

*the*knowledgeacademy

ISO 27001: 2022

Lead Auditor



About The Knowledge Academy

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

Course Syllabus

- **Module 1:** Introduction to ISO 27001
- **Module 2:** Information Security
- **Module 3:** ISMS and the ISO 27001 Standards Family
- **Module 4:** Interaction with ISO 27005
- **Module 5:** Context of the Organisation
- **Module 6:** Introduction to Auditing
- **Module 7:** Leadership



Course Syllabus

- **Module 8:** Performing ISO 27001 Audits
- **Module 9:** Internal Auditor
- **Module 10:** Risk Management
- **Module 11:** Risk Assessment and the Statement of Applicability (SOA)
- **Module 12:** Roles and Responsibilities of a Lead Implementer
- **Module 13:** Planning



Course Syllabus

- **Module 14:** Support
- **Module 15:** Operation
- **Module 16:** Launch and Implement an ISMS in an Organisation
- **Module 17:** Introduction to ISO 27001 Lead Auditor
- **Module 18:** Tasks of an Auditor
- **Module 19:** Performance Evaluation
- **Module 20:** Improvement



Module 1: Introduction to ISO 27001



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

(Continued)

- ❑ 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.

Introduction

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.

Scope

- ❑ This document describes the requirements to establish, execute, maintain, and continuously enhance an information security management system in the organisation's context.
- ❑ This document also contains requirements for assessing and treating information security risks specific to the organisation's requirements.
- ❑ In this document, the requirements are generic and intended to apply to all organisations, regardless of kind, size, or nature.



Terms and Definitions

1. **Access Control:** This means ensuring access to assets is authorised and limited based on security and business conditions.
2. **Attack:** An attempt to steal, damage, disable, expose, destroy, gain unauthorised access to, or use an asset.
3. **Audit:** Systematic, independent, and documented procedure for gathering audit evidence and assessing it objectively to ascertain the scope to which the audit criteria are met.



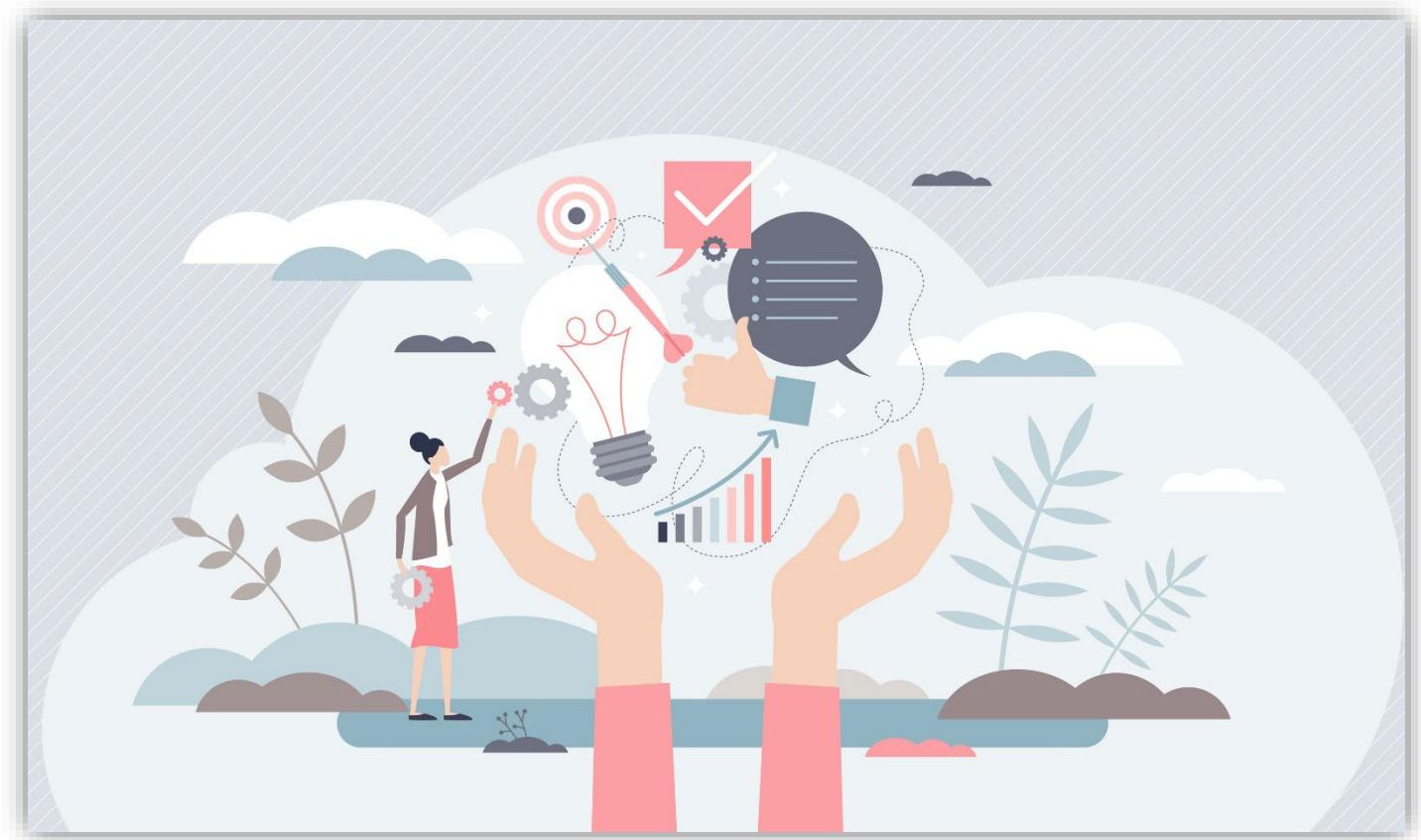
Terms and Definitions



4. ***Audit Scope:*** Extent and limitations of an audit.
5. ***Authentication:*** Condition of assurance that a claimed characteristic of an entity is true.
6. ***Authenticity:*** A thing that an entity actually is what it says it is.

Terms and Definitions

7. **Availability:** Being accessible and useable at any time by an authorised entity.
8. **Base Measure:** Measurement is described in terms of an attribute and the approach used to calculate it.
9. **Competence:** The capability of applying skills and knowledge to attain desired outcomes.



Terms and Definitions



Confidentiality

10. Confidentiality: Information should not be made available or revealed to unapproved people, entities, or processes.

11. Conformity: Fulfilment of a condition.

12. Consequence: The result of an event affecting goals.

Terms and Definitions

13. *Continual Improvement:* Regular activity to improve performance.

14. *Control:* Measure that is altering risk.

15. *Control Objective:* A statement explaining what is to be attained while executing controls.



Terms and Definitions

16. *Correction:* Action to eradicate a detected nonconformity.

17. *Corrective Action:* Action to eradicate a nonconformity's cause and stop it from happening again.

18. *Derived Measure:* A measure defined as the function of two or more base measure values.



Terms and Definitions

- 19. Documented Information:** The information must be controlled and kept maintained by an organisation and the media it is stored on.
- 20. Effectiveness:** The extent to which planned activities are carried out and outcomes are obtained.
- 21. Event:** The occurrence or modification of a specific set of circumstances.



Terms and Definitions



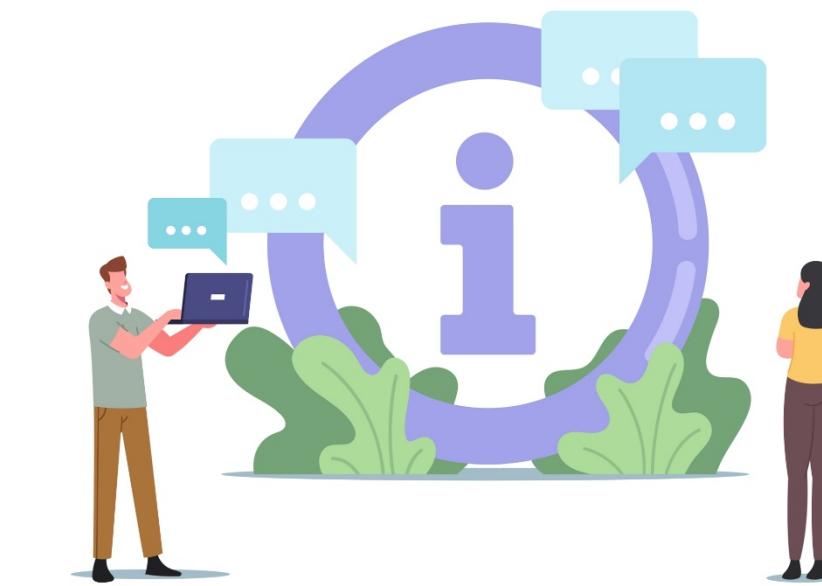
22. ***External Context:*** The external environment in which the organisation aims to accomplish its goals.
23. ***Governance of Information Security:*** System for managing and directing an organisation's information security activities.
24. ***Governing Body:*** Individuals or groups of persons responsible for the organisation's performance and conformity.

Terms and Definitions

25. *Indicator:* Measure that gives an evaluation or estimation.

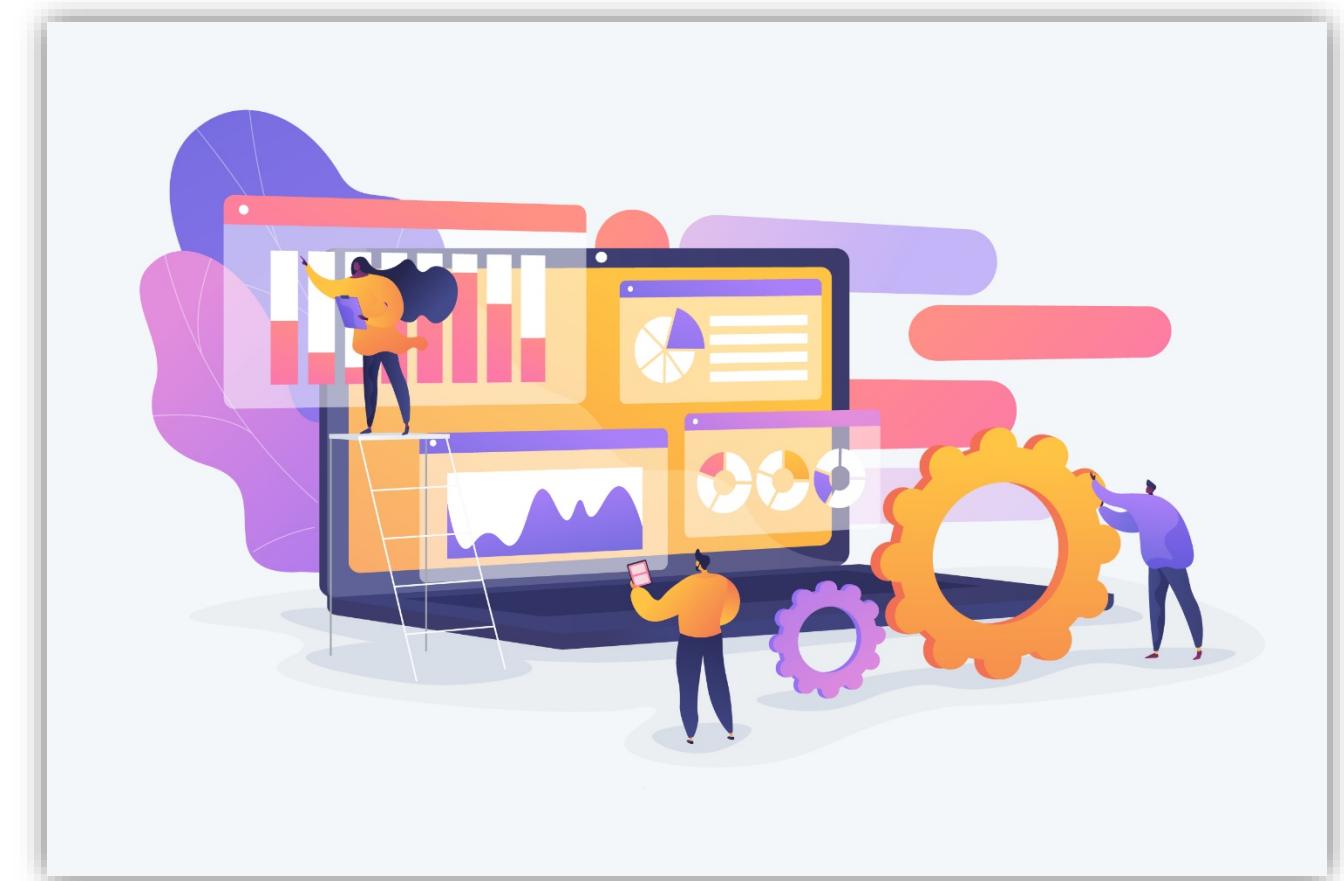
26. *Information Need:* Insight is required to manage goals, objectives, hazards and issues.

27. *Information Processing Facilities:* Any system for processing information, infrastructure or service, or the physical location accommodation it.



Terms and Definitions

- 28. *Information Security:*** Information availability, integrity, and confidentiality are maintained.
- 29. *Information Security Continuity:*** Procedures and processes for assuring continued information security operations.
- 30. *Information Security Event:*** A system, service, or network state identified as possibly indicating a violation of information security policy, a failure of controls, or a previously unidentified circumstance that may be security appropriate.

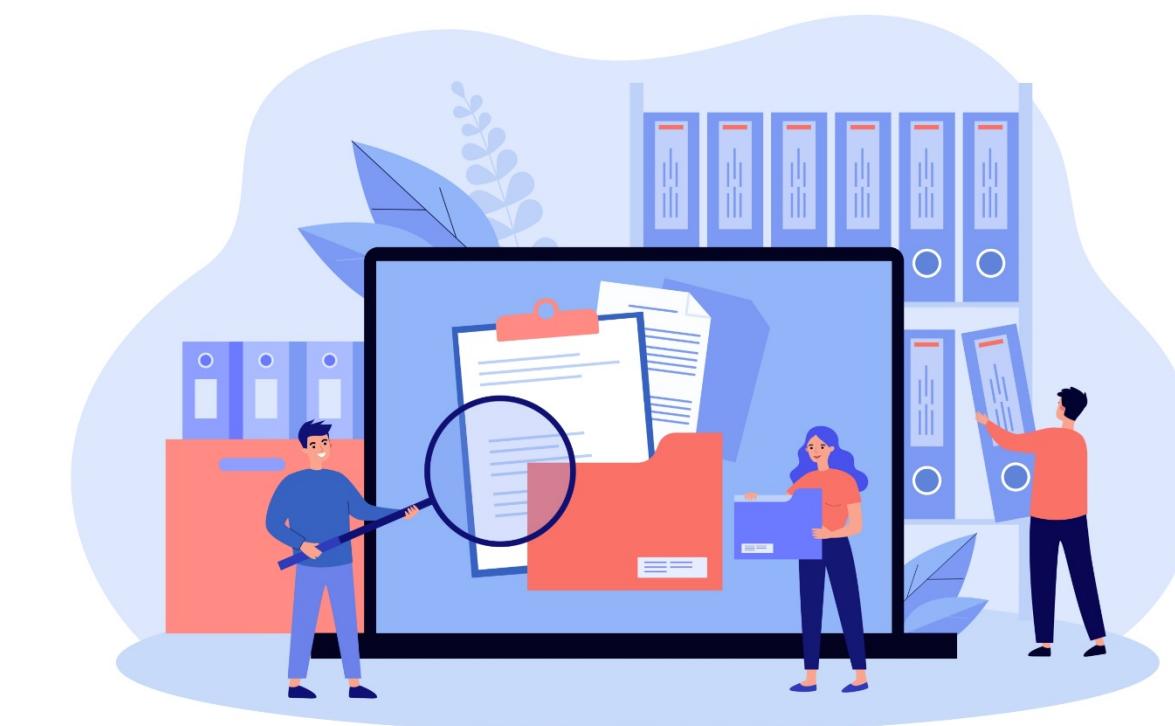


Terms and Definitions

- 31. *Information Security Incident:*** A single incident or a string of unexpected or unwanted information security occurrences has a significant chance of compromising business operations and risking information security.
- 32. *Information Security Incident Management:*** A collection of procedures for discovering, documenting, evaluating, responding to, managing, and learning from information security incidents.
- 33. *Information Security Management System (ISMS) Professional:*** A person who creates puts into place, keeps up, and constantly enhances one or more Information Security Management System processes.

Terms and Definitions

- 34. *Information Sharing Community:*** A collection of organisations that consent to share information.
- 35. *Information System:*** A group of applications, services, IT resources, or other elements that handle information.
- 36. *Integrity:*** Property of completeness and accuracy.



Terms and Definitions



37. Interested Party (Preferred Term)

Stakeholder (Admitted Term): A person or organisation that has the power to influence is affected by or perceives choice or action as influencing its action.

38. Internal Context: Internal environment in which the organisation strives to attain its goals.

39. Level of Risk: The magnitude of a risk is described in terms of the combination of outcomes and their probability.

Terms and Definitions

40. Likelihood: Possibility of something happening.

41. Management System: Group of interconnected or cooperating organisational components that work together to set policies, goals, and procedures for achieving those goals.

42. Measure: A variable receives a value after being measured.



Terms and Definitions

43. Measurement: This is a process for determining a value.

44. Measurement Function: Calculation or algorithm performed to carry out two or more base measures.

45. Measurement Method: When quantifying an attribute with regard to a specified scale, a logical set of operations is used.



Terms and Definitions

46. *Monitoring*: Determining a system, a process, or an activity's status.

47. *Nonconformity*: Non-fulfilment of a condition.

48. *Non-repudiation*: The capability of confirming the occurrence of a claimed event or activity and its originating entities.



Terms and Definitions



49. *Objective*: Outcome to be attained.

50. *Organisation*: An individual or group of people has its functions with accountabilities, relationships and authorities to attain its purposes.

51. *Outsource*: Make a plan where an outside organisation carries out a portion of a function or process.

Terms and Definitions

52. Performance: Measurable outcome.

53. Policy: The formal declarations of an organisation's top management regarding its intentions and direction.

54. Process: A group of interacting or interrelated activities that convert inputs into outputs.



Terms and Definitions

- 55. *Reliability*:** Property of constant intended behaviour and outcomes.
- 56. *Requirement*:** Requirement or anticipation that is stated is usually indicated or mandatory.
- 57. *Residual Risk*:** It refers to the remaining risk after risk treatment.



Terms and Definitions



58. *Review*: Undertake the activity to determine the suitability, sufficiency and significance of the subject matter to accomplish established purposes.

59. *Review Object*: Specific thing being examined.

60. *Review Objective*: A statement explaining what is to be attained as a consequence of a review.

Terms and Definitions

- 61. *Risk*:** Impact of uncertainty on purposes.
- 62. *Risk Acceptance*:** An informed decision to take a certain risk.
- 63. *Risk Analysis*:** Process for understanding risk's nature and determining the level of risk.



Terms and Definitions

64. Risk Assessment: It is a process of identifying, analysing, and evaluating risks overall.

65. Risk Communication and Consultation: An organisation uses a group of ongoing and iterative procedures to give, receive, or discuss information with stakeholders and to have a conversation about risk management.

66. Risk Criteria: Terms of reference against which the consequence of risk is estimated.



Terms and Definitions

- 67. *Risk Evaluation:*** Process of determining whether risk and its magnitude are acceptable or manageable by comparing the outcomes of risk analysis with risk criteria.
- 68. *Risk Identification:*** Process of discovering, identifying and explaining risks.
- 69. *Risk Management:*** Collaborative activities to lead and manage an organisation concerning risk.



Terms and Definitions



- 70. *Risk Management Process:*** Applying management processes, policies, and techniques systematically to consulting, communicating, establishing the context, and identifying, analysing, assessing, treating, and monitoring risk.
- 71. *Risk Owner:*** An individual or entity with the responsibility and authority to handle risk.
- 72. *Risk Treatment:*** Process to alter risk.

Terms and Definitions

- 73. *Security Implementation Standard:*** It refers to the document specifying authorised methods for realising security.
- 74. *Threat:*** A potential cause of an undesirable incident that could affect a system or organisation.
- 75. *Top Management:*** An individual or group of people who is accountable for an organisation's highest levels of direction and control.
- 76. *Trusted Information Communication Entity:*** Information sharing within a community is supported by an autonomous organisation.
- 77. *Vulnerability:*** Liability of control or an asset that can be manipulated by one or more threats.

Module 2: Information Security



What is Information 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.

What is Information Security?

(Continued)

- Multi-tier Classification System was created during the First World War with the sensitivity of the information in mind. The formal alignment of the classification system was completed with the outbreak of the Second World War.
- Alan Turing was responsible for successfully decrypting the Enigma Machine, which the Germans used to encrypt warfare data.

Triad of Information Security

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



Confidentiality



Integrity



Availability

Triad of Information Security

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.



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.



Triad of Information Security

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.



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.

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.



Need of Information Security

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.



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.



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.



Threats to Information Security

(Continued)

- **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.



Threats to Information Security

(Continued)

- **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:



Infection Methods

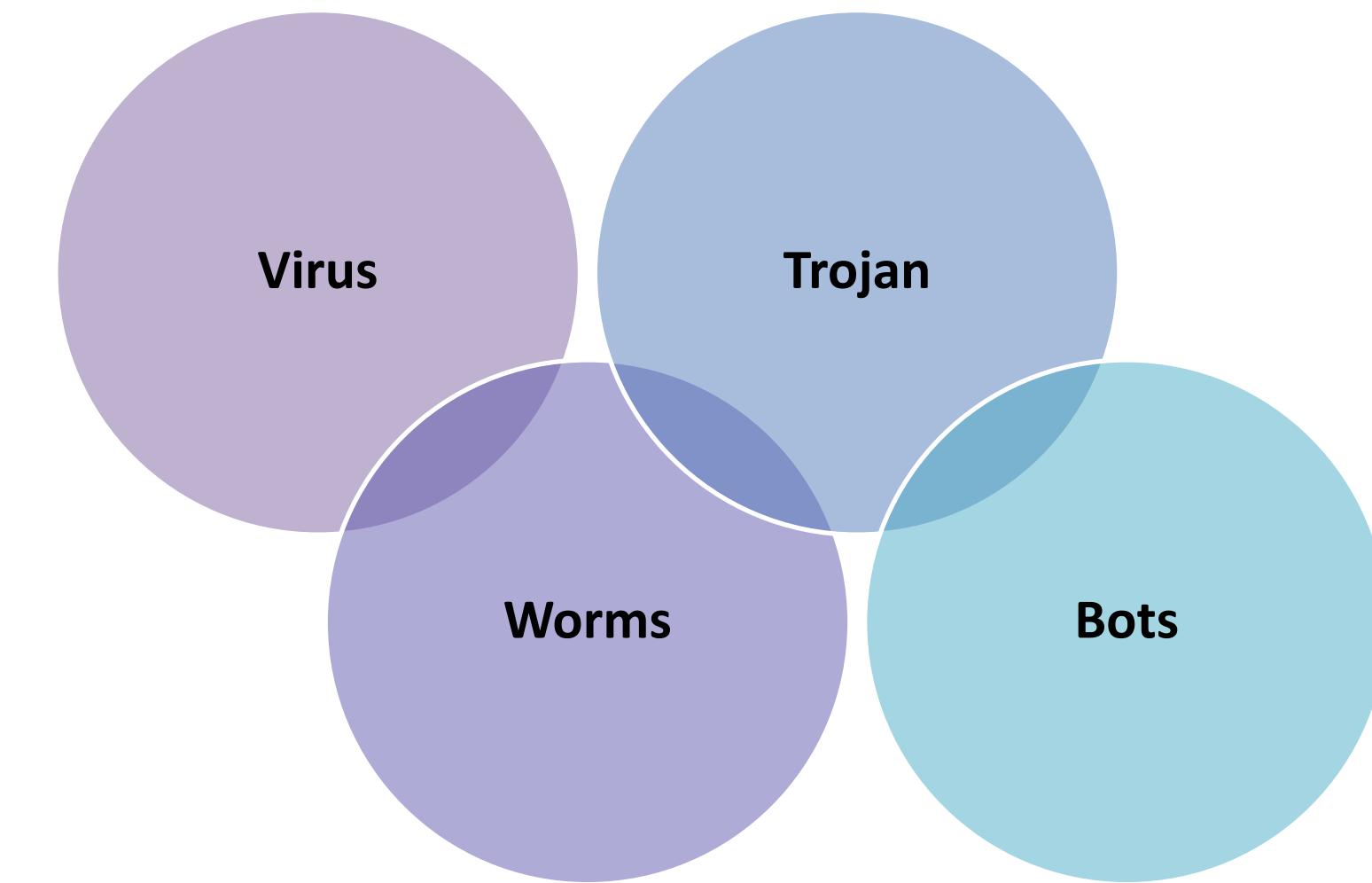


Malware Actions

Threats to Information Security

(Continued)

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



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.

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.

Threats to Information Security

(Continued)

- **Malware based on its actions:**

Adware

Spyware

Ransomware

Scareware

Rootkits

Zombies

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.

Threats to Information Security

2. 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.

3. 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.

Threats to Information Security

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.

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.

Active and Passive Attacks

Active Attacks

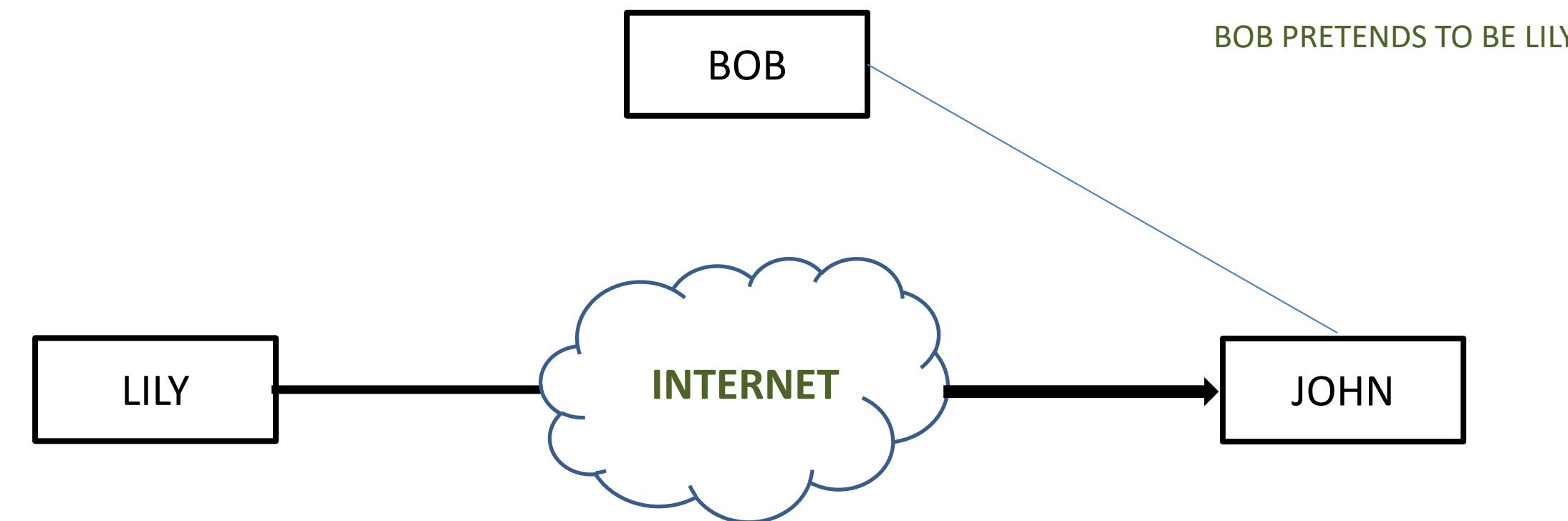
- An active attack tries to change system resources or interfere with their operability. Active attacks include some data stream modification or false statement creation.
- Active attacks can take the following forms:



Active and Passive Attacks

1. Masquerade

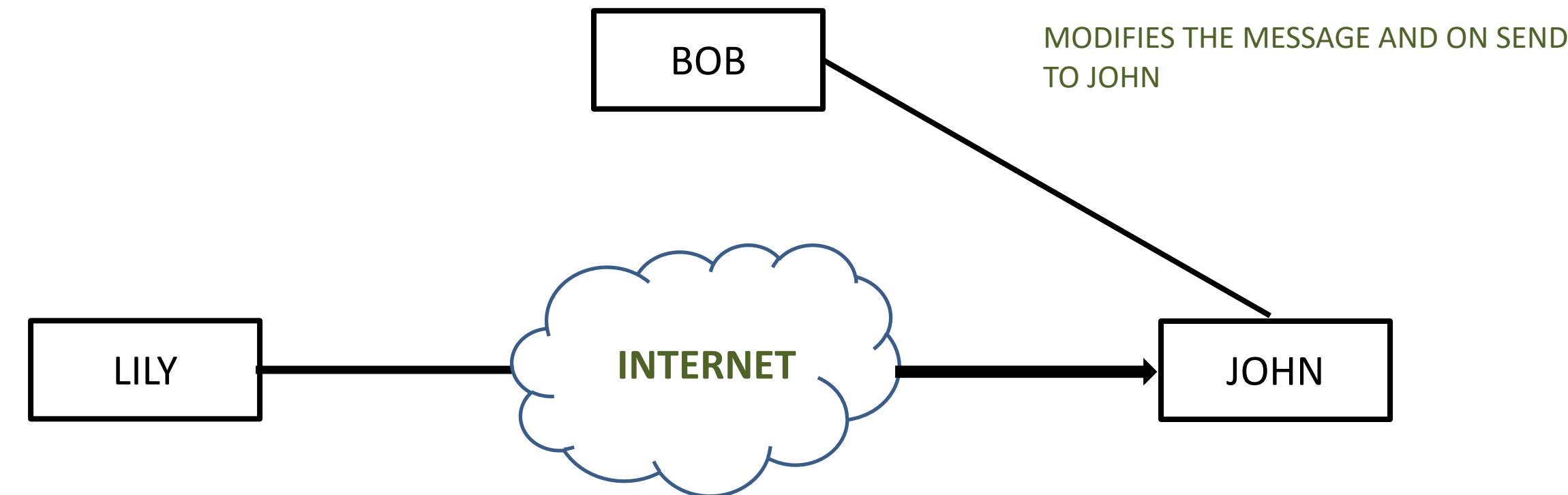
- When one entity impersonates another, a masquerade attack happens. One of the other types of active attacks is involved in a masquerade attack. If an approval process is not always completely protected, it may become extremely vulnerable to a masquerading attack.
- Masquerade attacks can be carried out using stolen passwords and logins, by finding gaps in programs, or by locating a way through the authentication process.



Active and Passive Attacks

2. Modification of Messages

- In essence, it indicates that unauthorised parties not only access data but also spoof it by initiating denial-of-service attacks, such as modifying transmitted data packets or flooding the network with false data.
- An assault on authentication is manufacturing. A message that initially said, "Allow JOHN to read confidential file X," for instance, is changed to read, "Allow Smith to read confidential file X."



Active and Passive Attacks

3. Repudiation

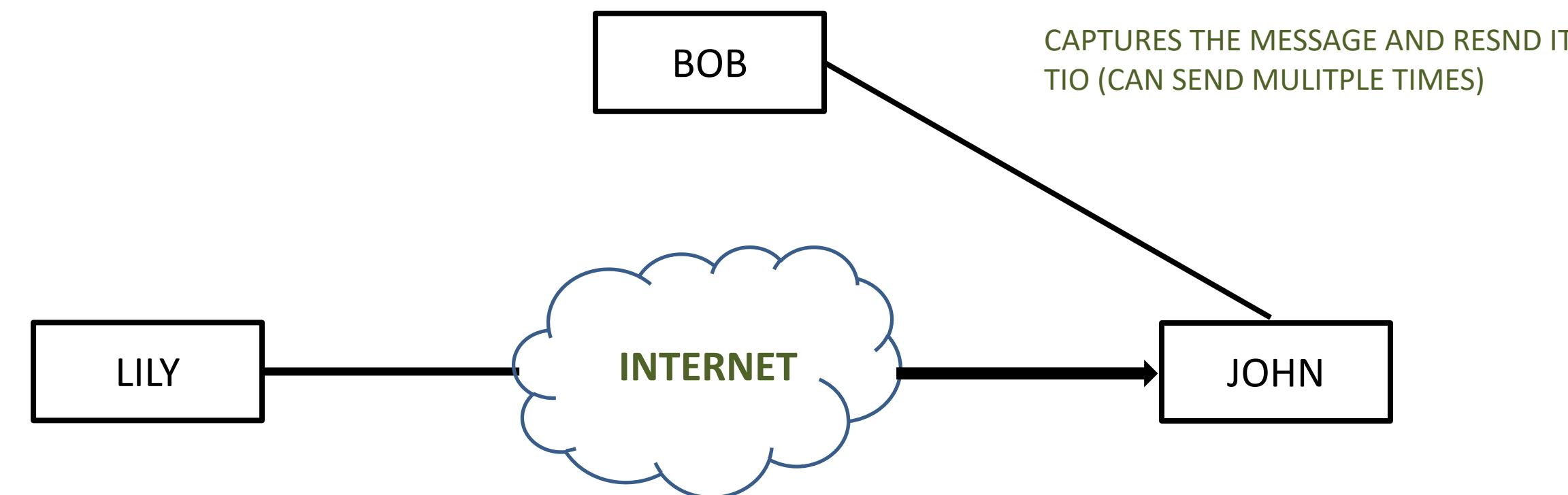
- This attack happens when the login control has been tampered with or the network is not completely secure.
- With this attack, the author's information can be altered by malicious user actions to save misleading information in log files, up to the general manipulation of data on behalf of others, equivalent to the spoofing of email messages.



Active and Passive Attacks

4. Replay

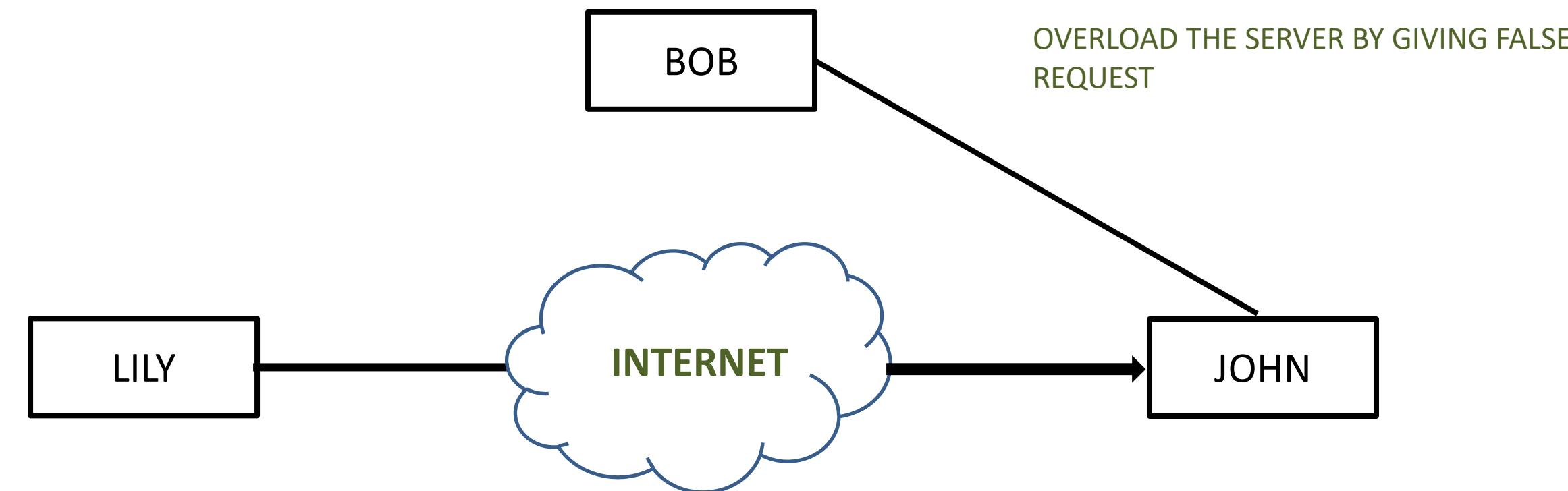
- This attack happens when the login control has been tampered with or the network is not entirely secure.
- With this attack, the author's information can be altered by malicious user actions to save misleading information in log files, up to the general manipulation of data on behalf of others, equivalent to the spoofing of email messages.



Active and Passive Attacks

5. Denial of Service

- It hinders the regular use of communication facilities. There may be a specific target for this attack.
- An entity might, for instance, suppress all messages sent to a specific location. Another example of service denial is when an entire network is disrupted through network disablement or message overload that lowers performance.



Case Study: Ensuring Information Security

- YZ has developed a world-class organisation since its founding in 1991 by comparing its client processes to exacting international norms in the fields of people management and process architecture.
- Additionally, YZ has continuously upgraded its procedures to raise the quality of its goods and services to meet its customers' demands.



Active and Passive Attacks

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.
- The opponent's objective is to receive the provided information. The following are examples of passive attacks:
 - Message content release
 - Traffic analysis

Case Study: Ensuring Information Security



Building the Information Security Management System

- Information security management systems are implemented using a management systems approach, as described in ISO/IEC 27001:2005, Information technology - Security Techniques - Information Security Management Systems - Requirements.
- It offers a framework for putting into place an Information Security Management System (ISMS) that can protect data assets while making the procedure simpler to manage, evaluate, and enhance.

Case Study: Ensuring Information Security

(Continued)

- Key clients required and expected YZ to demonstrate that it had a strong ISMS in place.
- Still, the company's primary motivation for pursuing ISO 27001 registration was to ensure that all risks and vulnerabilities had been adequately addressed.
- Information security controls are present in the majority of organisations. On the other hand, without an ISMS, the controls are frequently disjointed and disorganised as a matter of tradition or as ad hoc responses to particular problems.

Case Study: Ensuring Information Security

(Continued)

- Before implementing ISO 27001, YZ's security measures exclusively addressed certain facets of IT or data security, leaving non-IT information assets like paper documents and confidential information less safeguarded.
- YZ successfully implemented approximately 132 out of the 133 controls mandated by ISO 27001.
- This was done after conducting a gap analysis to help identify, manage, and mitigate the spectrum of hazardous information that is frequently exposed.

Case Study: Ensuring Information Security

(Continued)

- People are certain that both their IT and non-IT assets have been adequately cared for with the implementation of the ISMS and ISO 27001 certification by XY.
- "Business continuity planning and physical security, for instance, have been strengthened with the implementation of the ISMS".



Module 3: ISMS and the ISO 27001 Standards Family



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.
- ✓ Areas of focus are:
 - Business processes and assets.
 - Reducing risk to data assets and related systems.

What is an ISMS?

(Continued)

- ✓ 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:



What is an ISMS?

Role and Importance of ISMS

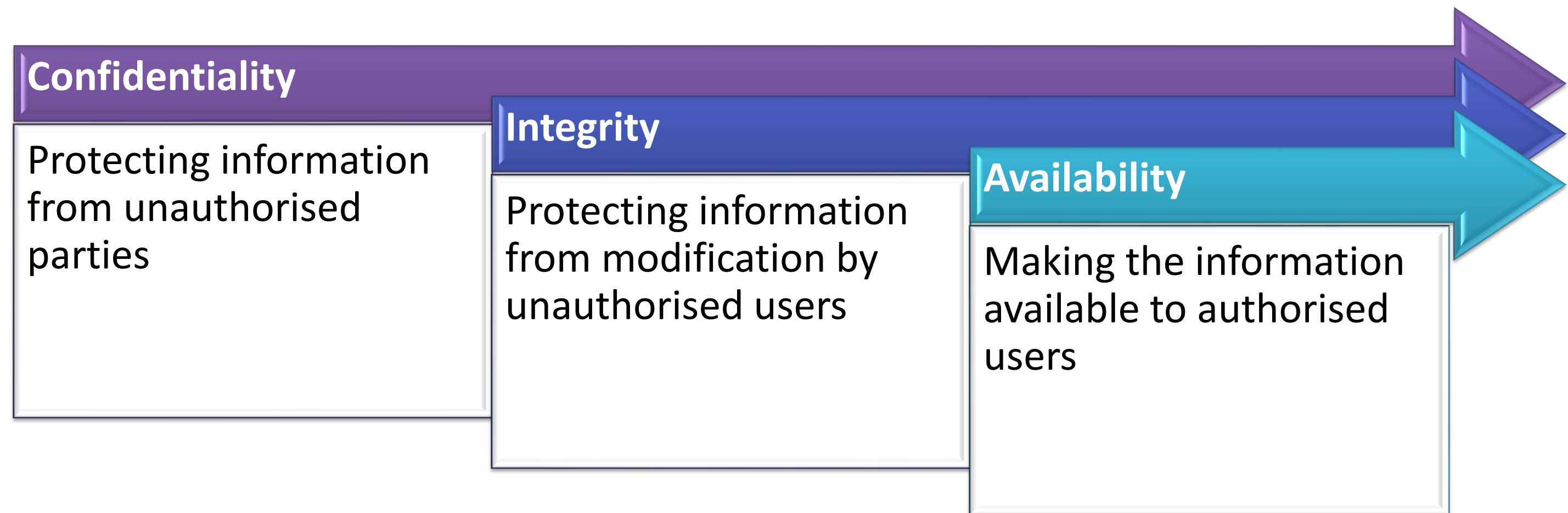
- ✓ Adopts a comprehensive management strategy to guarantee the information security controls meet the organisation's ongoing information security needs.
- ✓ A company's use of a systematic approach to identify, evaluate, and manage information security risk is strongly suggested by establishing, maintaining, and updating an ISMS.



What is an ISMS?

(Continued)

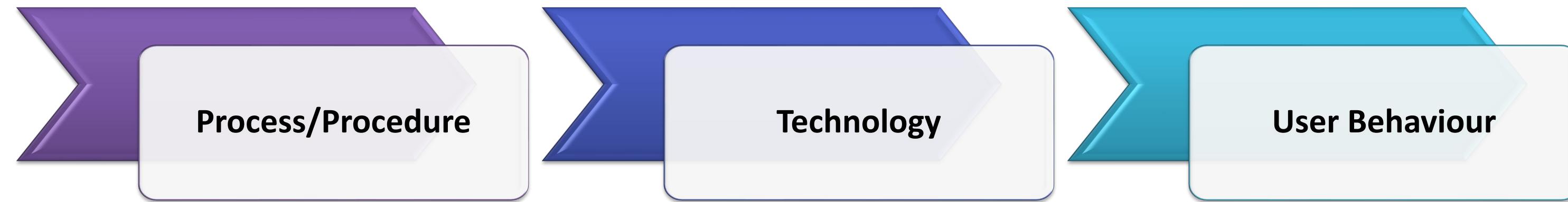
- ✓ Critical factors to an ISMS are:



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?

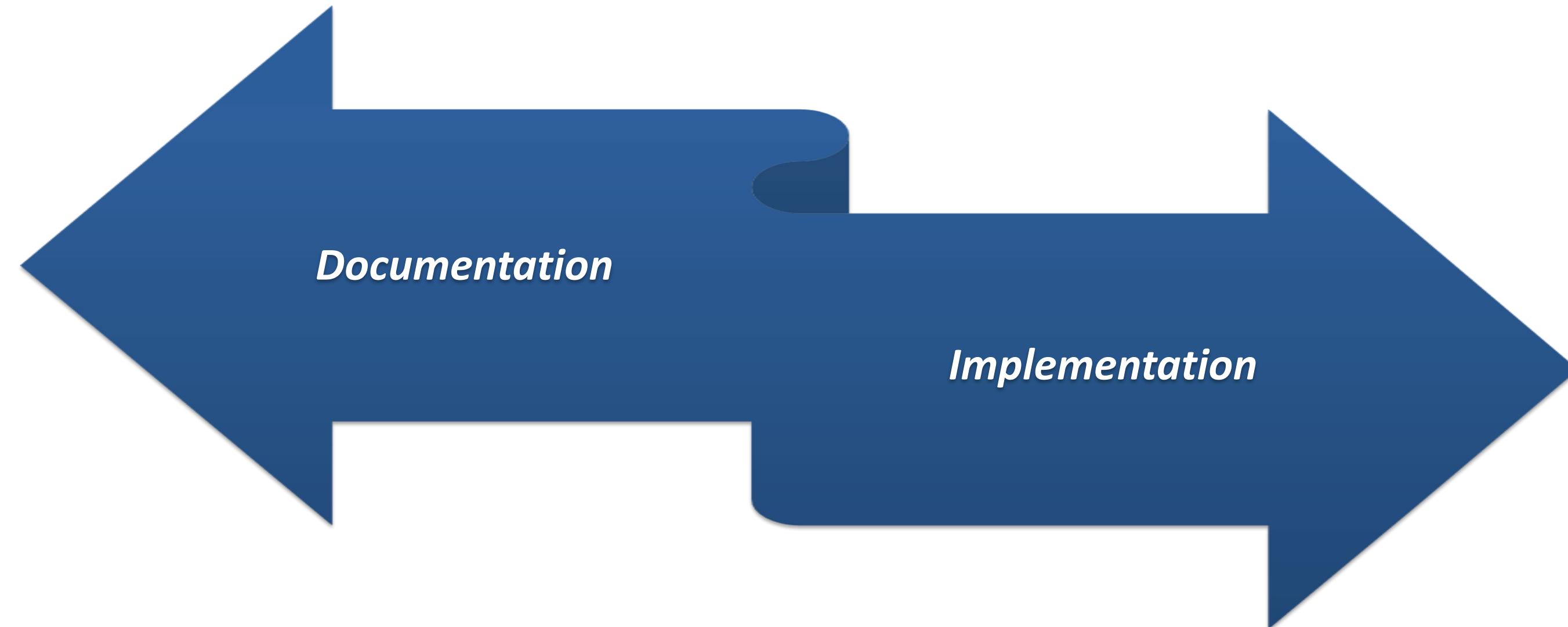
Objectives and Purposes of ISMS

- ✓ 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:



Project Plan

- ✓ Project Planning is divided into two groups of tasks:



Project Plan

Documentation

- ISO/IEC 27001 and its helping document, ISO/IEC 27002 (ISO/IEC 17799), detail 133 security measures, which are organised into 39 control objectives and 11 sections. These sections define the best practices for:

Business Continuity Planning

System Acquisition, Development and Maintenance

Information Security Incident Management

Communication and Operations Management

Physical and Environmental Security

Project Plan

(Continued)



Project Plan

Planning

- ✓ As in all certification and compliance initiatives, consideration of the size of the organisation, its business nature, the maturity of the process in implementing ISO 27001 and senior management's commitment is necessary.
- ✓ The most significant departments and activities that will be important to the success of the project include:



Project Plan

Internal Audit

- ✓ Internal audit participation during the initial planning stage will help create an implementation strategy, and early involvement of internal auditors will be helpful throughout the later certification phases that need management review.

IT

- ✓ The activities associated with the ISO 27001 objectives will require time and resources from the IT department.
- ✓ It will be helpful to evaluate how the current processes comply with ISO 27001 criteria by taking an inventory of existing IT compliance activities, procedures, and policies, as well as the maturity of existing IT processes and controls.

Project Plan

(Continued)

- ✓ Executing policies and procedures involve other departments significantly, even though it is generally thought of as an IT task.
- ✓ For instance, physical security and access restrictions are primarily the responsibility of facilities management.



Project Plan

Decision Making

- ✓ The decision of how and when to implement the standard may be affected by a number of factors, include:

Existing IT Maturity Levels

Customer Requirements

Existing Training Programs

Business Objectives and Priorities

Adherence to Internal Processes

Internal Audit Capability

Existing Compliance Efforts and Legal Requirements

The Enterprise's Ability to Adapt to Change

User Acceptability and Awareness

Contractual Obligations

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:

Define an ISMS Policy

Define the Scope of the ISMS

Perform a Security Risk Assessment

Manage the Identified Risk

Select Controls to be Implemented and Applied

Prepare an SOA

Project Plan

(Continued)

- ✓ 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

Project Plan

(Continued)

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

Phase 7: Set Up Policies and Procedures to Control Risks

Phase 8: Allocate Resources, and Train the Staff

Project Plan

(Continued)

Phase 9: Monitor the Implementation of the ISMS

Phase 10: Prepare for the Certification Audit

Phase 11: Conduct Periodic Reassessment Audits

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.
 - ❖ 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.

Project Plan

(Continued)

- ❖ Understanding information assets and performing efficient risk analyses.
- ❖ Maintaining the organisation's standing among top business leaders.
- ❖ Adherence to the rules of the industry.

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.

Project Plan

(Continued)

- The following activities/initiatives demonstrate management support:
 - ❖ A policy for information security.
 - ❖ Information security plans and objectives.
 - ❖ Information security roles and responsibilities, often known as a segregation of duties (SoD) matrix that lists the roles involved.
 - ❖ 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.

Project Plan

(Continued)

- ❖ 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.

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.

Project Plan

(Continued)

- The following details should be taken into account:
 - ❖ 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

(Continued)

- ❖ 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.

Project Plan

(Continued)

- ❖ 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.
- 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.

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.
- 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.

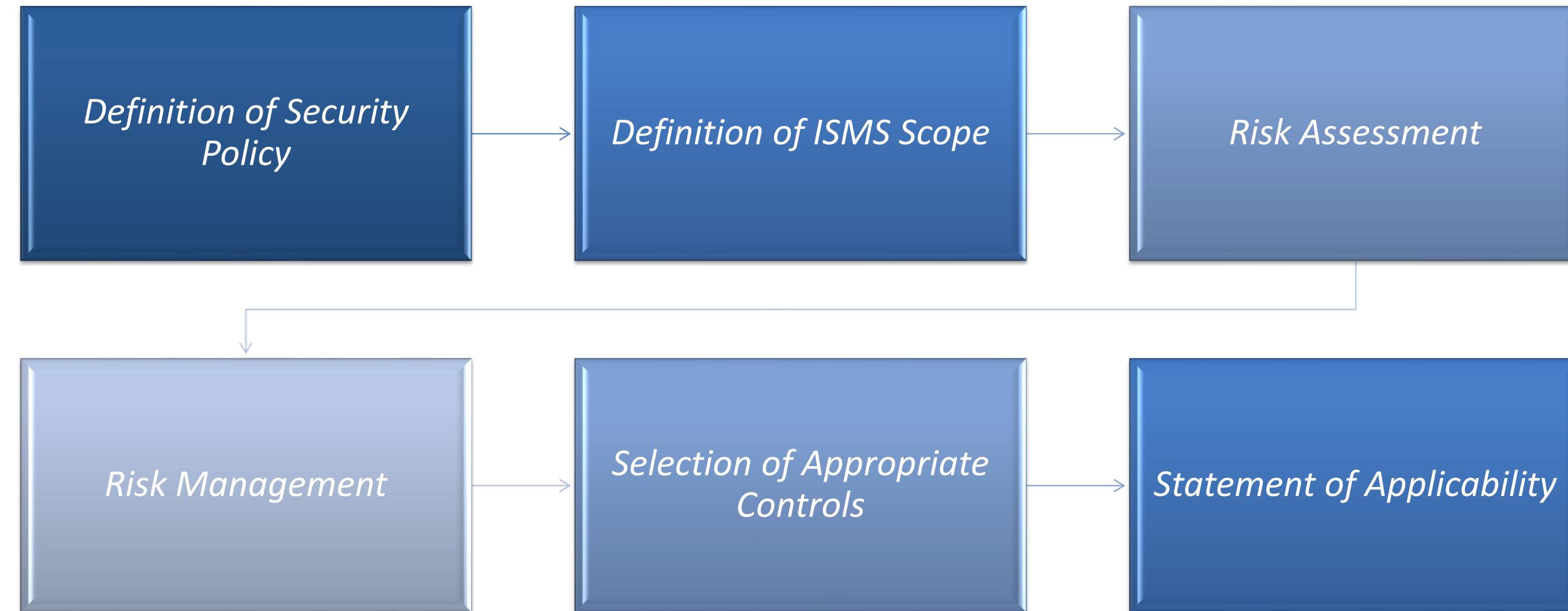
Project Plan

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

- ✓ The development of an ISMS framework based on ISO 27001:2013 entails the following six steps:



Management and Governance Frameworks

ISMS Frameworks

Step 1

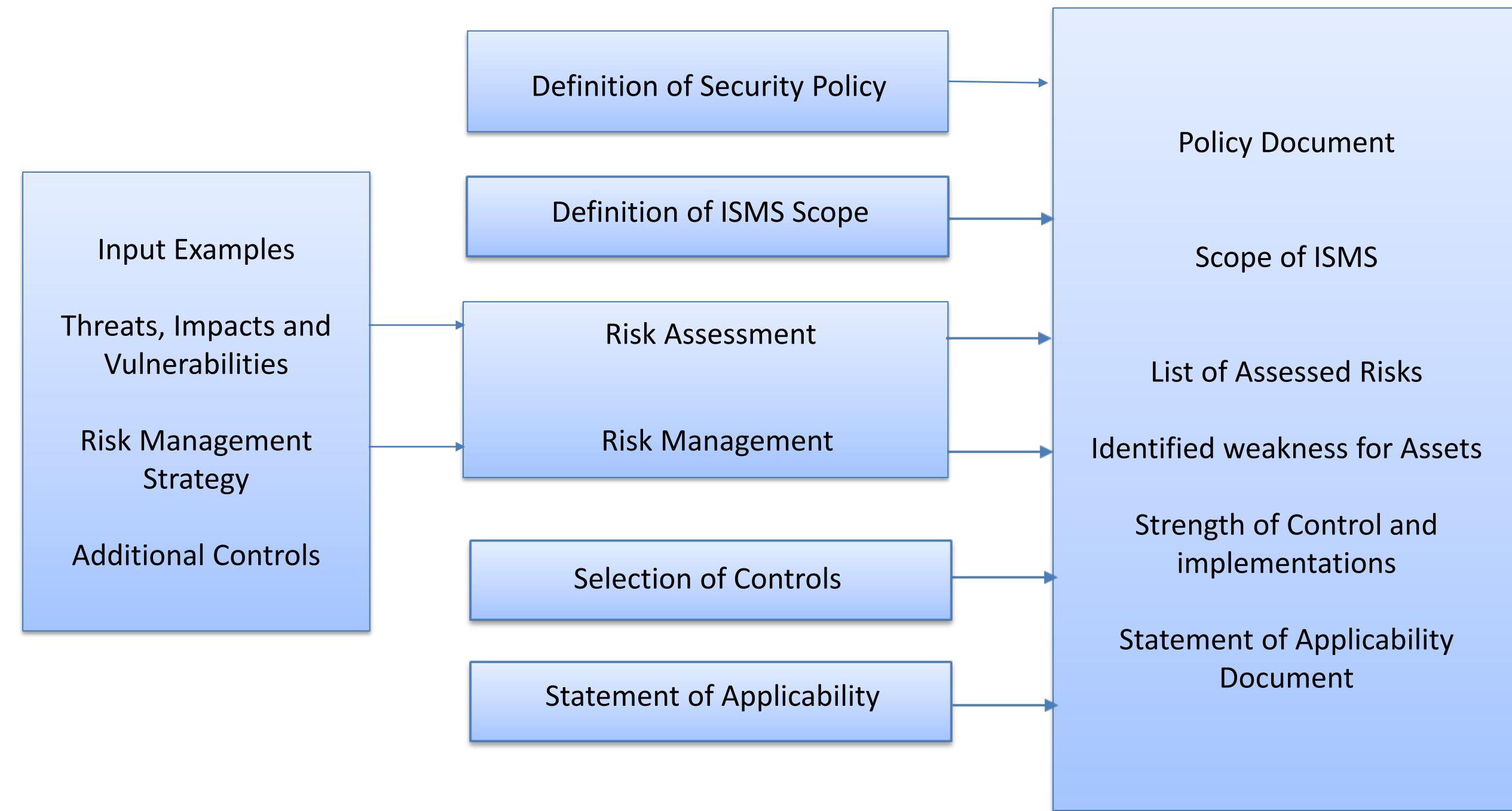
Step 2

Step 3

Step 4

Step 5

Step 6



ISMS Principles

- ✓ The following are the ISMS principles:

Customer Focus

Leadership

Stakeholder
Involvement

Being Process-
centric

Systematic
Approach to
Management

Continual
Improvement

Decisions Based on
Facts

Supply Chain
Relationships

ISMS Principles

- ✓ The main objective is to implement the appropriate measures to eliminate or minimise the impact that various 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:



ISMS Principles

(Continued)

- ✓ By preventing and minimising the impacts of security incidents, ISMS ensures business continuity and customer confidence, protects business investments and opportunities and reduces damage to the business.
- ✓ An organisation should design, implement, and maintain a consistent set of policies, processes, and systems to handle risks to its information assets in order to ensure acceptable levels of information security risk. This is the guiding principle of an ISMS.

ISMS Benefits

✓ The benefits of ISMS are as follows:

- Provides consumers and stakeholders with confidence in how you manage risk.
- Consistency in the delivery of your product or service.
- Enhanced customer satisfaction.
- Protects an organisation's assets, shareholders, and customers.



ISMS Benefits

(Continued)

- Keeps confidential information secure.
- Secure exchange of information.
- Provides organisations with a competitive advantage.
- Manages and minimises risk exposure.
- Builds a culture of security.



ISMS Benefits

(Continued)

- 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 based on ISO standards.

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.

Introduction to Management Systems



Introduction to Management Systems

Management Responsibility in Implementation

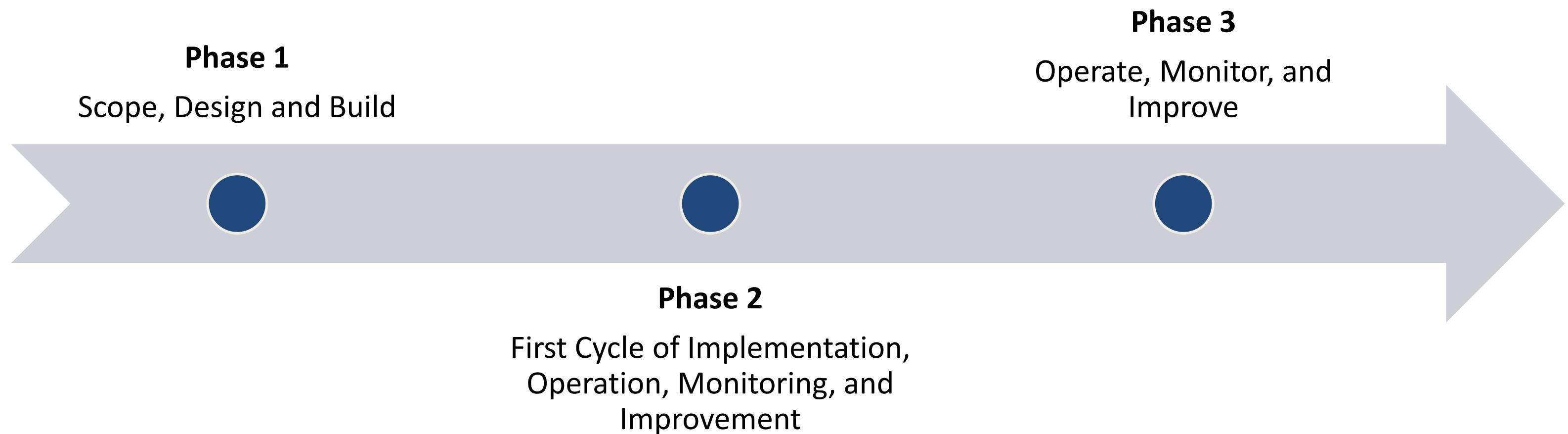
- ✓ Implementing an ISMS is something that ISO 27001 recognises, affecting the whole organisation.
- ✓ ISO 27001 requires management to communicate the importance of an effective information security management system and to conform to that system's requirements.
- ✓ Designing and establishing an ISMS 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.

Process Approach

(Continued)



Process Approach

(Continued)

- ✓ A two-phased approach should be followed in implementing an ISO 27001-compliant ISMS.
- ✓ Phase 1 is to set up the scope and foundation elements of the ISMS and define the scope of activities for the next phase.
- ✓ **Phase 1 includes the following:**
 - Identifying the gap between ISO 27001 and its current processes and controls.



Process Approach

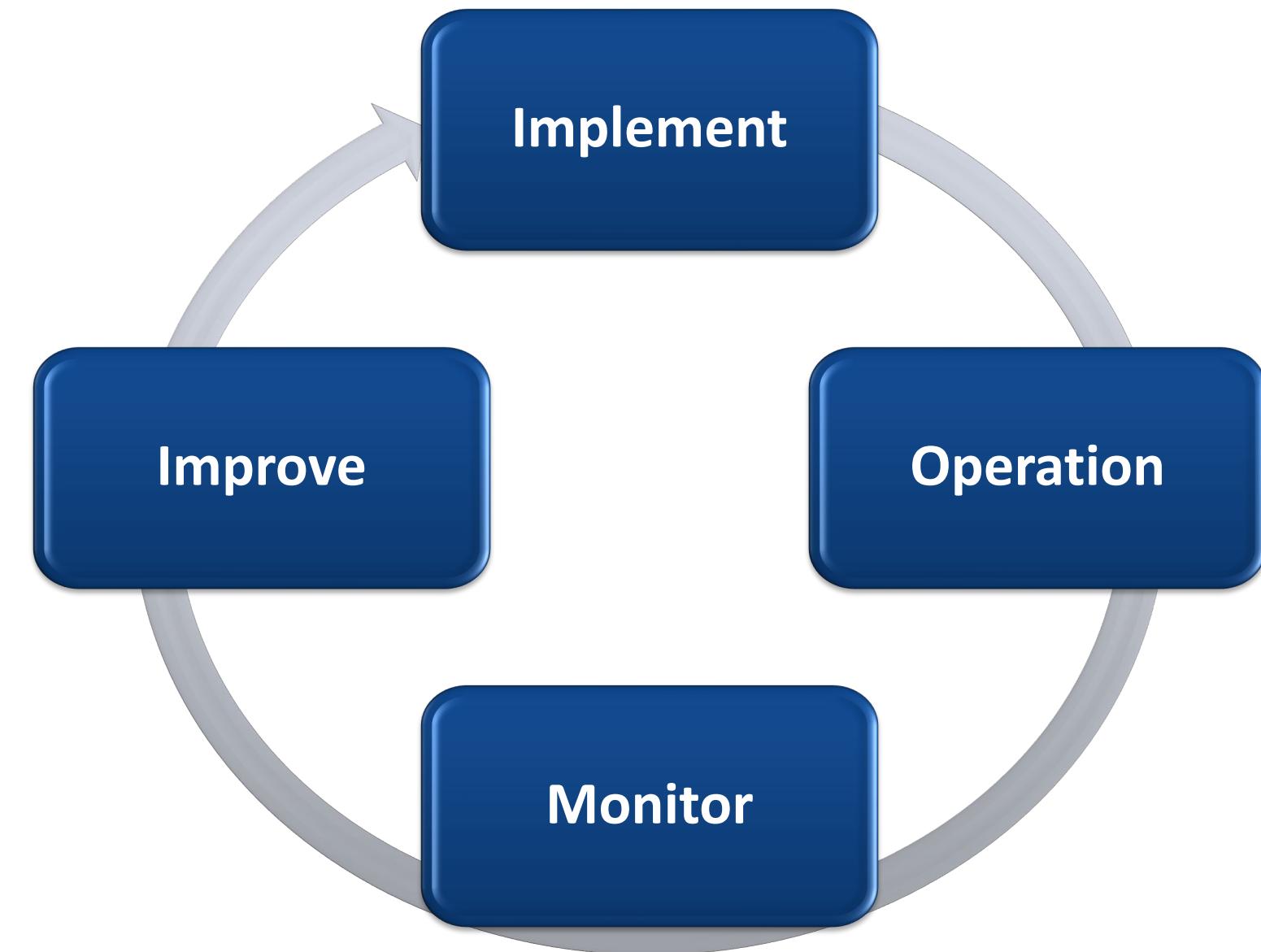
(Continued)

- Using or refining existing processes and controls to address these gaps will reduce the time and effort, but the design of new processes and controls is also required.
- Identifying and determining the value of information assets through workshops and one-to-one meetings with key personnel and management.
- Assessing the threats, vulnerabilities, and risks to information assets and determining the options for treating these risks.
- Preparing the ISO 27001 Statement of Applicability.
- Preparing the scope and programme of work for Phase 2 and providing input to further business cases.

Process Approach

(Continued)

- ✓ Phase 2 consists of four work streams:



Process Approach

1. 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.

2. 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.

Process Approach

3. 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).

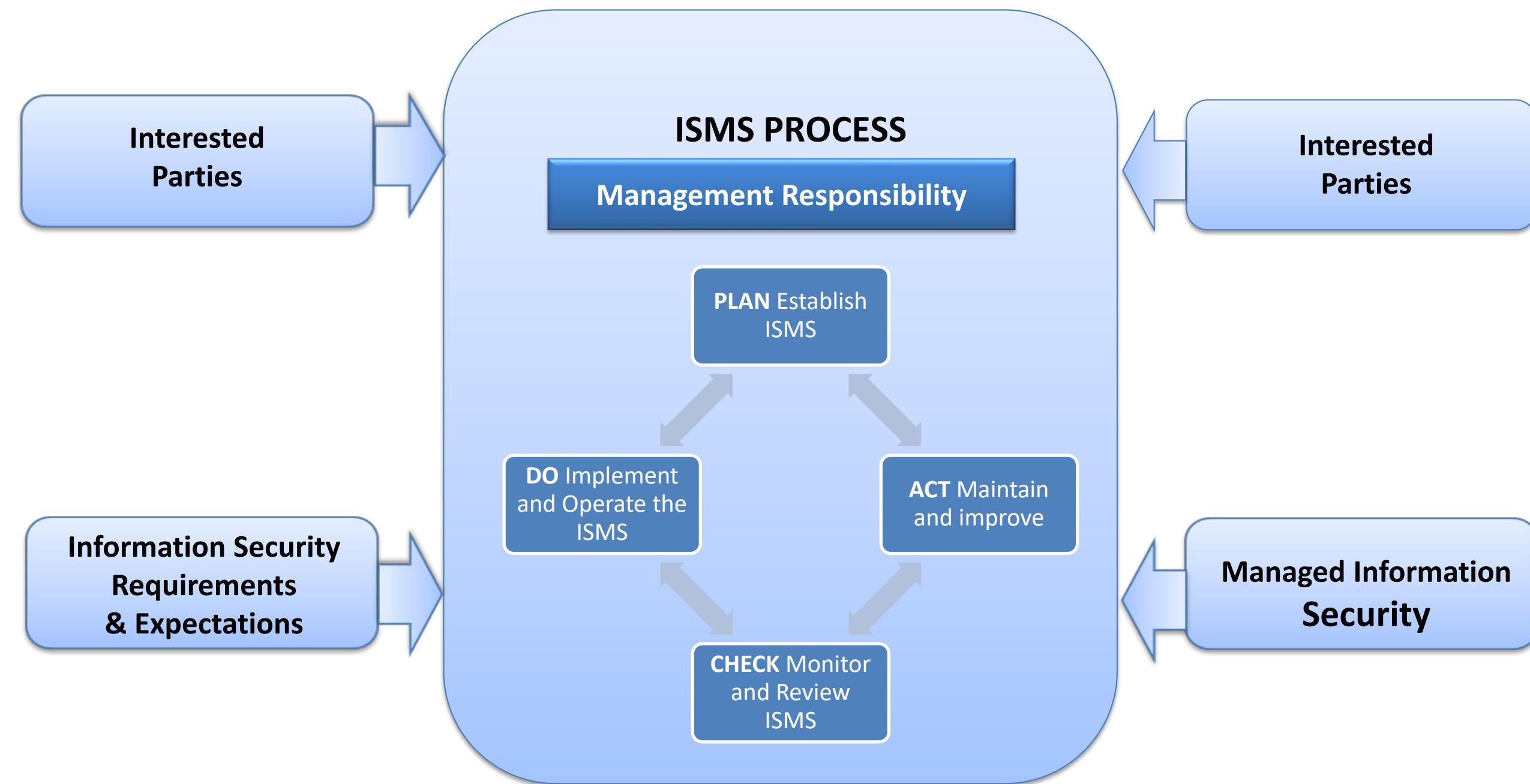
4. Improve

- ✓ 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.

Process Approach

(Continued)

- **Phase 3:**



Process Approach

(Continued)

- ✓ 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.
- ✓ 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

Plan (Establishing 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.

Do (Implementing and Workings of the ISMS)

- ✓ Implement and exploit the ISMS policy, processes, controls, and procedures.



The PDCA Cycle

Check (Monitoring and Review of the ISMS)

- ✓ Assess the performance against the Objectives, policy and practical experience and report results for management to review.

Act (Update and Improvement of the ISMS)

- ✓ 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.



Case Study: YZ Graphics

Customer Background

- YZ Graphics Ltd is a major graphic design and publishing company.
- As of 2018, YZ has a 6 billion euros valuation and more than 1400 employees, making it one of the unicorn firms with the quickest pace of growth.
- YZ offers a simple-to-use graphic design tool that includes many pre-built designs and templates to make the creative process easier.
- As one of the best IT employers, YZ is frequently mentioned in the news for its ideals and culture, which draw top talent from around the world.

Case Study: YZ Graphics

Key Objectives

- ❑ Establish a long-term risk management framework to improve YZ's security posture and maturity.
- ❑ Establish security as a " baked-in " culture to all business operations and naturally scales with the company.
- ❑ By speeding up the currently active security activities, you may increase the reputation and trust of the enterprise market.
- ❑ To lessen the possibility of future information security breaches, strengthen the security ecosystem.

Case Study: YZ Graphics

Challenges

- ❑ Setting up a solid security culture in a rapidly expanding organisation with many conflicting demands was difficult.
- ❑ It is essential to "bake in" security into all activities to stay up with the pace of the business due to the constant change in an organisation that is rapidly developing and integrating technology.
- ❑ Another crucial task for YZ is ensuring that the daily data on users, which is expanding exponentially, is secured and that there is the least possible exposure of personal data.
- ❑ Last but not least, YZians (those employed by YZ) have historically been granted enormous autonomy and agility to support its phenomenal growth.
- ❑ While implementing greater security governance and control in its operations, YZ needed to maintain that culture.

Case Study: YZ Graphics

Key Partner Criteria for YZ

- PI was familiar with the YZ working style and understood its values, culture, and the significance of delivering a solution that retained them. PI had previously worked with other tech giants.
- YZ chose to work with PI because of its track record of successfully implementing ISO27001-certified ISMS and because of the company's cultural fit, flexibility, and shared ideology regarding achieving security and risk management outcomes without impeding business growth.

Case Study: YZ Graphics

PI Solution

- ❑ The foundation of the PI governance model is the idea that "no two organisations are the same." This implies that every Information Security Management System (ISMS) is unique.
- ❑ Our organisation is built on the core principles of ownership and flexibility. We generally have a no-nonsense dedication, which enables us to adjust to the working environment at YZ readily.
- ❑ The team at YZ thrives on ongoing development and change, and PI worked with YZ to design an ISMS.
- ❑ They ensured the methodology was tailored to match the culture and specific demands of YZ and its operations.
- ❑ This was a crucial stage in the implementation process because "the personnel will not be able to execute if the risk methodology does not match with how the business is conducted, resulting in an inevitable collapse of the ISMS in the longer term."

Case Study: YZ Graphics

(Continued)

- ❑ Another important factor in system implementation was ensuring that every YZian could use and utilise it themselves.
- ❑ A free ISMS site that PI has developed and refined through years of real-world security operations and auditing is often offered to clients.
- ❑ With YZ, which required a solution tailored to its current productivity tools, this strategy would not be effective.
- ❑ Since PI used several of YZ's tools and technologies regularly, he was already familiar with them.
- ❑ YZ stakeholders were considerably more eager to implement the ISMS because YZ did not need to purchase any new security governance platforms.

Case Study: YZ Graphics

(Continued)

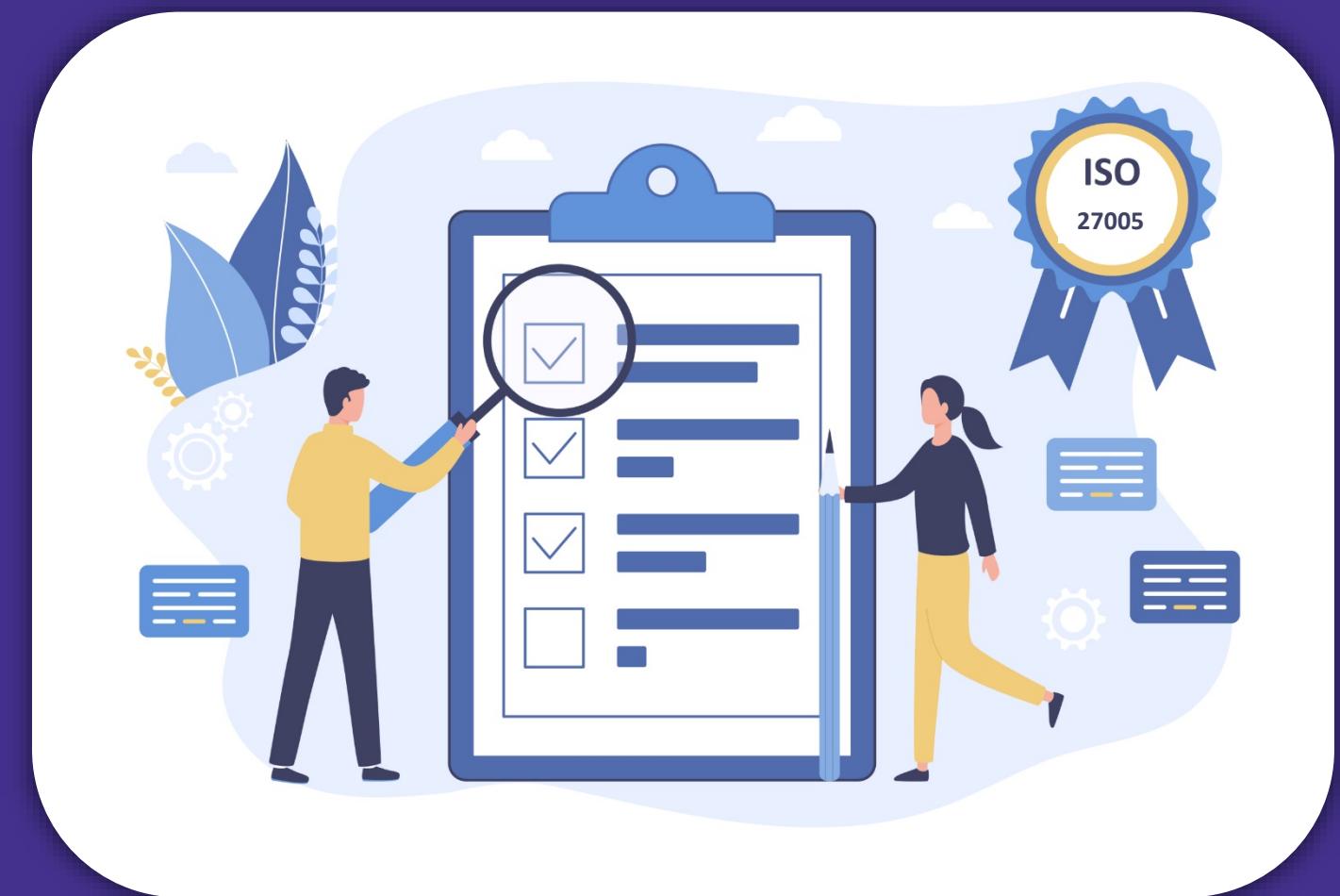
- ❑ In order to identify and formulate security risks at a level that YZ could manage, along with an actionable list of items that would work with the organisation, existing culture, processes, and technology choices, PI and YZ conducted interviews and workshops with everyone, from new hires to the founders.

Case Study: YZ Graphics

Results

- ❑ YZ implemented an ISMS created to best suit its organisational needs and evolving working practices.
- ❑ Security was prioritised at the organisational level and was directly controlled by the founder.
- ❑ YZ received ISO27001 certification. Through the certification procedure, PI represented YZ.
- ❑ A team of security champions was effectively established by YZ throughout the various company functions, ensuring that all significant business stakeholders participated and had security-related dialogues.

Module 4: Interaction with ISO 27005



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.

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

(Continued)

- ✓ 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.

ISO 27001 VS ISO 27005

(Continued)

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

Quantifying the Business Impact

(Continued)

- ✓ 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).

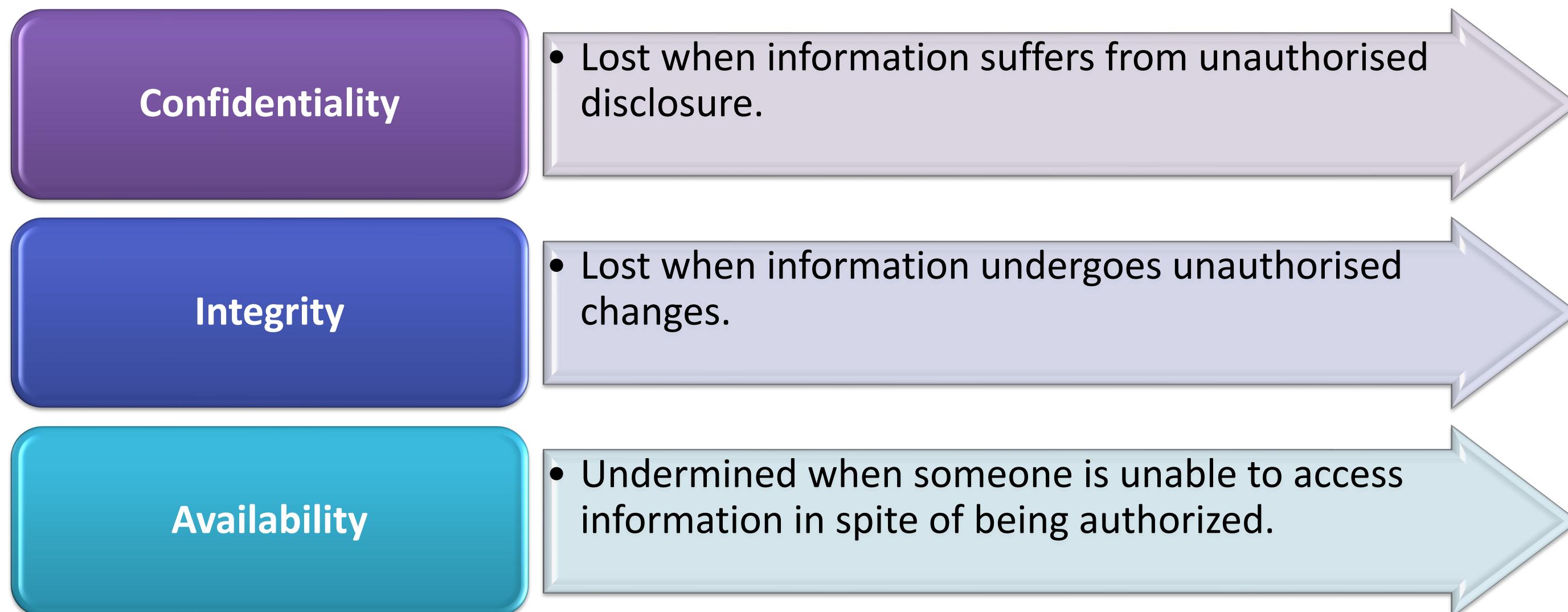
Impact Severity

- ✓ 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.

Impact Severity

(Continued)

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



Module 5: Context of the Organisation



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.

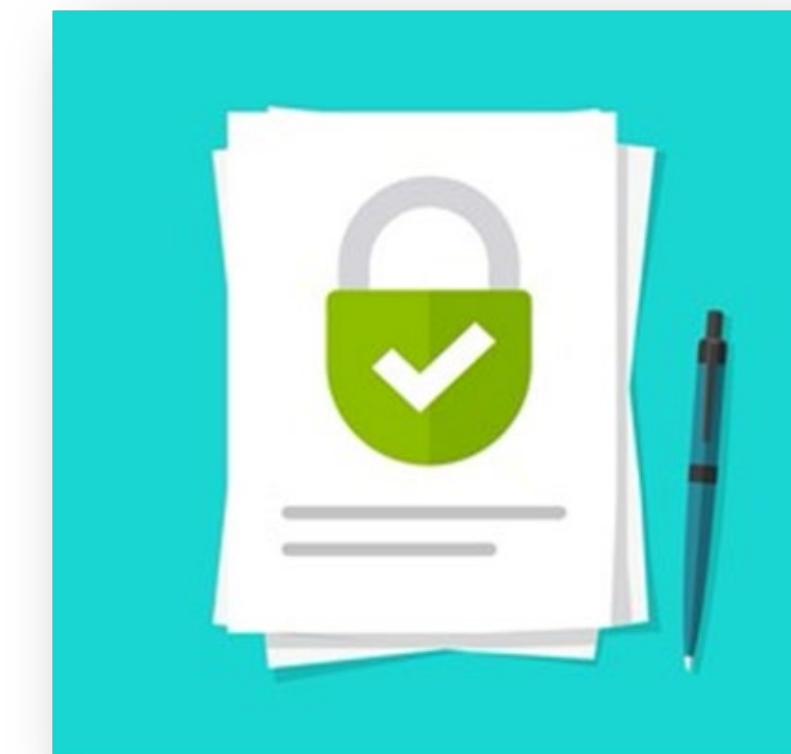


Determining the Scope of the Information Security Management System

- 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:***
 - a. The external and internal issues.
 - b. The requirements.
 - c. The organisation performs interfaces and dependencies between activities, and those that are performed by other organisations.
- As documented information, the scope shall be available.

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.



Case Study: Blaze Team Executive

Challenges

- ✓ Even though there was no immediate reason to obtain ISO 27001 certification, Blaze's executive team realised that the enterprise-level clients they attracted were becoming more interested in information security assurance.
- ✓ Blaze is constantly looking for methods to set itself apart via quality, and it wants to show this dedication by earning an approved ISO 27001 certification.
- ✓ The difficulty was typical, especially for an SME. Since Blaze lacked a full-time employee focused on information security, it sought to automate and streamline the procedure as much as possible.
- ✓ They had a limited understanding of the ISO 27001 standard and realised that a traditional consultancy-led approach might be costly and leave them with the requirement to develop an ISMS structure and think about how to manage and evidence the necessary work processes.

Case Study: Blaze Team Executive

Solution

- ✓ ISMS and Blaze rapidly saw overlaps in the respective organisational structures and methods of operation.
- ✓ The Blaze was thrilled to find an established cloud solution with a practical strategy for obtaining and keeping ISO 27001 certification.
- ✓ Without any training, the Blaze team jumped onto the stage.

Case Study: Blaze Team Executive

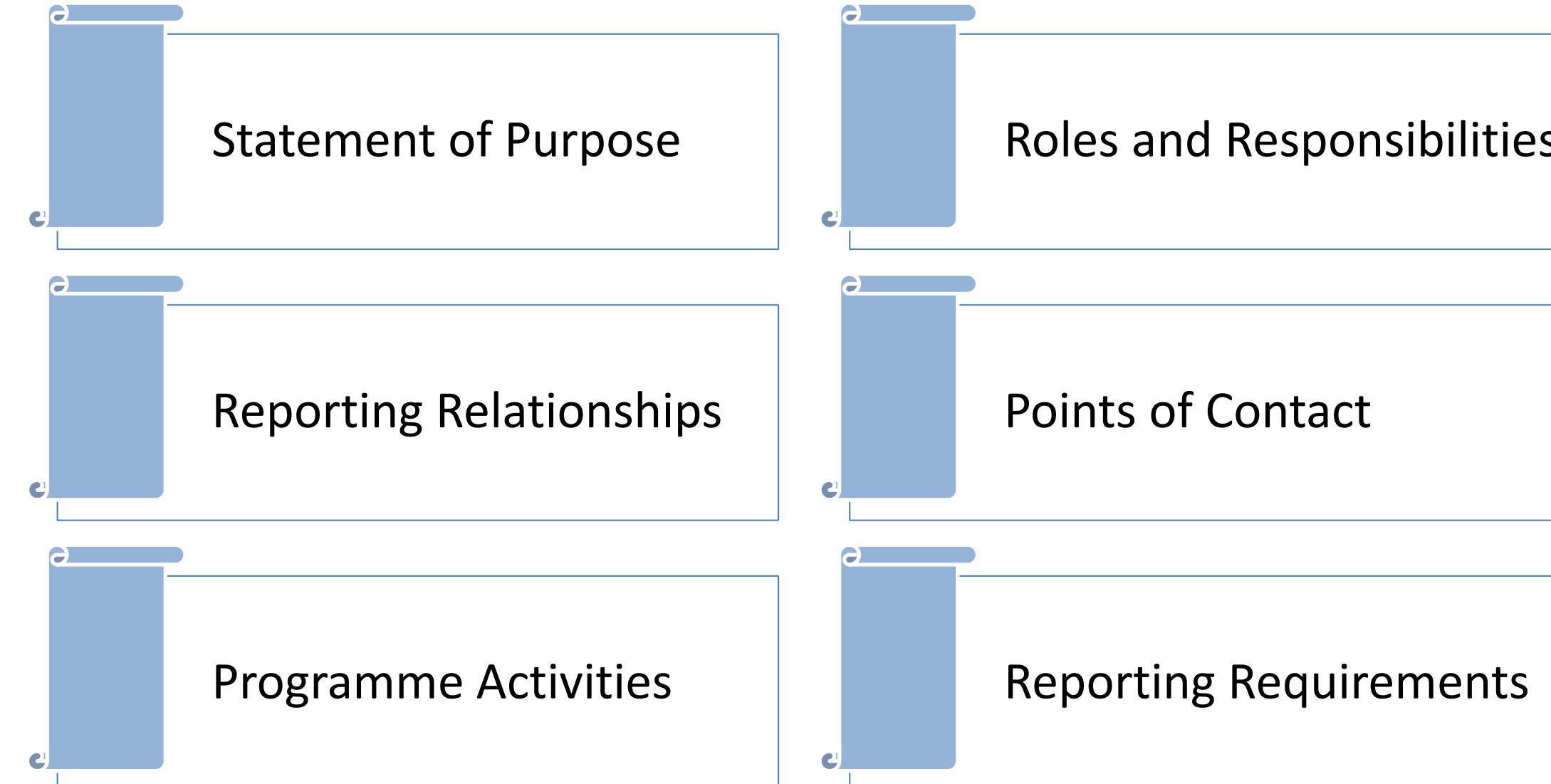
Result

- ✓ They obtained ISO 27001 certification with very little time investment and minimal disruption to business as normal, thanks to the structured approach in ISMS and their focus.
- ✓ Their business is now firmly grounded in excellent information security management, and the upkeep of the ISMS is low.

Module 6: Introduction to Auditing



Internal Audit Charter



Communicate with Organisation and Audit Committee



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



Types of Audit

- ***The following are some types of audit:***

Financial Audits or
Reviews

Operational Audits

Department Reviews

Information Systems
Audits

Integrated Audits

Investigate Audits or
Reviews

Follow-up Audits

Types of Audit

1. *Financial Audit*

- A historically based, independent evaluation performed to attest to the fairness, accuracy, and dependability of financial data.

2. *Operational Audit*

- A forward-thinking, systematic, and independent assessment of organisational activities.
- Although financial data can be used, the primary sources of evidence are operational policies and accomplishments related to organisational goals.
- During this type of review, internal controls and efficiencies may be evaluated.

Types of Audit

3. *Department Review*

- Current period analysis of administrative functions to evaluate the adequacy of controls, safeguarding of assets, efficient use of resources, compliance with related laws, regulations and University policy, and integrity of financial information.

4. *Information Systems Audit*

- There are three basic kinds of Information Systems Audits that may be performed:
 - i. General Controls Reviews.
 - ii. Application Controls Review.
 - iii. System Development Review.

Types of Audit

5. *Integrated Audit*

- This is a mixture of an operational audit, a department review, and a review of the IS audit application controls.

6. *Investigative Audit*

- This is an audit that takes place as a result of a report of unusual or suspicious activity on the part of an individual or a department.



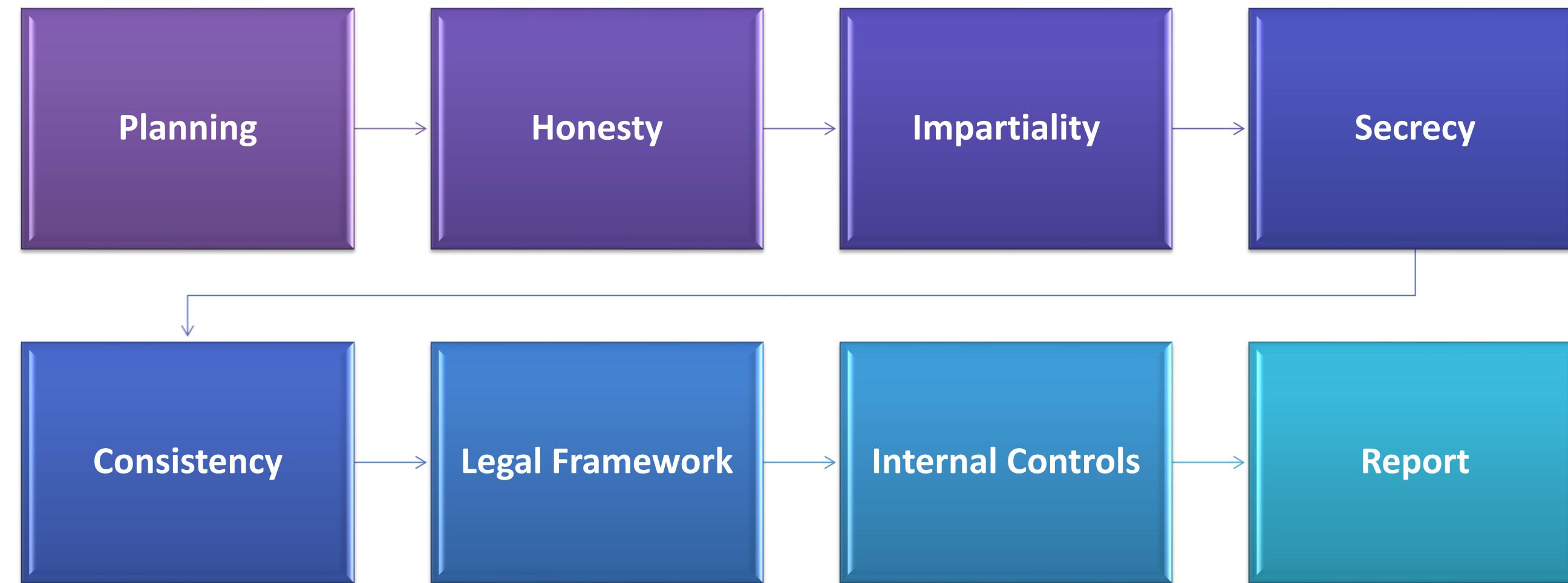
Types of Audit

7. *Follow-up Audit*

- These audits are carried out six months after an internal or external audit report has been released.
- They are intended to assess corrective action taken on audit issues reported in the original report.
- When these follow-up audits are performed on external auditors' reports, the findings may be reported to the external auditors.

Techniques and Principles

- *The main principles of auditing are:*



Techniques and Principles

- I. ***Planning:*** An auditor must take into account the system as well as internal control procedures.
- II. ***Honesty:*** Honesty and sincerity are important principles in auditing. The professional integrity of an auditor must be beyond doubt.
- III. ***Impartiality:*** The attitude of the auditor must be impartial. Their personal views may not influence or affect the audit report.



Techniques and Principles

- IV. *Secrecy*:** Secrecy must be maintained. An auditor may not disclose information to a third party.
- V. *Consistency*:** In the case of internet security audits, the auditor must follow the same processes in future years. There should be consistency between audits.
- VI. *Legal Framework*:** Business activities must run within rules and regulations. The rule of law must be applied to protect the rights of interested parties.
- VII. *Internal Controls*:** The auditor will examine the internal controls governing information security. Ensure evidence exists of control use (e.g. records of resolved incidents).
- VIII. *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.

Techniques and Principles

(Continued)

➤ *The techniques for auditing are:*

Examination of Record

Inquiry

Sampling

Confirmation

Analytical Review

Techniques and Principles

- I. ***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.
- II. ***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.
- III. ***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.



Techniques and Principles

- IV. *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.
- V. *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.



Phases of Audit

➤ ***There are several phases to an internal audit:***

1. Preparation and planning.
2. Execution and fieldwork.
3. Recording and reporting.
4. Follow-up and assessment.



Module 7: Leadership



Leadership and Commitment

- Leadership and commitment shall be demonstrated by the top management regarding the information security management system by:
 - a. Make sure that the information security policy and goals are established and compatible with the organisation's strategic direction.
 - b. Assure that the information security management system requirements are integrated into the processes of the organisation.
 - c. Ensuring the availability of the resources required for the information security management system.
 - d. Communicating the significance of effective information security management and adhering to the requirements of the information security management system.

Leadership and Commitment

- d. Assuring that the information security management system attains its intended result.
- e. Directing and assisting individuals in contributing to the effectiveness of the information security management system, encouraging continuous improvement.
- f. Assisting other appropriate management roles in showing leadership in their areas of responsibility.



Policy

- An information security policy shall be established by the top management that:
 - a. Is relevant to the organisation's objective.
 - b. Contains information security objectives or gives a framework to set information security goals.
 - c. Includes a commitment to meet applicable information security requirements; and
 - d. Includes a commitment to improving the information security management system on an ongoing basis.

Policy

(Continued)

- The information security policy shall:
 - e. Be available as documented information.
 - f. Be communicated in the organisation; and
 - g. As relevant, be available to interested parties.



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:
 - a) Ensuring that the information security management system meets the requirements of this document.
 - b) Reporting to top management on the performance of the information security management system.



Module 8: Performing ISO 27001 Audits



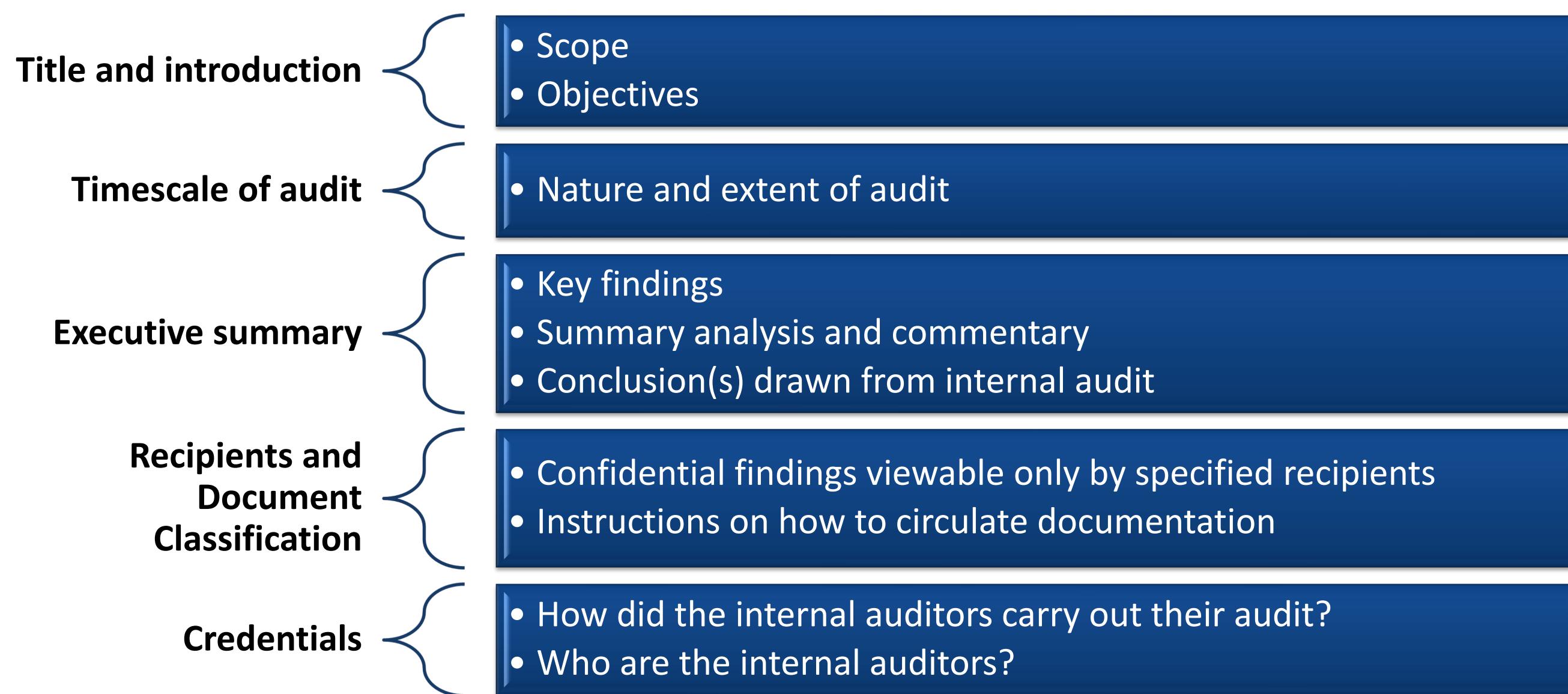
Preparing an Audit Report

- ✓ 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.

Preparing an Audit Report

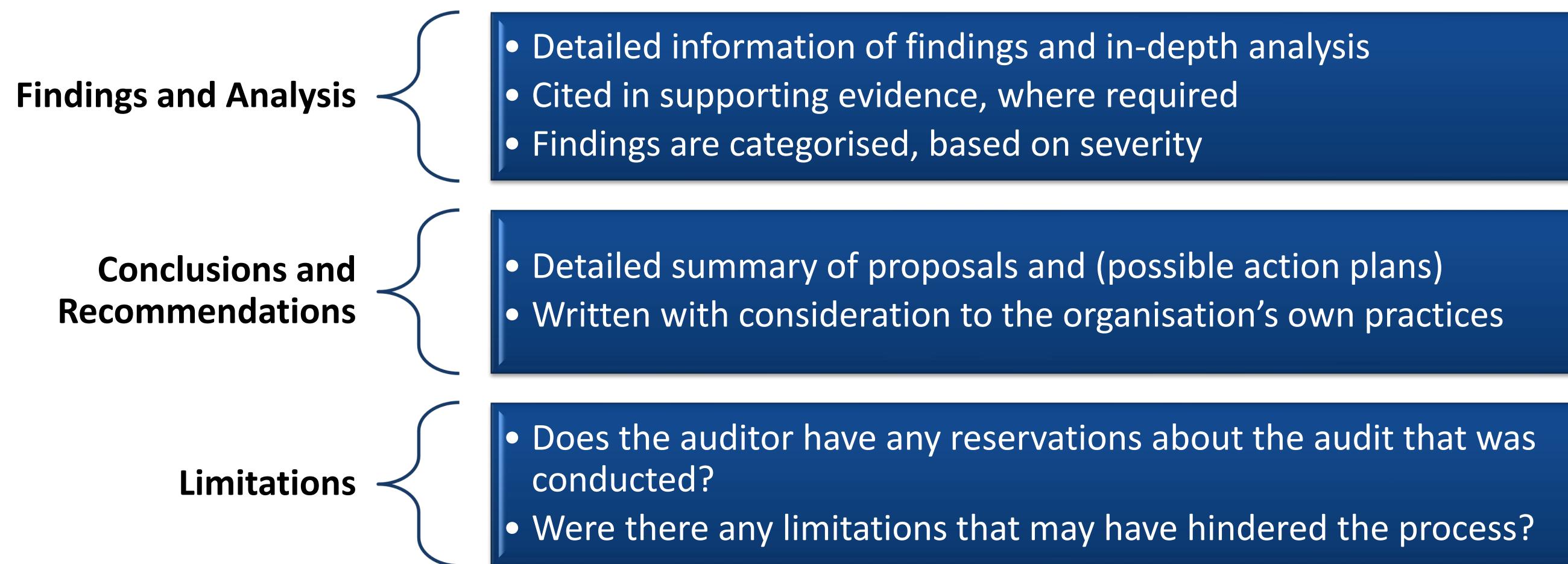
(Continued)

✓ What to include?



Preparing an Audit Report

(Continued)



Analysing Data

✓ Audit reports contain:

A Review and Analysis of Findings.

Consolidation of all Findings, Including Grouping and Tabulation.

Classification of Findings.

Preparation of Recommendations.

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	<ul style="list-style-type: none">• 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	<ul style="list-style-type: none">• 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

Auditing Procedures

(Continued)

STEP 2 : SUBMIT PLAN FOR APPROVAL

Responsibility	ISMS Audit Team
Input	<ul style="list-style-type: none">• Annual Audit Plan
Actions	<ul style="list-style-type: none">• 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	<ul style="list-style-type: none">• When approved: Proceed to step 3• When not approved: Proceed to step 1

Auditing Procedures

(Continued)

STEP 3 : PREPARE FOR AUDIT

Responsibility	ISMS Audit Team
Input	<ul style="list-style-type: none">• Annual Audit Plan• Periodic audit• Ad-hoc audit
Actions	<ul style="list-style-type: none">• 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	<ul style="list-style-type: none">• ISMS Audit Checklist

Auditing Procedures

(Continued)

STEP 4 : CONDUCT AUDIT & RECORD FINDINGS

Responsibility	ISMS Audit Team
Input	<ul style="list-style-type: none">• ISMS Audit Checklist• Annual Audit Plan
Actions	<ul style="list-style-type: none">• 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:<ul style="list-style-type: none">○ 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 from earlier audits and reviews have been executed○ ISMS is compliant with ISO 27001
Output	<ul style="list-style-type: none">• Output Audit Findings (if any)

Auditing Procedures

(Continued)

STEP 5 : CREATE & ARCHIVE AUDIT REPORT

Responsibility	ISMS Audit Team
Input	<ul style="list-style-type: none">• ISMS Audit Checklist• Annual Audit Plan
Actions	<ul style="list-style-type: none">• 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 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 be planned for resolution in a period of three months, and follow-up audit should be scheduled at the end period.
Output	<ul style="list-style-type: none">• Audit Report

Auditing Procedures

(Continued)

STEP 6 : DEVELOP ACTION PLAN

Responsibility	ISMS Audit Team
Input	<ul style="list-style-type: none">• Annual Report
Actions	<ul style="list-style-type: none">• 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	<ul style="list-style-type: none">• Action Plan• Follow up Audit

Reviewing Documents and Reports

Mandatory Documents by ISO 27001

- ✓ Scope of the ISMS (clause 4.3)
- ✓ Information security policy and objectives (clauses 5.2 and 6.2)
- ✓ Risk assessment and risk treatment methodology (clause 6.1.2)
- ✓ Statement of Applicability (clause 6.1.3 d)
- ✓ Risk treatment plan (clauses 6.1.3 e and 6.2)
- ✓ Risk assessment report (clause 8.2)
- ✓ Definition of security roles and responsibilities (clauses A.7.1.2 and A.13.2.4)
- ✓ Inventory of assets (clause A.8.1.1)

Reviewing Documents and Reports

(Continued)

- ✓ Acceptable use of assets (clause A.8.1.3)
- ✓ Access control policy (clause A.9.1.1)
- ✓ Operating procedures for IT management (clause A.12.1.1)
- ✓ Secure system engineering principles (clause A.14.2.5)
- ✓ Supplier security policy (clause A.15.1.1)
- ✓ Incident management procedure (clause A.16.1.5)
- ✓ Business continuity procedures (clause A.17.1.2)
- ✓ Statutory, regulatory, and contractual requirements (clause A.18.1.1)

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.



Classifying Findings

(Continued)

✓ Classification of findings is as follows:

Major Non-conformity

- This pertains to a major deficiency in the ISMS
- A non-conformity pertains to one or more element of the ISO 27001 not being implemented

Minor Non-conformity

- A minor deficiency
- One or more elements of the ISMS is only partially complied
- Minor non-conformity has an indirect effect on information security

Planning, Organising, and Prioritising

- ✓ The ISMS scope is broken down using the audit checklist.
- ✓ The timing and resourcing of the audit are agreed upon in the audit plan/schedule.
- ✓ Preliminary bookings are made for audit report/discussion meetings at the end of the audit, allowing senior participants to participate.
- ✓ The audit plan will include “checkpoints” at which informal feedback to management will occur, allowing both parties to raise concerns.
- ✓ The timing of audit work may be determined according to aspects that present the greatest risk to the organisation.

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.

Module 9: Internal Auditor



Roles and Responsibilities

➤ ***Internal auditors must:***

- 
- Attend meetings with the auditee
 - Travel to onsite locations to meet staff and obtain documents
 - Report on risk management processes
 - Provide advice to managers and staff
 - Perform risk assessments

Roles and Responsibilities

(Continued)



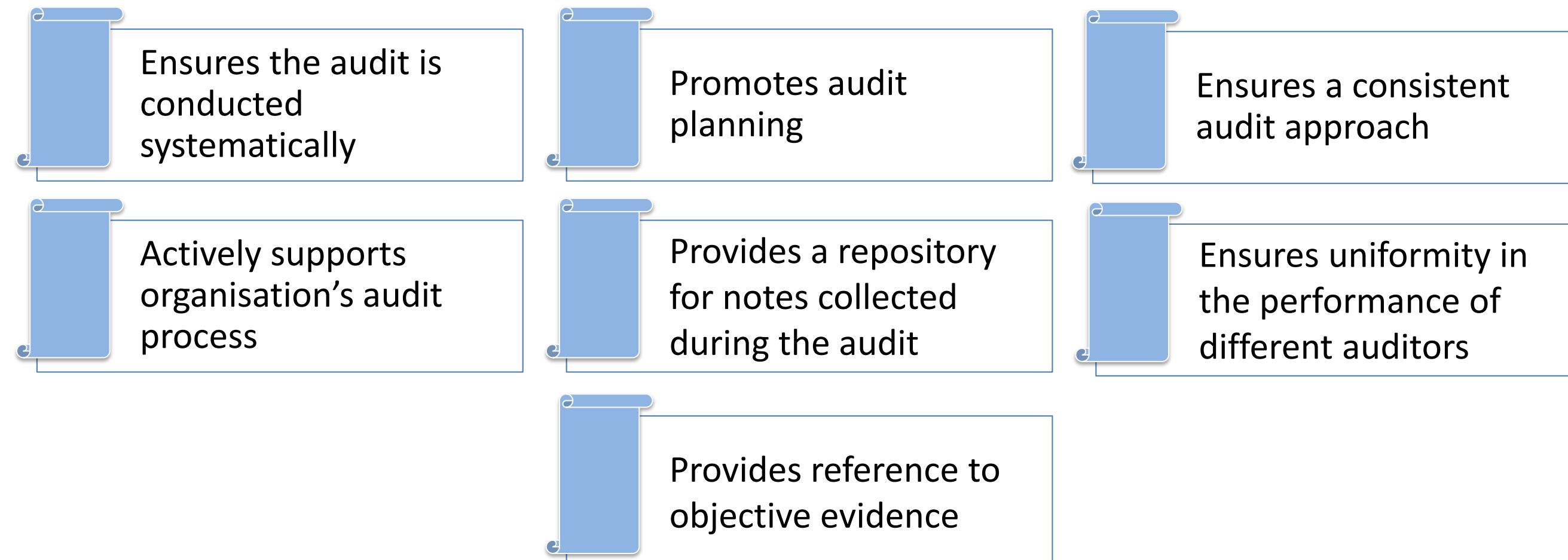
Record Review Activities

- 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

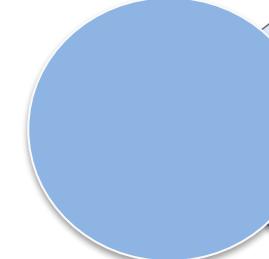
- One of the tools available to ensure audits address the essential requirements is the audit checklist.
- It serves as a reference point before, during, and after the audit process, and if developed for and used correctly, it will provide the following benefits:

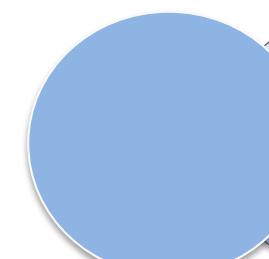


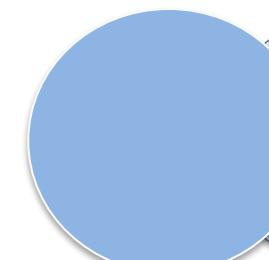
Internal Auditor Checklist

(Continued)

- 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:

 Knowledge of the client's business and its ISMS

 Development of audit strategies or overall plan

 Preparation of audit programme

Internal Auditor Checklist

(Continued)

➤ ***Benefits of a Checklist:***

1. Conducting regular audits can help a small business identify problems and highlight strengths within the business.
2. 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.
3. An audit checklist identifies areas of concern, allowing management to take corrective action.

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

(Continued)

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.

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

(Continued)

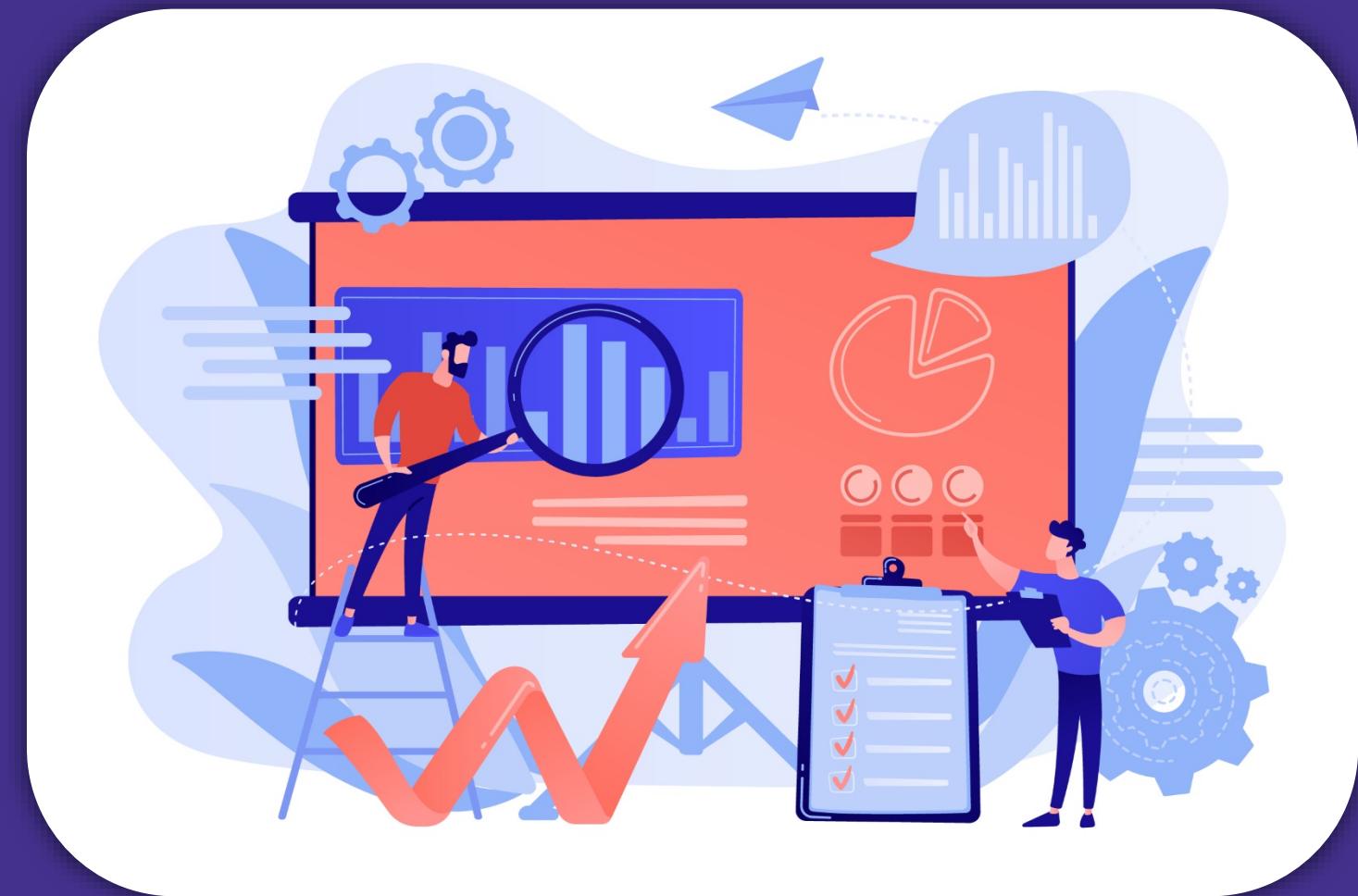
- A list of specific recipients (since the contents may be confidential) and appropriate document classification or circulation instructions.
- An outline of the credentials, audit methods, and other information pertaining to individual auditors and team members.
- Audit findings and analysis, supported upon occasion by extracts from the audit files to aid understanding.

Drafting Reports and Test Plans

(Continued)

- 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.

Module 10: Risk Management



Analysing and Evaluating Risks

- ✓ Below are five basic actions that can help auditors in arriving at sound professional decisions:
 - Identify and define the problem.
 - Collect the facts and information, and identify the pertinent literature.
 - Identify alternatives and perform the analysis.
 - Make the conclusion.
 - Complete and review the documentation and rationale for the conclusion.

Managing Risk Approaches

- ✓ It is the auditor's task to question management and others to understand the organisation, its operations, and any shortcomings and potential breaches that may occur in the ISMS.
- ✓ Performing analytical procedures on expected or unexpected variances in account balances or classes of transactions.
- ✓ Observing the physical inventory count.
- ✓ Confirming accounts receivable and other accounts with a third party.
- ✓ It is an auditor's responsibility to work with trustees and management to ensure a system is in place which ensures that all major risks to the company are identified and analysed on an annual basis.
- ✓ Auditors spend most of their time looking at risks that arise internally and their countermeasures.

Managing Risk Approaches

(Continued)

- ✓ Auditors see a “risk” as anything that could impact an organisation achieving its objectives.
- ✓ “Internal controls” are measures taken to cope with or reduce risk.
- ✓ Internal risks can be anything from incompetence to dishonesty.

Case Study: Law Firm

- **Top Law firm**
 - Required for ISO 27001 to:
 - More readily answer client surveys.
 - Set themselves out from the competitors.
- **Thirty-day YZZ Resource to support the initiative**
 - Project management
 - Using viewpoint and some Coal-face work

Case Study: Law Firm

(Continued)

- **Client Resource:** IT Manager and two IT security staff
- **Scope: IT function.**
 - Two locations
 - Statement of Applicability to reflect properly

Case Study: Law Firm

Issues

- **Resource**
 - Information Security Office is absent.
 - It was challenging to make time for the project.
- **Development of Documentation**
 - There are hardly any documented IT security protocols.
 - Key staff members keep too much information in their heads rather than on paper.

Case Study: Law Firm

(Continued)

➤ **Gap vs Risk Analysis**

- There should be two distinct sets: no problem with Gap, but why Risk?
- Identifying important assets.

➤ **Policies**

- Simple policies exist, but there is no organisation, little awareness, and no enforcement.

Case Study: Law Firm

Solutions

- **Resource**
 - Virtual Information Security Office was offered by YZZ.
 - Project management reserved several days.
- **Development of Documentation**
 - They provided significant library assistance, but correct integration was still required.
 - Meetings were facilitated so that information could be documented.

Case Study: Law Firm

(Continued)

➤ **Gap vs Risk Analysis**

- YZZ performed a Gap Analysis.
- Organised a meeting

➤ **Policies**

- Meetings with HR were scheduled to get the Policies on track, adopted, distributed, and enforced.

Module 11:

Risk Assessment and

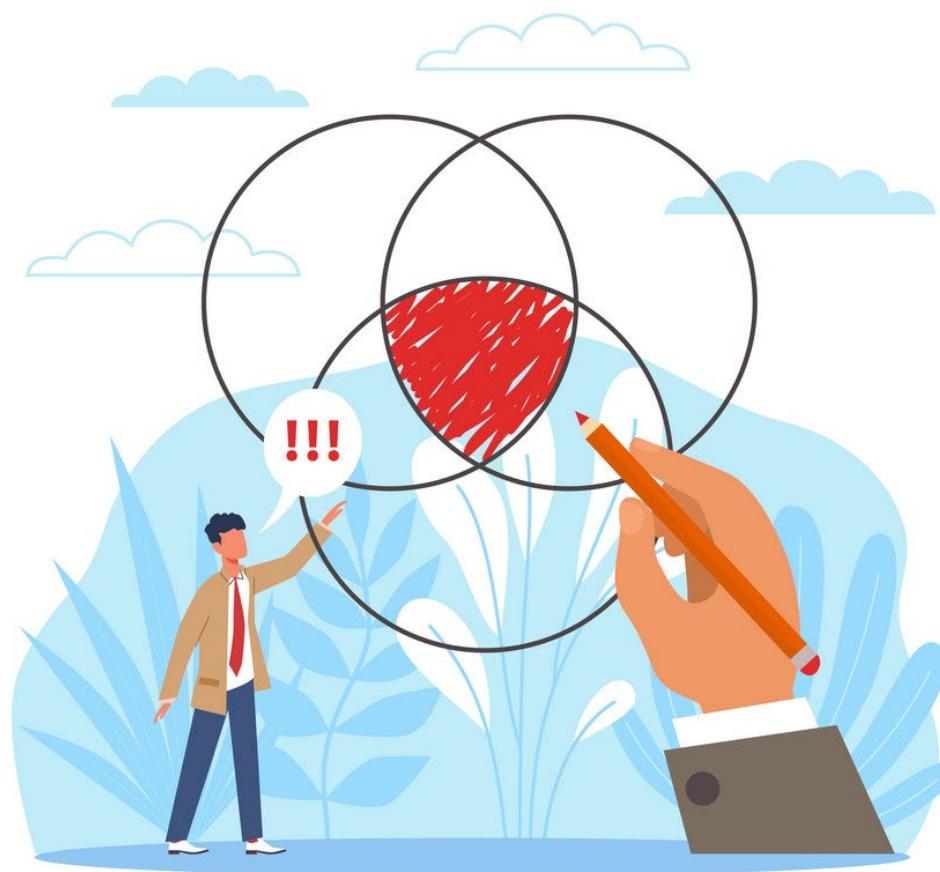
the Statement of

Applicability (SOA)



Risk Assessment

- The risk assessment helps an organisation to recognise, analyse and assess vulnerability in their information security processes.
- It is a central part of ISO 27001, the international standard which describes best practice for maintaining and implementing an Information Security Management System (ISMS).



Risk Assessment

(Continued)

- It is vital to that process, assisting the organisation in the:
 - Understand the particular situations in which their data can be compromised.
 - Evaluate the damage every situation can cause.
 - Determine how possible such situations are to occur.

Conducting Risk Assessments

- For risk assessment of ISO 27001 to be successful, it is required to reflect the view of an organisation on risk management, and it should produce consistent, valid, and comparable results.
- The risk assessment procedure must be detailed and explain who is liable for each task, how they should be completed, and in what order.



Conducting Risk Assessments

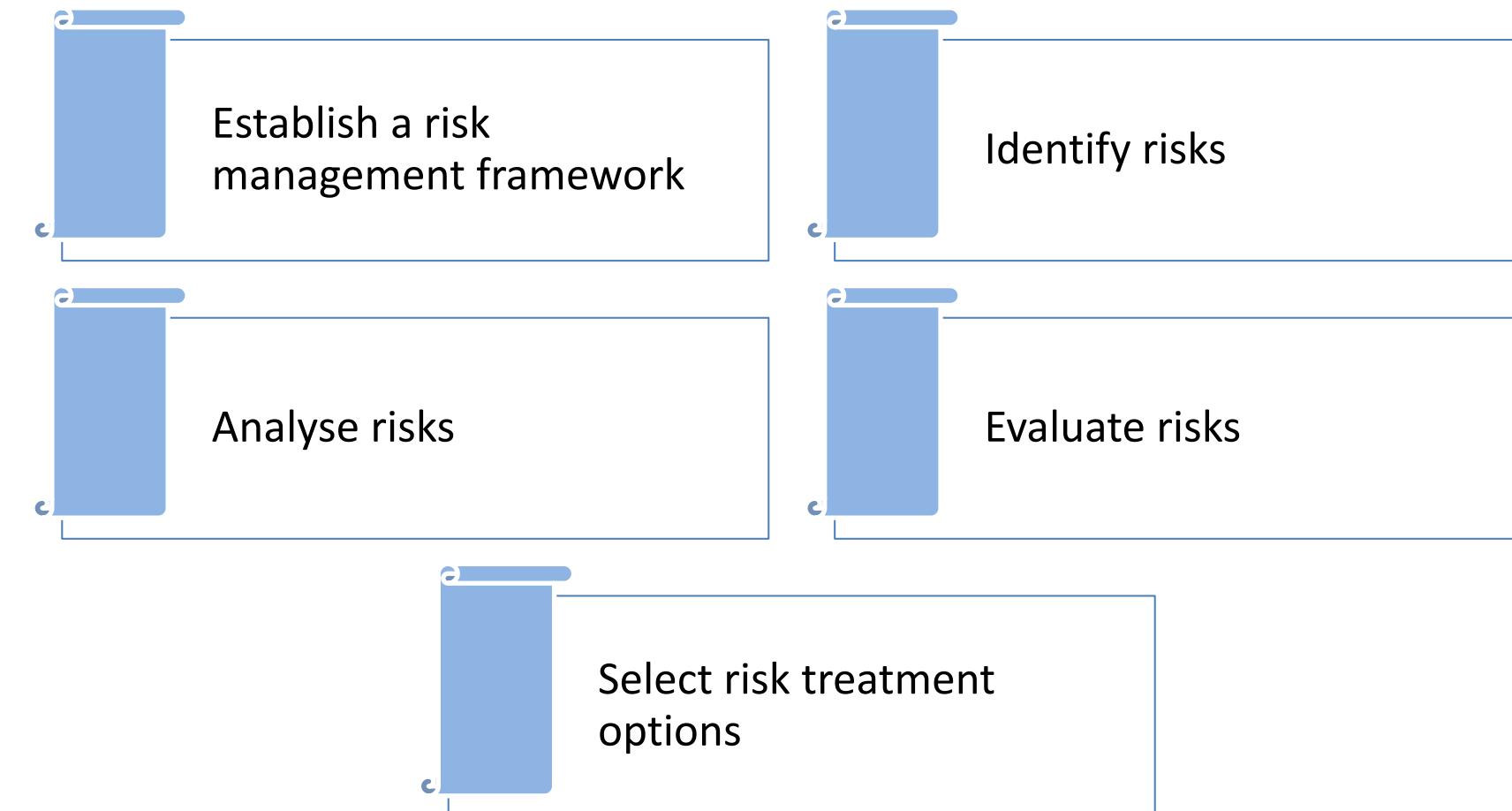
(Continued)

- This could be a daunting task for many. Inexperienced assessors frequently trust spreadsheets, spend hours interviewing individuals in their organisation, exchange methodologies and documents with other departments and do data filling.
- They would probably realise that spreadsheets are quite inconvenient as
 - They are error-prone
 - Hard to maintain.
 - They do not automatically conform to ISO 27001.
 - It is not easy to find relevant data in multiple tabs.

Conducting Risk Assessments

(Continued)

- Five steps to conduct a successful risk assessment:



Risk Assessment Methodology

Risk Assessment Methodology

- Define an overarching risk management approach for the entire organisation
- Qualitative or quantitative?
- Qualitative risk assessment scales?
- Define acceptable levels of risk

Risk Assessment Methodology

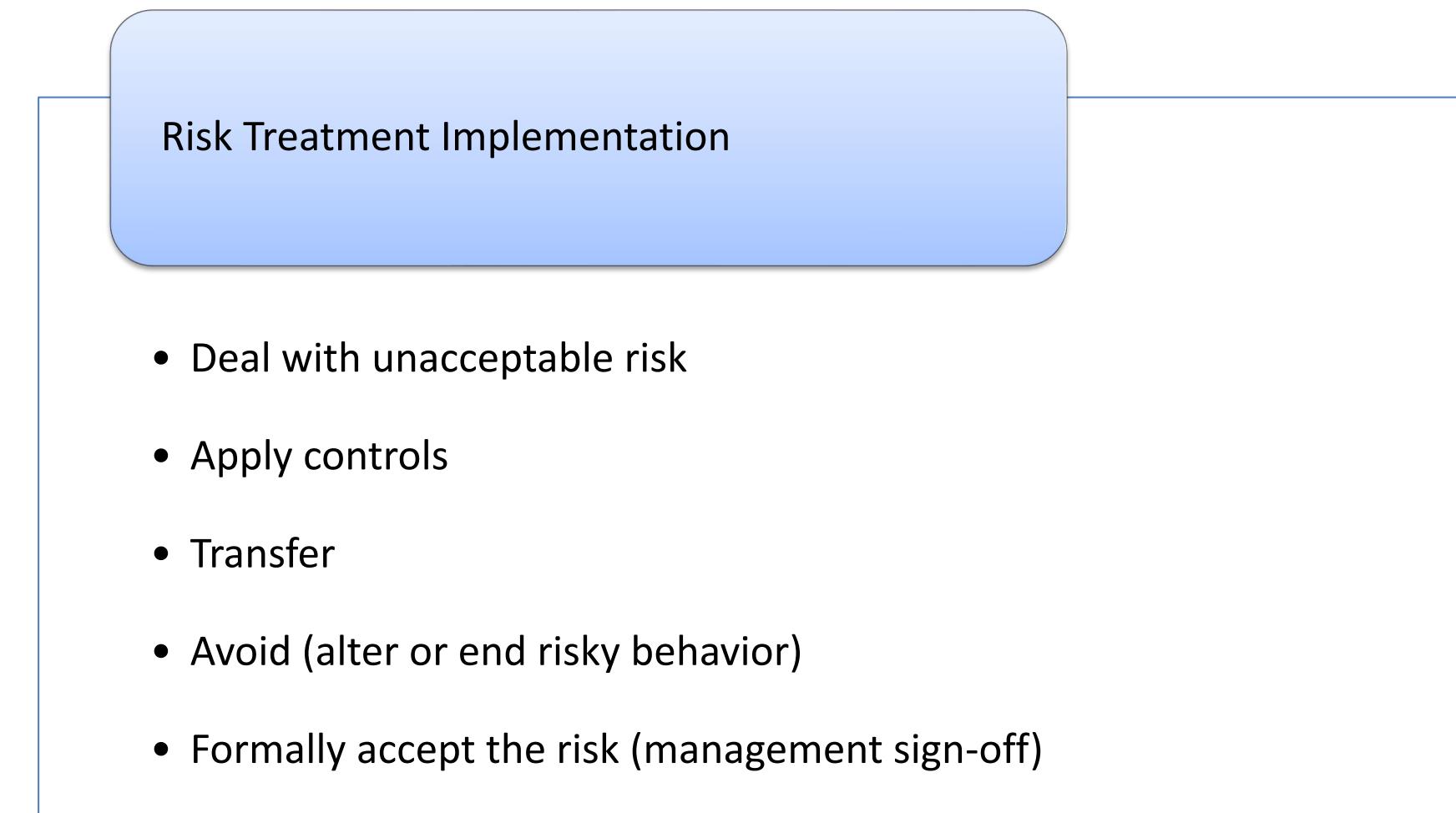
Risk Assessment Implementation

Risk Assessment Implementation

- Inventory all assets, threats to, and vulnerabilities of each
- Assess the impact and likelihood for each combination of assets/threats/vulnerabilities (chains of dependency)
- Calculate the level of risk

Risk Assessment Methodology

(Continued)



ISMS Risk Assessment Report

- Getting the risk assessment process right is essential, but you should remember that it is the first step to adequate security.
- You should report on findings and implement an action plan once you have completed the assessment.
- You should produce various reports based on risk assessment for certification and audit processes. The below two are the most essential:



ISMS Risk Assessment Report

1. *SOA (Statement of Applicability)*

- As an auditor, the SOA serves as the primary guide for auditors, covering all aspects of Annex A.
- The SOA is based on the Risk Treatment Plan results and represents the organisation's security profile.
- It identifies the organisation's information security objectives and controls and defines appropriate rules.

ISMS Risk Assessment Report

(Continued)

- Addresses residual risks.
- Records formal approval for implementation of the described controls.
- It must be reviewed on a defined and regular basis.
- Used to demonstrate to third parties the degree of security that has been implemented.

ISMS Risk Assessment Report

(Continued)

- An auditor must ensure there is evidence that ISMS controls are in operation rather than just part of policy.
- Look for evidence of incidents that have been confirmed and addressed through the necessary processes.
- Information security management processes must be proved to exist.

ISMS Risk Assessment Report

(Continued)

- There are some steps which help to develop an effective ISO 27001 SoA:



ISMS Risk Assessment Report

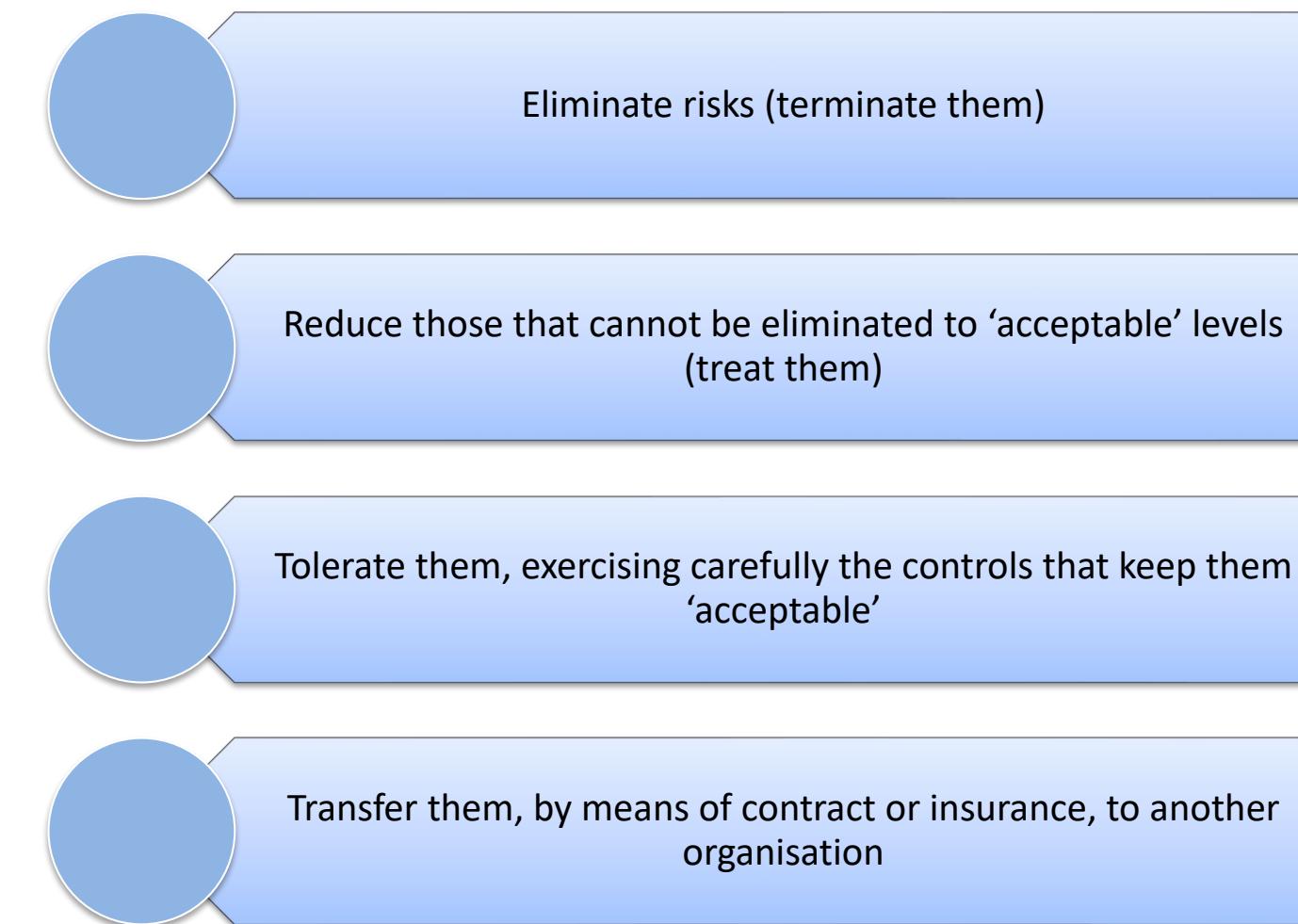
2. RTP (*Risk Treatment Plan*)

- ISO27001 Clause 6.1.3 requires the organisation to formulate a risk treatment plan.
- This plan should identify the appropriate management action, responsibilities, and priorities for managing information security risks.
- The risk treatment plan should be documented.
- This plan should be set within the organisation's information security policy.
- It should identify the organisation's approach to risk and its criteria for accepting risk.
- These criteria should be consistent with the requirements of ISO 27001.

ISMS Risk Assessment Report

Objectives of Risk Treatment Plans

- Risk treatment plans have four linked objectives, which are:



Threats and Vulnerabilities

Threats

- Threats could exploit vulnerabilities of an information asset or group of information assets, thereby causing harm to an organisation.
- Threats are things that can go wrong or can ‘attack’ the identified assets.
- Threats can be either external or internal.
- Threats vary according to the industry and the scope of the ISMS.



Threats and Vulnerabilities

Vulnerabilities

- Vulnerabilities leave open systems to attack by something classified as a threat or allow an attacker to have some success or more significant impact.
- A threat can exploit a vulnerability.



Threats and Vulnerabilities

(Continued)

- Vulnerability Assessment Tools:
 - Vulnerability assessment tools are also known as security scanning tools.
 - It plays a role in many information security management systems, and its position is determined by the risk treatment plan which arises from the risk assessment.
 - They assess the security of network or host systems and report system vulnerabilities.
 - These tools are automated and designed to scan networks, firewalls, servers, routers and software applications for vulnerabilities.
 - In evaluating a vulnerability assessment tool, consider how frequently it is updated to include the detection of new weaknesses, security flaws and bugs.

Threats and Vulnerabilities

(Continued)

- Vulnerability assessment tools are not usually run in real-time but are commonly run periodically.
- The tools can generate technical and management reports, including text, charts, and graphs.
- Vulnerability assessment reports can classify what weaknesses exist and how to fix them.

Module 12: Roles and Responsibilities of a Lead Implementer



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.



Roles and Responsibilities

(Continued)

- ✓ The Lead Implementer ensures the project is implemented within contractual obligations and regulatory requirements is another responsibility.
- ✓ The Lead Implementer will be responsible for managing multiple client projects simultaneously.
- ✓ They will also be responsible for participating in internal projects as needed.



Roles and Responsibilities

(Continued)

- ✓ 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.



Case Study: ABC's ISO 27001

- Despite their success in delivering best-in-class, ABC, a seasoned team of highly qualified scientific and Quality Assurance professionals, recognised that ISO 27001 was outside their area of expertise.
- So they sought assistance from XYZ. The bioanalytical laboratory ABC specialises in large molecule bioanalysis and works with sponsors to create and provide biological discoveries that have the potential to change the world.

Case Study: ABC's ISO 27001

The Outcome

- It would be an understatement to say that ABC's ISO certification journey was successful; not only did they finish it much faster than the moderate consumer, but they also had no control failures in their stage 2 process.
- ABC was able to grasp what documents and evidence auditors would be looking for with the assistance of XYZ's platform.
- Ultimately, everything was organised and delivered to their auditor on time, removing the requirement for unneeded or time-consuming interactions.

Case Study: ABC's ISO 27001

The Challenge

- A frequent request for information about security and controls comes from ABC, a dependable partner to many of the world's leading pharma and biotech businesses.
- As is the case with any first-time pursuit, ABC had never attempted to comply with ISO 27001. Thus they had no idea what they did not know.
- Although they had policies in place, they were still determining which ones applied to ISO 27001 and which ones did not.

Case Study: ABC's ISO 27001

The XYZ Partnership

- The XYZ-ABC engagement started in July 2021, and by December 2021, both stages 1 and 2 had been finished by ABC.
- They obtained their ISO 27001 certification in January 2022, about 40–50% faster than the normal ISO engagement.
- Along with providing their usual services for customer success, XYZ also conducted an internal audit for ABC, evaluating their entire programme.

Module 13: Planning



Actions to Address Risks and Opportunities

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:
 - a) Make sure the information security management system can attain its intended result.
 - b) Avert, or decrease, undesired effects.
 - c) Attain continuous improvement.

Actions to Address Risks and Opportunities

(Continued)

- The organisation shall plan:
 - d) Taking steps to address these risks and opportunities; and
 - e) How to:
 1. Integrate and execute these actions into the processes of its information security management system; and
 2. Assess the efficacy of these actions.

Actions to Address Risks and Opportunities

2. *Information Security Risk Assessment*

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

Actions to Address Risks and Opportunities

- c) The information security risks should be identified:
 - 1. 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
 - 2. The risk owners must be identified.
- d) Analyses the risks to information security:
 - 1. Evaluate the potential consequences if the identified risks were to materialise.
 - 2. Assess the realistic likelihood of the risks happening; and
 - 3. Determine the risk levels.

Actions to Address Risks and Opportunities

- e) Assesses the information security risks:
1. Compare the risk analysis outcomes to the risk criteria; and
 2. Prioritise the risks that have been analysed for risk treatment.
- The organisation shall keep documented information regarding the information security risk assessment process.



Actions to Address Risks and Opportunities

3. *Information Security Risk Treatment*

- An information security risk treatment process shall be defined and applied by the organisation that:
 - a) Select relevant information security risk treatment options, considering the outcomes of the risk assessment.
 - b) Determine all controls required to execute the chosen information security risk treatment option.
 - c) Compare the controls and verify that no essential controls have been left out.

Actions to Address Risks and Opportunities

- d) 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.
 - e) Create a plan for dealing with information security risks; and
 - f) 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:
 - a) Be in accordance with the information security policy.
 - b) Be quantifiable (if possible).
 - c) Consider applicable information security requirements, as well as risk assessment and risk treatment results.



Information Security Objectives and Planning to Achieve Them

- d) Be observed.
- e) Must be communicated.
- f) Be updated as needed.
- g) Be accessible as documented information.



Information Security Objectives and Planning to Achieve Them

(Continued)

- 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:
 - a) What will be completed.
 - b) What resources will be needed.
 - c) Who will be accountable.
 - d) When it will be finished; and
 - e) How the outcomes will be assessed.

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.



Module 14: Support



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

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

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

Documented Information

(Continued)

- Storage and preservation, involving legibility preservation
- Changes' in control
- Retention and disposal

Case Study: Implementing ISO 27001

The Client

- The client offers goods and services to the NHS and other clients in the healthcare industry. It is a minor subsidiary of a major international corporation.
- The client must have confidence that Patient Identifiable Data is adequately handled because they deal with it in electronic and paper-based formats.



Case Study: Implementing ISO 27001

The Problem

- To more effectively demonstrate that they have information security in place and to help with the conditions of the NHS Information Governance Toolkit, the client sought ISO 27001 accreditation.
- Although ISO 9001 was already in existence, it was understood that it would soon need to be updated to meet the revised standard.
- The client has little to no influence over, for example, the IT operations because the IT and other head office services are centrally located and based outside.

Case Study: Implementing ISO 27001

The Solution

- A thorough Information Security Management System (ISMS) was created by XY Solutions in close collaboration with the client and their quality consultant, allowing the client to move forward with certification.
- The ISMS was written in a way that simplified the primary documentation to include the quality-related requirements of ISO 9001:2015.
- Additionally, audit methods that would assure the client that centralised functions, including IT, were correctly adhering to their protocols and meeting the risk management and control needs were identified.

Case Study: Implementing ISO 27001

(Continued)

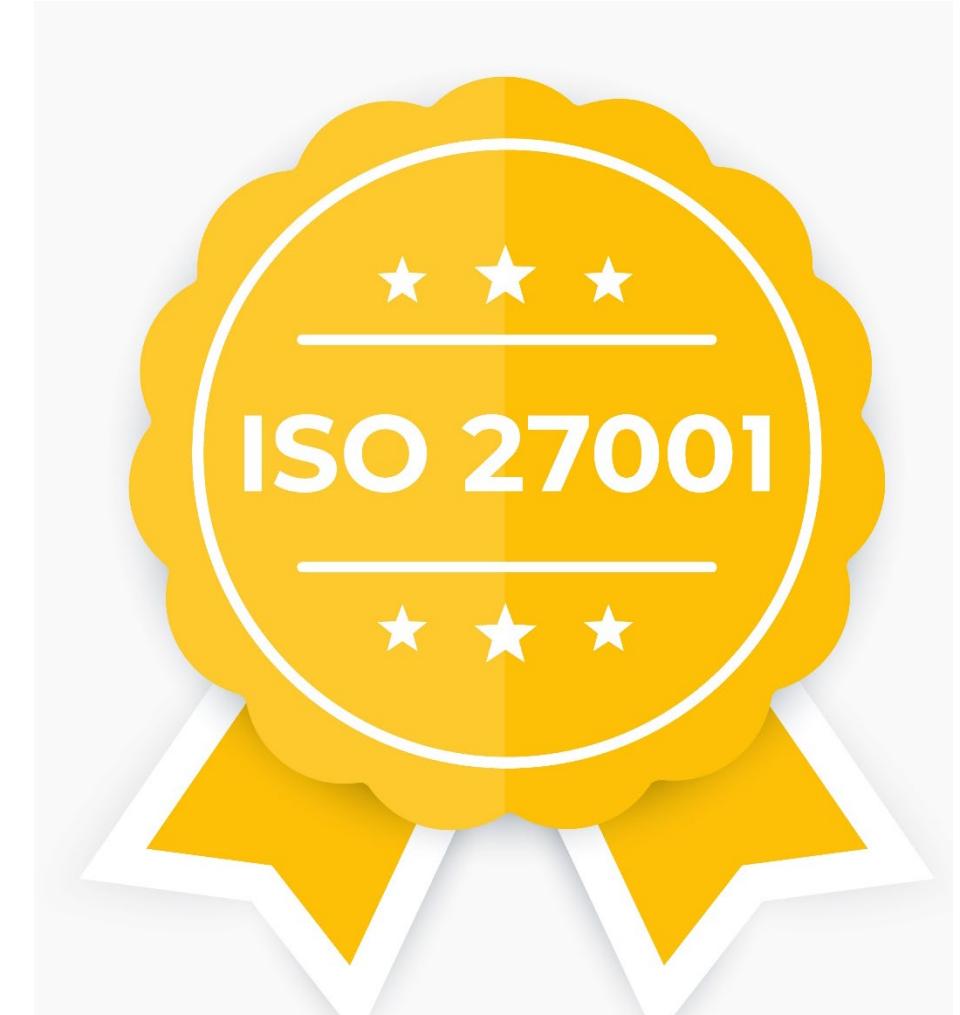


- When the customer was successfully accredited to ISO 27001, people were thrilled since it proved that information security is in place and is kept up to date.
- The tender process has also benefited from this, and it will continue to help the client if they wish to pursue a higher rating on the NHS Information Governance Toolkit.

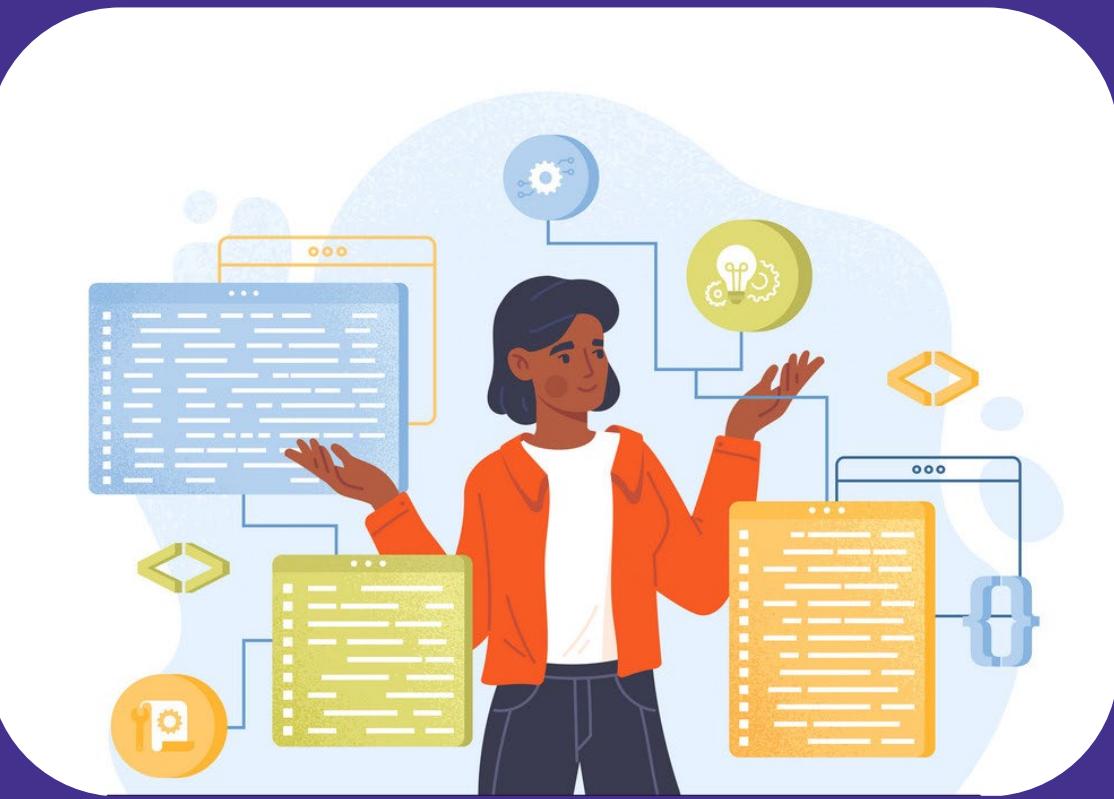
Case Study: Implementing ISO 27001

(Continued)

- Since then, XY Solutions has provided more assistance, such as advice on the controls the client should demand from vendors and potential outsourcing partners.
- Additionally, XY Solutions helped to update the processes for ISO 9001 certification and afterwards for ISO 22301 certification.



Module 15: Operation



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.

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.

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).

Module 16: Launch and Implement an ISMS in an Organisation



Apply the Frameworks

ISMS Frameworks

Step 1

Definition of Security Policy

Policy Document

Step 2

Definition of ISMS Scope

Scope of ISMS

Step 3

Input Examples
Threats, Impacts and Vulnerabilities

Risk Assessment

List of Assessed Risks

Step 4

Risk Management Strategy

Risk Management

Identified weakness for Assets

Step 5

Additional Controls

Selection of Controls

Strength of Control and implementations

Step 6

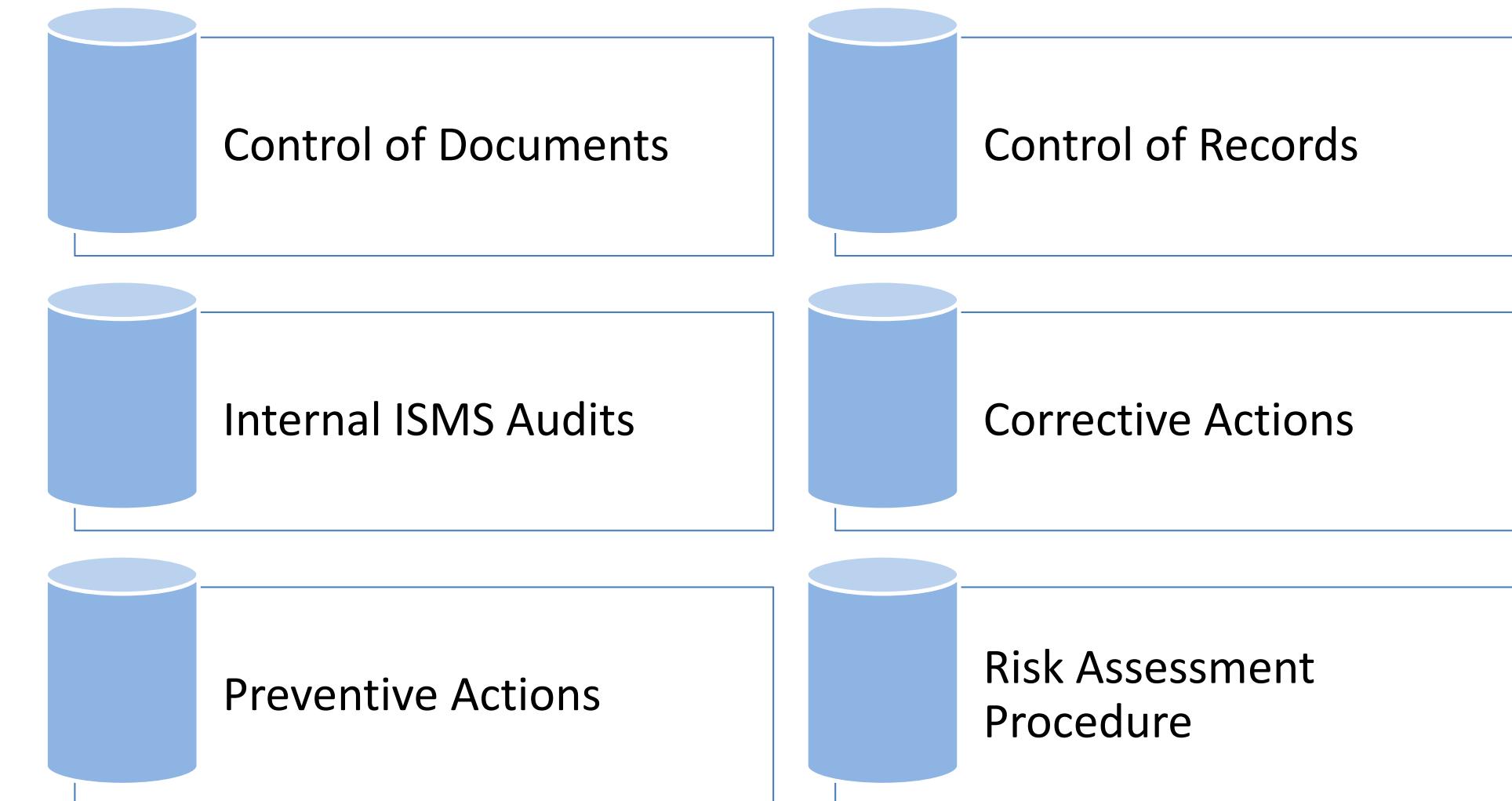
Statement of Applicability

Statement of Applicability Document

Procedures and Controls

Procedures

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



Procedures and Controls

(Continued)

- 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

Monitoring of Use of Information System

Review of User Access Rights

Procedures and Controls

(Continued)

Acceptable Use of Assets

Acceptance Criteria for New Info System

Software Change Control

Incident Management including Reporting

Control against Malicious Software

Information Labelling & Handling

Procedures and Controls

(Continued)

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

Procedures and Controls

Controls

- Each clause of Annex A deals with one or more security categories, and each security category has a control objective and one or more controls that will serve to secure that objective.
- The clauses, security categories, control objectives, and control names are explained in the slides that follow, as well as the detailed control requirements that are contained in the standard.

Procedures and Controls

(Continued)

- ***There are following controls:***

- Annex A.5 – Information Security Policies
- Annex A.6 – Organisation of Information Security
- Annex A.7 – Human Resource Security
- Annex A.8 – Asset Management
- Annex A.9 – Access Control
- Annex A.10 – Cryptography
- Annex A.11 – Physical & Environmental Security

Procedures and Controls

(Continued)

Annex A.12 – Operations Security

Annex A.13 – Communications Security

Annex A.14 – System Acquisition, Development & Maintenance

Annex A.15 – Supplier Relationships

Annex A.16 – Information Security Incident Management

Annex A.17 – Information Security Aspects of Business
Continuity Management

Annex A.18 – Compliance

Implementing the Controls

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

Asset Identification and Valuation

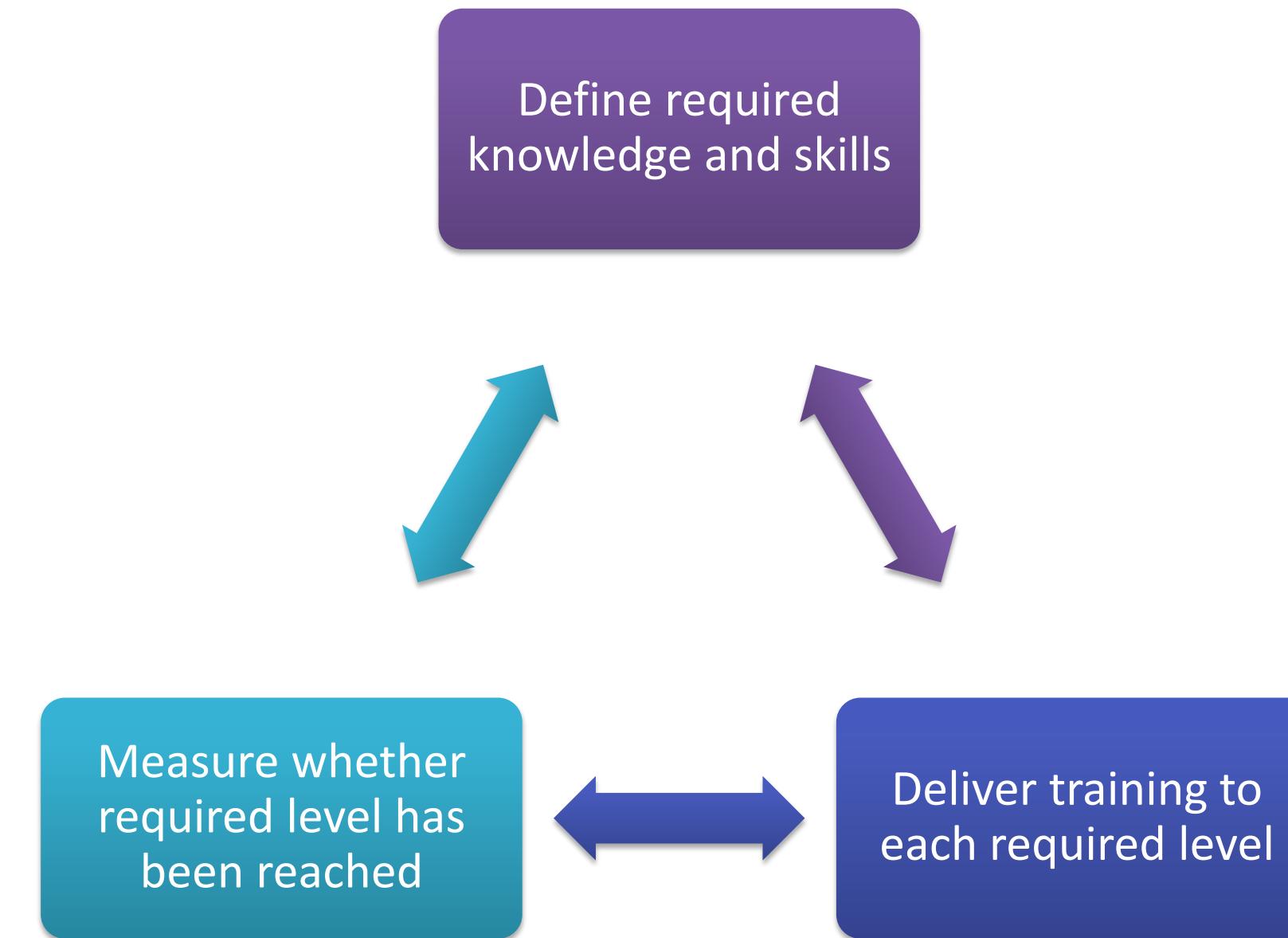
Conduct a Detailed Risk Assessment

Establish the ISMS

Training and Awareness Programme

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

Training Cycle



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.



Training and Awareness Programme

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.

Training and Awareness Programme

(Continued)

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

Training and Awareness Programme

(Continued)

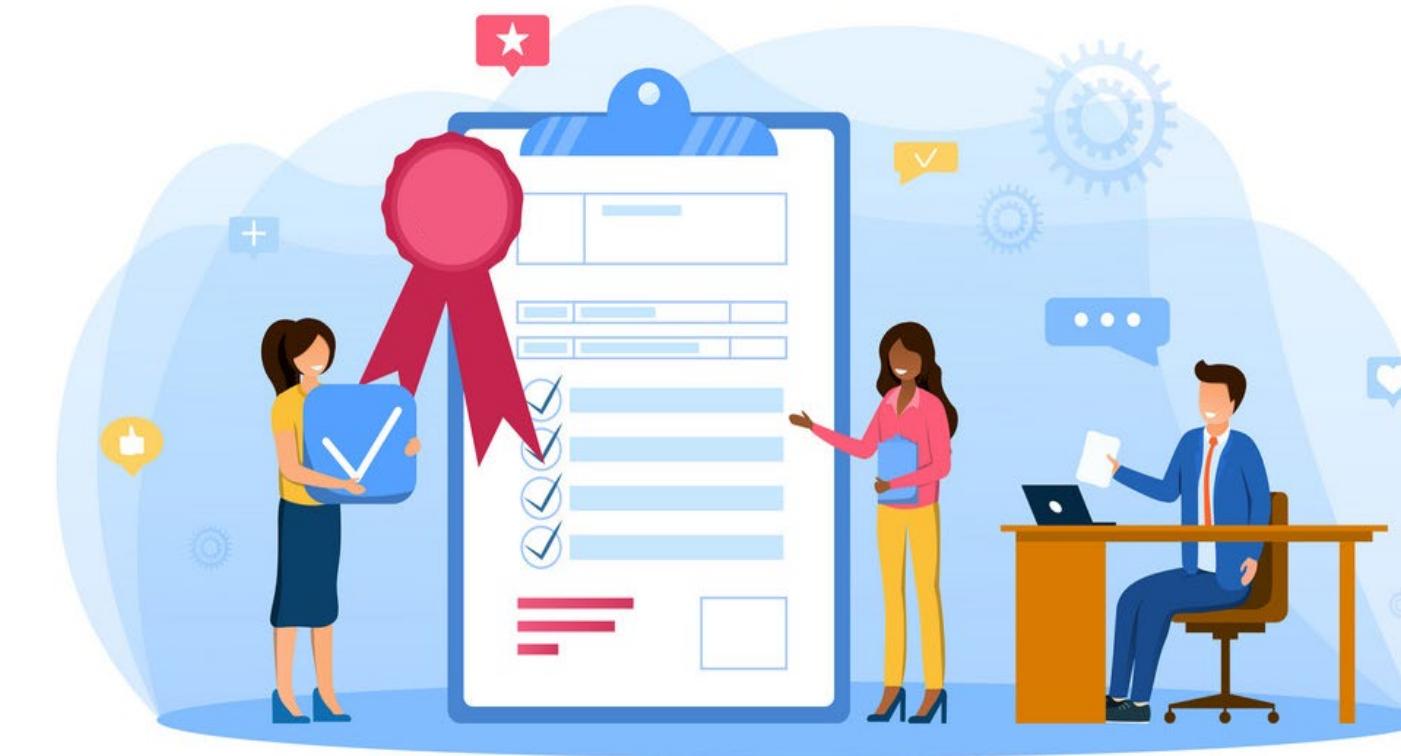
Videos are a very powerful presentation method, as we can distribute them via email, through the intranet, etc.

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

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.



Management's Role

(Continued)

- 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.



Management's Role

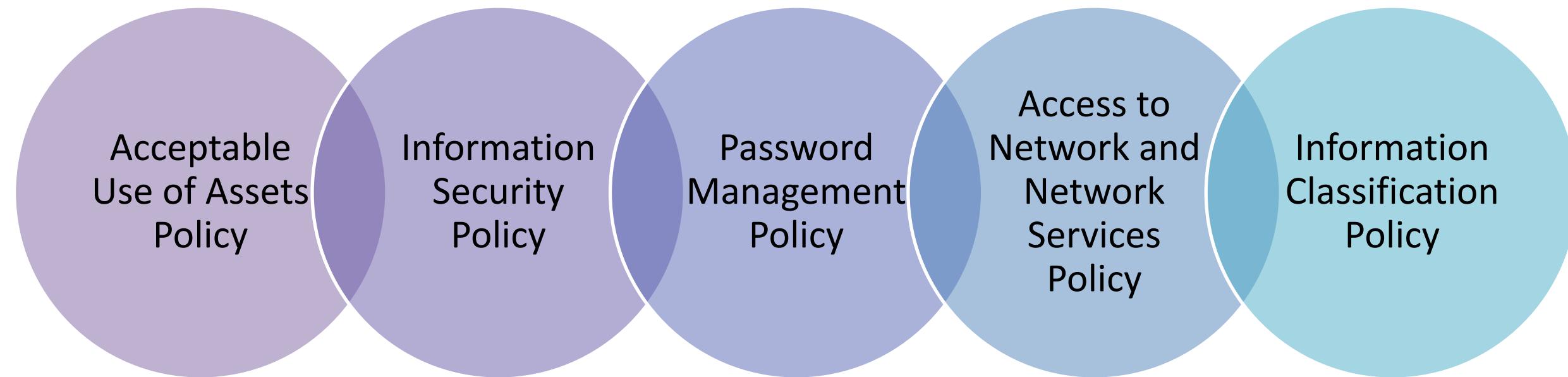
(Continued)

- 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.



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:



Module 17:

Introduction to ISO 27001 Lead Auditor



Qualifications of an Auditor

Experience

- Auditor requirements should be set based on the number of days spent performing internal audits of ISO 27001.
- An internal auditor should also have experience as a consultant in implementing the ISO 27001 standard.
- In this case, a requirement could be established that they should have participated in the least of 2-3 implementation projects.



Qualifications of an Auditor

(Continued)

- Project and personnel management experience (scheduling, time management, budgeting, etc.).
- Business management experience is recommended to understand an organisation's situation and goals.
- Experience delivering training/awareness courses for ISO 27001 is useful.



Qualifications of an Auditor

Knowledge

- Having knowledge about ISO 27001 and information security is necessary.
- This knowledge can be developed through training courses.
- It is highly recommended that the auditor has completed an ISMS Lead Auditor course. It would also be helpful if they had completed an ISMS implementer training course.



Qualifications of an Auditor

(Continued)

- Knowledge of other information security standards/frameworks/regulations is not necessary but useful.
- Knowledge of the advantages and disadvantages of qualitative and quantitative risk assessment/analysis.



Qualifications of an Auditor

Soft Skills

- They must have high ethical standards and integrity and be beyond reproach.
- Able to make use of negotiation skills.
- A pragmatic outlook.
- Very organised and motivated.



Qualifications of an Auditor

(Continued)

- Able to work under stress and with frequent interruptions.
- Able to deal with conflict effectively.
- A capable communicator can explain information security issues in both a written and verbal manner.



Conformance and Compliance

- Conformance can be defined as choosing to do something in a recognised way following standards (e.g. ISO 9001) or recognised methods (e.g. agreed test methods for ring tests under ISO 17025).
- Compliance is “doing what is told”, i.e. abiding by the law and meeting legislative requirements.
- If someone mandates to meet the requirements of a standard or test method, then conformance becomes compliance.

Conformance and Compliance

(Continued)

- These are the following differences between Conformance and Compliance:

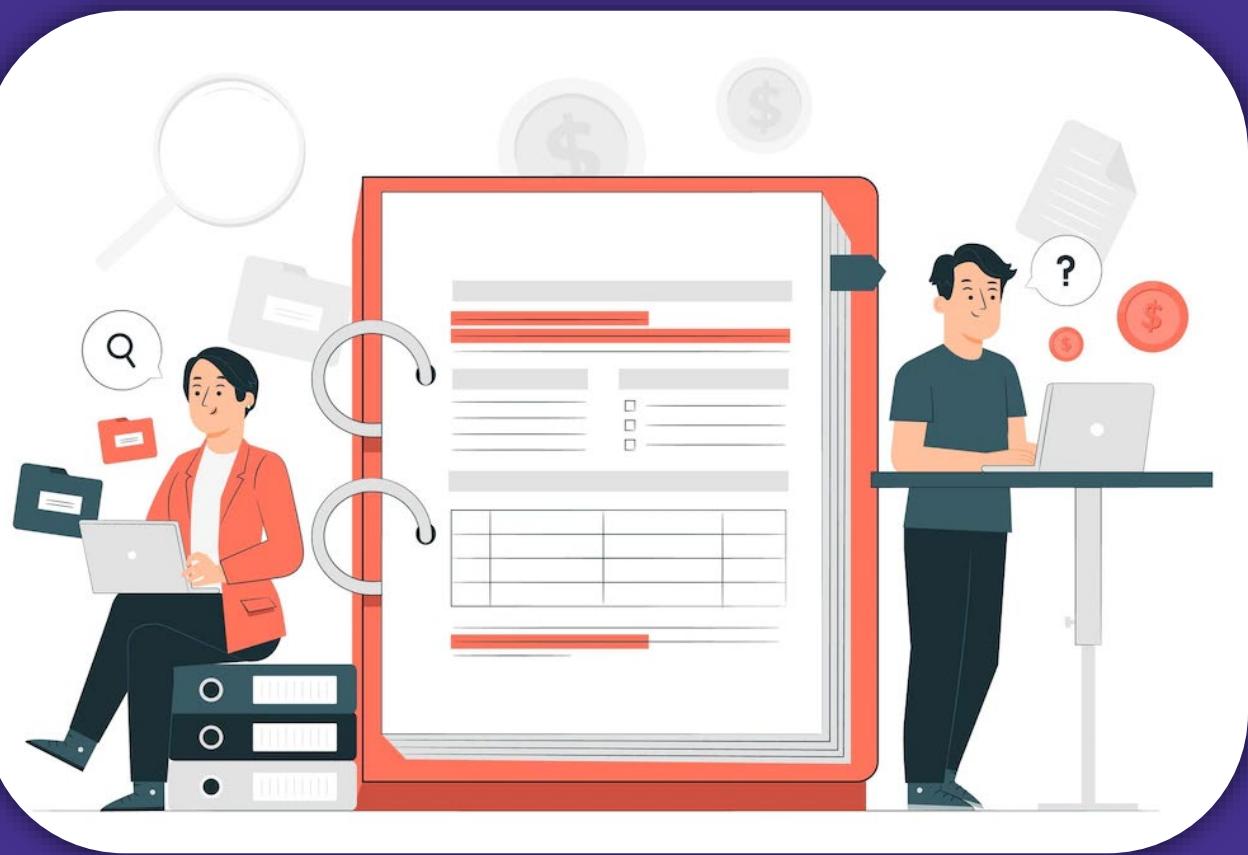
Conformance	Compliance
<ul style="list-style-type: none">• Basic starting point.	<ul style="list-style-type: none">• More detailed, systematic application of standards.
<ul style="list-style-type: none">• Achievable at low cost.	<ul style="list-style-type: none">• Implementation of ISMS with information security controls.
<ul style="list-style-type: none">• Generalises which standards will be applied and to what extent.	<ul style="list-style-type: none">• Specifies which standards are required to be met.

Conformance and Compliance

(Continued)

Conformance	Compliance
<ul style="list-style-type: none">Limited reassurance to third parties about security status of the company.	<ul style="list-style-type: none">Can assure third parties with limited obligation for proof.
<ul style="list-style-type: none">Has little meaning without more detail.	<ul style="list-style-type: none">Conformance becomes more informed and obligatory.

Module 18: Tasks of an Auditor



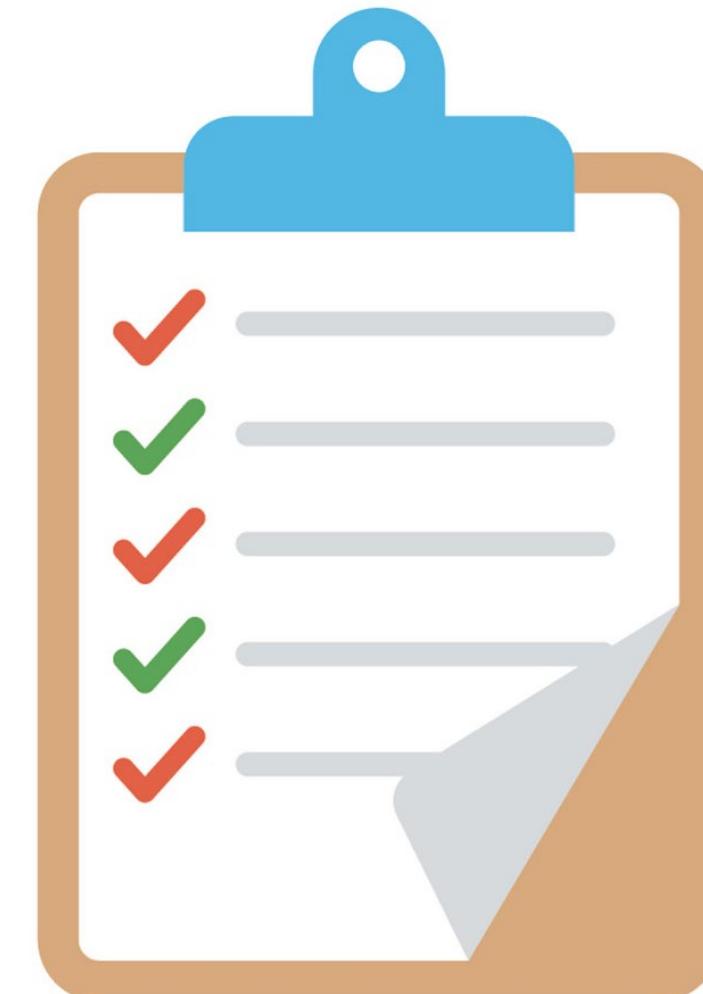
Preparing Audit Plans and Checklists

- One of the tools available in the audit checklist, helps to ensure that audits address the necessary requirements.
- It serves as a reference point before, during, and after the audit process, and if developed and used correctly for a specific audit process, it will provide the following benefits:
 - ✓ Ensures the audit is conducted systematically.
 - ✓ Promotes audit planning.
 - ✓ Ensures a consistent audit approach.

Preparing Audit Plans and Checklists

(Continued)

- ✓ Actively supports the organisation's audit process.
- ✓ Provides a repository for notes collected during the audit.
- ✓ Ensures uniformity in the performance of different auditors.
- ✓ Provides a reference to objective evidence.



Defining Targets

- Targets are typically set at 100%, and that is the standard in audits.
- Targets can be set below 100% for the following reasons:
 - In the event that national benchmarks are considered.
 - In the event that a target is in reference to an activity that does not take place.
- The table given below is an example of a framework to use in order to define a target:

Audit Criteria	Target	Exceptions	Source of Evidence
	100%		

Monitoring and Logging

Administrator and Operator Logs

- Privileges of administrators and operators of systems are different from normal users, meaning that they can perform more actions.
- Systems should register information on all users, regardless of privileges.

Clock Synchronisation

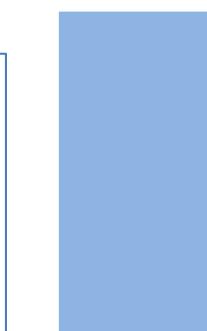
- All systems should be configured with the same time and date. If an incident occurs and a traceability test is required, difficulties arise when each system has a different configuration.

Monitoring and Logging

Benefits to Monitoring and Logging



Providing baselines, test results, and general IT insight.



The needs are met of stakeholders in an Audit.



The tools are on hand to resolve a complete range of IT issues.



Business risk is ultimately reduced through manager being able to detect and react to events.



Managers are also able to respond to process exceptions.

Monitoring and Logging

(Continued)

Compliance, risk management, and governance are all at the core of the information that monitoring and logging provide.

Performance indicators can be put in to place.

Log information can assist with managerial decisions by either approving or disproving them.

Log information can assist with security breaches by being used as evidence.

Handling Stressful Situations

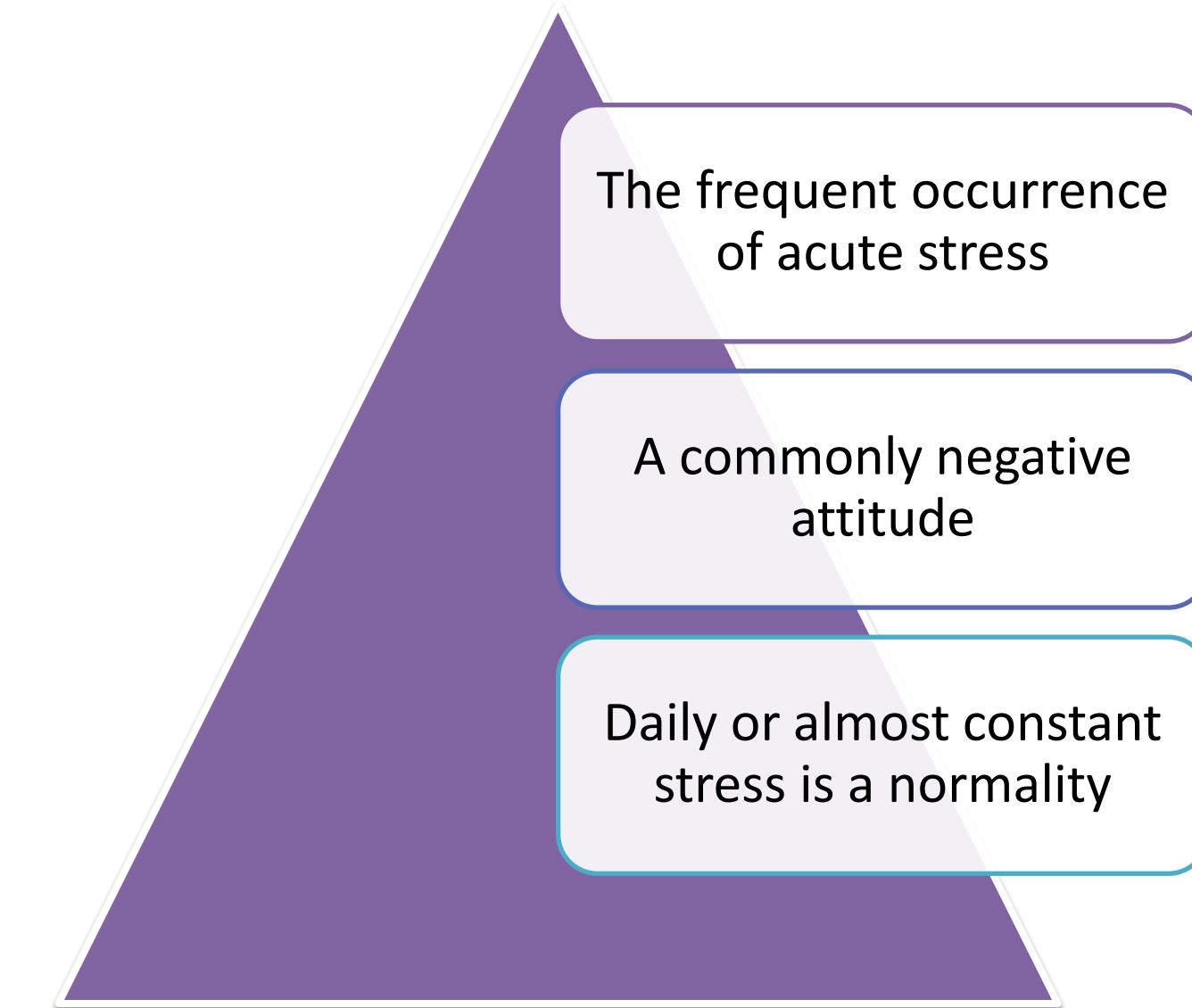
- Auditors must have the strength of mind, stability, and patience to be able to cope with and react to stressful situations effectively.
- An auditor requires a high degree of maturity, a good sense of humour, and understanding.
- The auditor must be aware that the outcome of the audit may result in angry/insulting outbursts from auditee personnel.



Handling Stressful Situations

Types of Stress

1. Episodic Acute Stress



Handling Stressful Situations

2. Chronic Stress

Constant stress with little to no gaps or relief.

Difficult factors that are a part of daily life; unhappy home life, stressful work life, finance or debt issues.

Handling Stressful Situations

Techniques of Stress Management

- The flowchart represents techniques of Stress Management:



Handling Stressful Situations

(Continued)

- The following are some ways used to incorporate clear communication and humour in times of high stress:
 - Ensure that all of the information used has a clear purpose.
 - Practice your delivery.
 - Avoid sarcasm or slapstick humour that may cause offence.
 - Try to practice inclusive humour – “we are all in this together” type humour.
 - Observational humour (surroundings/objects).

Intrusion and Penetration Testing

Intrusion Detection

- Intrusion detection often does not automatically identify an imminent attack in security.
- The level of ability in intrusion detection is typically examined in a security audit.



Intrusion and Penetration Testing

Penetration Testing

- Penetration testing is often used in security audits.
- Testing of this type is the deciding factor in a company or organisation's success in the prevention of intrusion.
- A penetration test, also called as a Pen Test, is an authorised cyber-attack that identifies exploitable susceptibilities on computer systems. Penetration tests imitate real attacks in order to extract accurate results.
- They are generally used to enhance a web application firewall in the context of web application security.

Intrusion and Penetration Testing

(Continued)

- They can involve the attempted breaching of any number of application systems, like frontend/backend servers and application protocol interfaces (APIs), to uncover susceptibilities.
- Automated or manual technologies are used to carry out penetration tests in order to methodologically weaken servers.
- Testers may endeavour to use the compromised system to launch successive exploits at other internal resources once susceptibilities have been effectively exploited on a system.
- The objective of penetration testing is to measure the probability of a system's compromise and assess any associated consequences.

Intrusion and Penetration Testing

Benefits of Penetration Testing

- A Penetration test involves stimulation of intrusions.
- Manual and Automatic tools will be used in Penetration testing.
- The manual tool is very useful, and they can uncover weaknesses that the automatic tools fail to do.
- The intrusions will consist of a variety of attack scenarios.

Intrusion and Penetration Testing

(Continued)

- ***Why Perform Penetration Testing?***
- These are the following are the reasons for penetration testing:

High costs following security infringements and other services disruptions.

Impossible to continuously protect all the data of a company.

Helps identify and highlight the major risks in the system.

Intrusion and Penetration Testing

1. *High costs following security infringements and other service disruptions*

- Security infringements and other service disruptions often mean the vulnerability of the business's information.
- This leads to financial costs, threatened reputation, in turn, losing customers due to low protection of their information, destructive press and even charges and penalties.



Intrusion and Penetration Testing

2. *Impossible to continuously protect all the data of a company*

- Businesses are known to create layers and layers of security mechanisms to protect all their systems.
- However, with the continued implementation of new technological systems, it is almost impossible to keep up security and locate the business's vulnerable areas.



Intrusion and Penetration Testing

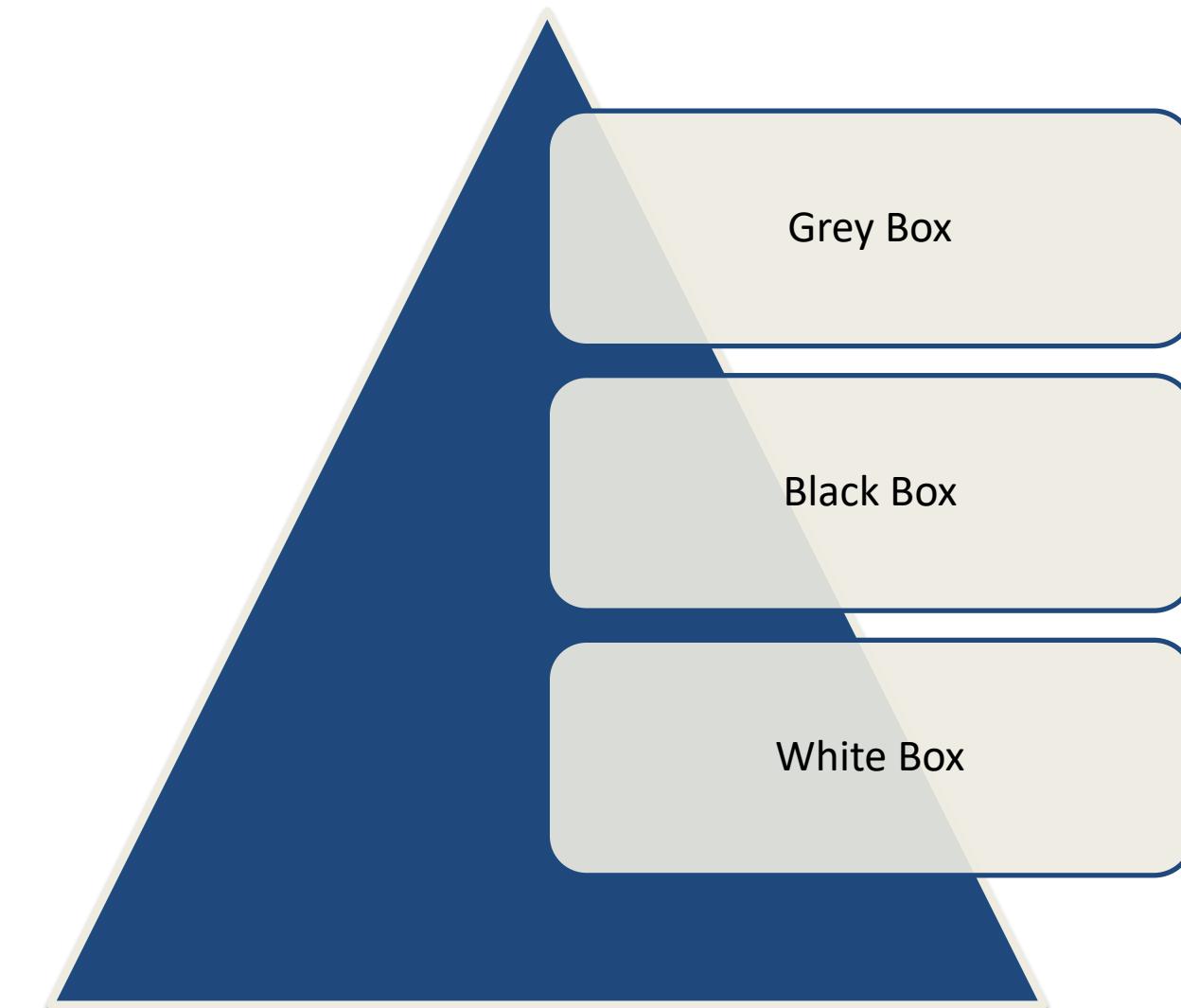
3. Helps identify and highlight the major risks in the system

- It is important to assess the business' capability to prevent attacks on their networks, applications, and user.
- Assessing them both externally and internally is important, as attacks can come from anywhere.



Intrusion and Penetration Testing

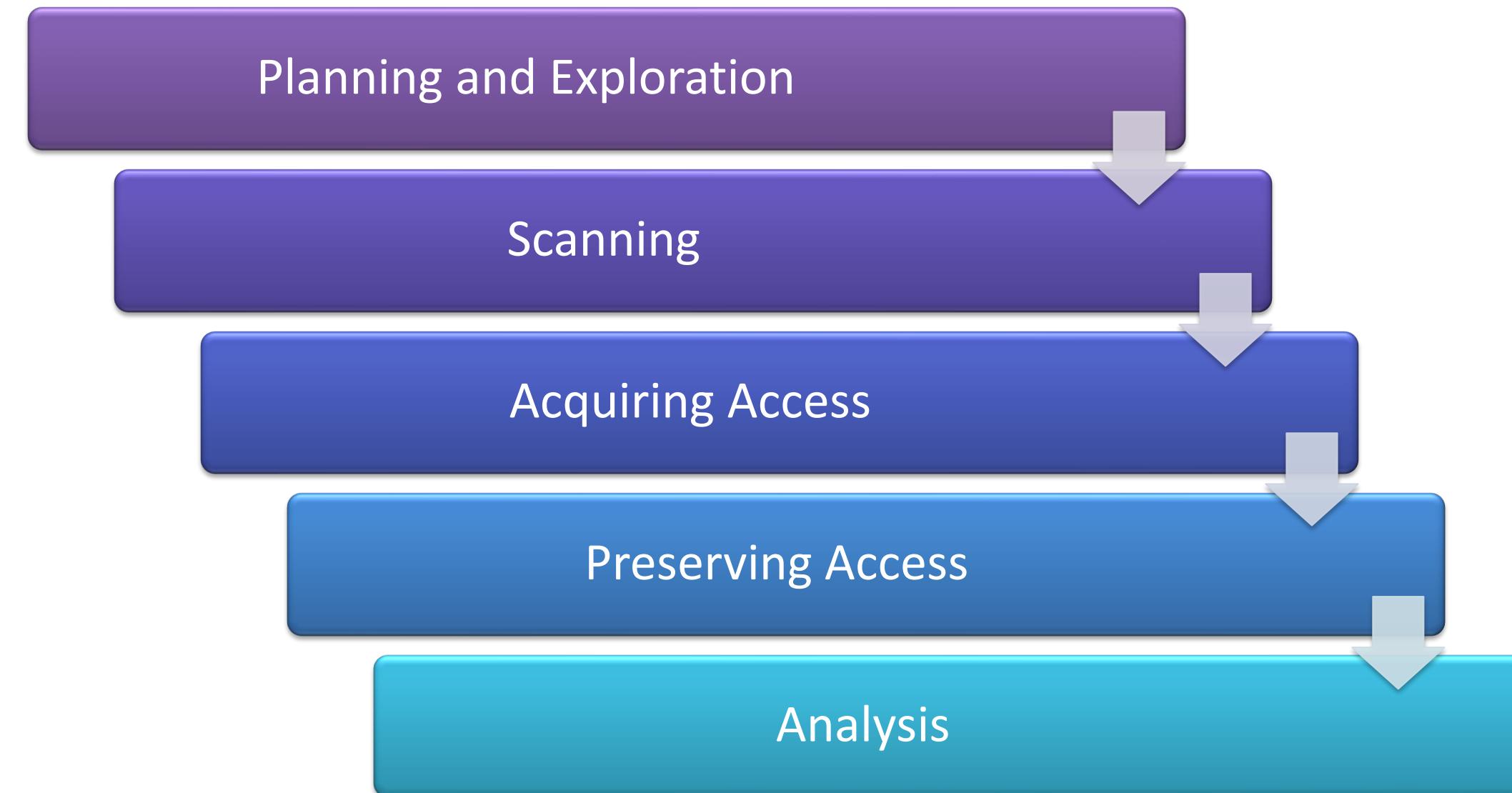
Types of Penetration Testing



Intrusion and Penetration Testing

The Penetration Testing Process

- The Penetration Testing process is made up of five stages:



Intrusion and Penetration Testing

Penetration Testing Methods

- The following are different penetration testing methods that can be used:

External Testing

Internal Testing

Blind Testing

Intrusion and Penetration Testing

(Continued)

Double-Blind Testing

Targeted Testing

Cloud and Virtualisation

Wireless Security

Inspection

Key Steps in the Audit Inspection Process



Inspection

1. *Planning*

- The planning process ensures execution of the inspection is efficient and effective.
- Planning consists of meeting with the firm to discuss the inspection process and requesting information from the firm related to audit quality and auditor independence.



PLANNING

Inspection

2. *Performance*

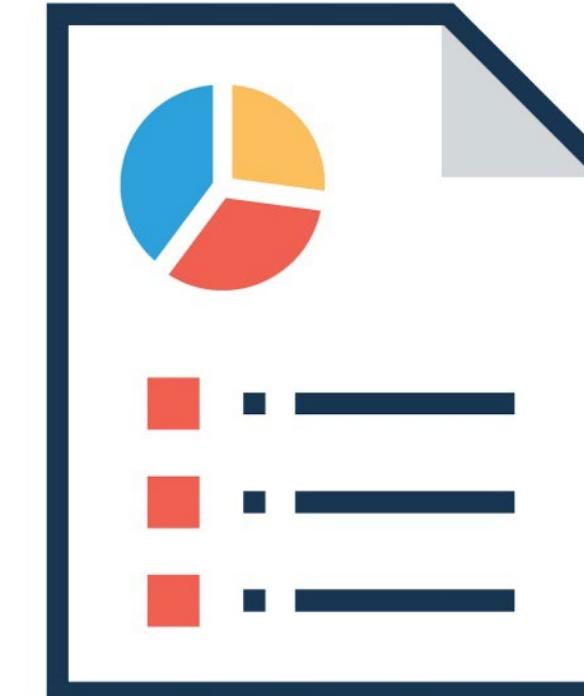
- The auditor reviews the notice material produced by the audit firm before commencing an onsite inspection.
- During the onsite phase, the auditor conducts interviews with audit firm personnel (leadership and staff) to clarify and confirm the audit quality and auditor independence policies and practices in place.



Inspection

3. *Reporting*

- The auditor prepares a private, confidential report for the firm describing the inspection process, observations, and findings, along with suggested corrective actions.
- The firm's response to the observations and findings is included in the final report.



Reporting Audits

- ***Audit Reporting includes:***

1. Review and analysis of findings.
2. Consolidation of all findings, including grouping and tabulation.
3. Classification of findings.
4. Preparation of recommendations



Reporting Audits

- ***Audit Reports Serve to:***

1. Facilitate corrective action.
2. Garner higher management support.
3. Offer managers insight into operations.
4. Gives an objective evaluation of performance.
5. Acts as a source of objective information on the current state.
6. Promotes standardisation.



Follow-up Actions

- Follow-up actions will be documented as an Observation or Opportunity for improvement statement.
- Recommendations that the auditor may provide an organisation with post-audit are not compulsory.
- Recommendations are advised, and the management can either follow them up or not.
- The actions to follow up on any advice must be decided upon by management.



Auditing Results

- ***Results of Internal or External Audits***

- ✓ The audit is one of the most effective tools in identifying opportunities for improvements since the outputs of the audit indicate whether a nonconformity or opportunity for improvement was detected.

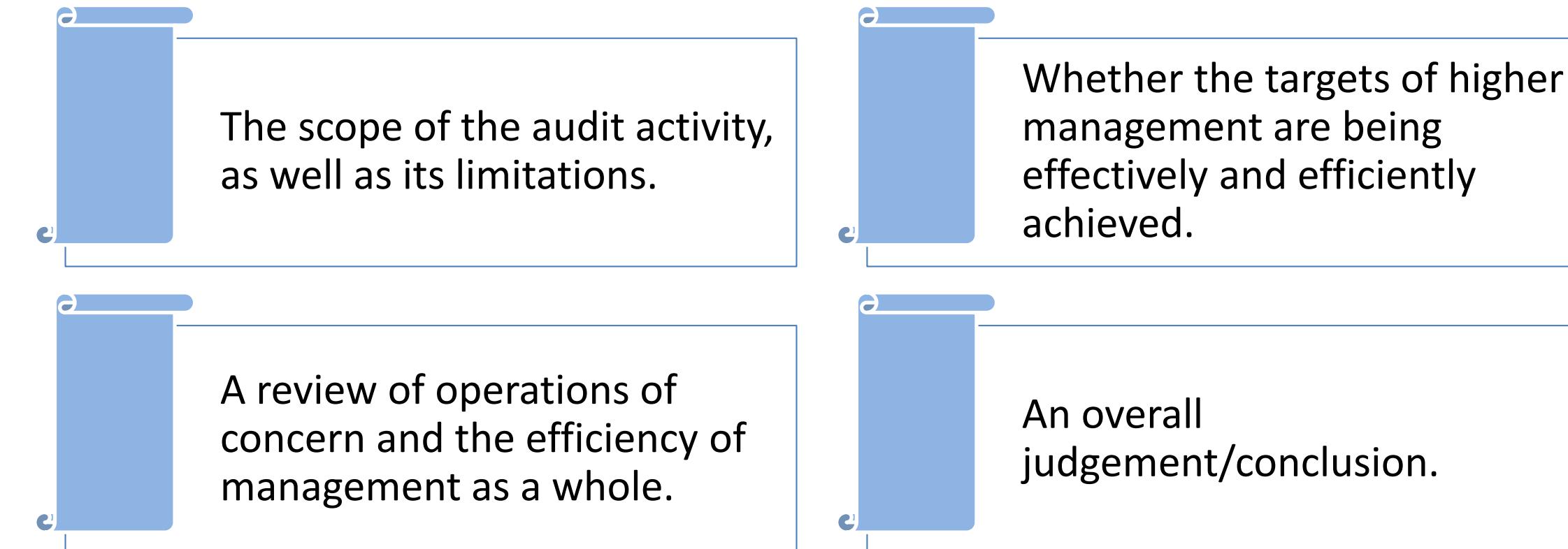
- ***Data Analysis***

- ✓ A quality activity that indicates the status of your quality management system in comparison to its objectives.



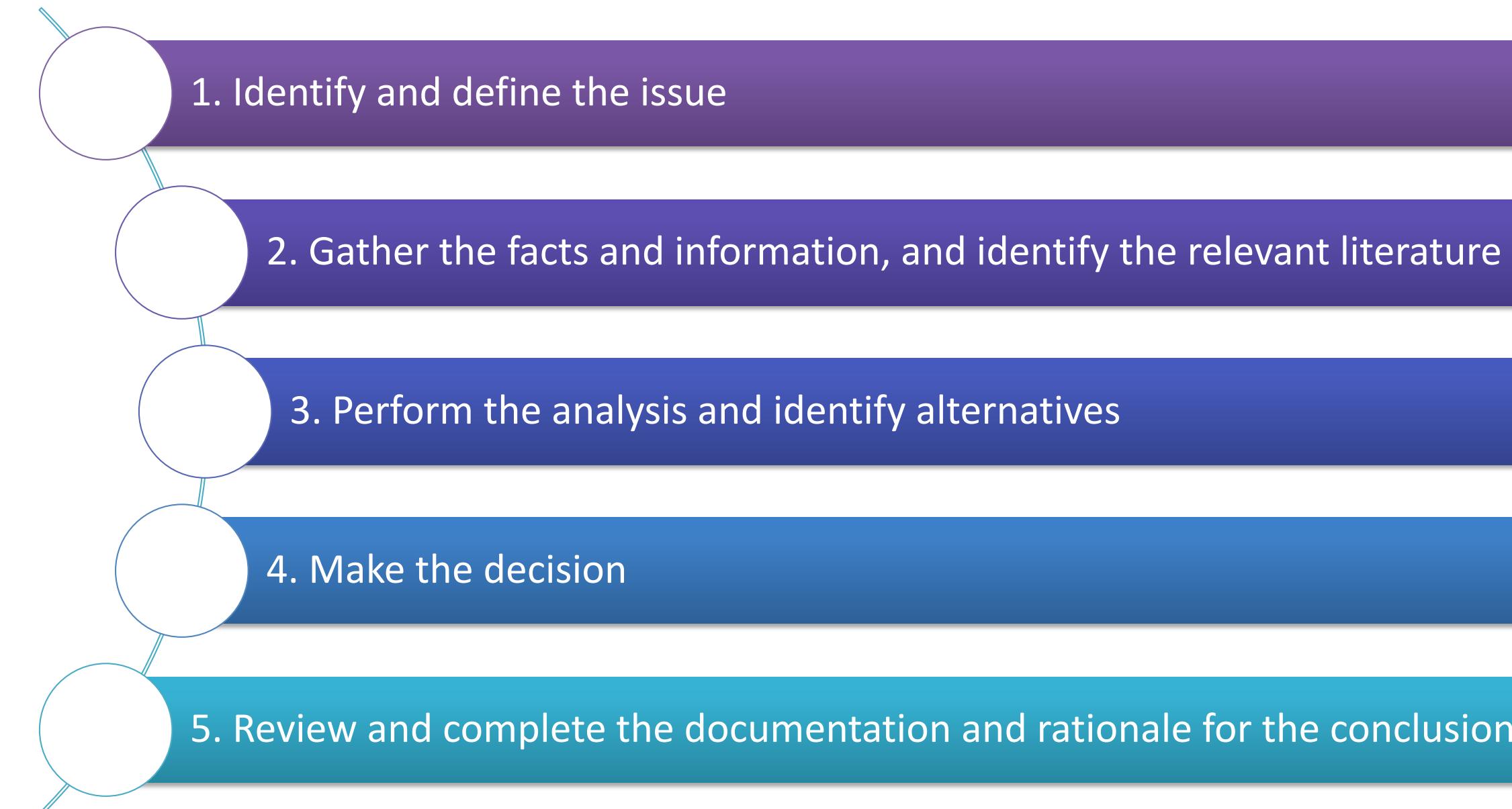
Submitting Reports to Higher Management

- *An auditor's reports to higher management should contain the following:*



Decision Making

- ***Below are the five basic actions that can help auditors in arriving at sound professional decisions:***



Module 19: Performance Evaluation



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:
 - a) What requires to be observed and measured involves information security processes and controls.
 - b) The methods to monitor, measure, analysis and evaluation to make sure valid outcomes, as applicable.



Monitoring, Measurement, Analysis, and Evaluation

- c) When the monitoring and measuring shall be carried out
- d) Who is responsible for monitoring and measuring
- e) When the monitoring and measurement must be analysed and assessed; and
- f) Who will analyse and assess these outcomes?
 - The organisation must keep appropriate documentation as proof of monitoring and measurement results



Internal Audit

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

Internal Audit

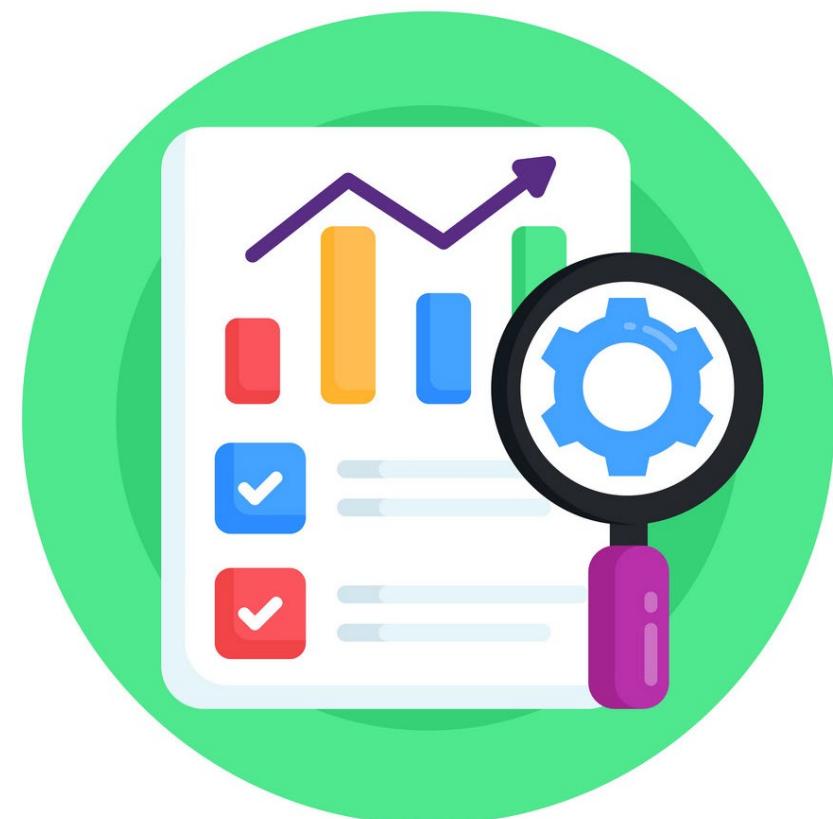
(Continued)

- 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.

Internal Audit

(Continued)

- Assure that the audit results are reported to the appropriate management.
- Keep documentation as evidence of the audit programme and the audit results.



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:
 1. Corrective and nonconformities actions
 2. Results of monitoring and measurement

Management Review

3. Audit results
4. Achievement of information security goals
 - 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.

Module 20: Improvement



Continual Improvement



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

Nonconformity and Corrective Action

- When a non-conformity happens, the organisation shall:
 - a) Respond to the non-conformity, and if necessary:
 - Take appropriate action to control and fix it, and
 - Deal with the consequences
 - b) 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.

Nonconformity and Corrective Action

- c) Execute any necessary action
- d) Review the efficacy of any corrective action taken.
- e) 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:
- f) The nonconformities' nature, as well as any subsequent actions, are taken.
- g) Any corrective action outcomes.



Congratulations

Congratulations on completing this course!

Contact Us

info@theknowledgeacademy.com

www.theknowledgeacademy.com/tickets

<https://uk.trustpilot.com/review/theknowledgeacademy.com>

theknowledgeacademy