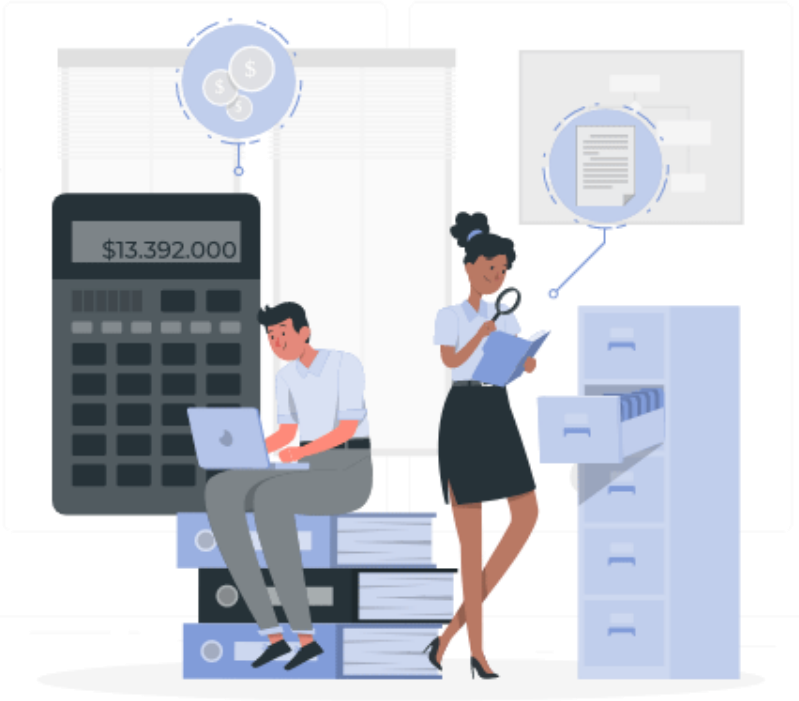
Le certificazioni vengono fatte a livello personale o azienda, devono essere riconosciuto dall'iaf (International Accreditation Forum)
Certificazioni elencate in base alla "difficoltà", ovvero si parte dal primo per poi arrivare all'ultimo:
- ISO 27001 internal auditor -> fare auditing internamente all'azienda, l'auditor esterno lo aiuta.
- ISO 27001 auditor -> quello che fa l'auditor ma da esterno
- ISO 27001 lead implementer -> chi implementa

theknowledgeacademy

ISO 27001: 2022 Lead Implementer



theknowledgeacademy

theknowledgeacademy
Awarded and Trusted

About Us

The world's largest provider of classroom and online training courses

- ✓ World Class Training Solutions
- ✓ Subject Matter Experts
- ✓ Highest Quality Training Material
- ✓ Accelerated Learning Techniques
- ✓ Project, Programme, and Change Management, ITIL® Consultancy
- ✓ Bespoke Tailor Made Training Solutions
- ✓ PRINCE2®, MSP®, ITIL®, Soft Skills, and More

theknowledgeacademy

Course Syllabus

theknowledgeacademy

Course Syllabus

theknowledgeacademy

Module 1: Introduction to ISO 27001

- ✓ Introduction
- ✓ Compatibility with Other Management System Standards
- ✓ ISO 27001:2022 and its Clauses

Introduction

General

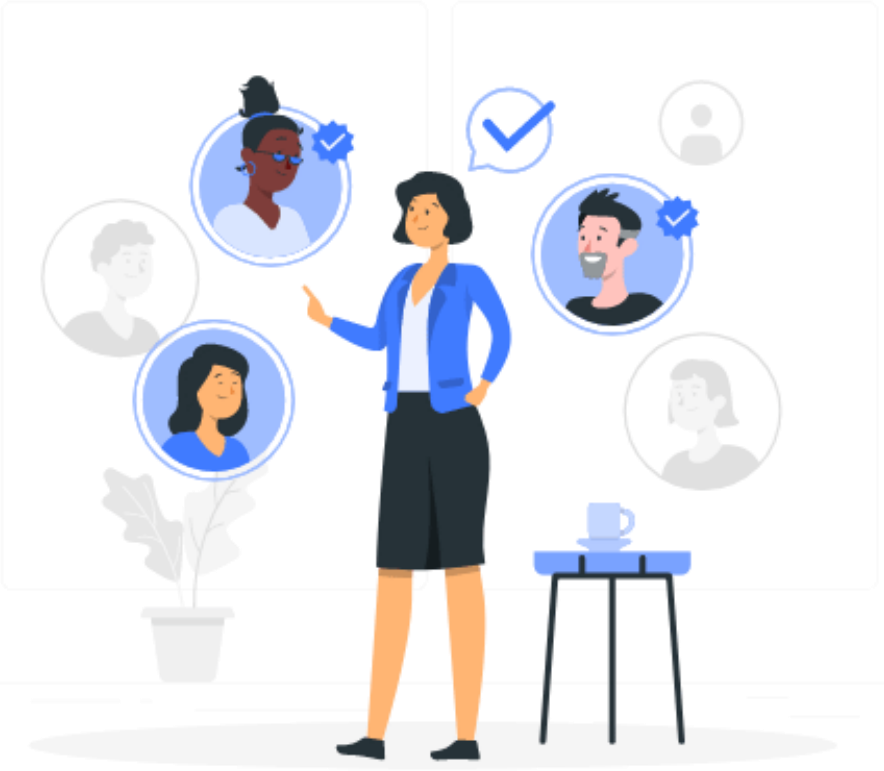
- ✓ In order to establish, implement, maintain, and continuously improve an information security management system, this document has been prepared.
- ✓ The information security management system's adoption is a strategic decision for an organisation.
- ✓ The needs and objectives of the organisation, security requirements, organisational procedures utilised, and the size and structure of the organisation all influence the establishment and execution of an organisation's information security management system.
- ✓ All of these impacting elements are expected to adjust over time.
- ✓ The information security management system protects information confidentiality, integrity, and availability through a risk management process, giving interested parties confidence that risks are properly handled.

Introduction

- ✓ Significantly, the information security management system is integrated into, and part of the organisation's process and overall management structure and that information security is thought about in the design of processes, information systems, and controls.
- ✓ An information security management system's execution is expected to be scaled per the organisation's requirements.
- ✓ Internal and external parties can use this document to evaluate the organisation's capacity to complete its information security requirements.
- ✓ The order in which the requirements are given in this document does not indicate their significance nor imply the order in which they will be executed.

Compatibility with Other Management System Standards

- ✓ In order to maintain compatibility with other management system standards that have adopted Annex SL, this document applies the high-level structure, identical sub-clause titles, identical text, common terms, and core definitions defined in Annex SL of ISO/IEC Directives, Part 1, Consolidated ISO Supplement.
- ✓ For organisations that decide to operate a single management system that satisfies the requirements of two or more management system standards, the common approach described in Annex SL will be helpful.



ISO 27001:2022 and its Clauses

Clauses to ISO/IEC 27001

- ✓ Clause 1: Scope
- ✓ Clause 2: Normative references
- ✓ Clause 3: Terms and definitions

Clauses 1 to 3 are not directly audited against, but because they provide context and definitions for the rest of the standard, not that of the organisation, their contents must be taken into account

theknowledgeacademy

theknowledgeacademy

Module 2: Information Security

- ✓ What is Business?
- ✓ Industries
- ✓ Risk
- ✓ SWOT Analysis
- ✓ Constructs & Characteristics of Assets
- ✓ Security
- ✓ Privacy
- ✓ Triad of Information Security

theknowledgeacademy

Module 2: Information Security

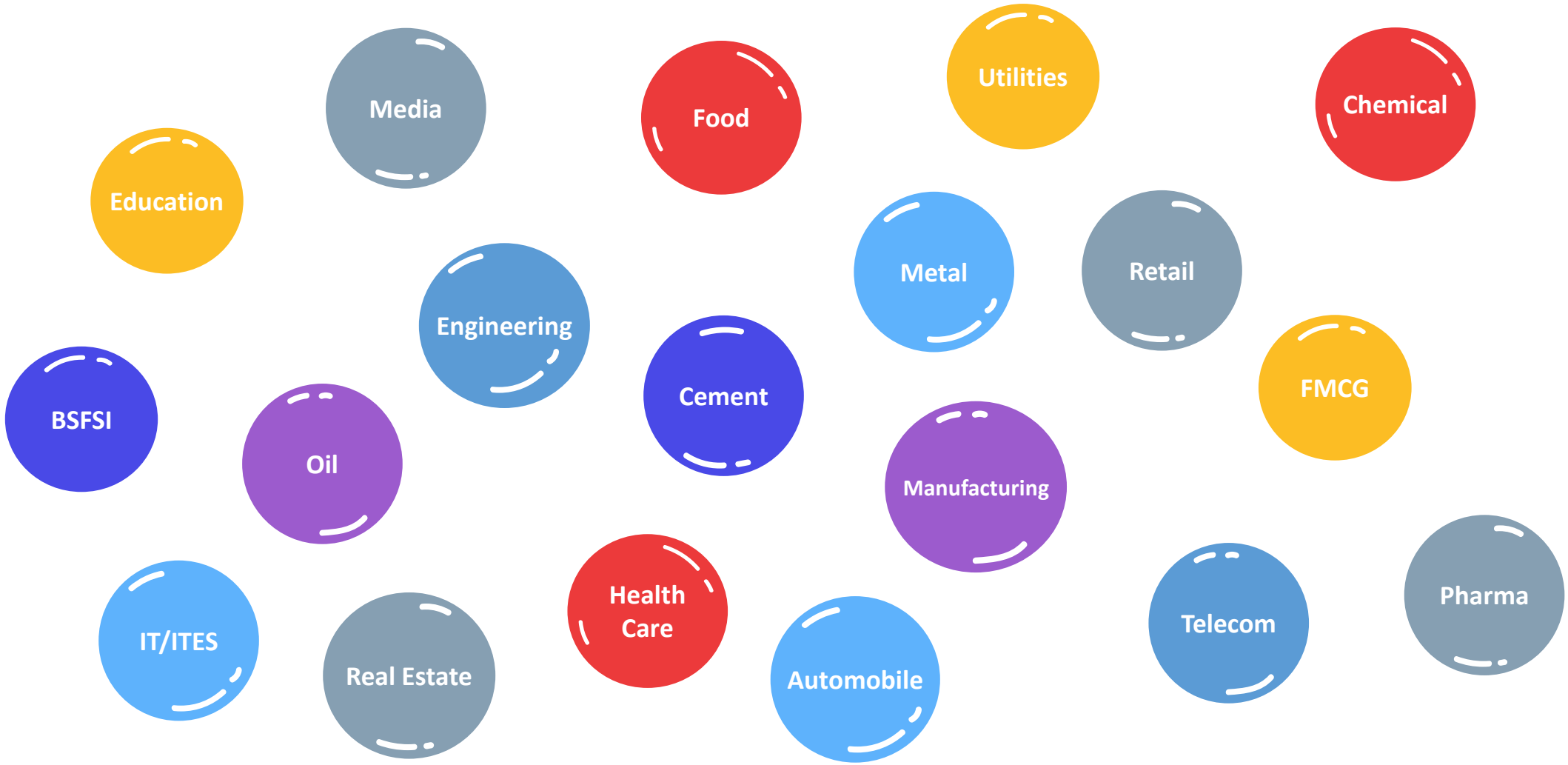
- ✓ Cyber security is everyone’s responsibility
- ✓ Cybersecurity Landscape
- ✓ What is Information Security?
- ✓ Information Security Management
- ✓ Need of Information Security
- ✓ Threats to Information Security
- ✓ Active and Passive Attacks

What is Business?

- ✓ An organisation or economic system where goods and services are exchanged for one another or for money.
- ✓ Every business requires some form of investment and enough customers to whom its output can be sold on a consistent basis in order to make a profit.
- ✓ Businesses can be privately owned, not-for-profit or public owned..

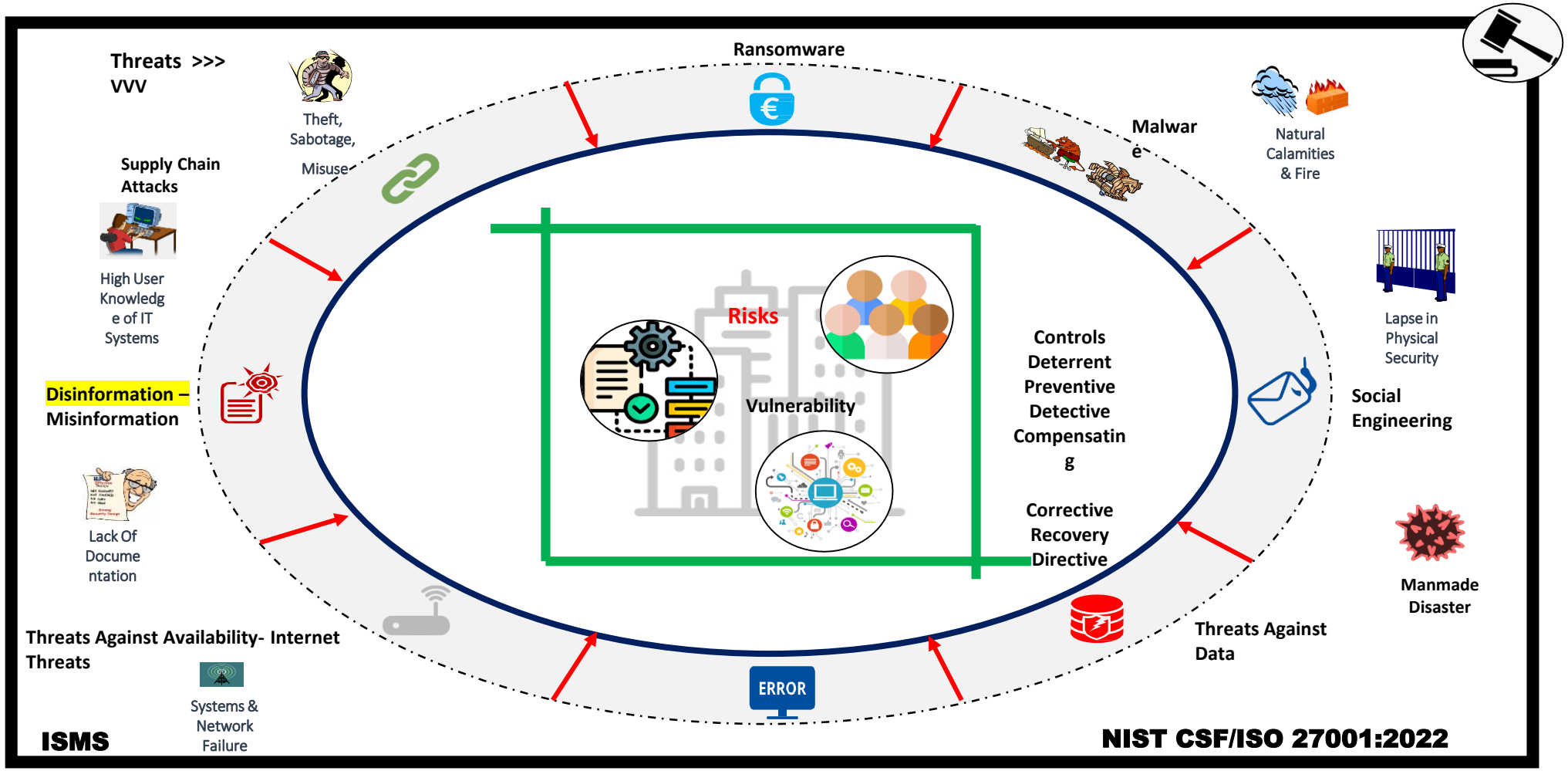
theknowledgeacademy

Industries



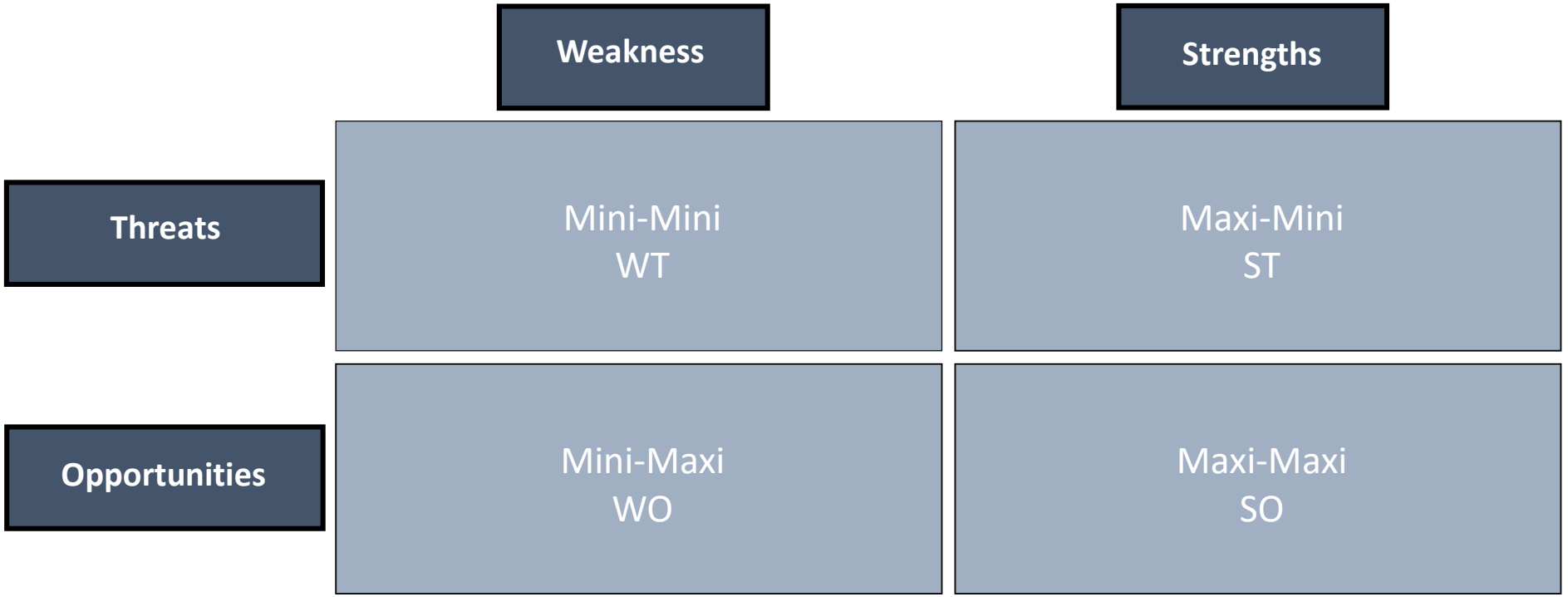
theknowledgeacademy

Risk



theknowledgeacademy

SWOT Analysis



theknowledgeacademy

Constructs & Characteristics of Assets

MERCURY	Assets Transformation	Information Assets
✓ Raw facts, figures & events (quantitative) ✓ Collected by observation & recording ✓ Stored in a specific location (physical) ✓ No context (little meaning until organised, arranged & developed)	✓ Set of people, processes, services & resources that collects & transforms data into information and disseminates & presents this information ✓ The "information system" or "ICT system"	✓ Transformed data (qualitative) ✓ Created by analysis and structured presentation of data ✓ Virtual (logical) – not stored in a specific location ✓ Context (has meaning through organisation & presentation)

theknowledgeacademy

Security

To provide confidence & assurance

- ✓ Business can depend upon and trust our technologies
- ✓ Business is not exposed to unacceptable risk
- ✓ Business can meet its objectives and grasp opportunities

To protect business assets Qualsiasi cosa che ci sia all'interno dell'azienda.

- ✓ Technology and are our use of it is ‘secure’
- ✓ Information and our use of it is ‘secure’

To support the business objectives l'obbiettivo del businnes non lo decido io.

- ✓ What is our mission?
- ✓ What are our strategic, tactical & operational business objectives?

theknowledgeacademy

Privacy

Protecting the privacy of information:

- ✓ Keep sensitive information off the network, if possible
- ✓ Encrypt sensitive information
- ✓ Protect access to your system
- ✓ Don’t share sensitive information
- ✓ Password protection

Preventing Unauthorised Modification of Information:

- ✓ Emails
- ✓ Data
- ✓ Digital Downloads
- ✓ Log/Audit files

theknowledgeacademy

Privacy

Reliability/Trustworthiness of information

- ✓ Hijacked websites
- ✓ Email with modified content
- ✓ Corrupted files

Danial of Service Attacks

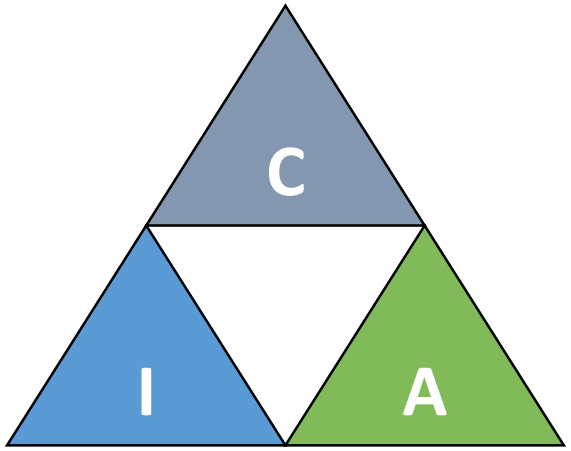
- ✓ Denial of Service Attacks and Distributed Denial of Service Attacks
- ✓ Expect the Unexpected
- ✓ Beware of Natural/Manmade disasters

theknowledgeacademy

Triad of Information Security

Bisognerebbe tenere conto anche la tracciabilità

Confidentiality, Integrity, and Availability (CIA) are the three main goals of information security programs



1. Confidentiality

- ✓ Confidentiality means that information is not disclosed to groups, organisations, or processes that are not authorised
- ✓ For instance, let's say I had a password for my Gmail account, but someone witnessed me logging in. In that case, both my password and confidentiality have been compromised

theknowledgeacademy

Triad of Information Security

2. Integrity

- ✓ Means ensuring data accuracy and completeness. This means that information cannot be altered without authorisation
- ✓ For instance, if an employee leaves an organisation, all relevant data for that employee should be updated to reflect JOB LEFT status in order to ensure that the data is accurate and complete. In addition, only authorised individuals should be permitted to edit employee data

3. Availability

- ✓ Availability means that information must be accessible when required
- ✓ For instance, working with various organisational teams like network operations, development operations, incident response, and policy/change management is necessary if one needs to access information about a specific employee to determine whether they have exceeded the allowed number of leaves. One of the factors that can affect the accessibility of information is a denial of service attack

theknowledgeacademy

Cyber Security is Everyone's Responsibility

Cybersecurity is everyone's concern:

theknowledgeacademy

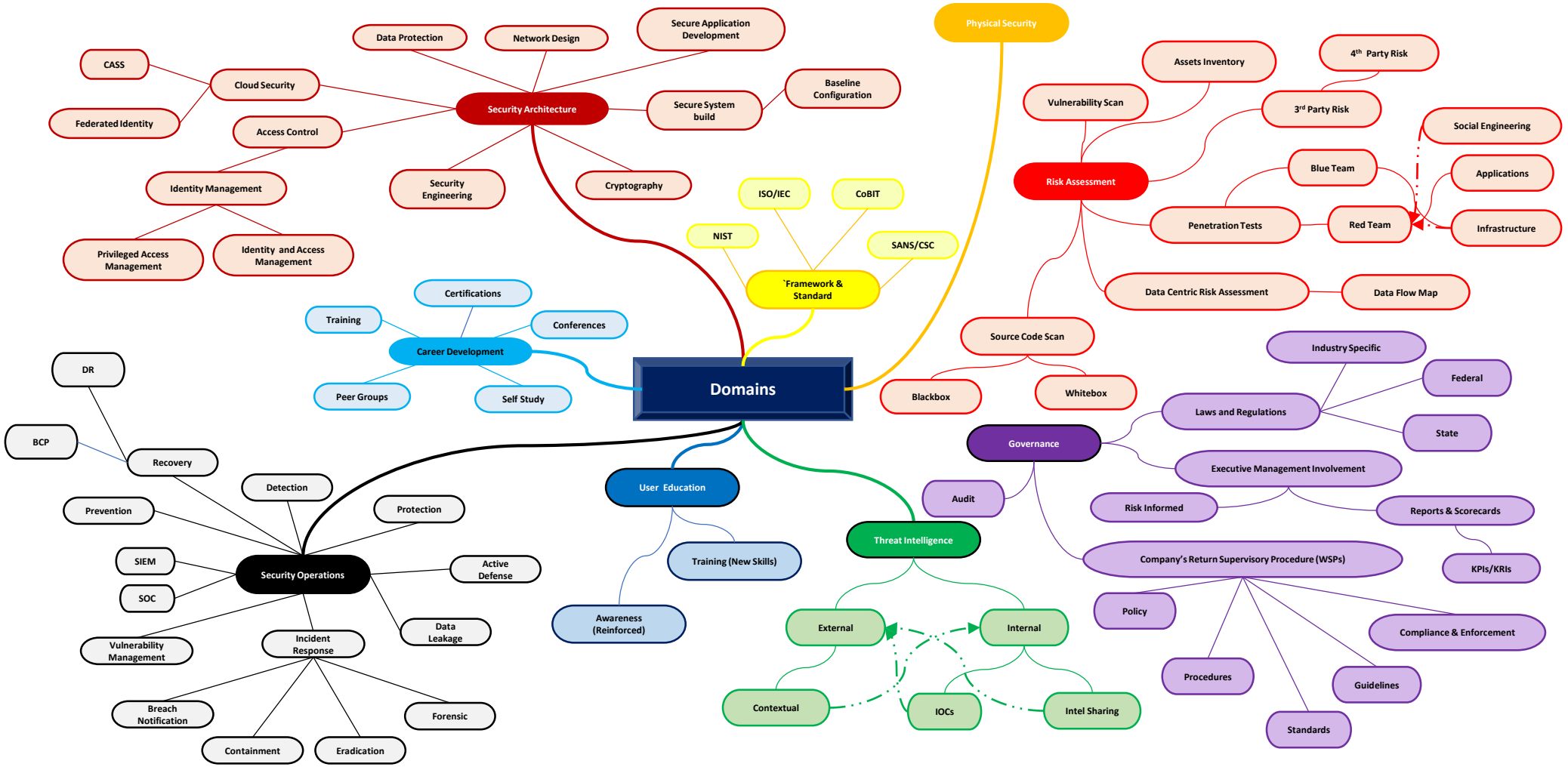
Cyber Security is Everyone's Responsibility

Security breaches leads to:

- ✓ Reputation loss
- ✓ Financial loss
- ✓ Intellectual property loss
- ✓ Legislative Breaches leading to legal actions (Cyber Law)
- ✓ Loss of customer confidence
- ✓ Business interruption costs

theknowledgeacademy

Cybersecurity Landscape



theknowledgeacademy

Information Security Management

Sistema che traccia tutte le azioni, dalla prospettiva della security

- ✓ Information security encompasses more than just protecting data from unauthorised access
- ✓ The practise of preventing unauthorised access, use, disclosure, disruption, modification, inspection, recording, or destruction of information is known as information security. Information comes in both physical and digital forms
- ✓ Information can be either physical or electronic. Information can include your personal information, your social media profile, your mobile phone data, your biometrics, and so on
- ✓ Thus, information security encompasses numerous research areas such as cryptography, mobile computing, cyber forensics, online social media, etc

Information Security Management

Information security management is about preserving the 'Confidentiality, Integrity and Availability' of information and associated information processing facilities, whether that's systems, services, infrastructure or the physical locations. It ensures business continuity by minimising business damage by preventing and reducing the impact of security incidents.

C – Confidentiality: The property that information is not made available or disclosed to unauthorised individuals, entities or processes

I – Integrity: The property of safeguarding the accuracy and completeness of assets

A – Availability: The property of being accessible and usable upon demand by an authorised entity

Information Security Management

The purpose of the ISMS is to:

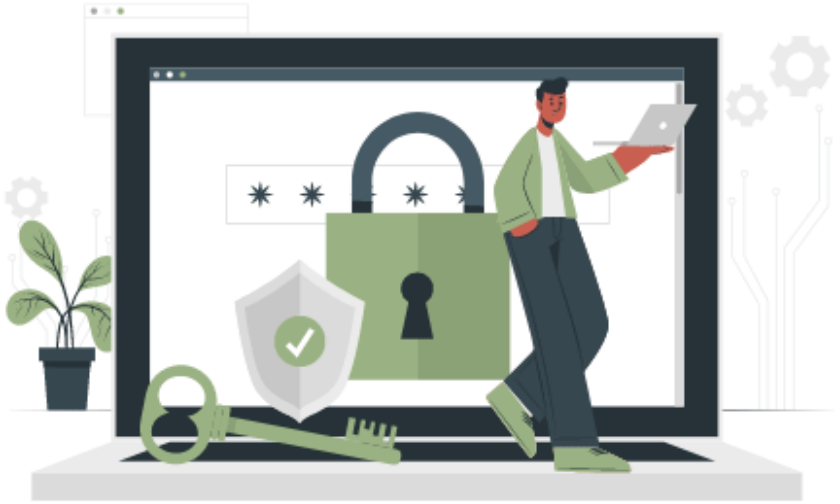
- ✓ Understand the organisation's needs and the necessity for establishing information security management policy and objectives
- ✓ Implement and operate controls and measures for managing the organisation's overall capability to manage information security incidents
- ✓ Monitor and review the performance and effectiveness of the ISMS
- ✓ Continually improve the organisation's information security based on objective measurement

theknowledgeacademy

Information Security Management

Rules for ISMS:

- ✓ A weak foundation amplifies risk.
- ✓ If a bad guy tricks you into running his code on your computer, it's not your computer anymore.
- ✓ There's always a bad guy out there who's smarter, more knowledgeable, or better-equipped than you.
- ✓ Know the enemy, think like the enemy.
- ✓ Know the business, not just the technology.
- ✓ Technology is only one-third of any solution.
- ✓ Every organisation must assume some risk.



Need of Information Security

- ✓ Information system refers to the process of evaluating available controls or countermeasures inspired by vulnerabilities discovered and identifying an area that requires additional research.
- ✓ By preventing and reducing the effects of security incidents, data security management aims to ensure business continuity and reduce business damage.

The need for Information security:

1. Preserving the organisation's functionality

- ✓ Organisational decision-makers are responsible for establishing policies and running their business in accordance with complicated, changing legislation and applications that are effective and capable.

theknowledgeacademy

Need of Information Security

2. Enabling the safe operation of applications

- ✓ The organisation is under tremendous pressure to obtain and run integrated, efficient, and capable applications.
- ✓ The modern organisation must establish a setting that protects applications using its IT systems, especially those applications that are crucial to the organisation's infrastructure.

3. Data protection for the organisation's collection and use

- ✓ In an organisation, data can exist in two states: at rest or in motion. Data in motion is being used or processed by the system at the moment
- ✓ Attackers were motivated to steal or corrupt the data by its values. The values and integrity of the organisation's data depend on this. Data in motion and data at rest are both protected by information security.

theknowledgeacademy

Need of Information Security

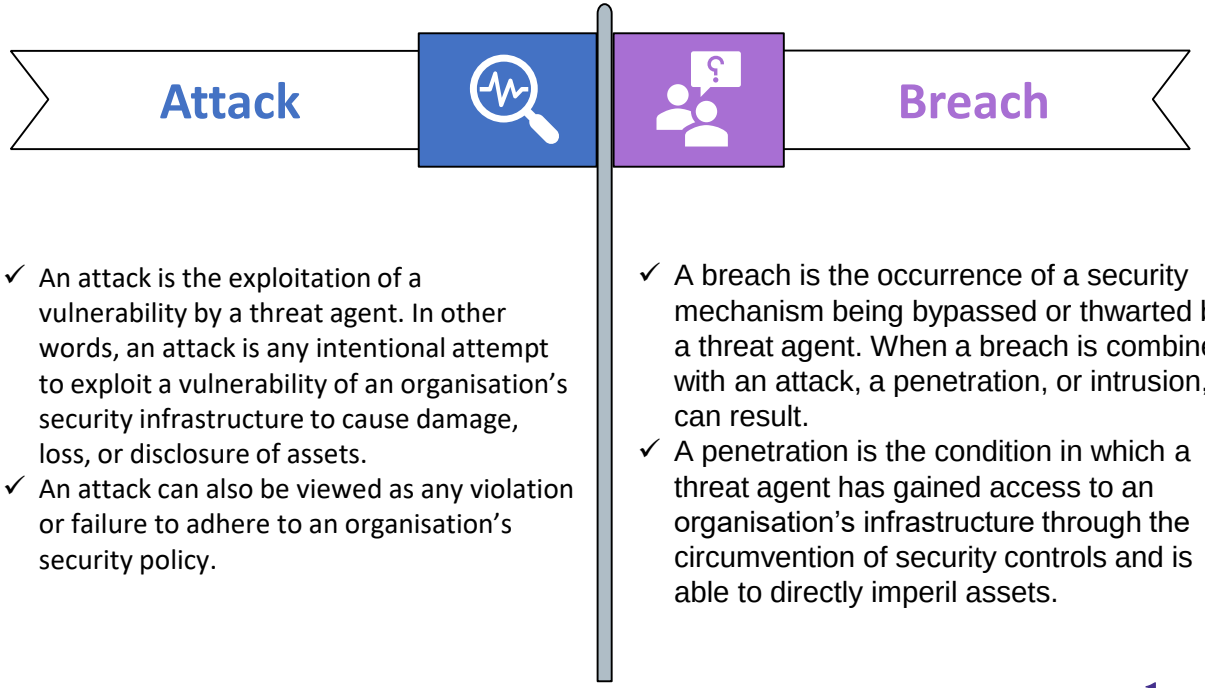
4. Organisational technology asset protection

- ✓ Depending on its size and scope, the organisation must add intrastate services. The need for public key infrastructure, or PKI—a comprehensive system of software and encryption techniques—could arise as a result of organisational growth.
- ✓ In contrast to a small organisation, a large organisation uses a complex information security mechanism. Small businesses typically favour symmetric key data encryption.

theknowledgeacademy

Threats to Information Security

- ✓ Threats to information security can take many different forms, including software attacks, intellectual property theft, identity theft, equipment theft, information theft, sabotage, and information extortion
- ✓ **Threats** include anything that has the potential to breach security, harm one or more valuable objects, or negatively alter, erase, or otherwise affect them
- ✓ **Attack & Breach:**



- ✓ An attack is the exploitation of a vulnerability by a threat agent. In other words, an attack is any intentional attempt to exploit a vulnerability of an organisation's security infrastructure to cause damage, loss, or disclosure of assets.
- ✓ An attack can also be viewed as any violation or failure to adhere to an organisation's security policy.

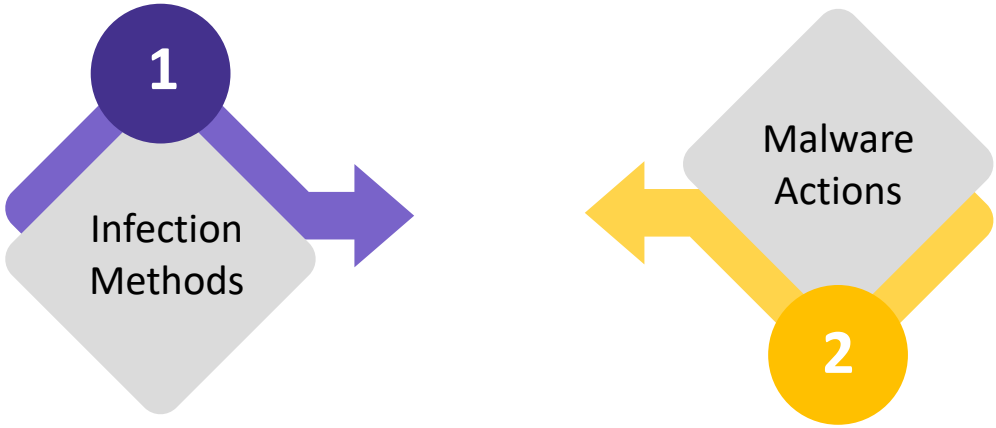
- ✓ A breach is the occurrence of a security mechanism being bypassed or thwarted by a threat agent. When a breach is combined with an attack, a penetration, or intrusion, can result.
- ✓ A penetration is the condition in which a threat agent has gained access to an organisation's infrastructure through the circumvention of security controls and is able to directly imperil assets.

theknowledgeacademy

Threats to Information Security

- ✓ **Software Attacks** include viruses, worms, Trojan horses, and other malware. Many users think that malware, viruses, worms, and bots are all the same.
- ✓ However, they are not identical; the only thing they have in common is that each is malicious software that behaves differently.
- ✓ **Malware** is a combination of the words malicious and software. So malware is defined as malicious software, including intrusive program code or anything else created to harm a system.

Malware can be categorised into two groups:



theknowledgeacademy

Threats to Information Security

The following list of malware is based on the manner of infection:

- Virus
- Trojan
- Worms
- Bots

theknowledgeacademy

Threats to Information Security

1. Virus

- ✓ They can reproduce themselves and spread throughout the Internet by connecting to the host computer's software, such as music or videos
- ✓ The Creeper Virus was initially identified on ARPANET. Examples of viruses include file viruses, macro viruses, boot sector viruses, stealth viruses, etc

2. Worms

- ✓ In nature, worms can also replicate themselves, but they do not affix themselves to the host computer's software
- ✓ Worms are network-aware, which is their primary difference from viruses. They can quickly switch from one machine to another if a network is available
- ✓ They will not harm the target machine, but they might slow it down by taking up hard disc space, for example

theknowledgeacademy

Threats to Information Security

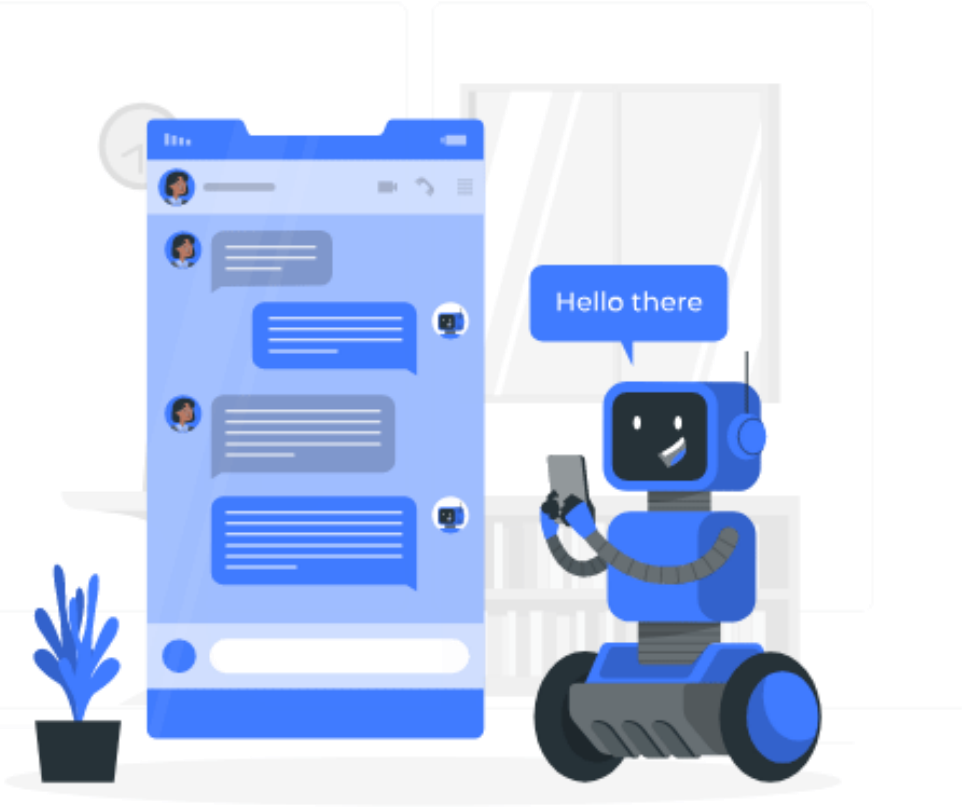
3. Trojan

- ✓ A Trojan is absolutely unrelated to a virus or worm in terms of its concept
- ✓ Greek mythology's "Trojan Horse" tale, which relates how the Greeks invaded the walled city of Troy by disguising their men within a huge wooden horse that had been presented to the Trojans as a gift, is where the word "Trojan" originates
- ✓ The Trojans loved horses so much that they trusted the gift. The soldiers entered the city during the night and began an internal uprising
- ✓ The software will carry out its mission of either stealing information or performing any other function for which it was designed when it is executed. They aim to conceal themselves inside software that seems to be trustworthy

Threats to Information Security

4. Bots

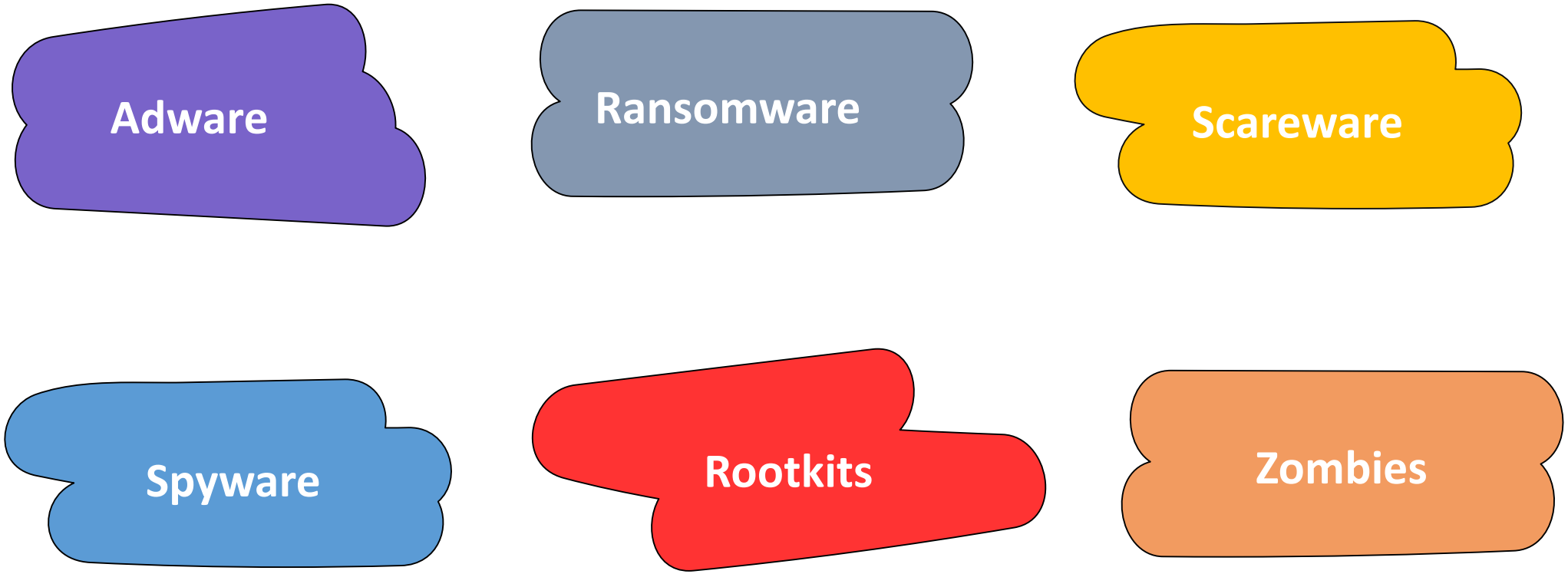
- ✓ Worms that have advanced more are known as bots.
- ✓ They are automated processes designed for online communication without human contact.
- ✓ They are both viable options. A malicious bot can infect one host, after which it connects to the main server and sends commands to all other hosts linked to that botnet.



theknowledgeacademy

Threats to Information Security

Malware based on its actions:



theknowledgeacademy

Threats to Information Security

1. Adware

- ✓ Adware violates users' privacy even though it is not specifically dangerous.
- ✓ They display adverts in particular programmes or on the desktop of a computer.
- ✓ They come bundled with free software, which is how these developers primarily make money.
- ✓ Your preferences are tracked, and they show you relevant ads.
- ✓ If harmful code is included in the software, the adware can monitor your computer's operations and possibly compromise it.

2. Ransomware

- ✓ It is malware that either locks the computer, rendering it partially or completely unusable or encrypts all files. Then a screen will display and ask for money or a ransom

theknowledgeacademy

Threats to Information Security

3. Spyware

- ✓ It is a programme, or should we say software, that monitors internet actions and discloses the information to anyone who may be interested
- ✓ Most frequently, spyware is released through viruses, Trojan horses, and worms. Once dropped, they establish themselves and keep quiet to avoid being discovered

4. Scareware

- ✓ Although it appears to be a programme to help you fix your system, once the software is launched, it will either infect or break your system
- ✓ In order to frighten you and convince you to take some sort of action, like paying them to fix your system, the software will display a message

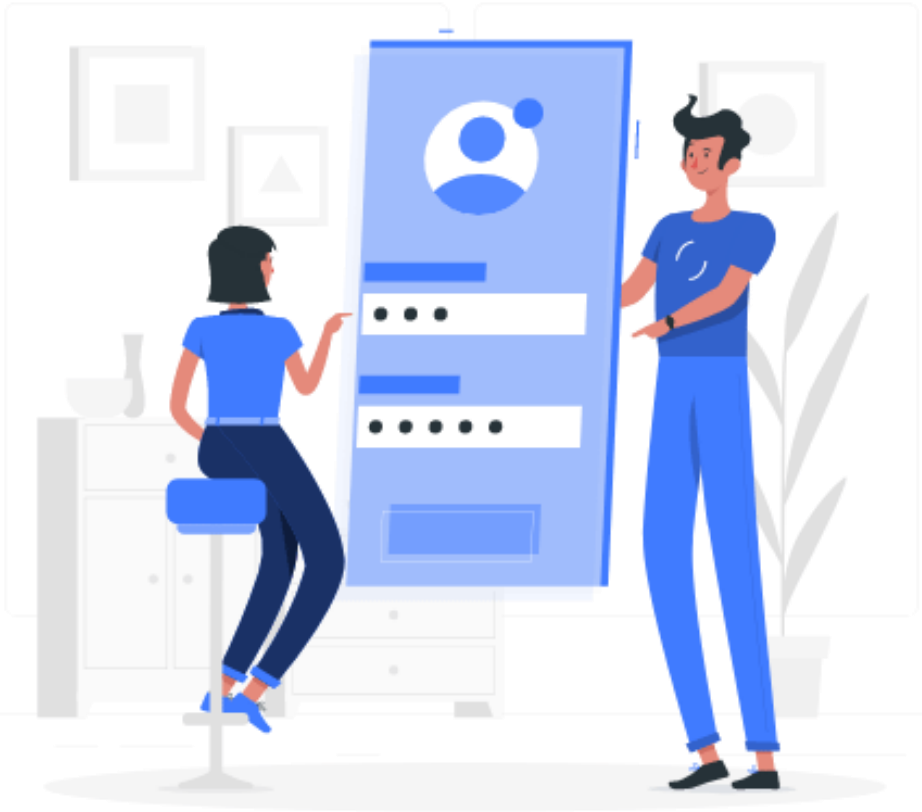
Threats to Information Security

5. Rootkits

- ✓ Root access usually referred to as administrative rights, is what rootkits are designed to achieve on the user system. The exploiter can steal anything, including confidential files and data, once they have root access

6. Zombies

- ✓ Similar to spyware, they operate. The infection mechanism is the same, but they wait for a hacker's order instead of spying and stealing data



theknowledgeacademy

Active and Passive Attacks

Active Attacks

An active attack tries to change system resources or interfere with their operability. Active attacks include some data stream modification or false statement creation

Passive Attacks

A passive assault does not affect system resources but tries to get or use information from the system

Eavesdropping or transmission monitoring are both passive attacks

theknowledgeacademy

theknowledgeacademy

Module 3: Context of the Organisation

- ✓ Organisation and Its Context
- ✓ Needs and Expectations of Interested Parties
- ✓ Scope of the Information Security Management System
- ✓ Information Security Management System

Understanding the Organisation and Its Context

External and internal issues shall be determined by the organisation that is relevant to the purpose and affect its capability of achieving the intended result of its information security management system

Understanding the Needs and Expectations of Interested Parties

The organisation shall determine:

- ✓ Interested parties that are appropriate to the information security management system
- ✓ These interested parties' requirements are relevant to information security
- ✓ Which of these requirements will be met by the information security management system

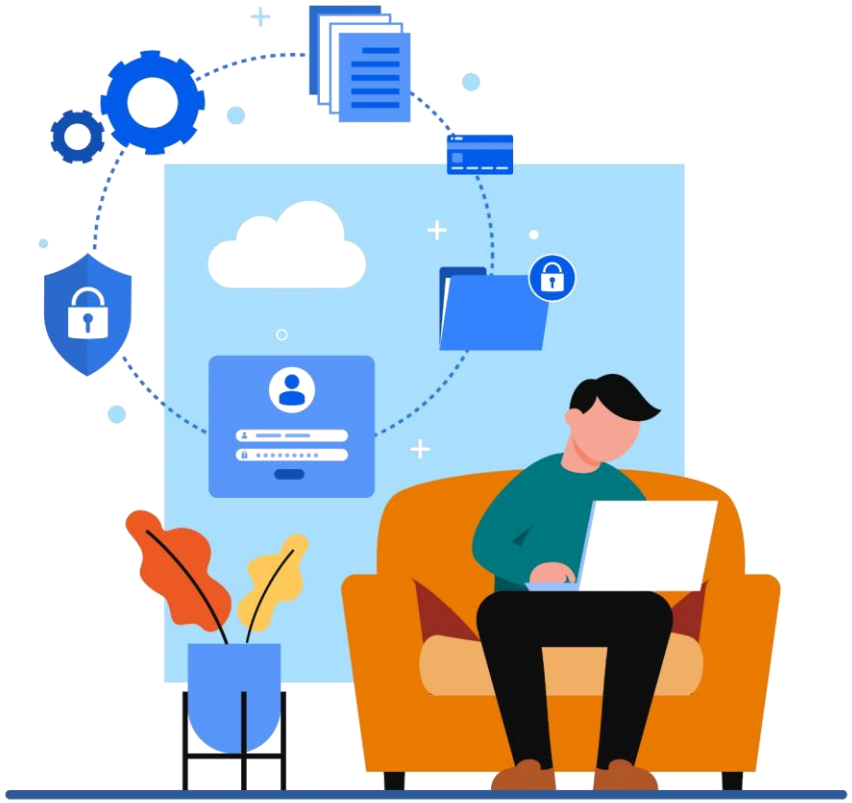
Determining the Scope of the Information Security Management System

- ✓ In order to establish its scope, the organisation shall determine the boundaries and applicability of the information security management system

The organisation shall think about when determining this scope:

- The external and internal issues
- The requirements
- The organisation performs interfaces and dependencies between activities, and those that are performed by other organisations

- ✓ As documented information, the scope shall be available



theknowledgeacademy

Information Security Management System

- ✓ In accordance with this document's requirements, the organisation shall establish, implement, maintain, and continuously improve an information security management system, including the processes required and their interactions

theknowledgeacademy

Module 4: Leadership

- ✓ Leadership and Commitment
- ✓ Policy
- ✓ Roles, Responsibilities, and Authorities

Leadership and Commitment

- ✓ Leadership and commitment shall be demonstrated by the top management regarding the information security management system by:
  - Make sure that the information security policy and goals are established and compatible with the organisation's strategic direction
  - Assure that the information security management system requirements are integrated into the processes of the organisation
  - Ensuring the availability of the resources required for the information security management system
  - Communicating the significance of effective information security management and adhering to the requirements of the information security management system
  - Assuring that the information security management system attains its intended result
  - Directing and assisting individuals in contributing to the effectiveness of the information security management system, encouraging continuous improvement
  - Assisting other appropriate management roles in showing leadership in their areas of responsibility

theknowledgeacademy

Policy

- ✓ An information security policy shall be established by the top management that:
  - Is relevant to the organisation's objective.
  - Contains information security objectives or gives a framework to set information security goals
  - Includes a commitment to meet applicable information security requirements; and
  - Includes a commitment to improving the information security management system on an ongoing basis
- ✓ The information security policy shall:
  - Be available as documented information
  - Be communicated in the organisation; and
  - As relevant, be available to interested parties

theknowledgeacademy

Organisational Roles, Responsibilities, and Authorities

- ✓ Top management must confirm that responsibilities and authorities for information security roles are assigned and communicated throughout the organisation
- ✓ Top management must delegate responsibility and authority for the following tasks:
  - Ensuring that the information security management system meets the requirements of this document
  - Reporting to top management on the performance of the information security management system

theknowledgeacademy

theknowledgeacademy

Module 5: Planning

- ✓ Actions to Address Risks and Opportunities
- ✓ Information Security Objectives and Planning
- ✓ Planning of Changes

Organisational Roles, Responsibilities, and Authorities

1. General

- ✓ When planning for an information security management system, the organisation shall think about the issues and requirements, as well as determine the risks and opportunities that must be addressed:
  - Make sure the information security management system can attain its intended result
  - Avert, or decrease, undesired effects
  - Attain continuous improvement
- ✓ The organisation shall plan:
  - Taking steps to address these risks and opportunities; and
  - How to Integrate and execute these actions into the processes of its information security management system; and
  - Assess the efficacy of these actions

theknowledgeacademy

Organisational Roles, Responsibilities, and Authorities

2. Information Security Risk Assessment

- ✓ An information security assessment process shall be defined and applied by the organisation that:
  - Establishes and keeps information security risk criteria, which include the following:
    - ❑ Criteria for risk acceptance; and
    - ❑ Criteria for conducting risk assessments in information security
  - Make sure that repeated assessments of information security risk produce consistent, valid, and comparable outcomes

theknowledgeacademy

Organisational Roles, Responsibilities, and Authorities

- The information security risks should be identified:
  - ❑ Use the information security risk assessment process to recognise risks related to the loss of information's confidentiality, integrity, and availability in the scope of the information security management system; and
  - ❑ The risk owners must be identified
- Analyses the risks to information security:
  - ❑ Evaluate the potential consequences if the identified risks were to materialise
  - ❑ Assess the realistic likelihood of the risks happening;
  - ❑ Determine the risk levels

theknowledgeacademy

Organisational Roles, Responsibilities, and Authorities

- Assesses the information security risks:
  - ❑ Compare the risk analysis outcomes to the risk criteria; and
  - ❑ Prioritise the risks that have been analysed for risk treatment

✓ The organisation shall keep documented information regarding the information security risk assessment process

theknowledgeacademy

Organisational Roles, Responsibilities, and Authorities

3. Information Security Risk Treatment

- ✓ An information security risk treatment process shall be defined and applied by the organisation that:
  - Select relevant information security risk treatment options, considering the outcomes of the risk assessment
  - Determine all controls required to execute the chosen information security risk treatment option
  - Compare the controls and verify that no essential controls have been left out
  - Produce an Applicability statement that includes the required controls and justification for inclusions, whether or not they are executed, as well as justification for control exclusions from Annex A
  - Create a plan for dealing with information security risks; and
  - Receive approval from risk owners for the information security risk treatment plan and acceptance of residual information security risks
- ✓ Documented information shall be kept by the organisation regarding the information security risk treatment process

Information Security Objectives and Planning to Achieve Them

- ✓ At relevant functions and levels, the organisation must establish information security objectives. The information security objectives must include the following:
  - Be in accordance with the information security policy.
  - Be quantifiable (if possible) bisognerebbe sempre quantificare.
  - Consider applicable information security requirements, as well as risk assessment and risk treatment results
  - Be observed
  - Must be communicated
  - Be updated as needed
  - Be accessible as documented information

theknowledgeacademy

Information Security Objectives and Planning to Achieve Them

- ✓ The organisation must keep documented information on its information security goals. The organisation must decide the following when planning how to achieve its information security objectives:
  - What will be completed
  - What resources will be needed
  - Who will be accountable
  - When it will be finished; and
  - How the outcomes will be assessed

theknowledgeacademy

Planning of Changes

- When the organisation determines that changes to the information security management system are required, the changes must be implemented in a planned manner.

theknowledgeacademy

NON IMPORTANTE

Module 6: Support

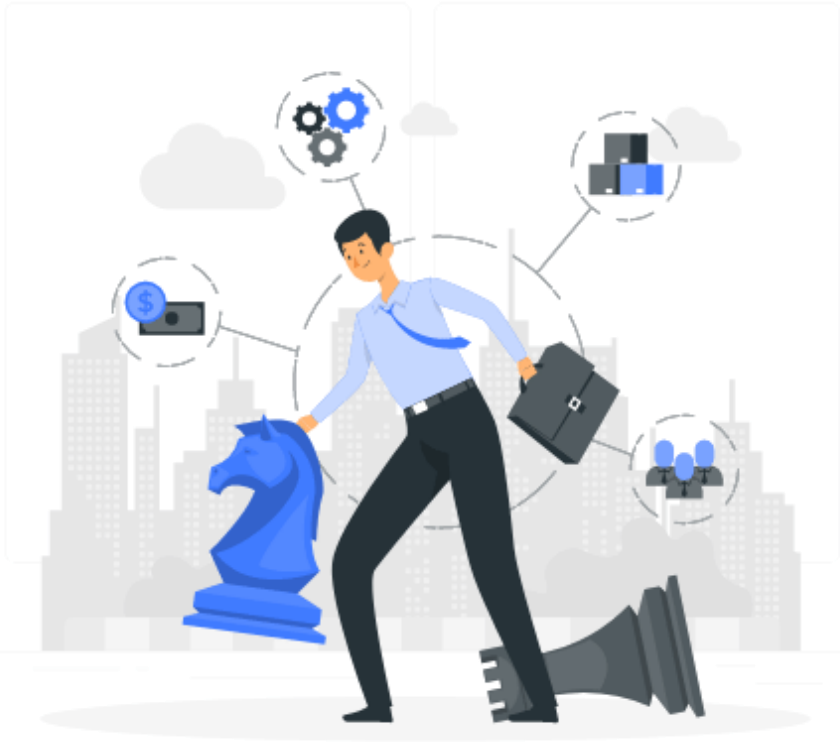
- ✓ Resources
- ✓ Competence
- ✓ Awareness
- ✓ Communication
- ✓ Documented Information

Resources

The resources that are required for the establishment, execution, maintenance and continual improvement of the information security management system shall be determined and given by the organisation.

Competence

- ✓ The organisation shall:
  - Determine the required competence of any individual performing work under its control that impacts its information security performance
  - Make sure these individuals are competent based on relevant education, training, or experience
  - Take action to obtain the essential competence where applicable, and assess the effectiveness of the actions taken
  - Maintain appropriate documentation as evidence of competence



Awareness

- ✓ Individuals performing work under the organisation's control shall be aware of the following:
  - The policy on information security
  - Their contribution to the information security management system's effectiveness involves the advantages of improved information security performance
  - The implications of failing to meet the requirements of the information security management system

Communication

- ✓ The organisation shall determine the requirement for internal and external communications appropriate to the information security management system involving:
  - On what to communicate
  - When to communicate
  - With whom to communicate
  - How to communicate

theknowledgeacademy

Documented Information

1. General

✓ The information security management system of the organisation must include:

- This International Standard requires documented information
- The organisation determines documented information as being essential for the effectiveness of the information security management system

2. Creating And Updating

✓ When making and updating documented information, the organisation shall make sure relevant:

- Description and identification
- Media and format
- Review and approval for appropriateness and sufficiency

theknowledgeacademy

Documented Information

3. Control of documented information

- ✓ The information security management system requires documented information and, by this International Standard, must be controlled to make sure:
  - It is readily available and appropriate for use where and when it is required
  - It is adequately safeguarded
- ✓ The organisation shall address the following activities, as applicable, for the control of documented information:
  - Distribution, retrieval, access and usage
  - Storage and preservation, involving legibility preservation
  - Changes' in control
  - Retention and disposal

theknowledgeacademy

NON IMPORTANTE

theknowledgeacademy

Module 7: Operation

- ✓ Operational Planning and Control
- ✓ Information Security Risk Assessment
- ✓ Information Security Risk Treatment

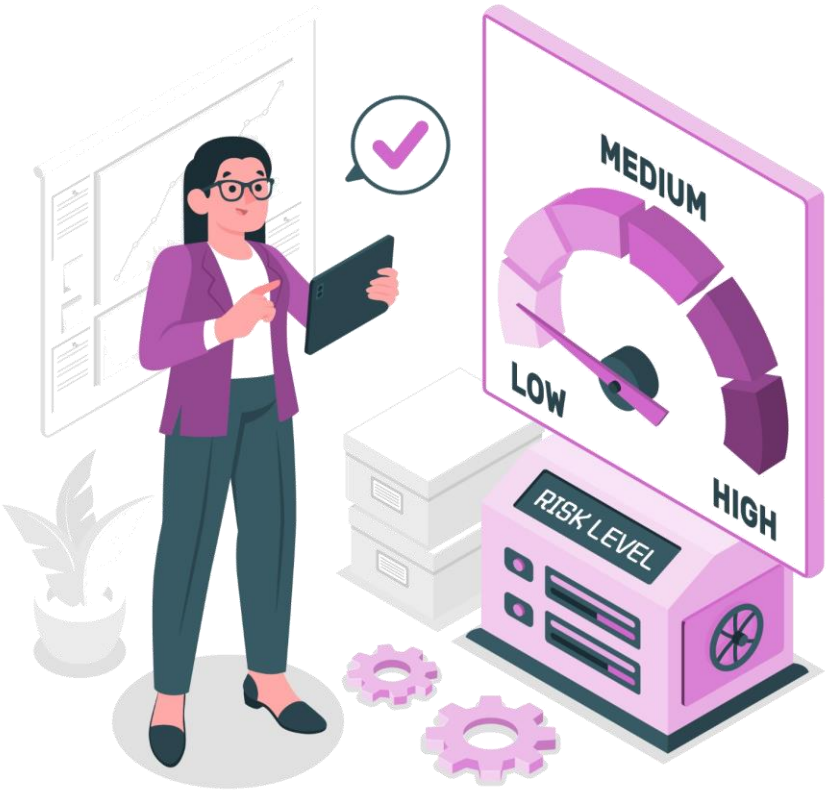
Operational Planning and Control

- ✓ This clause is very easy to explain the evidence against if the organisation has been already ‘showed its workings’
- ✓ In evolving the information security management system to concede requirements 6.1, 6.2 and in particular 7.5, where the entire ISMS is well structured and documented, this also accomplishes 8.1 at the same time
- ✓ The organisation is responsible for planning, implementing, and overseeing the procedures required to satisfy information security requirements and implement the chosen course of action

theknowledgeacademy

Information Security Risk Assessment

- ✓ This clause of ISO 27001 is automatically finished
- ✓ The organisations have already evidenced the information security management work in line with requirements 6.1 and 6.2, and the whole ISMS is documented
- ✓ The organisation should perform information security risk assessments as per planned intervals and when changes are required, which should be documented



theknowledgeacademy

Information Security Risk Treatment

- ✓ Under clause 8.3, the organisation needs to enforce the information security risk treatment plan and maintain documented information on the outcomes of that risk treatment
- ✓ Therefore, this requirement ensures that the risk treatment process described in clause 6.1 occurs
- ✓ This should incorporate evidence and transparent audit trials of reviews and actions, demonstrating the movements of the risk over time as outcomes of investments emerge (not least also providing the organisation and the auditor confidence that the risk treatments are accomplishing their objectives)

theknowledgeacademy

theknowledgeacademy

Module 8: Performance Evaluation

- ✓ Monitoring, Measurement, Analysis, and Evaluation
- ✓ Internal Audit
- ✓ Management Review

Monitoring, Measurement, Analysis, and Evaluation

- ✓ The organisation will assess the information security performance and the effectiveness of the information security management system
- ✓ The organisation shall determine the following:
  - What requires to be observed and measured involves information security processes and controls
  - The methods to monitor, measure, analysis and evaluation to make sure valid outcomes, as applicable
  - When the monitoring and measuring shall be carried out
  - Who is responsible for monitoring and measuring
  - When the monitoring and measurement must be analysed and assessed; and
  - Who will analyse and assess these outcomes?
- ✓ The organisation must keep appropriate documentation as proof of monitoring and measurement results

theknowledgeacademy

Internal Audit

- ✓ The organisation shall conduct internal audits at planned intervals to give information on whether the information security management system:
- ✓ Conforms to
  - The organisation's information security management system requirements
  - This International Standard's requirements
- ✓ Is successfully executed and maintained

è utile avere un sistema che permetta di aggiornare l'inventario, tenere solo l'inventario non è sufficente, si ha bisogno di tenerlo aggiornato.

theknowledgeacademy

Internal Audit

- ✓ The organisation shall:
  - Plan, establish, implement, and maintain an audit programme, including the frequency, methods, responsibilities, planning needs, and reporting requirements
  - The audit programme shall consider the significance of the processes involved and the outcomes of earlier audits
  - Define each audit's audit criteria and scope
  - Select auditors and conduct audits that ensure the audit process's objectivity and impartiality
  - Assure that the audit results are reported to the appropriate management
  - Keep documentation as evidence of the audit programme and the audit results

theknowledgeacademy

Management Review

- ✓ Top management must conduct planned reviews of the organisation's information security management system to assure its continued suitability, adequacy, and effectiveness
- ✓ The management review shall take into account:
- ✓ The status of previous management reviews' actions
- ✓ Changes in internal and external issues that are appropriate to the information security management system
- ✓ Feedback on the performance of information security, involving trends in:
    - Corrective and nonconformities actions
    - Results of monitoring and measurement
    - Audit results
    - Achievement of information security goals

theknowledgeacademy

Management Review

- ✓ Feedback from interested parties
- ✓ The outcome of the risk assessment and the status of the risk treatment plan
- ✓ Opportunities for continuous improvement
- ✓ The management review's outputs shall contain decisions on opportunities for continuous improvement and any requirements for changes to the information security management system
- ✓ The organisation shall keep documented information as evidence of the outcomes of management reviews

theknowledgeacademy

theknowledgeacademy

Module 9: Improvement

- ✓ Nonconformity and Corrective Action
- ✓ Continual Improvement

Nonconformity and Corrective Action

When a non-conformity happens, the organisation shall:

- ✓ Respond to the non-conformity, and if necessary:
  - Take appropriate action to control and fix it, and
  - Deal with the consequences
- ✓ Assess the requirement for action to eliminate the causes of nonconformity so that it does not reoccur or happen elsewhere by:
  - Review the nonconformity
  - Determine the causes of the nonconformity
  - Determining whether similar nonconformities exist or could happen

theknowledgeacademy

Nonconformity and Corrective Action

- ✓ Execute any necessary action
- ✓ Review the efficacy of any corrective action taken
- ✓ If essential, make changes to the information security management system
    - Corrective actions shall be relevant to the nonconformities encountered effects
    - The organisation shall keep documented information as evidence of the following:
- ✓ The nonconformities' nature, as well as any subsequent actions, are taken
- ✓ Any corrective action outcomes

theknowledgeacademy

Continual Improvement

Continual improvement is fundamental to achieving and sustaining information security's effectiveness and propriety

theknowledgeacademy

Module 10: Introduction to Auditing

- ✓ Internal Audit Charter
- ✓ Communicate with Organisation and Audit Committee
- ✓ Auditing Reflects
- ✓ General and Internal Auditing Standards and Guidance
- ✓ Auditing Types
- ✓ Auditing Techniques
- ✓ Auditing Principles
- ✓ Phases of Audit

Internal Audit Charter

- Statement of Purpose
- Roles and Responsibilities
- Reporting Relationships
- Points of Contact
- Programme Activities
- Reporting Requirements

theknowledgeacademy

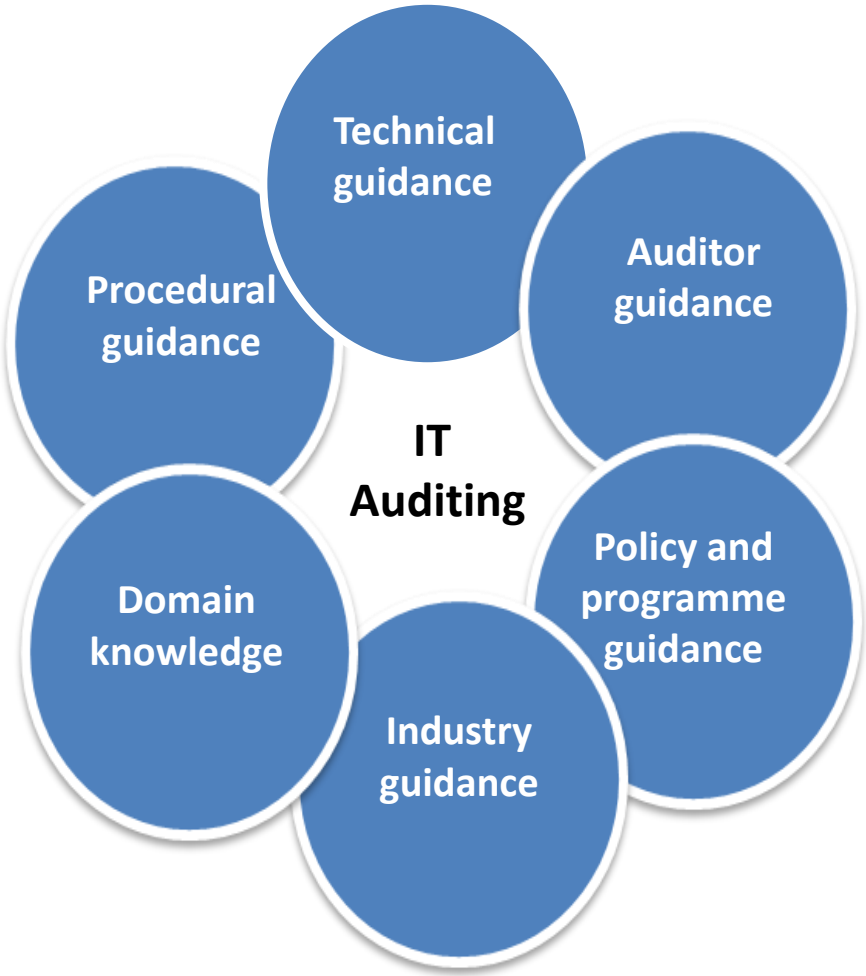
Communicate with Organisation and Audit Committee

theknowledgeacademy

Auditing Reflects

- ✓ Organisational policy
- ✓ Programme perspectives on what to audit and how different types of audits are conducted
- ✓ Generally Accepted Auditing Standards (GAAS) are examples of such standards
- ✓ Applicable subject matter knowledge

General and Internal Auditing Standards and Guidance



theknowledgeacademy

Auditing Types

First Party Audit

- ✓ Is an internal audit where a person from the inside of an organisation will conduct the Audit

Second Party Audit

- ✓ Also called external audit – an organisation will bring in a qualified second-party company to perform an audit, making sure that the organisation comply with a standard or legislation

Third Party Audit

- ✓ Where an organisation organises the audit of a third party (often a supplier) to ensure they are complying with an agreed contract

theknowledgeacademy

Auditing Techniques

Auditing Techniques

- ✓ ISO Auditors will use various audit techniques to get the required objective proof and obtain the objectives of every internal audit sessions Here are some audit techniques which are as follows:

Sampling

- ✓ This technique is one of the most efficient ways to obtain audit objectives
- ✓ Auditors must be able to reach valid conclusions about large systems However, it's often impractical or too costly to study every single item in a large system
- ✓ There may be just too many items to examine or they may be spread over a large geographical area
- ✓ As a result, auditors work with smaller samples

theknowledgeacademy

Auditing Techniques

- ✓ Sampling can be further divided into two types:

Judgement-Based Sampling

- ✓ Judgment-based sampling depends on the knowledge, skill, and experience of audit team members When using this approach, auditors use their personal judgment to select audit samples

Statistical Sampling

- ✓ Your statistical sampling plan should help you to achieve your audit objectives and should be based on what is known about the characteristics that define the population you intend to study
- ✓ ISO 19011 mentions two statistical sampling techniques: attribute-based sampling and variable-based sampling
- ✓ Attribute sampling is used when there are two possible outcomes (attributes) for each sample: yes/no, pass/fail, correct/incorrect
- ✓ Variable-based sampling is used when outcomes occur along a range of values

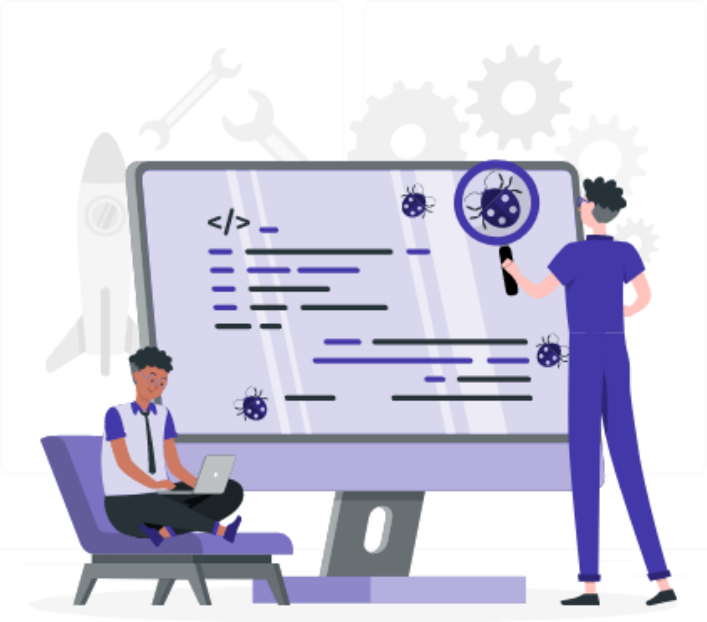
Auditing Techniques

Observation

- ✓ Auditors can observe a work process in review or action a physical feature of premises to determine if a method is efficient in obtaining intended results
- ✓ It can be an inactive observation while individuals carry on their work, or a directed walkthrough where an auditor will ask questions to get a better understanding

Testing

- ✓ In some situations, sampling or observing live data will not be possible, for instance if doing an activity generates unnecessary risk or too much disruption to the organisation



theknowledgeacademy

Auditing Techniques

Interview

- ✓ Showing the commitment of the leadership of the organisation is a major requirement, and one way to audit this is using interviews
- ✓ Our auditors can meet with individuals from across the organisation to ask them about various factors of the management system
- ✓ This is an excellent way to test awareness of critical policies and methods

Data Analytics (the science of analysing raw data in order to make conclusions about that information)

- ✓ Some processes can create a large amount of data which can be examined to determine if an intended result has been obtained
- ✓ This is a more technical method but it can be a beneficial technique

theknowledgeacademy

Auditing Techniques

Onsite Vs Offsite

- ✓ Most audits are performed on-site; but, with the emergence of video conferencing, remote execution of some of the above techniques is becoming increasingly feasible
- ✓ At the planning stage of the audit programme, the balance between on-site and off-site audits should be carefully considered, and it should be remembered that some audit techniques can only be performed on-site

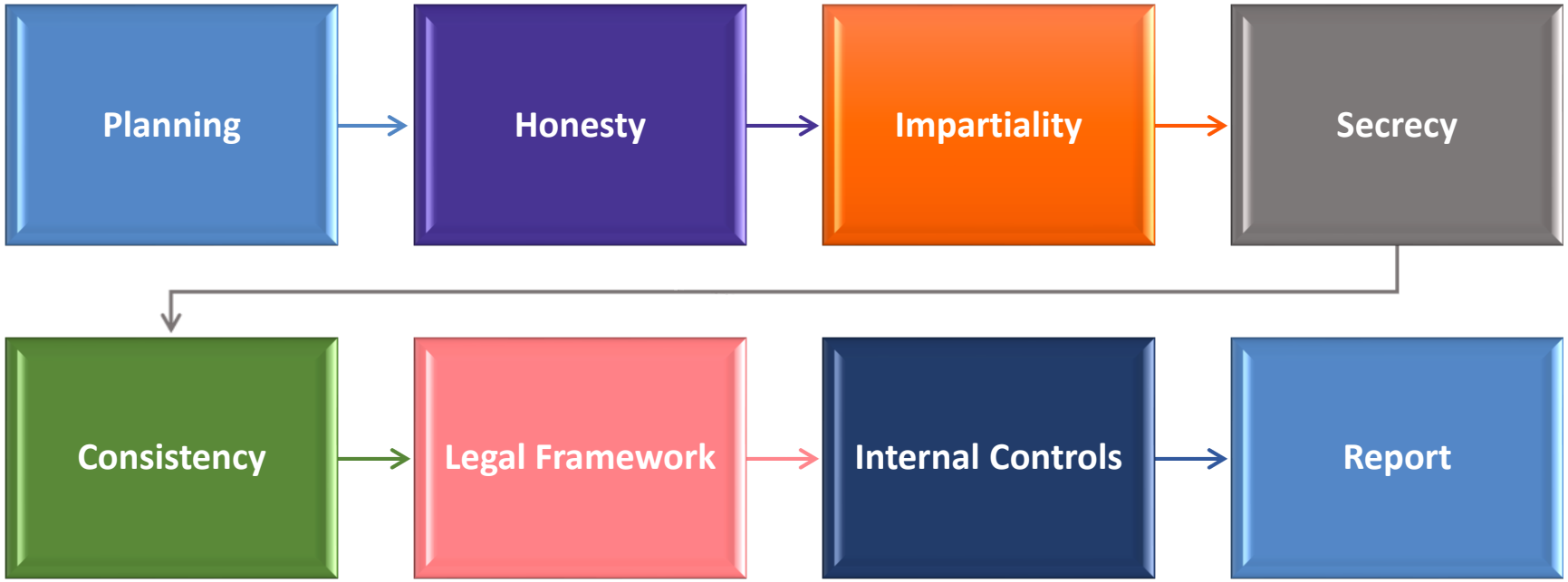
Human Interaction Vs No Human Interaction

- ✓ Individuals are an essential part of the ISMS of an organisation and are also a key to discovering what is happening within a management system
- ✓ Most of our audit time will be spent working with members of the site being audited

theknowledgeacademy

Auditing Principles

✓ The main principles of auditing are:



theknowledgeacademy

Auditing Principles

- ✓ **Planning:** An auditor must take into account the system as well as internal control procedures
- ✓ **Honesty:** Honesty and sincerity are important principles in auditing The professional integrity of an auditor must be beyond doubt
- ✓ **Impartiality:** The attitude of the auditor must be impartial Their personal views may not influence or affect the audit report
- ✓ **Secrecy:** Secrecy must be maintained An auditor may not disclose information to a third party
- ✓ **Consistency:** In the case of internet security audits, the auditor must follow the same processes in future years There should be consistency between audits

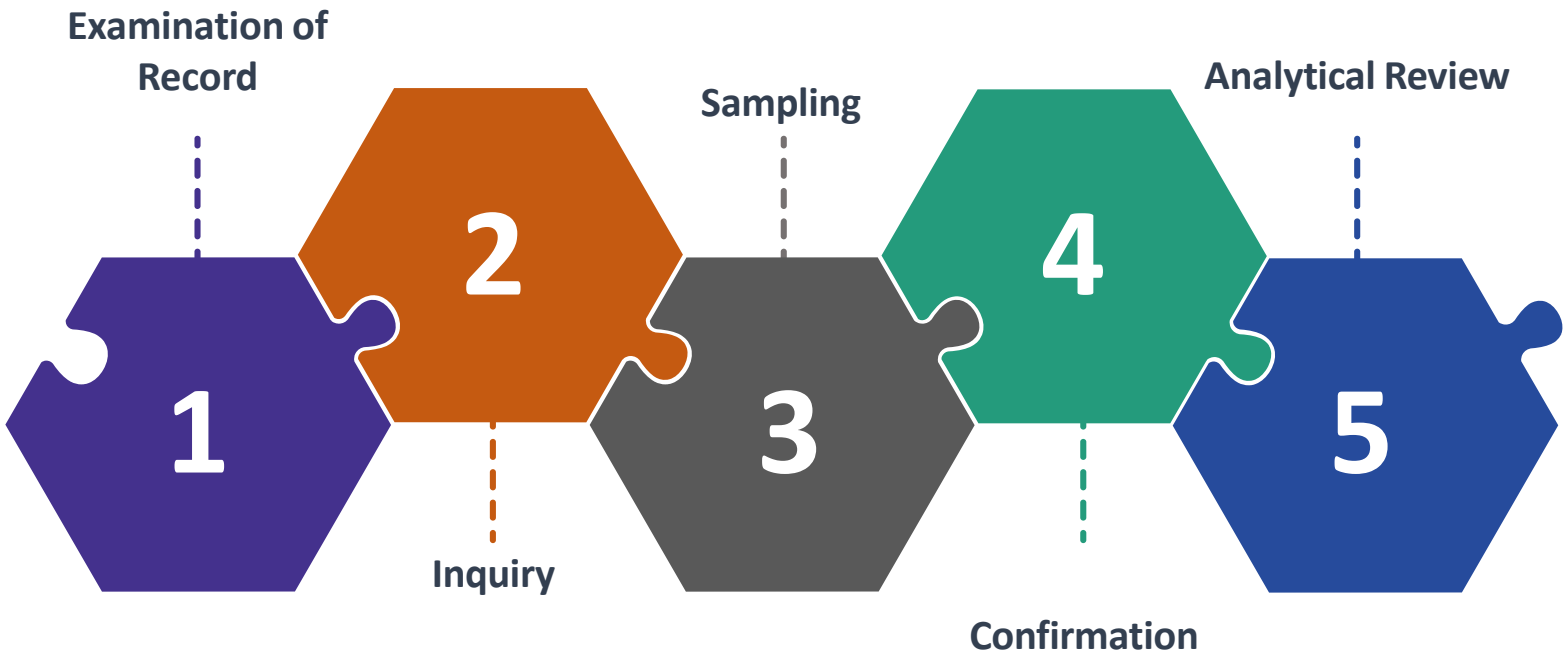
theknowledgeacademy

Auditing Principles

- ✓ **Legal Framework:** Business activities must run within rules and regulations The rule of law must be applied to protect the rights of interested parties
- ✓ **Internal Controls:** The auditor will examine the internal controls governing information security Ensure evidence exists of control use (eg records of resolved incidents)
- ✓ **Report:** A report should be prepared by the auditor at the end of an audit The auditor can draw conclusions and disclose relevant facts and figures as general information

Auditing Principles

✓ The techniques for auditing are:



theknowledgeacademy

Auditing Principles

- ✓ **Examination of Record:** This is commonly done by auditors The inspection of documentation is to verify the validity of data ISO focus should be on documentation and records

- ✓ **Inquiry:** An auditor can make inquiries/interview others An auditor can accumulate information from those inside and outside the organisation, often through the designated contact

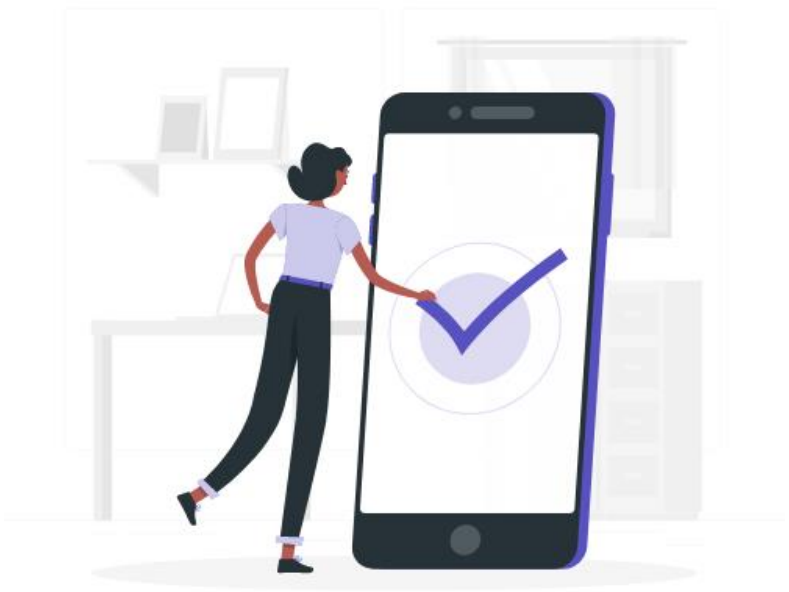
- ✓ **Sampling:** An auditor can select certain items from all of the available information to create samples This allows the auditor to obtain and evaluate the evidence to be extrapolated This is helpful in forming conclusions

theknowledgeacademy

Auditing Principles

- ✓ **Confirmation:** To ensure the accuracy of data, an auditor collects information from stakeholders Confirmation is a response to an inquiry to prove certain data recorded

- ✓ **Analytical Review:** This consists of studying significant ratios, trends, and investigating changes This review procedure is based on the expectation of a relationship between past and present data



theknowledgeacademy

Phases of Audit

There are several phases to an internal audit:

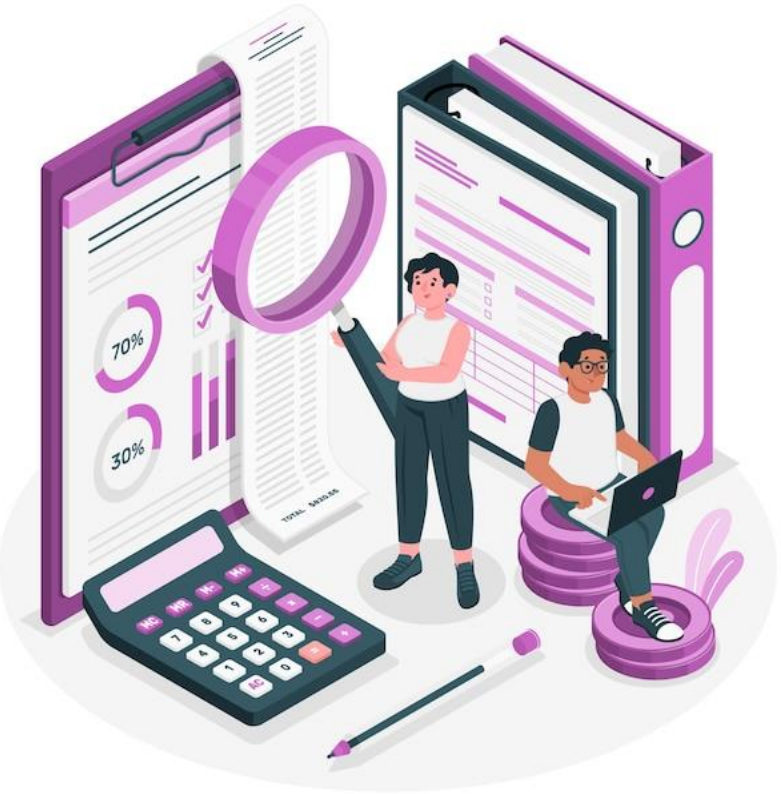
- ✓ Preparation and planning
- ✓ Execution and fieldwork
- ✓ Recording and reporting
- ✓ Follow-up and assessment

Phases of Audit

Audit Preparation

- ✓ Audit preparation consists of anything that is done in advance by interested parties, such as the auditor, the lead auditor, the client, and the audit program manager to ensure that the audit meets its goals

- ✓ The preparation stage of an audit begins with the decision to conduct the audit, and ends when the audit itself begins



theknowledgeacademy

Phases of Audit

Audit Performance

- ✓ Audit performance is the evidence collection stage of the audit and covers the time period from arrival at the audit location up to the exit meeting

- ✓ It consists of activities including
  - on-site audit management meeting with the auditee,
  - understanding the process and system controls,
  - verifying that these controls work,
  - communicating among team members,
  - communicating with the auditee

theknowledgeacademy

Phases of Audit

Audit Reporting

- ✓ The purpose of the audit report is to communicate the results of the investigation
- ✓ The report should provide correct and clear data that will be effective as a management aid in addressing important organisational issues

theknowledgeacademy

Phases of Audit

Audit Follow-up and Closure

- ✓ The audit is completed when all the planned audit activities have been carried out or agreed with the audit client and the report is produced
- ✓ Follow-up occurs after the audit is completed to check that concerns raised in the audit have been effectively addressed
- ✓ The audit cannot be closed until satisfactory evidence that the concerns have been addressed has been obtained

theknowledgeacademy

theknowledgeacademy

Module 11: Performing ISO 27001 Audits

- ✓ Preparing an Audit Report
- ✓ Assessment of Audit Reports and Documents
- ✓ Report Preparation, Findings, Reconciliation, and Conclusions
- ✓ Reviewing Documents and Reports
- ✓ Auditing Procedures
- ✓ Reviewing Documents and Reports
- ✓ Classifying Findings

Preparing an Audit Report

- ✓ The audit scope should be split down in the ISMS audit plan/checklist This should include timings and priorities
- ✓ Resourcing should be negotiated and agreed upon with the management of the organisation and auditing team
- ✓ Preliminary bookings should be made for formal audit reports/discussions, allowing participants to confirm attendance
- ✓ Specific “checkpoints” should be put in place to give auditors and management contacts opportunities to meet for discussion

Assessment of Audit Reports and Documents

- ✓ The internal audit is one of the key activities in ISO 27001, which assures that the information security management system (ISMS) is working efficiently and accurately
- ✓ An audit report is read by
  - People who were audited, or were present at the closing meeting
  - Senior management who were not present at the audit for review
  - The audit report needs to address the needs of both audiences
- ✓ The report is required to contain
  - The findings of the audit team supported by evidence evidence
  - The auditors opinion as to whether the auditee is compliant with ISO 27001
  - Any concerns raised and corrective measures required

theknowledgeacademy

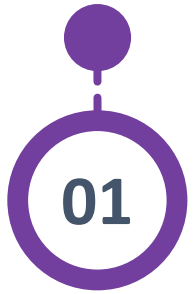
Assessment of Audit Reports and Documents

✓ ISO 19011 recommends the following items are to be included in the certification audit report :

theknowledgeacademy

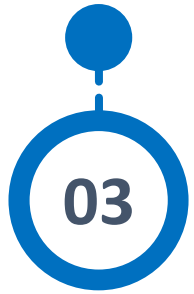
Assessment of Audit Reports and Documents

The following information is useful to internal audit



Summary of Audit Process & Obstacles

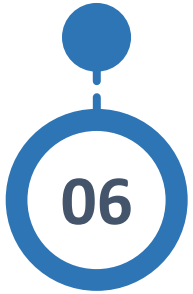
Audit Plan



Disagreement between Auditor and Auditee

Any Areas not Covered

Agreed Follow-up Plans



Opportunities for Improvement

theknowledgeacademy

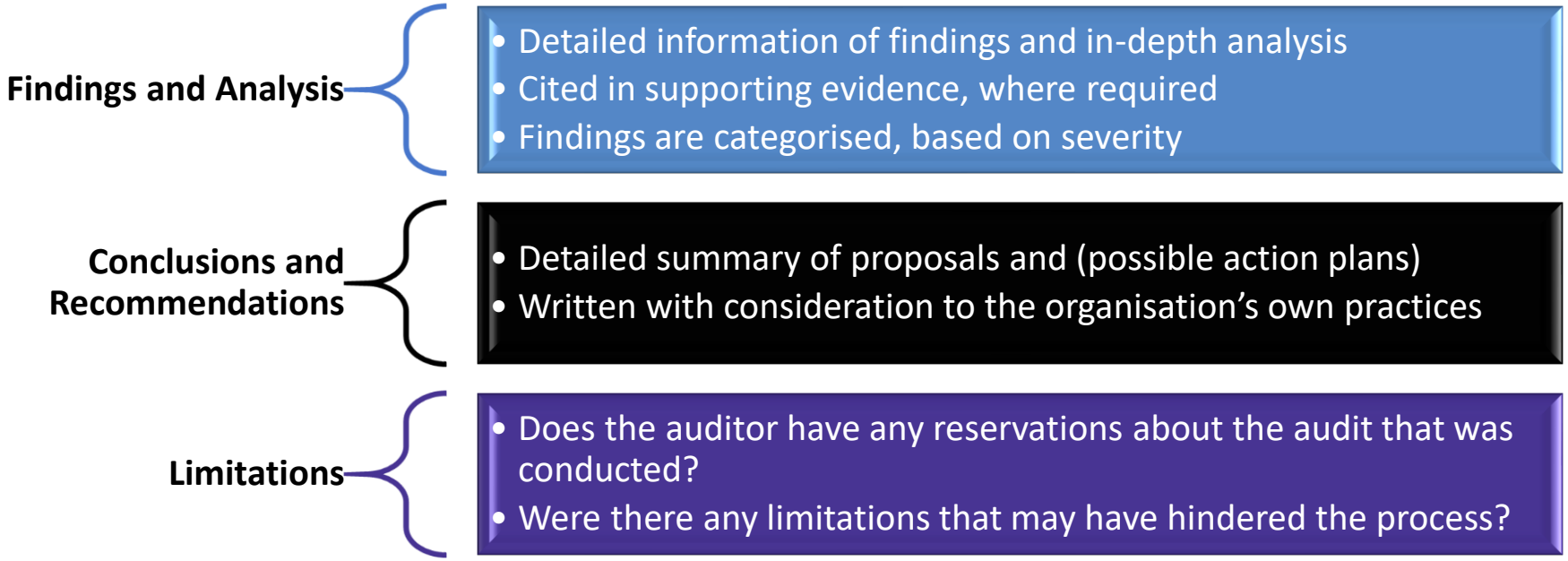
Preparing an Audit Report

✓ What to include?

Title and introduction	• Scope • Objectives
Timescale of audit	• Nature and extent of audit
Executive summary	• Key findings • Summary analysis and commentary • Conclusion(s) drawn from internal audit
Recipients and Document Classification	• Confidential findings viewable only by specified recipients • Instructions on how to circulate documentation
Credentials	• How did the internal auditors carry out their audit? • Who are the internal auditors?

theknowledgeacademy

Preparing an Audit Report



theknowledgeacademy

Report Preparation, Findings, Reconciliation, and Conclusions

- ✓ Below is the list of items that should be included in an Audit Report

Audit Objectives

- ✓ What is the purpose of the audit?
- ✓ Is this a regular audit of a process, or a follow-up on a corrective action?
- ✓ All Audits are done to demonstrate the compliance with the requirements, but was there anything else that was being done?

theknowledgeacademy

Report Preparation, Findings, Reconciliation, and Conclusions

Audit Scope

- ✓ What were the boundaries of the audit?
- ✓ If there is more than one manufacturing line that is using the process, how many were audited?
- ✓ Was a night shift or evening shift excluded?

Audit Client

- ✓ Who was the process owner or owners that the audit was performed for?

Audit Criteria

- ✓ What were the processes audited against? For instance, this could be the ISO 27001 standard, internal company procedures and policies, or customer requirements

theknowledgeacademy

Report Preparation, Findings, Reconciliation, and Conclusions

Audit Dates and Places

- ✓ It is essential to be able to demonstrate the timeframe when all of your audits of the system take place Also, for management review, it may be important to know the chronology of the audits that are being reviewed

Audit Findings

- ✓ What are the results of the evidence found? It is important to include the audit evidence for these findings including contract numbers that were reviewed, but leave out names of people who were audited

theknowledgeacademy

Report Preparation, Findings, Reconciliation, and Conclusions

Audit Conclusions

- ✓ What is the summary of the outcome of the audit?
- ✓ Were there too many findings to determine if the process was properly implemented?
- ✓ What is the assessment of the effectiveness of the QMS from this audit?

theknowledgeacademy

Auditing Procedures

There are some activities/steps which are carried out in the procedure:

STEP 1 : PREPARE ANNUAL AUDIT PLAN	
Responsibility	**ISMS Audit Team**
Input	• Security-related incidents which are occurred since the last audit • Security-related personnel problems that have occurred since the last audit • Results of any risk assessment are initiated since the last audit and proposed controls discussion • To manage risk designation of processes or people • Proposed changes to the Security Policy • Previously decided actions' implementation progress reports
Actions	• The information security management system's Audit Team makes the Annual Audit Plan which covers the audits types as well as the frequency and audit methods The plan of annual audit takes into consideration the importance and status of the areas and processes to be audited, the Risk Assessment report, as well as the results of earlier audits
Output	Annual Audit Plan

theknowledgeacademy

Auditing Procedures

STEP 2 : SUBMIT PLAN FOR APPROVAL	
Responsibility	**ISMS Audit Team**
Input	• Annual Audit Plan
Actions	• The plan is submitted by the ISMS Audit Team to the ISMS Manager for consent After having the permission of the annual audit plan, the ISMS Audit Team communicates the plan to the interested parties
Output	• When approved: Proceed to step 3 • When not approved: Proceed to step 1

theknowledgeacademy

Auditing Procedures

STEP 3 : PREPARE FOR AUDIT	
Responsibility	**ISMS Audit Team**
Input	• Annual Audit Plan • Periodic audit • Ad-hoc audit
Actions	• The ISMS Audit Team gathers and studies earlier audit findings and possible outstanding concerns Also, all the relevant documents are prepared by the team that will be required for the realisation of the audit Work-programs or checklists are instrumental in helping thorough, efficient and uniform • Periodical audit work-programs/ checklists should be in-depth and based on ISO 27001, that follows a predefined path and checking adherence with controls Follow-up audit work-programs/checklists should be limited to involve only the findings of the relative audit Ad-hoc audit work-programs/ checklists should always be focused on a trigger event So, ad-hoc audit checklists should be created to a new before every ad-hoc audit
Output	• ISMS Audit Checklist

theknowledgeacademy

Auditing Procedures

STEP 4 : CONDUCT AUDIT & RECORD FINDINGS	
Responsibility	**ISMS Audit Team**
Input	• ISMS Audit Checklist • Annual Audit Plan
Actions	• The ISMS Audit Team conducts the audit and completes pre-defined audit report During the audit course, the audit and ISMS audit Team tries to find out proper proofs to determine that: ○ The information security policy is an absolute reflection of the needs of the business ○ A proper risk assessment methodology is used ○ Documented processes are being followed and meeting their desired goals ○ Technical controls are in place, rightly configured and working as planned ○ Assessing residual risk correctly, acceptable to the company's management ○ Actions that are agreed form earlier audits and reviews have been executed ○ ISMS is compliant with ISO 27001
Output	• Output Audit Findings (if any)

theknowledgeacademy

Auditing Procedures

STEP 5 : CREATE & ARCHIVE AUDIT REPORT	
Responsibility	**ISMS Audit Team**
Input	• ISMS Audit Checklist • Annual Audit Plan
Actions	• The ISMS Audit Team makes the report of the audit, that is based on the audit findings This is a report related to non-compliance, high residual risks, unsolved issues, etc Audit findings should be labelled as per its priority level • Audit findings that are marked as Priority 1 are important nonconformities and should be planned for resolution in a period on of two weeks, and follow-up audit should be scheduled at the end period If it is considered critical, the resolution of the certain audit findings are needed ASAP • Audit findings that are marked as Priority 2 are less non-conformities and should bee planned for resolution in a period of three months, and follow-up audit should be scheduled at the end period
Output	• Audit Report

theknowledgeacademy

Auditing Procedures

STEP 6 : DEVELOP ACTION PLAN	
Responsibility	**ISMS Audit Team**
Input	• Annual Report
Actions	• In accordance with the audit findings and the non-conformance level, an action plan and follow-up audit should be developed Follow-up audits are scheduled and performed when an earlier audit has found critical non-conformances The scope of follow-up audits is restricted to the non-conformance and mechanisms of the same audit that produces the finding are used
Output	• Action Plan • Follow up Audit

theknowledgeacademy

Reviewing Documents and Reports

Mandatory Documents by ISO 27001

- ✓ Scope of the ISMS (clause 43)
- ✓ Information security policy and objectives (clauses 52 and 62)
- ✓ Risk assessment and risk treatment methodology (clause 612)
- ✓ Statement of Applicability (clause 613 d)
- ✓ Risk treatment plan (clauses 613 e and 62)
- ✓ Risk assessment report (clause 82)
- ✓ Definition of security roles and responsibilities (clauses A712 and A1324)
- ✓ Inventory of assets (clause A811)

theknowledgeacademy

Reviewing Documents and Reports

Mandatory Documents by ISO 27001

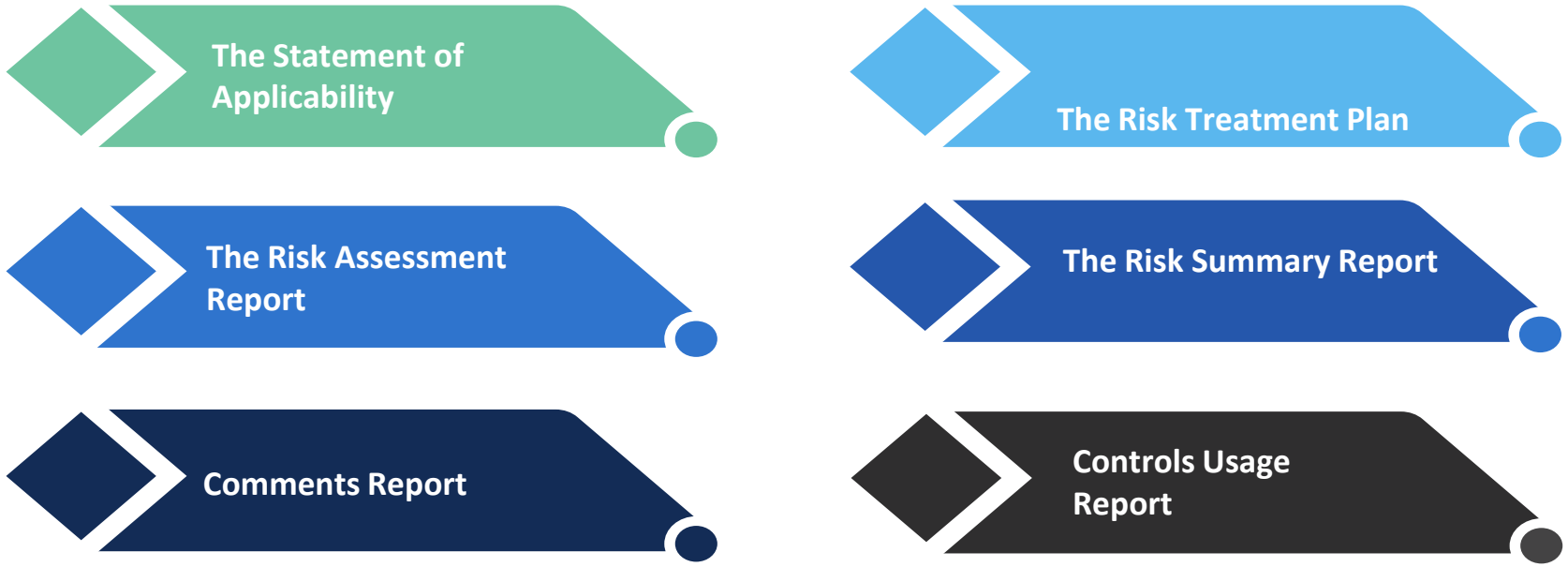
- ✓ Acceptable use of assets (clause A813)
- ✓ Access control policy (clause A911)
- ✓ Operating procedures for IT management (clause A1211)
- ✓ Secure system engineering principles (clause A1425)
- ✓ Supplier security policy (clause A1511)
- ✓ Incident management procedure (clause A1615)
- ✓ Business continuity procedures (clause A1712)
- ✓ Statutory, regulatory, and contractual requirements (clause A1811)

theknowledgeacademy

Reviewing Documents and Reports

Reports

✓ The following are the six best reports for ISO 27001 audit:



Classifying Findings

- ✓ The audit findings are the auditor's summary or description and analysis of an inadequately mitigated risk to the organisation
- ✓ Audit findings are collected through interviews, examination of documents, and observation of activities and conditions in the areas of concern
- ✓ The audit team will review their findings to determine whether they should be reported as non-conformities or observations

theknowledgeacademy

Classifying Findings

Finding	Definition/Impact	Action/Mitigation
COMPLIANT	Compliant means adherence with the requirements of the standard and the QMS The process is implemented and documented and records exist to verify this	Continue to monitor trends/indicators
OFI	A low risk issue that offers an opportunity to improve current practice Processes may cumbersome or overly complex but meet their targets and objectives Unresolved OFIs may degrade over time to become non-compliant	Review and implement actions to improve the process(s) Monitor trends/indicators to determine if improvement was achieved
MINOR N/C	A medium risk, minor non-conformance resulting in deviation from process practice not likely to result in the failure of the management system or process that will not result in the delivery of non-conforming products nor reduce the effectiveness of the QMS	Investigate root cause(s) and implement corrective action by next reporting period or next scheduled audit
MAJOR N/C	A high risk, major non-conformance which directly impacts upon customer requirements, likely to result in the customer receiving non-conforming products or services, or which may reduce the effectiveness of the QMS	Implement immediate containment action, investigate root cause(s) and apply corrective action Re-audit in 4 weeks to verify correction

theknowledgeacademy

The Reliability of Audit Findings

The following are the aspects that impact the reliability of audit findings:

- ✓ Relevant scope of the audit
- ✓ Auditee name and title
- ✓ Time, date and venue
- ✓ Needs of the standard
- ✓ State what is seen and how it does not satisfy the needs
- ✓ Document names, versions of documents and date of the last update

theknowledgeacademy

theknowledgeacademy

Module 12: Internal Auditor

- ✓ Roles and Responsibilities
- ✓ Audit Plan
- ✓ Opening Meeting
- ✓ Record Review Activities
- ✓ Internal Auditor Checklist
- ✓ Communication Between Departments
- ✓ Drafting Reports and Test Plans

Roles and Responsibilities

✓ Internal auditors must:

theknowledgeacademy

Roles and Responsibilities

theknowledgeacademy

Audit Plan

- ✓ The ISO 19011 standard tells management about the auditing activities for auditing to ISO 27001
- ✓ This official methodology can help to assure the consistency and effectiveness in your internal audits and shapes the integrity of the system of internal audit
- ✓ These are not compulsory steps (eg, small companies can miss some of them), but they are a best practices for conducting an audit

Audit Plan

Prepare an audit plan This plan should involve the following components and considerations:

1. Roles and responsibilities of each audit team member
2. Risk-based approach to audit planning
3. Scheduling and coordination of audit activities
4. Scope and complexity of the audit
5. Sampling techniques for collecting evidence
6. Opportunities for improvement
7. Risks of inadequate planning
8. Impact of the audit on auditee activities

theknowledgeacademy

Opening Meeting

- ✓ An opening meeting between the auditee and all relevant parties should be held
- ✓ During the opening meeting, confirm the following with all relevant parties:
  - Audit programme plans
  - Audit scope
  - Audit objectives
  - Audit criteria
  - Audit plans

Opening Meeting

- Roles and responsibilities of the audit team
- That all planned activities can be performed, and proper authorisation is acquired
- Language of the audit
- Information security protocol
- Relevant access and arrangements for the audit team
- Notable on-site activities that could impact audit process

Opening Meeting

- ✓ During the opening meeting, the following items should be clearly communicated:
  - Methods for reporting and communicating audit progress
  - Conditions of audit termination
  - Procedures for dealing with audit findings during the audit
  - Procedures for receiving feedback from the auditee in response to findings during the audit

Record Review Activities

- ✓ Internal auditors should keep in regular contact to ensure adherence to the audit plan.
- ✓ Regular face-to-face meetings and the use of audit working papers allows internal auditors and lead auditors to track progress according to the internal audit checklist and plan.
- ✓ Meetings set out in the plan with management contacts allow for auditors to request access to certain information, as well as potential problems with the process.

Internal Auditor Checklist

- ✓ One of the tools available to ensure audits address the essential requirements is the audit checklist.
- ✓ It serves as a reference point before, during, and after the audit process, and if developed for and used correctly, it will provide the following benefits:

- Ensures the audit is conducted systematically
- Promotes audit planning
- Ensures a consistent audit approach
- Actively supports organisation's audit process
- Provides a repository for notes collected during the audit
- Provides reference to objective evidence
- Ensures uniformity in the performance of different auditors

theknowledgeacademy

Internal Auditor Checklist

- ✓ An audit plan is a list of guidelines to be followed when conducting the audit; this will be particular to the nature of the organisation and its ISMS, as well as its specific needs.

To prepare the audit plan, the following are required:

Internal Auditor Checklist

Benefits of a Checklist:

- ✓ Conducting regular audits can help a small business identify problems and highlight strengths within the business.
- ✓ The use of an audit checklist not only helps small business review their practices but will also help them to prepare in the event of a third-party audit in the future.
- ✓ An audit checklist identifies areas of concern, allowing management to take corrective action.

theknowledgeacademy

Communication Between Departments

Here are some tips for communication during an audit:

Do not Rely on Email

- ✓ Email should be used for basic tasks and for keeping people informed.
- ✓ Face-to-face and telephone interaction force parties to commit to an action, speeding up the process

Less Jargon

- ✓ Avoid using audit jargon when communicating with stakeholders, as it increases the potential for confusion
- ✓ Be ready to take time explaining aspects

Communication Between Departments

Here are some tips for communication during an audit:

Keep Meeting Short and Relevant

- ✓ Avoid wasting stakeholders' time; the information shared should be actionable.
- ✓ Do state when additional information is required to move forward.
- ✓ Keeping things concise and relatable gives the auditee more chances and incentives to help.

theknowledgeacademy

Drafting Reports and Test Plans

- ✓ A typical ISMS audit report will contain some of the following elements, some of which may be split into appendices or separate documents:
  - Title and introduction naming the organisation and clarifying scope, objectives, period of coverage and the nature, timing and extent of the audit work performed.
  - An executive summary indicative of the key audit findings with a short analysis and commentary, and an overall conclusion, typically phrased as:
    - ❑ “We find the ISMS compliant with ISO/IEC 27001 and worthy of certification” or “Aside from [significant concerns], we are impressed with the coverage and effectiveness of the information security controls within the ISMS”.

Drafting Reports and Test Plans

- ✓ A list of specific recipients (since the contents may be confidential) and appropriate document classification or circulation instructions.
- ✓ An outline of the credentials, audit methods, and other information pertaining to individual auditors and team members.
- ✓ Audit findings and analysis, supported upon occasion by extracts from the audit files to aid understanding.
- ✓ The audit conclusions and recommendations are to be discussed with management and eventually integrated if agreed upon as action plans depending on the organisation's practices.
- ✓ A formal statement of the auditors' reservations, qualifications, scope limitations, or other caveats with respect to the audit.
- ✓ Management may be invited to provide a short commentary or formal response, accepting the results of the audit and stating a commitment to agreed plans.

theknowledgeacademy

Module 13:
ISMS and the ISO 27001 Standards Family

- ✓ What is an ISMS?
- ✓ Project Plan
- ✓ Management and Governance Frameworks
- ✓ ISMS Benefits
- ✓ Scope of ISMS in an organisation
- ✓ Introduction to Management Systems
- ✓ Process Approach
- ✓ Fundamentals
- ✓ The PDCA Cycle

What is an ISMS?

- ✓ An ISMS is simply an application of 27001. A set of policies and procedures for the holistic management of sensitive data and related systems on various levels
- ✓ A series of guidelines for documentation, auditing, continual improvement, and corrective and preventive action
- ✓ The overarching goal is to ensure confidentiality, integrity, and availability of information (resiliency)
- ✓ ISMS incorporates continuous feedback and improvement processes (more on PDCA shortly). ISMS intends to address changes over time, such as threats, vulnerabilities, and impacts

theknowledgeacademy

What is an ISMS?

Areas of focus are:

- ✓ Business processes and assets
- ✓ Reducing risk to data assets and related systems
- ✓ It can be targeted towards specific data classes or implemented comprehensively
- ✓ An ISMS is not a tactical instrument. The main goals of ISMS are generally to:

theknowledgeacademy

What is an ISMS?

Role and Importance of ISMS

- ✓ Adopts a comprehensive management strategy to guarantee the information security controls meet the organisation's ongoing information security needs

- ✓ A company's use of a systematic approach to identify, evaluate, and manage information security risk is strongly suggested by establishing, maintaining, and updating an ISMS

What is an ISMS?

Key Components of ISMS

- ✓ Below are the three key components of implementing an information security policy:

- ✓ The ISO 27001 standard requires that an organisation's needs and objectives directly influence the design and implementation of an ISMS, security requirements and the organisational processes used, and the size and structure of the organisation

What is an ISMS?

Objectives and Purposes of ISMS

- ✓ The main objective of Information Security Management Systems is to implement the appropriate measures to eliminate or minimise the impact that various information security-related threats and vulnerabilities might have on an organisation.

- ✓ Doing so will help in the development of desirable characteristics for the services offered by the organisation, **such as:**

Availability of Services

Preservation of Data Confidentiality

Integrity

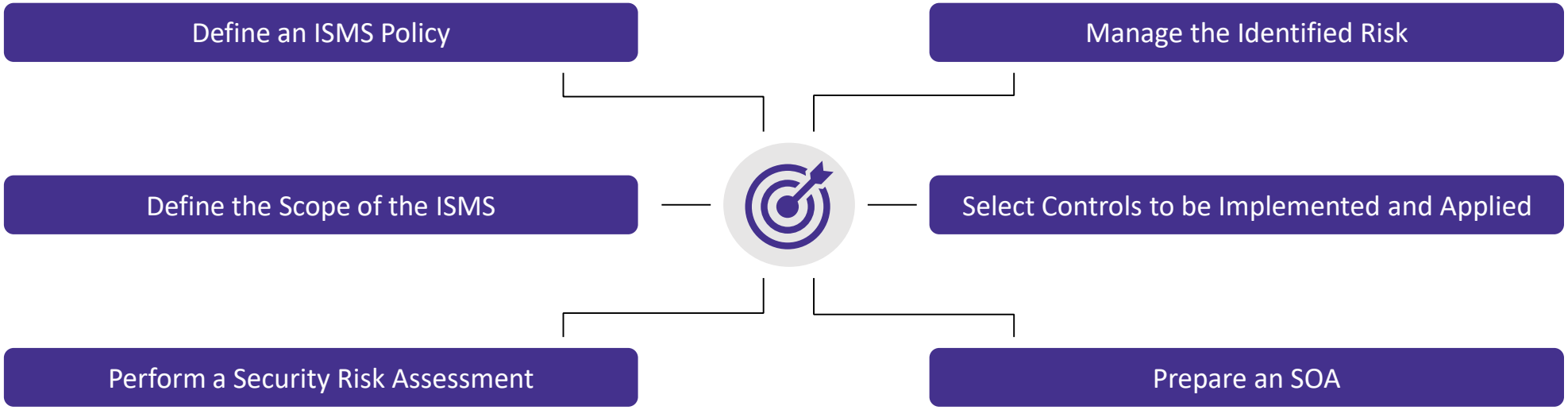
theknowledgeacademy

Project Plan

Implementation Phases

- ✓ An organisation must also have a detailed understanding of PDCA implementation phases to manage the project's costs

- ✓ The PDCA cycle matches each auditable international standard: ISO 18001, 9001 and 14001. ISO/IEC 27001:2005 dictates the PDCA steps for an organisation to follow, which are as below:



Project Plan

There are Eleven Phases of Implementation:

Phase 1 Identify Business Objectives

Phase 2 Obtain Management Support

Phase 3 Select the Proper Scope of Implementation

Phase 4 Define a Method of Risk Assessment

Phase 5 Prepare an Inventory of Information Assets to Protect, and Rank Assets According to Risk Classification Based on Risk Assessment

Phase 6 Manage the Risks, and Create a Risk Treatment Plan

theknowledgeacademy

Project Plan

There are Eleven Phases of Implementation:

Phase 7 Set Up Policies and Procedures to Control Risks

Phase 8 Allocate Resources, and Train the Staff

Phase 9 Monitor the Implementation of the ISMS

Phase 10 Prepare for the Certification Audit

Phase 11 Conduct Periodic Reassessment Audits

theknowledgeacademy

Project Plan

Phase 1: Identify Business Objectives

- ✓ Stakeholders must buy-in; the step that will win management support is establishing and prioritising objectives
- ✓ The organisation's mission, strategic plan, and IT goals can all be used to create primary objectives. **The objectives can be:**
  - Increased possibilities for marketing
  - Assuring business partners of the organisation's information security status

Project Plan

Phase 1: Identify Business Objectives

- Assurance of the company's dedication to information security, privacy, and data protection to partners and customers
- Offering the best level of protection for customers' sensitive data will increase revenue and profitability
- Understanding information assets and performing efficient risk analyses
- Maintaining the organisation's standing among top business leaders
- Adherence to the rules of the industry

Project Plan

Phase 2: Obtain Management Support

- ✓ The ISMS must be established, planned for, implemented, run, monitored, reviewed, maintained, and improved by management
- ✓ The commitment must guarantee that all personnel impacted by the ISMS have the appropriate training, awareness, and competency and that the right resources are available to work on the ISMS

The following activities/initiatives demonstrate management support:

- A policy for information security
- Information security roles and responsibilities, often known as a segregation of duties (SoD) matrix that lists the roles involved

Project Plan

Phase 2: Obtain Management Support

- A statement or message to the organisation stressing the value of following the information security policy
- Enough resources to administer, create, maintain, and apply the ISMS
- Determining the acceptable risk threshold
- Every so often, the ISMS is reviewed by management
- Assurance that the training is given to the employees who the ISMS will impact
- Appoint qualified individuals to the positions and duties they will be fulfilling
- Information security plans and objectives

Project Plan

Phase 3: Select the Proper Scope of Implementation

- ✓ According to ISO 27001, any implementation scope may include all or a part of an organisation
- ✓ For certification to take place, only the business units, processes, and external vendors or contractors falling within the implemented scope must be identified
- ✓ Companies must also list any scope exclusions and the justifications for them by the standard. The organisation may save time and money by determining the implementation's scope

The following details should be taken into account:

- In order to accomplish the determined business objectives, the chosen scope is important

Project Plan

Phase 3: Select the Proper Scope of Implementation

- ✓ In order to accomplish the determined business objectives, the chosen scope is important
- ✓ The organisation's overall size of activities is a crucial factor in determining the degree of complexity of the compliance process.
- ✓ Organisations must consider the number of people, business procedures, work locations, and products or services to assess the proper scale of operations.
- ✓ Which organisational departments, locations, resources, and technology will be under the ISMS's control?
- ✓ Will suppliers have to follow the ISMS?

Project Plan

Phase 3: Select the Proper Scope of Implementation

- ✓ Dependencies on other organisations exist? Should they be taken into account?
- ✓ It is important to note any legal or regulatory requirements relevant to the ISMS's coverage areas
- ✓ The organisation's industry, local, state, or federal governments, as well as worldwide regulatory organisations, may provide such standards
- ✓ The scope should be modest, and it might be wise to focus exclusively on a logical or physical grouping inside the organisation

Project Plan

Phase 4: Define a Method of Risk Assessment

- ✓ Companies must specify and document a risk assessment approach in order to comply with ISO/IEC 27001 criteria.

The risk assessment method is not specified in the ISO/IEC 27001 standard. It's important to take into account the following:

- How will the risk to certain information assets be evaluated?
- Which risks are unaffordable and must be mitigated?
- Using carefully established rules, processes, and controls to manage the remaining risks

Project Plan

Phase 5: Prepare an Inventory of Information Assets to Protect, and Rank Assets According to Risk Classification Based on Risk Assessment

- ✓ A list of the information assets that the company needs to safeguard must be made
- ✓ It is important to identify the risk connected to each asset, as well as its owners, location, criticality, and replacement value
- ✓ It will be helpful to have information on asset grouping, data categorisation, and asset inventory documents

The following actions are suggested:

- Determine the assets' high, medium, and low CIA effect levels
- Determine the risks and categorise them based on their gravity and exposure

theknowledgeacademy

Project Plan

Phase 5: Prepare an Inventory of Information Assets to Protect, and Rank Assets According to Risk Classification Based on Risk Assessment

- Determine the risks and categorise them based on their gravity and exposure
- Assign values to the risks after determining the hazards and the CIA levels
- Determine the risk's tolerability based on risk values and then decide whether to put a control in place to remove or decrease the risk. Establishing risk levels for assets will be guided by the risk assessment approach

✓ The information assets with intolerable risk and hence needing controls will be determined once the assessment is complete

✓ At that point, a report that details the risk value for each asset is prepared and is occasionally referred to as a risk assessment report

Project Plan

Phase 6: Manage the Risks, and Create a Risk Treatment Plan

- ✓ The organisation must accept, avoid, transfer, or decrease the risk to an acceptable level by utilising risk-mitigating procedures to control the impact associated with risk
- ✓ The next step is to do a gap analysis using the standard's controls to produce an RTP and an SOA
- ✓ For the suggested residual risks, management approval is crucial

Project Plan

Phase 6: Manage the Risks, and Create a Risk Treatment Plan

The RTP provides the following:

- Effective risk management (accept, transfer, reduce, avoid)
- Gap analysis is used to identify operational controls and extra proposed controls
- A suggested timetable for implementing controls

Project Plan

Phase 7: Set Up Policies and Procedures to Control Risks

- ✓ The organisation will need policy statements or a comprehensive procedure and responsibility document to establish user roles for the consistent and efficient application of policies and procedures for the controls implemented, as illustrated in the SOA
- ✓ ISO/IEC 27001 stipulates that policies and procedures must be documented
- ✓ The organisation's structure, locations, and assets will determine the applicable policies and procedures

Project Plan

Phase 8: Allocate Resources, and Train the Staff

One of the key commitments for management is highlighted by the ISMS process: having the resources to manage, develop, maintain, and implement the ISMS. The training must be documented to pass an audit

Project Plan

Phase 9: Monitor the Implementation of the ISMS

- ✓ For monitoring and evaluation, a recurring internal audit is essential. Controls and corrective and preventative measures are examined during an internal audit review
- ✓ The internal audit gaps must be addressed by determining corrective and preventative controls and the company's compliance based on a gap analysis to complete the PDCA cycle
- ✓ Management must examine the ISMS regularly at predetermined periods for it to be effective
- ✓ The evaluation comes after modifications/improvements to staffing decisions, policies, procedures, and controls
- ✓ The project management review is a crucial stage in the procedure. The findings of audits and regular reviews are kept on the document and updated

Project Plan

Phase 10: Prepare for the Certification Audit

- ✓ For an organisation to be certified, it must complete a full cycle of internal audits, management reviews, and PDCA process activities
- ✓ It must also keep records of its actions in response to those reviews and audits
- ✓ Risk analyses, the RTP, the SOA, and policies and procedures should all be reviewed by ISMS management at least once a year
- ✓ To ascertain the scope and content of the ISMS, an external auditor will first review the ISMS documentation

Project Plan

Phase 10: Prepare for the Certification Audit

- ✓ A significant amount of evidence and review/audit papers must be provided to an auditor for examination for the review and audit to be successful
- ✓ The documentation and supporting proof will show how well the organisation's and its business divisions' implementation of the ISMS has worked

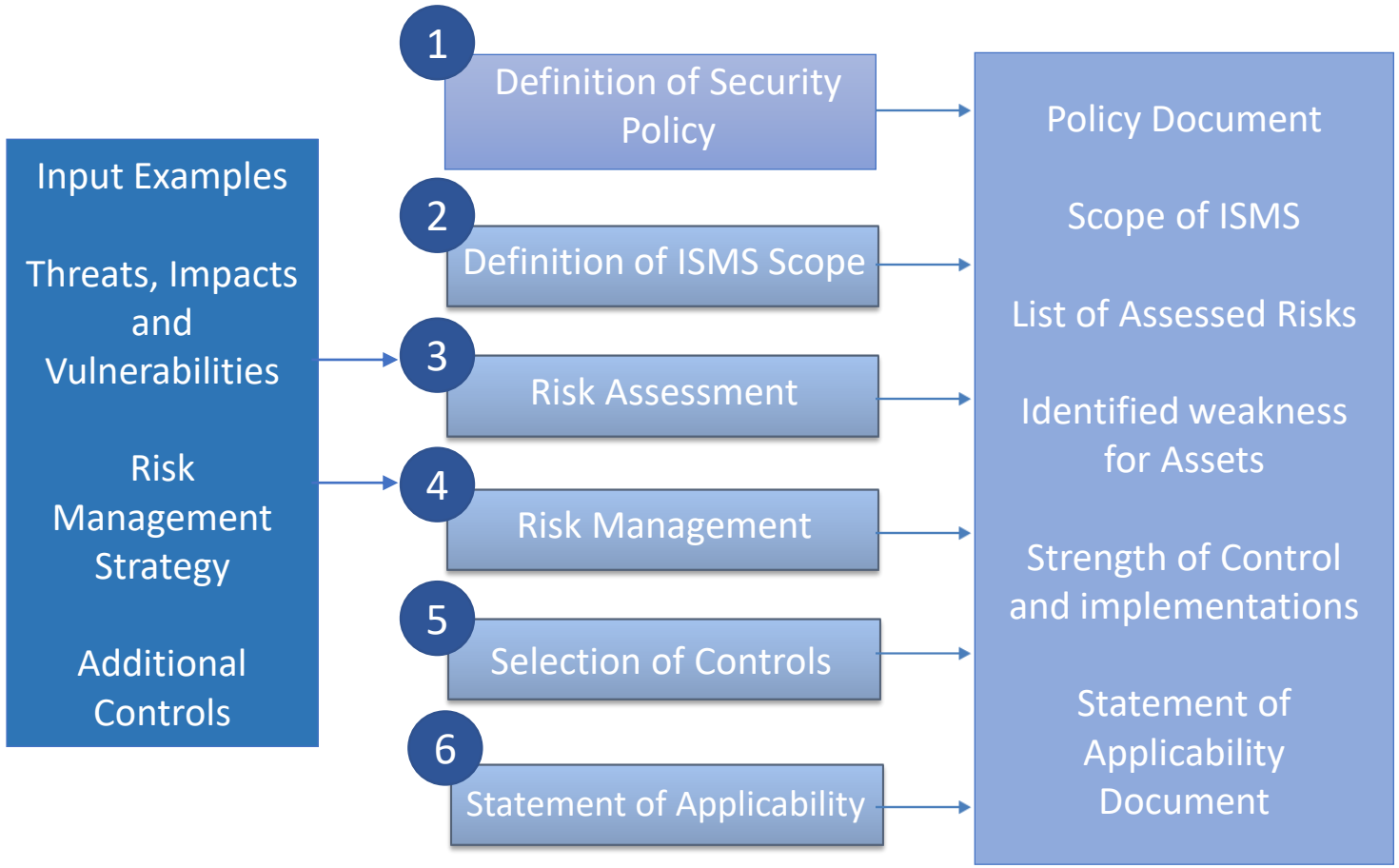
Project Plan

Phase 11: Conduct Periodic Reassessment Audits

- ✓ Periodic audits or follow-up evaluations verify that the organisation complies with the standard
- ✓ Reassessment audits are necessary for certification maintenance to verify that the ISMS is operating as planned and defined
- ✓ The PDCA cycle is followed by ISO 27001, just like all other ISO standards, and it helps ISMS management understand how well and how far the company has come in terms of this cycle's progression
- ✓ This directly affects how much time and money is projected to achieve compliance

Management and Governance Frameworks

ISMS Frameworks



theknowledgeacademy

ISMS Benefits

The benefits of ISMS are as follows:

01 Provides consumers and stakeholders with confidence in how you manage risk

02 Consistency in the delivery of your product or service

03 Enhanced customer satisfaction

04 Protects an organisation's assets, shareholders, and customers

05 Keeps confidential information secure

06 Secure exchange of information

theknowledgeacademy

ISMS Benefits

The benefits of ISMS are as follows:

07 Provides organisations with a competitive advantage

08 Manages and minimises risk exposure

09 Builds a culture of security

10 Adherence to a well-vetted and accepted standard lends

- A clearer definition of processes, roles, and responsibilities, resulting in better efficiency
- Alignment with Annex SL lends shared language and concepts across all management system implementations baon ISO standards.

theknowledgeacademy

Scope of ISMS in an organisation

- ✓ When designing an ISMS, defining the ISMS scope and boundaries is completed first
- ✓ ISMS scope should correlate with business requirements, organisational structure, technologies, and information assets
- ✓ No limits to ISMS scope – it can be as small or large as the organisation wishes
- ✓ Defined by security aims, threats to security, security procedures, and organisation size
- ✓ Depends on how complex the ISMS would need to be – smaller organisation, simpler ISMS
- ✓ Top management should decide the scope
- ✓ ISMS should evolve at the same pace as risks develop
- ✓ Organisations can measure their compliance with ISO 27001 by becoming certified with the standard

theknowledgeacademy

Introduction to Management Systems

Management Responsibility in Implementation

- ✓ Implementing an ISMS is something that ISO 27001 recognises, affecting the whole organisation
- ✓ ISO 27001 requires management to communicate the importance of an effective information security management system and to conform to that system's requirements
- ✓ Designing and establishing an ISMS is difficult without management support and direction

Process Approach

- ✓ It is recommended that an organisation should adopt a process approach when it establishes, implements, operate, monitors, reviews, maintains, and improves the organisation's ISMS
- ✓ In the process approach, processes are any activities managed using management resources to transform inputs into outputs
- ✓ A process approach means identifying the processes within an organisation, grasping their interaction, and applying and managing a series of those processes as a system
- ✓ Adopting this process approach provides organisations with the benefit of effectively operating their ISMS through managing combinations of interaction among processes and with links to individual processes

theknowledgeacademy

Process Approach

Phase 1

Scope, Design and Build

Phase 2

First Cycle of Implementation, Operation, Monitoring, and Improvement

Phase 3

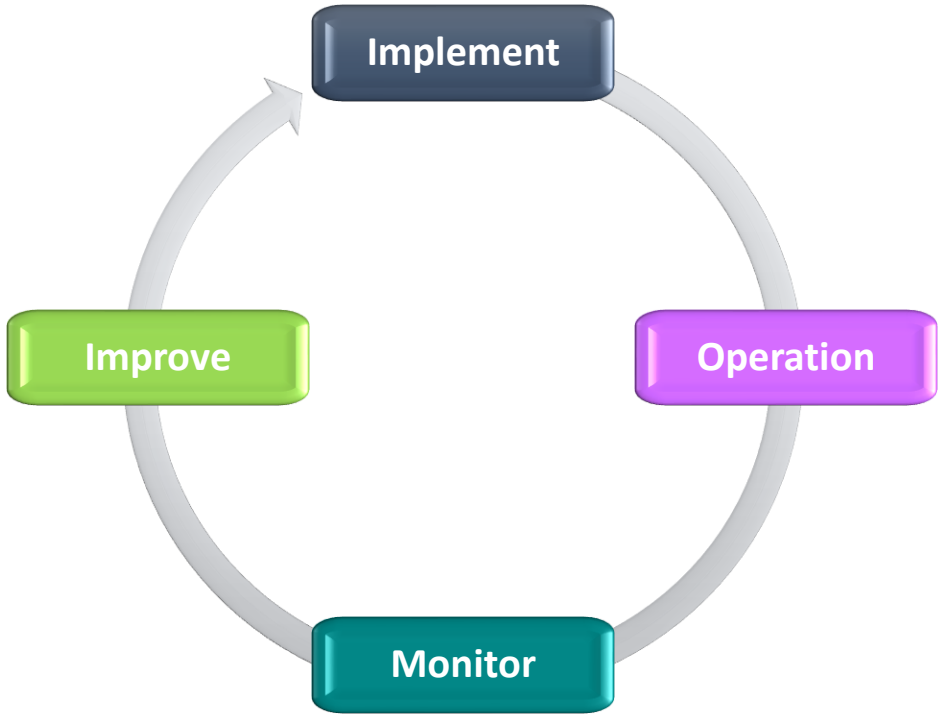
Operate, Monitor, and Improve

theknowledgeacademy

Process Approach

- ✓ Preparing the ISO 27001 Statement of Applicability
- ✓ Preparing the scope and programme of work for Phase 2 and providing input to further business cases

Phase 2 consists of four work streams: come il PDCA (Plan, Do, Check, Act)



theknowledgeacademy

Process Approach

Implement

- ✓ It is defined by the gap analysis and risk assessment activities from Phase 1
- ✓ Implementation will focus on integrating new and revised security processes and controls into an operational security environment, including training personnel, earmarked for operating these processes and controls
- ✓ An implementer role in this work stream would be conducting project management, facilitating integration, and providing training

theknowledgeacademy

Process Approach

Operation

- ✓ Operations include the management of information, security resources, security incident management, and training and awareness
- ✓ A lead implementer's role in this workstream will be providing support and hand-holding to staff responsible for running the ISMS

theknowledgeacademy

Process Approach

Monitor

- ✓ Monitoring includes assessing control KPIs, testing control effectiveness, internal auditing of the ISMS, and management review
- ✓ A lead implementer's role in this workstream would be performing effective reviews and internal audits of the ISMS (on the implementer's behalf)

theknowledgeacademy

Process Approach

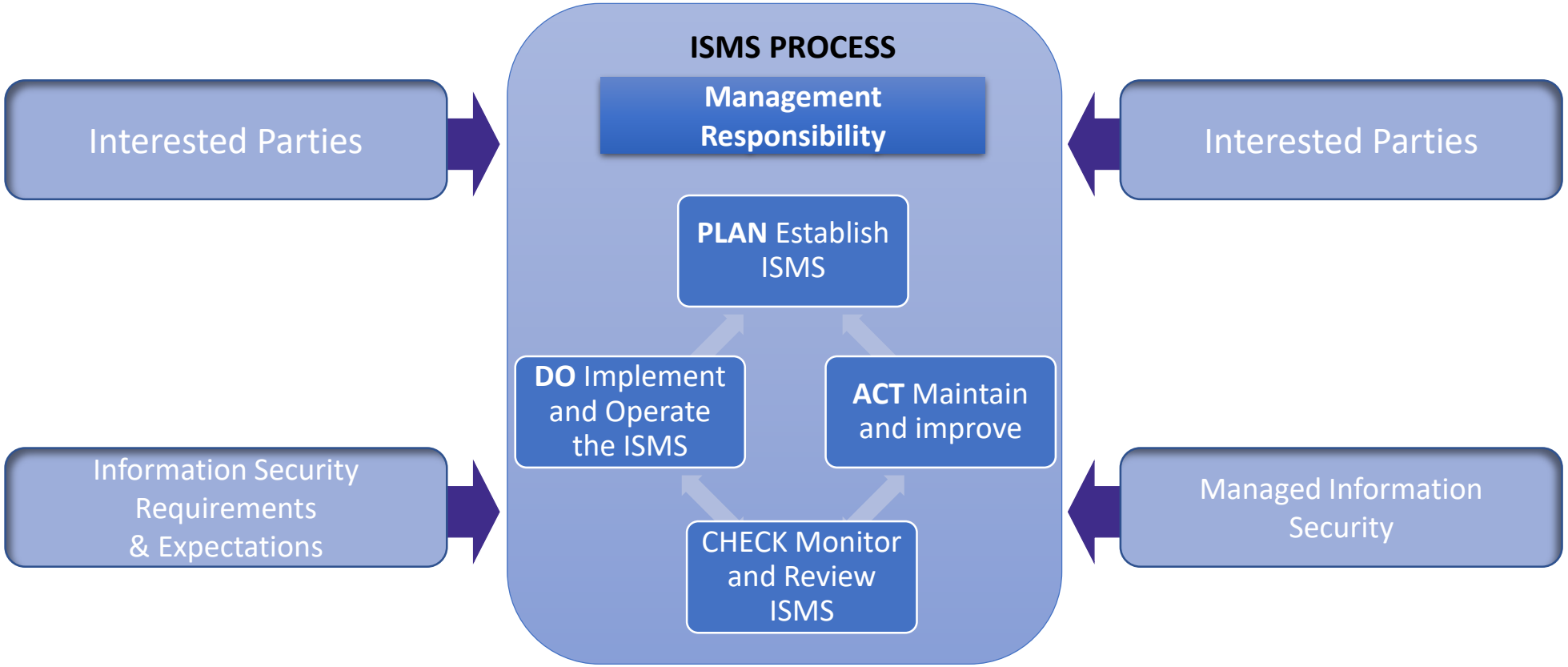
Improve

- ✓ Improve is about taking the outputs from the work stream to identify and determine improvements that can be made to the ISMS and its security controls
- ✓ A Lead Implementer's role would be to help design improvements and integrate these improvements back into the operational ISMS

theknowledgeacademy

Process Approach

Phase 3:



theknowledgeacademy

Process Approach

- ✓ When the integration of the ISMS processes and controls is complete, the ISMS becomes a BAU (Business as Usual) system
- ✓ The ISMS will now be fully operated by staff continuously monitoring and improving information security within the business
- ✓ It will support the PDCA cycle required for continuous improvement of the ISMS by providing resources and expertise for effectiveness reviews and performing the checks required for internal audits of the ISMS

Fundamentals

Introduction

- ✓ ISMS adoption is a strategic decision
- ✓ An organisation's ISMS design and implementation are influenced by its business and security objectives, security risks and control requirements, the processes employed, and the size and structure of the organisation. In other words, a simple situation will only require a simple ISMS
- ✓ In response to changing risks, the ISMS will evolve systematically in response to said changes
- ✓ Compliance with ISO27001 can be assessed and certified formally. A certified ISMS builds confidence in the organisation's approach to information security management among stakeholders

Fundamentals

Scope of ISMS

If commonplace controls are not applicable, they should be justified and documented in the Statement of Applicability (SOA)

In the event of this, the certification auditors will refer to the documentation

The PDCA Cycle

Scope of ISMS

Plan (Establishing the ISMS)	Do (Implementing and Workings of the ISMS)	Check (Monitoring and Review of the ISMS)	Act (Update and Improvement of the ISMS)
Establish the policy, the ISMS processes, procedures and objectives related to risk management and the improvement of information security, providing results in line with the objectives and global policies of the organisation	Implement and exploit the ISMS policy, processes, controls, and procedures	Assess the performance against the Objectives, policy and practical experience and report results for management to review	Undertake preventive and corrective actions based on outcomes of the ISMS internal audit and management review or other appropriate information for continually improving the said system

theknowledgeacademy

theknowledgeacademy

Module 14:

Interaction with ISO 27005

- ✓ What is ISO 27005 ?
- ✓ ISO 27001 VS ISO 27005
- ✓ Quantifying the Business Impact
- ✓ Impact Severity

What is ISO 27005 ?

- ✓ ISO 27005 is a set of guidelines for Information Security Risk Management
- ✓ Created by the International Organisation for Standardisation and the International Electrotechnical Commission in 2008, this guideline supports ISO 27001
- ✓ ISO 27005 can be implemented for an entire organisation or any discrete unit, from departments to services
- ✓ It applies to all organisations intending to manage risks that may impair their information security
- ✓ This standard describes the information security risk management process and its various facets

theknowledgeacademy

ISO 27001 VS ISO 27005

- ✓ Effective risk management is widely accepted as being the key to achieving certification and maintaining compliance with ISO 27001.

- ✓ **The underpinning facets of ISO 27005 correspond as they involve:**

  - Identifying the risk
  - Determining if the existing organisational measures are capable of dealing with the identified risk
  - Calculating whether the risk should be approached or avoided – potential rewards against potential loss
  - Reduce the level of its risk by adding precautions or control measures if deemed necessary

ISO 27001 VS ISO 27005

- ✓ ISO 27001 specifies that an ISMS should:

> "Align with the organisation's strategic risk management context", "establish criteria against which risk will be evaluated", and "identify a risk assessment methodology that is suited to the ISMS"

- ✓ However, despite specifically stating the requirement for a risk assessment, ISO 27001 does not describe the suitable methodology, hence why it is often complimented by ISO 27005, which is more precise regarding the terms and actions required

- ✓ It is recommended that these are used with each other as ISO 27005 offers guidelines for information security risk management, and 27001 is designed to assist the implementation of an ISMS-based approach

- ✓ In fact, before implementing or striving to meet the standards required within ISO 27005, managers and stakeholders should understand the concepts, models, and processes described in ISO 27001 and, to a certain extent ISO 27002 (Security Techniques)

Quantifying the Business Impact

- ✓ ISO 27005 allows organisations to modify and utilise their approach to risk assessment and management, as each situation varies, given that it is based on the objectives and aims of each organisation at a given time

- ✓ This flexibility is where ISO 27005 and ISO 27001 are preferred over alternative popular risk management systems, including Octave and NIST SP 800-30 – which are more rigid in their pursuit of effective management and business productivity engagement

- ✓ ISO 27005 supports the flexible needs of all versatile organisations due to taking the following approach when used parallel with ISO 27001:
    - Identify threats
    - Identify Existing Controls
    - Identify vulnerabilities and the impact of their exploitation

Quantifying the Business Impact

- Risk = (the probability of a threat exploiting a vulnerability) x (total impact of the vulnerability being exploited)

✓ In addition, it is fundamental that you quantify the probability and business impact of potential threats that the risk can become a reality. Consequently, you should have a specialised focus on the following:

- The frequency with which the risk could take advantage of the vulnerability
- Extent and cost of physical and financial damage that the risk could cause
- Value is lost if confidential information is leaked – from a data protection perspective, this could be substantial given the implementation of the GDPR
- Cost of recovering from a virus attack (financial, physical, and reputational)

Impact Severity

✓ The impact severity is calculated as shown below:

Impact severity = Asset value x Threat severity x Vulnerability severity (*)

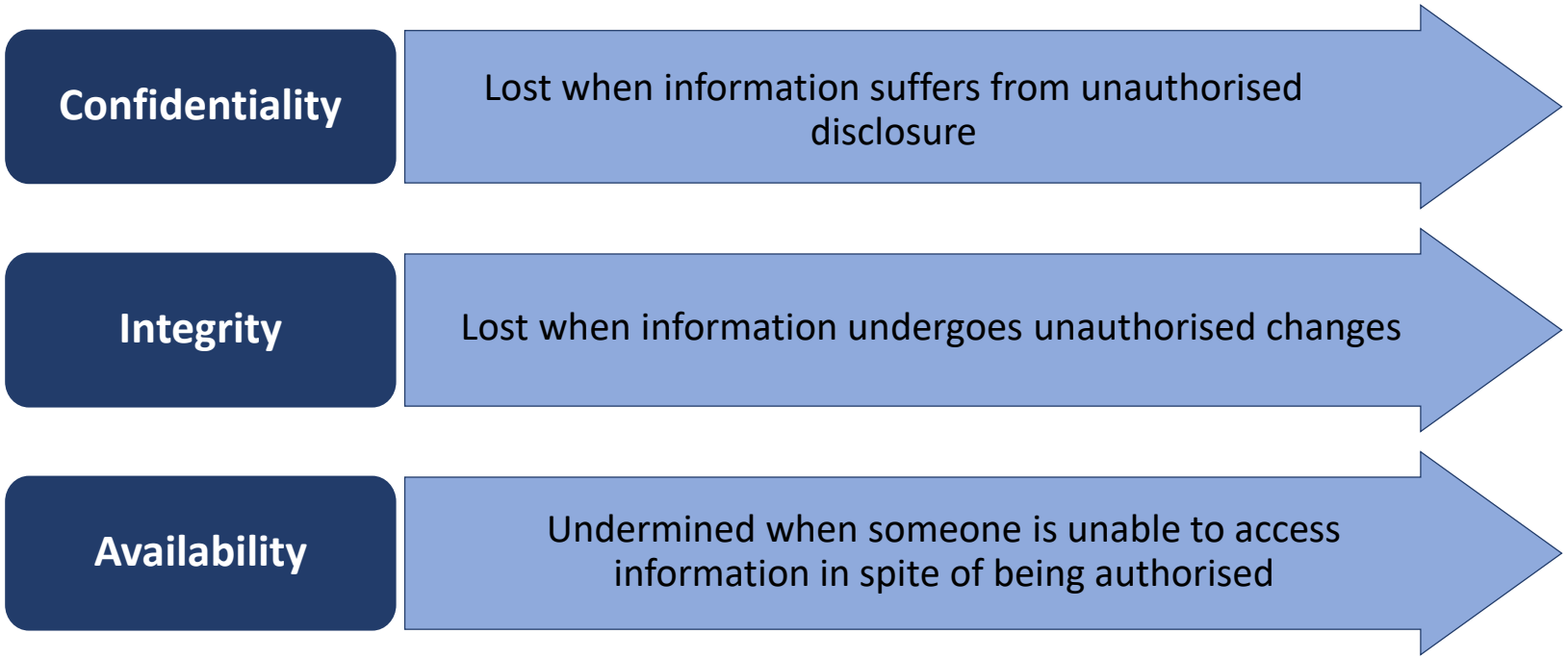
In this instance, the aim is to determine the impact that the suspected risk will exploit another vulnerability within the organisation

Analysis, based on numerous factors, including architecture, system security, strength, and known vulnerabilities, are likely to sway the decisions of risk managers and senior stakeholders on whether to take the risk in order to pursue greater rewards or whether to take mitigation steps

theknowledgeacademy

Impact Severity

ISO 27001 is concerned with negative impacts, described as loss or degradation of the asset's confidentiality, integrity, or availability



theknowledgeacademy

theknowledgeacademy

Module 15:

Roles and Responsibilities of a Lead Implementer

- ✓ Roles and Responsibilities
- ✓ Case Study: ABC's ISO 27001

Roles and Responsibilities

- ✓ The primary responsibility of the Lead Implementer is to lead successful communication of campaign implementations, oversee budget requirements, and ensure deadlines are met
- ✓ The Lead Implementer coordinates and prioritises project tasks, manage timelines, maintains project plans, and communicates status to Engagement Managers, Senior Management and Clients as needed
- ✓ The Lead Implementer ensures the project is implemented within contractual obligations and regulatory requirements is another responsibility

theknowledgeacademy

Roles and Responsibilities

- ✓ The Lead Implementer will be responsible for managing multiple client projects simultaneously
- ✓ They will also be responsible for participating in internal projects as needed
- ✓ This role is responsible for scope management, change management, and estimating the impacts of scope change
- ✓ E.g. Timeline and cost, as well as managing project resources

theknowledgeacademy

Case Study: ABC's ISO 27001

Background

- ✓ ***Company Overview:*** ABC is a software development company specialising in creating custom software solutions for businesses.
- ✓ ***Pre-ISO 27001 Situation:*** The company faced challenges in protecting intellectual property and customer data, and experienced inefficiencies in handling information security.

Objectives for Implementing ISO 27001

- ✓ ***Enhance Data Security****:* Strengthen the protection of sensitive company and customer data.
- ✓ ***Regulatory Compliance:*** Ensure compliance with global data protection regulations.
- ✓ ***Market Competitiveness****:* Improve market positioning by demonstrating a commitment to information security.

Case Study: ABC's ISO 27001

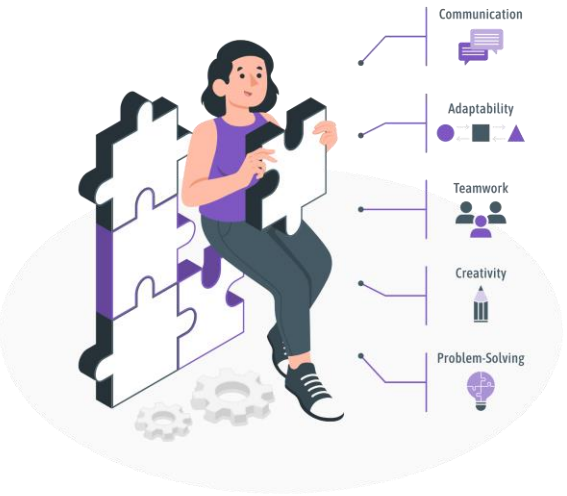
Implementation Process

- ✓ ***Initial Assessment:*** Conducting a thorough review of existing security measures and identifying gaps.
- ✓ ***Risk Management:*** Implementing a risk management process to identify, analyse, and address information security risks.
- ✓ ***Developing Policies and Procedures:*** Creating comprehensive policies and procedures to govern information security.
- ✓ ***Staff Training and Awareness:*** Ensuring all employees are trained on the new policies and understand their role in maintaining security.
- ✓ ***Technical and Physical Controls:*** Implementing appropriate technical and physical measures to secure information.
- ✓ ***Continuous Monitoring and Review:*** Establishing a process for ongoing monitoring, review, and continuous improvement of the ISMS.

Case Study: ABC's ISO 27001

Challenges and Solutions

- ✓ ***Resource Allocation:*** Balancing the need for robust security with budget constraints. Solved by prioritising key areas of risk and implementing scalable solutions.
- ✓ ***Change Management:*** Overcoming resistance to change within the organisation. Addressed through comprehensive staff training and demonstrating the benefits of the new system.
- ✓ ***Integration with Existing Systems:*** Ensuring the new security protocols are seamlessly integrated with existing IT systems. Achieved through careful planning and phased implementation.



Case Study: ABC's ISO 27001

Results and Benefits

- ✓ ***Increased Security:*** Significant reduction in security incidents and data breaches.
- ✓ ***Compliance with Regulations:*** Successfully meeting international data protection standards.
- ✓ ***Enhanced Reputation:*** Gaining customer trust and opening new business opportunities due to recognised commitment to data security.

theknowledgeacademy

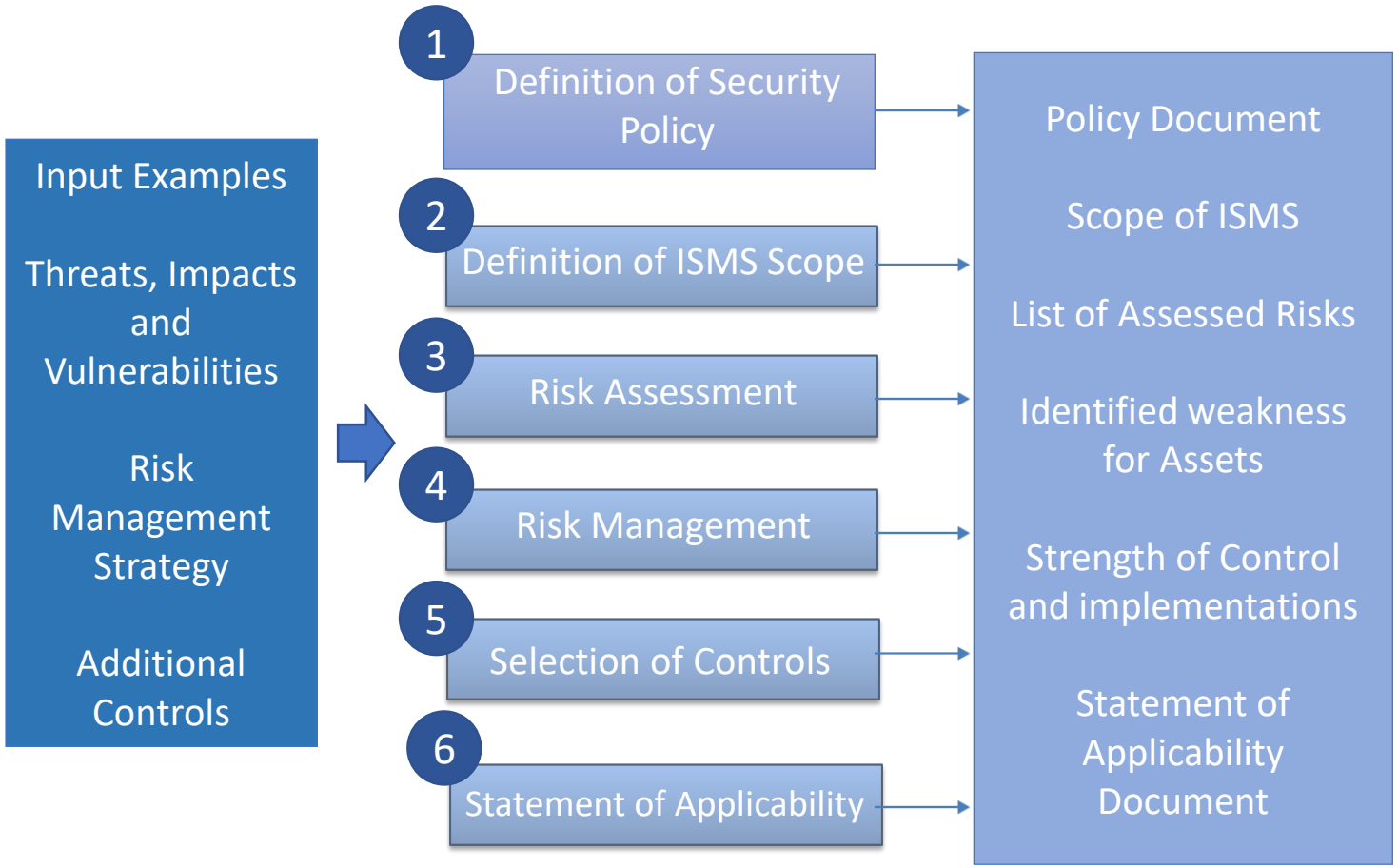
Module 16:

Launch and Implement an ISMS in an Organisation

- ✓ Apply the Frameworks
- ✓ Procedures and Controls
- ✓ Implementing the Controls
- ✓ Training and Awareness Programme
- ✓ Management’s Role
- ✓ Responsibilities of Employees

Apply the Frameworks

ISMS Frameworks



theknowledgeacademy

Procedures and Controls

Procedures

In the mandatory section of ISO 27001 documented procedures are required:

Control of Documents

Control of Records

Internal ISMS Audits

Corrective Actions

Preventive Actions

Risk Assessment Procedure

theknowledgeacademy

Procedures and Controls

To support selected controls, documented procedures are required

✓ In security policy operating procedures are identified

Procedures Required by Organisation

- Disciplinary Process
- Handling & Storage of Information
- Review of User Access Rights
- Monitoring of Use of Information System
- Acceptable Use of Assets
- Acceptance Criteria for New Info System

theknowledgeacademy

Procedures and Controls

Procedures Required by Organisation

- Software Change Control
- Incident Management including Reporting
- Control against Malicious Software
- Information Labelling & Handling
- User Reg. & De-reg
- Control of Operational Software
- Roles and Responsibilities
- Access Control Policy
- Key Management System
- Identification of Appl. Legislation
- Migration of Software
- Allocation of Passwords

theknowledgeacademy

Procedures and Controls

Controls

- ✓ The ISO 27001:2022 Annex controls have been updated to address current security challenges, while the core ISMS management processes remain the same
- ✓ The controls have been restructured and consolidated into four categories: Organisational, People, Physical, and Technological
- ✓ Each control now includes a set of suggested attributes, which align with common industry language and international standards
- ✓ These attributes can be used to quickly select appropriate controls based on risk assessments and the Statement of Applicability (SoA)

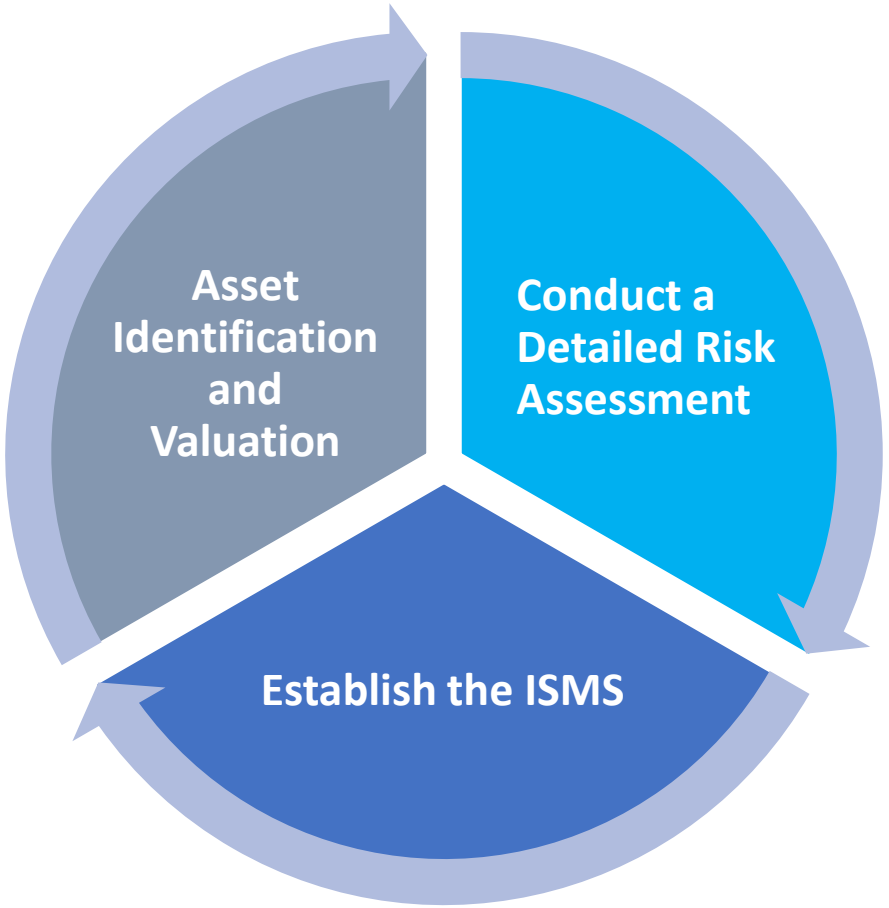
Procedures and Controls

There are following controls:

theknowledgeacademy

Implementing the Controls

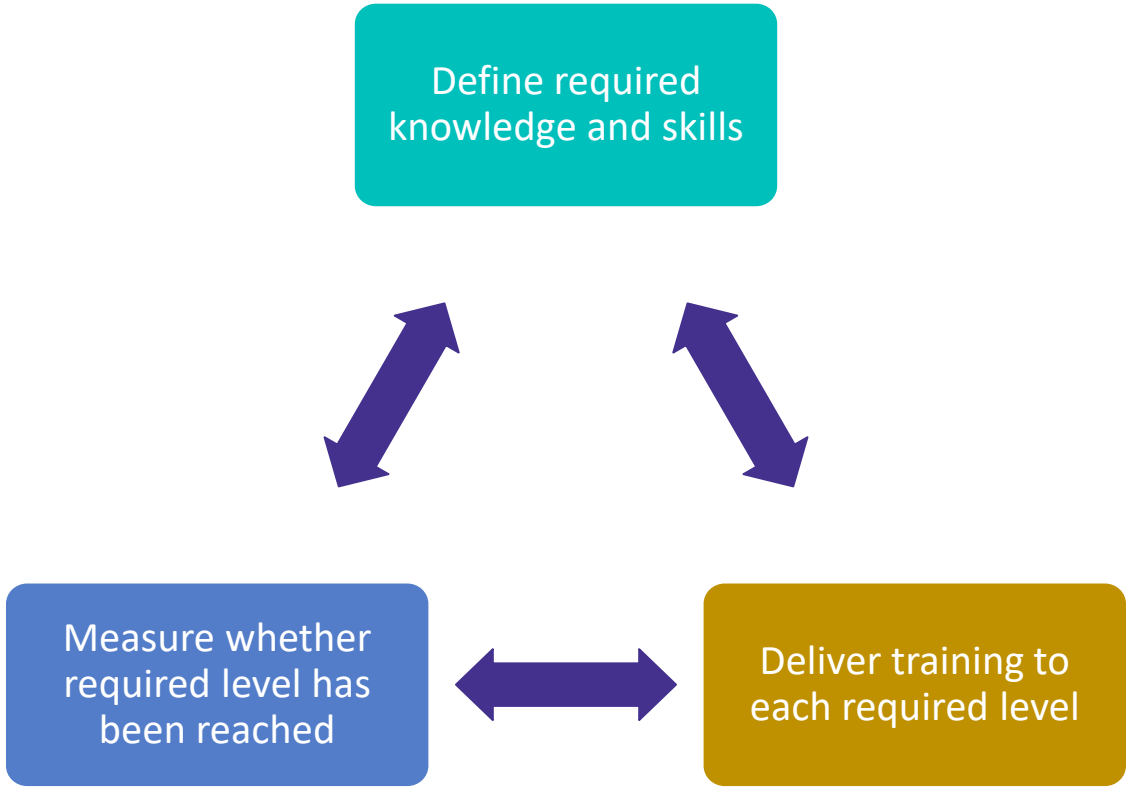
The following are the steps to implement ISMS at your organisation:



theknowledgeacademy

Training and Awareness Programme

ISO 27001 requires training in a systematic manner to perform as follows:



theknowledgeacademy

Training and Awareness Programme

Step 1

- ✓ Define which kind of knowledge and skills are required for a particular person who has a role in an information security management system (ISMS), or business continuity management system (BCMS)
- ✓ LIs need to go through every ISMS or BCMS document and see what knowledge and skills are required of every responsible person mentioned in the document

Step 2

- ✓ Deliver training to reach the desired level of knowledge and skills

Step 3

- ✓ Measure whether each individual has achieved the desired level of knowledge and skills through testing, interviews, and so on

Training and Awareness Programme

Methods of Awareness Raising

Include employees in documentation development

Before publishing the documents, ask employees to give their inputs

Presentations

- ✓ Organise shorter meetings, during which Lis can explain what new policies and procedures are being published
- ✓ Ask your employees for opinions about them and clarify any misunderstandings

theknowledgeacademy

Training and Awareness Programme

Methods of Awareness Raising

Articles on intranet or newsletter

Initiate and participate in discussions and questions arising from information security/ business continuity

Discussions through internal forums

- ✓ Create short online courses that explain the significance of these topics and can be training aids for employees

theknowledgeacademy

Training and Awareness Programme

Methods of Awareness Raising

- Videos are a very powerful presentation method, as we can distribute them via email, through the intranet, etc
- Occasional messages via email or via intranet can be used not only to distribute videos, but also to send relevant news and tips for business continuity
- Meetings can be organised throughout the company

theknowledgeacademy

Management's Role

- ✓ The responsibility of management is to oversee the maintenance, development, and implementation of the Information Security Management System
- ✓ It includes defining the organisation's information security objectives, allocating money to be spent on information security, and ensuring the enforcement and compliance of the implementation
- ✓ For the organisation, management has particular goals

theknowledgeacademy

Training and Awareness Programme

Management should also make sure security controls are integrated throughout the organisation by performing the following:

- Make sure the security process is administered through organisational practices and policies that are continuously applied
- Require that information with identical sensitivity and criticality characteristics be continuously protected irrespective of where it resides in the organisation
- Implement compliance with the security program across the organisation in a consistent and balanced manner
- With physical security coordinate information security

theknowledgeacademy

Responsibilities of Employees

- ✓ The knowledge and capabilities of persons assigned to this role are essential for meeting the purposes of the organisation concerning data protection.
- ✓ They must work according to the policies applicable, processes, and procedures that constitute ISMS.
- ✓ **The essential policies applicable to this role involve:**

theknowledgeacademy

theknowledgeacademy

Congratulations

The World's Largest Global Training Provider

theknowledgeacademy.com

info@theknowledgeacademy.com

/The.Knowledge.Academy.Ltd

/TKA_Training

/the-knowledge-academy

/TheKnowledgeAcademy