see Tab C)		€ -			€ -
TOTAL RECURRING COSTS	€ -	€ 112,000.00	€ -	€ -	€ 112,000.00
TOTAL COSTS	€ 2,540,000.00	€ 112,000.00	€ -	€ -	€ 2,652,000.00

3) **Quantitative analysis for Cryptographic Controls (ISO/IEC 27001, A.10.1)**

Estimated Value of Production environment

USD 7 Million (SLE)

4/12= 0.3 (ARO)

4 = Number of incidents in 1 year

12= Number of months in 1 year

ALE = SLE × ARO

ALE= 7 million * 0.3

ALE= USD 14 million

Pharm Universe can expect USD 14 million loss every year if the database gets revealed or leaked due to any hack.

APPENDIX 5 – Security Policy

1) Implementing System and application access control (ISO/IEC 27001, A.9.4):-

Policies for Information Access Restriction (ISO/IEC 27001, A.9.4.1):

- Using menus to restrict access to application system features.
- Limiting the information to which a particular user has access.
- Read, write, remove, and execute control capabilities for users.
- Regulating the access privileges of other programmes.
- Lowering the outputs' data density.
- To separate sensitive applications, application data, and systems from the rest of the network, use physical or logical access control.

Policies for Secure log-on Procedures (ISO/IEC 27001, A.9.4.2):

- To avoid interception and unauthorised use, authentication data should be transferred and kept in encrypted form.
- Log-on procedures should be designed in a way that makes it difficult to bypass them in order to prevent interception and misuse.
- Additionally, a notice indicating access is only permitted by those with authorization should be included.
- Both successful and unsuccessful log-ons and log-offs should be securely documented in order to provide forensic evidence, and notifications for failed attempts and suspected lock-outs should be taken into consideration.
- Depending on the system, access may need to be limited to particular days or times of the week or even to particular places.

2) Implementation of policy on the use of Cryptographic Controls (ISO/IEC 27001, A.10.1):-

- Users who need it are given instruction on how to apply cryptographic controls and secure general information.
- A risk assessment process must contain the essential computations relating to the strength, kind, and quality of the encryption method.
- use of encryption to protect data sent by portable or mobile media devices.
- Develop plans for keeping encryption keys secure.
- Implementing policy, key management, and quality generation are among the roles and duties.
- Follow the rules of encryption.

3) Implementing Controls against malware (ISO/IEC 27001, A.12.2.1):-

- An establish a written policy prohibiting the usage of illegal software.
- Putting in place safeguards to stop or catch the usage of unlicensed software.
- Implement measures to prevent or identify the usage of known or suspected harmful websites.
- Establish a defined risk management policy that outlines the security precautions to be followed while receiving files and information from or via external networks.

- Reducing malware-exploitable weaknesses, for example, by managing technological weaknesses.
- Undertake regular software and data quality inspections of programmes that support crucial activities.
- A formal examination into the discovery of unauthorised files or modifications will be conducted.
- Installing and maintaining malware and repair programmes as a preventative measure or routine test for scanning media and systems; administered scanning ought to consist of:
    - Before utilising any files downloaded from networks or any storage media, check them for viruses.
    - Checking for viruses in downloaded files and email attachments; the scan will be carried out at many locations, including mobile devices, email servers, and network access points for the company.
    - Web pages are scanned for malware.
- Specify malware prevention policies and obligations for systems, training on using them, reporting, and malware recovery.
- Putting in place the essential business continuity strategies, such as the software backup and recovery setups required to recover from malware assaults.
- Use of information-gathering techniques, such as subscribing to mailing lists or websites that provide updates on malware.
- Putting in place malware information verification processes to verify the precision and calibre of the material in advisory bulletins; Managers should make sure that a qualified source, such as recognised journals, trustworthy websites, or software vendors, is used to distinguish between fake malware and actual malware.
- Settings in isolation that could have disastrous consequences.
- Restricting removable media while using the company's system.

4) Implementing Technical vulnerability management (ISO/IEC 27001, A.12.6)

Policies for Management of technical vulnerabilities (ISO/IEC 27001, A.12.6.1):

- Informational resources, which will be updated when the inventory changes and may also contain new resources, are targeted at finding and bringing to light technical flaws in software and other technologies.
- establishing a timetable for reacting to alerts about potential technological vulnerabilities.
- The organisation will take action to reduce the risks when a possible technology flaw is discovered; such may include patching vulnerable software or implementing additional safeguards.
- Information security incident response processes and change management protocols should be followed depending on how quickly a technical issue has to be fixed.
-
- If a patch is available from a reliable source, it should be installed after analyzing the risk of doing so (comparing the danger posed by the vulnerability with the risk of doing so).
- Before downloading, the patch has to be examined and checked to ensure that it is secure and won't have any negative impacts.
- For each operation carried out, audit logs should be kept.

- High-risk systems ought to come first.
- putting in place a strategy for dealing with vulnerabilities when no workable defences are available. The organisation should evaluate the risks involved in dealing with such a vulnerability and create the proper investigative and remedial actions.

Policies for Restrictions on software installations (ISO/IEC 27001, A.12.6.2):

- Employees are not permitted to bring software from home or download it from the Internet without permission. It is not allowed.
- A request needs to be sent to the IT department whenever an employee notices a requirement for the use of a certain piece of software. The request may be kept on file as a record or as proof.
- The IT division will ascertain whether the company has a licence for the required programme.
- If a licence is available, the IT department contacts the worker and runs the required programme on the user's computer.
- In the absence of a licence, a responsible party must determine whether the requested software is required for the employee to fulfil their job. If the programme is expensive, it is also necessary to consider the purchase's financial viability when performing the evaluation.
- Whether the programme is expensive, should be examined to see if there are any cheaper or even free alternatives available (Total Cost of Ownership must be calculated).
- The top management should be involved in the selection of new software.
- Once a choice has been chosen, the IT staff will go ahead and install the programme and add it to their inventory.

5) Implementing Network Security Management (ISO/IEC 27001, A.13.1)

Policies for Network Controls (ISO/IEC 27001, A.13.1.1):

- Responsibility and processes for managing networking equipment should be defined.
- When required, the responsibility for network operations can be separated from computer operations.
- Specific controls may also be required to preserve the availability of network services and linked computers, as well as the confidentiality and integrity of data transfer via public networks, wireless networks, and secured networks and applications.
- To capture and identify behaviours that may or may not be relevant to information security, appropriate logging and monitoring should be utilised.
- To strengthen the service supplied to the organisation and to guarantee efficient control of all information processing infrastructures, close coordination of management operations should be provided.

Policies for Network Controls (ISO/IEC 27001, A.13.1.2):

- Technologies including authentication, encryption, and network connection restrictions are used to secure network services.

- The security and network connection rules specify the technical requirements for a secure connection to the network services.
- When necessary, the network service uses procedures to limit access to network services or applications.

Policies for Segregation in networks (ISO/IEC 27001, A.13.1.3):

- Split up massive networks.
- Think about logical and physical division.
- Set domain boundaries.
- Define the domain-to-domain traffic rules.
- Utilize user-level network access control, encryption, and authentication methods.

6) Implementing Management of information security incidents, events, and weaknesses (ISO/IEC 27001, A.16.1)

Policies for Responsibilities & Procedures (ISO/IEC 27001, A.16.1.1):

- Designing an incident response plan.
- Information security event monitoring, detection, analysis, and reporting.
- Keeping track of incident management actions.
- Forensic evidence handling.
- Evaluating information security incidents and vulnerabilities and making decisions.
- Responding both internally and internationally to a security situation.

Policies for Response to Information Security Incidents (ISO/IEC 27001, A.16.1.5):

- Quickly gathering proof.
- Forensic investigation of information security.
- Incidents are being escalated as necessary.
- Recording all reaction actions for analysis in the future.
- Giving appropriate internal and external parties the specifics of the information security event.
- Addressing any information security flaws that are the cause or a contributing factor.
- Once all issues have been resolved and action taken, formally closing and documenting the event.
- Examining the occurrence to determine its cause.

APPENDIX 6 – Key Barriers

- The management's current attitude and executives' lack of understanding and engagement in achieving an open state of increased information security is the primary obstacle in the pharmaceutical industry. Overcoming this barrier will require a significant effort on the part of the pharmaceutical industry to meet its security goals.
- The difficulty in communicating with the Research Team Manager is that he is extremely busy. We can deploy on-premises storage for the formula instead of storing IP on the cloud. Gaining confidence in this approach is a difficult task.
- They are unconcerned about data security and the majority of them take it for granted. Additionally, their "wait and see" attitude makes it difficult to achieve information security.
- How personnel leave the company is another major problem. Significant research output and intellectual property may be stolen by departing staff, and this has to be addressed on a more personal level.
- Given how challenging and unapproachable the documentation for ISO 27001 is, it may be the most significant obstacle to the deployment of an ISMS. Documentation is crucial, and a non-skilled individual might provide a barrier to installation.
- Although the CEO has claimed that he is taking a "wait and watch" attitude to information security, the present budget of the pharm universe security team includes the payroll as well as a few network security initiatives that were started before I arrived. Budgetary Obstacle: Because it requires several resources, including the installation of suggested technologies, staff training, documentation, software, equipment, and licence fees, among others, implementing ISMS controls is not a cost-effective procedure. ISMS restrictions can end up being more expensive for Pharm Universe.
- The information security team is short-staffed.

References

[1] National Institute of Standards and Technology. (n.d.). NVD - CVSS v3 Calculator. Nvd.nist.gov. https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator

[2] Mahendru, P. (2022, October 26). The State of Ransomware in Manufacturing and Production 2022. Sophos News. https://news.sophos.com/en-us/2022/10/26/the-state-of-ransomware-in-manufacturing-and-production-2022/

[3] DDoS Attack Trends for Q4 2021. (2022, January 10). The Cloudflare Blog. https://blog.cloudflare.com/ddos-attack-trends-for-2021-q4/

[4] ISO 27001 - Annex A.9 - Access Control - DataGuard. (n.d.). Www.dataguard.co.uk. https://www.dataguard.co.uk/blog/iso-27001-annex-a.9-access-control

[5] ISO 27001 Controls: What is Annex A:10? (2020, November 17). Best Practice. https://bestpractice.biz/iso-controls-27001-what-is-annex-10/

[6] Annex A.12 Operations Security - DataGuard. (n.d.). Www.dataguard.co.uk. Retrieved December 15, 2022, from https://www.dataguard.co.uk/blog/iso-27001-annex-a.12-operations-security

[7] editor. (2021, June 24). ISO 27001 Annex: A.12.6 Technical Vulnerability Management - InfoSec Solutions. https://www.solutions-inc.co.uk/iso-27001-annex-a-12-6-technical-vulnerability-management/

[8] ISO 27001 - Annex A.13 - Communications Security - DataGuard. (n.d.). Www.dataguard.co.uk. Retrieved December 15, 2022, from https://www.dataguard.co.uk/blog/iso-27001-annex-a.13-communications-security/

[9] ISO 27001 - Annex A.16 - Information Security Incident Management. (n.d.). Www.dataguard.co.uk. Retrieved December 15, 2022, from https://www.dataguard.co.uk/blog/iso-27001-annex-a.16-information-security-incident-management/

[10] Best ISO, IEC, 27001, Implementatin, Certification, Services | Certaim.com. (n.d.). We Have 17 Years of Experience and Expertise in Implementation of ISO 27001, ISO 20000, ISO 22301, ISO 9001, ISO 22000 and Certification Support across All Verticals of Business. https://certaim.com/isoiec-27001-certification/