Section 14

Documented information management

- Value and types of documented information
- Master list of documented information
- Creation of templates
- Documented information management process
- Implementation of a documented information management system
- Management of records

2.1 Documented Information Management

Examples of documented information that can be determined by the organization to be necessary for ensuring effectiveness of its ISMS are:

- *the results of the context establishment;*
- *the roles, responsibilities and authorities;*
- *reports of the different phases of the risk management;*
- *resources determined and provided;*
- *the expected competence;*
- *plans and results of awareness activities;*
- *plans and results of communication activities;*
- *documented information of external origin that is necessary for the ISMS;*
- *process to control documented information;*
- *policies, rules and directives for directing and operating information security activities;*
- *processes and procedures used to implement, maintain and improve the ISMS and the overall information security status;*
- *action plans; and*
- *evidence of the results of ISMS processes (e.g. incident management, access control, information security continuity, equipment maintenance, etc.).*

ISO/IEC 27001 Requirements

ISO/IEC 27001, clause 7.5.2

When creating and updating documented information the organization shall ensure appropriate:

a) identification and description (e.g. a title, date, author, or reference number);

b) format (e.g. language, software version, graphics) and media (e.g. paper, electronic); and

c) review and approval for suitability and adequacy.

ISO/IEC 27001 Requirements

ISO/IEC 27001, clause 7.5.3

Documented information required by the information security management system and by this document shall be controlled to ensure:

a) *it is available and suitable for use, where and when it is needed; and*

b) *it is adequately protected (e.g. from loss of confidentiality, improper use, or loss of integrity).*

ISO/IEC 27001 Requirements

ISO/IEC 27001, clause 7.5.3

For the control of documented information, the organization shall address the following activities, as applicable:

c) *distribution, access, retrieval and use;*

d) *storage and preservation, including the preservation of legibility;*

e) *control of changes (e.g. version control); and*

f) *retention and disposition.*

Documented information of external origin, determined by the organization to be necessary for the planning and operation of the information security management system, shall be identified as appropriate, and controlled.

NOTE

Access can imply a decision regarding the permission to view the documented information only, or the permission and authority to view and change the documented information, etc.

ISMS Documented Information

Types of documents

Describes the governance framework	Level 1	Policies, Statement of Applicability, scope statement, management review, and other strategic documents
Describes the processes, security controls, and procedures (who, what, when, how, where, and why)	Level 2	Description of the security processes, controls, and procedures
Describes in detail how the tasks and activities are conducted	Level 3	Worksheets, forms, checklists
Provides objective evidence of the compliance with the ISO/IEC 27001 requirements	Level 4	Records

ISMS Documented Information

Documented information required by ISO/IEC 27001

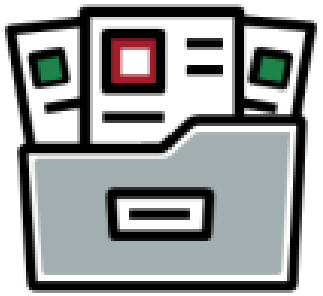
- ISMS scope (clause 4.3)
- Information security policy (clause 5.2)
- Actions to address risks and opportunities (clause 6.1)
- Information security objectives and plans (clause 6.2)
- Competence (clause 7.2)
- Operational planning and control (clause 8.1)
- Information security risk assessment (clause 8.2)
- Information security risk treatment (clause 8.3)
- Monitoring, measurement, analysis and evaluation (clause 9.1)
- Internal audit (clause 9.2)
- Management review (clause 9.3)
- Nonconformity and corrective action (clause 10.2)

- Terms and conditions of employment (control 6.2)
- Inventory of information and other associated assets (control 5.9)
- Acceptable use of information and other associated assets (control 5.10)
- Access control (control 5.15)
- Documented operating procedures (control 5.37)
- Confidentiality or non-disclosure agreements (control 6.6)
- Secure system architecture and engineering principles (control 8.27)
- Information security in supplier relationships (control 5.19)
- Response to information security incidents (control 5.26)
- Information security during disruption (control 5.29)
- Legal, statutory, regulatory and contractual requirements (control 5.31)

Value of Documented Information

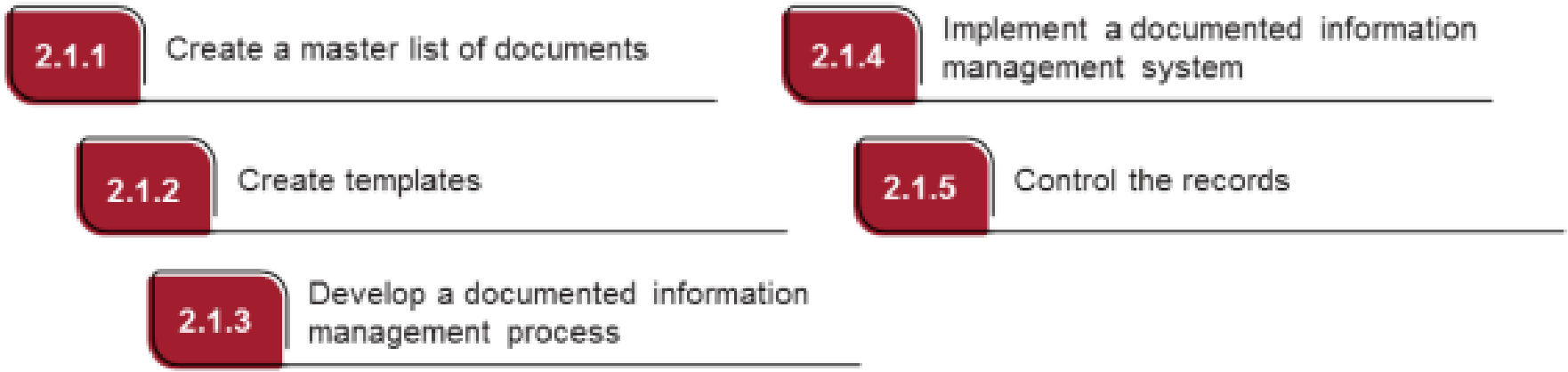
Important note

- The preparation of documents should not be a target itself. This must be a value-adding activity to the ISMS.
- Highly voluminous documented information is unnecessary because it is difficult to manage and, often, not understood by users.
- Each organization determines the necessary documented information and media for the communication of information.



2.1 Documented Information Management

List of activities

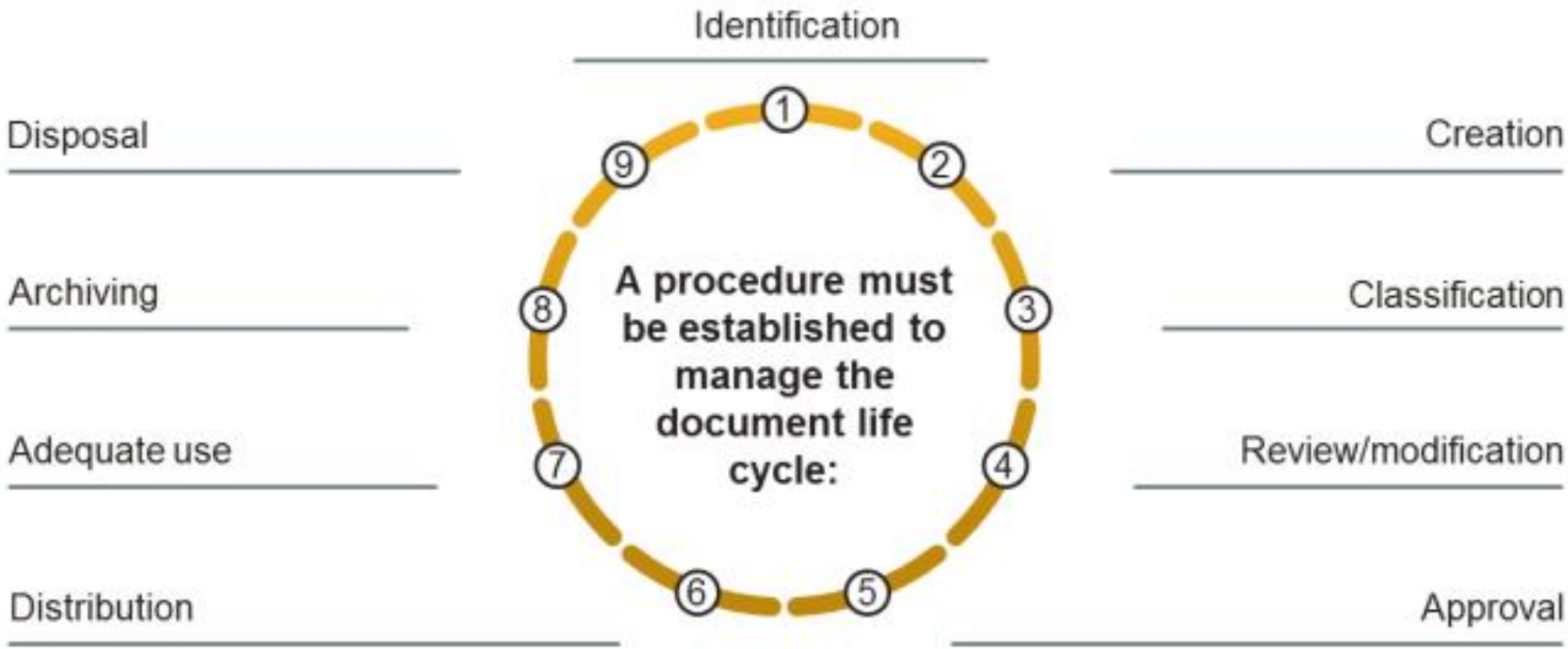


2.1.1 Create a Master List of Documents

It is recommended to make a list of all documented information related to the ISMS with basic information, such as:

- Unique identifier (e.g., 05010-Physical Security Policy, where 05010 is the unique identifier)
- Title
- Document type
- Functions and names of authors
- Function and name of the approver and the date of approval
- Date of issue
- Version and revision date
- Page number
- Classification

2.1.3 Develop a Documented Information Management Process



2.1.4 Implement a Documented Information Management System

- Facilitating access, referencing, dissemination, and archiving of documented information
- Managing the entire document life cycle
- Ensuring traceability
- Securing document access

Records Register

Example

Identification	Stored	Responsibility	Retention	Classification
Visitor log	Reception	Administrative assistant	One year	Internal use
Incidents report sheet	Service Center	Service center director	Three years	Confidential
Employee record	HR Department	HR director	Five years after the termination of employment	Highly confidential
Management review	Executive Committee	Secretary of the executive committee	Seven years	Highly confidential

1. **What should an organization do in order to comply with ISO/IEC 27001?**
    A. Develop a procedure for the control of the documented information
    B. Develop a form for the control of the documented information that is visible only to the top management
    C. Develop a guideline for the control of the documented information only when requested by an executive
2. **In order to comply with ISO/IEC 27001, organizations should fulfill some mandatory requirements on how to document controls.**
    A. True
    B. False
3. **What does a master list of documents in the context of ISMS contain?**
    A. All documentation related to the ISMS in a single list
    B. Key parts of the documentation related to the ISMS in single lists
    C. A group of the most accessed documents in a single list
4. **What does a procedure describe?**
    A. An orderly sequence of actions aimed at achieving a goal
    B. A guide to an actual description of policies
    C. A detailed explanation of the functioning of a process

5.Which is the correct sequence of actions when establishing a procedure to manage the document life cycle?

A. Approval, identification, classification, modification, disposal, archiving, adequate use, and distribution
B. Creation, identification, classification, modification, approval, distribution, adequate use, archiving, disposal
C. Distribution, identification, modification, classification, disposal, archiving, adequate use, and creation

6.During which of the following cases is the implementation of a documented information management system especially useful?

A. Facilitating access to, referencing, disseminating, and archiving documents
B. Losing traceability of the documented information
C. Managing parts of the document life cycle

Section 15

Selection and design of controls

- Organization's security architecture
- Preparation for the implementation of controls
- Design and description of controls

2.2 Selection and Design of Controls

1. Define and establish		2. Implement and operate		3. Monitor and review		4. Maintain and improve	
1.1	Initiation of the ISMS implementation	2.1	Documented information management	3.1	Monitoring, measurement, analysis, and evaluation	4.1	Treatment of nonconformities
1.2	Understanding the organization and its context	2.2	Selection and design of controls	3.2	Internal audit	4.2	Continual improvement
1.3	ISMS scope	2.3	Implementation of controls	3.3	Management review		
1.4	Leadership and project approval	2.4	Communication				
1.5	Organizational structure	2.5	Competence and awareness				
1.6	Analysis of the existing system	2.6	Security operations management				
1.7	Security policy						
1.8	Risk management						
1.9	Statement of Applicability						

Continual communication and awareness

Selection and Design of Controls

Operational planning and control

- The organization should plan, implement, control, and continually improve the processes needed to meet information security requirements.
- The organization should, following the risk assessment process, select controls and implement them.
- Documented information should be regularly maintained in order to ensure that the processes have been carried out as planned.
- Planned and unplanned changes should be controlled in order to mitigate their consequences and adverse effects.
- The organization should also ensure that outsourced processes are properly determined and controlled.

2.2 Selection and Design of Controls

List of activities

2.2.1 Define the Organization's Security Architecture

- The organization's security architecture represents a holistic approach to incorporate building blocks of security across the entire organization.
- It focuses on the following:
  - Representing a simple and long-term view of security controls
  - Providing a unified vision for common security controls tied to business objectives
  - Leveraging existing technology investments and maximizing benefits from new ones
  - Providing a flexible approach to current and future threats and also the needs of core functions
  - Providing efficiency: the right assets, at the right time, in the right places

Concepts and Security Models

Common security services

A number of security functions serve as foundations for common security services in the organization and may be used to build the organization's security architecture. Some of these functions are:

- Identity and access control services
- Boundary control services
- Integrity services
- Cryptographic services
- Audit and monitoring services

2.2.2 Prepare for the Implementation of Controls

- The organization's overall security architecture helps in identifying all the types of security controls to be implemented (information security controls, in particular).
- When preparing for the implementation of information security controls, the organization should:
  - Allocate the required resources and physical means to implement every control that is listed in the Statement of Applicability
  - Conduct a cost analysis
  - Assess the competence of the people involved in the process of implementing controls to perform the assigned tasks
  - Allocate the time, including the complete schedule for the implementation of each control
  - Prepare the required documented information
  - Prepare a detailed list of activities and tasks to be performed during the implementation process
  - Outline the intended results and outputs

2.2.2 Prepare for the Implementation of Controls

- The organization's overall security architecture helps in identifying all the types of security controls to be implemented (information security controls, in particular).
- When preparing for the implementation of information security controls, the organization should:
  - Allocate the required resources and physical means to implement every control that is listed in the Statement of Applicability
  - Conduct a cost analysis
  - Assess the competence of the people involved in the process of implementing controls to perform the assigned tasks
  - Allocate the time, including the complete schedule for the implementation of each control
  - Prepare the required documented information
  - Prepare a detailed list of activities and tasks to be performed during the implementation process
  - Outline the intended results and outputs

2.2.3 Design and Describe the Controls

Practical tips

- The design and description of the security controls selected for the ISMS should be properly documented.
- ISO/IEC 27001 does not provide any specific documentation method to be used.
- Since the organization's security architecture divides security controls into groups, it is best practice to divide their respective documents into groups, as well. For example, all the information security controls should be included in a single document.
- Documentation must be concise and reader-friendly.

1. **What does an organization's security architecture represent?**
   A. A set of disciplines used to design solutions to address security requirements at a human level
   B. A set of disciplines used to design solutions to address security requirements at an operational level
   C. A set of disciplines used to design solutions to address security requirements at a system level
2. **Which services aim at normalizing user identification and promoting shared authentication across the organization?**
   A. Boundary control services
   B. Access control services
   C. Cryptographic services
3. **Boundary control services control the transfer of information from a state or set of systems to another.**
   A. True
   B. False
4. **What are some of the steps to take when preparing for the implementation of information security controls?**
   A. Conduct a cost analysis and prepare the required documented information
   B. Conduct a cost analysis and avoid the intended results and outputs
   C. Conduct a cost analysis and prepare a general list of activities without providing details

6.Why is it important to involve employees in the draft, review, and validation processes?

A. Because it helps them gain experience and expertise for their personal intellect
B. Because it helps them implement the information security controls within the organization
C. Because it helps them automate procedures easily and work faster

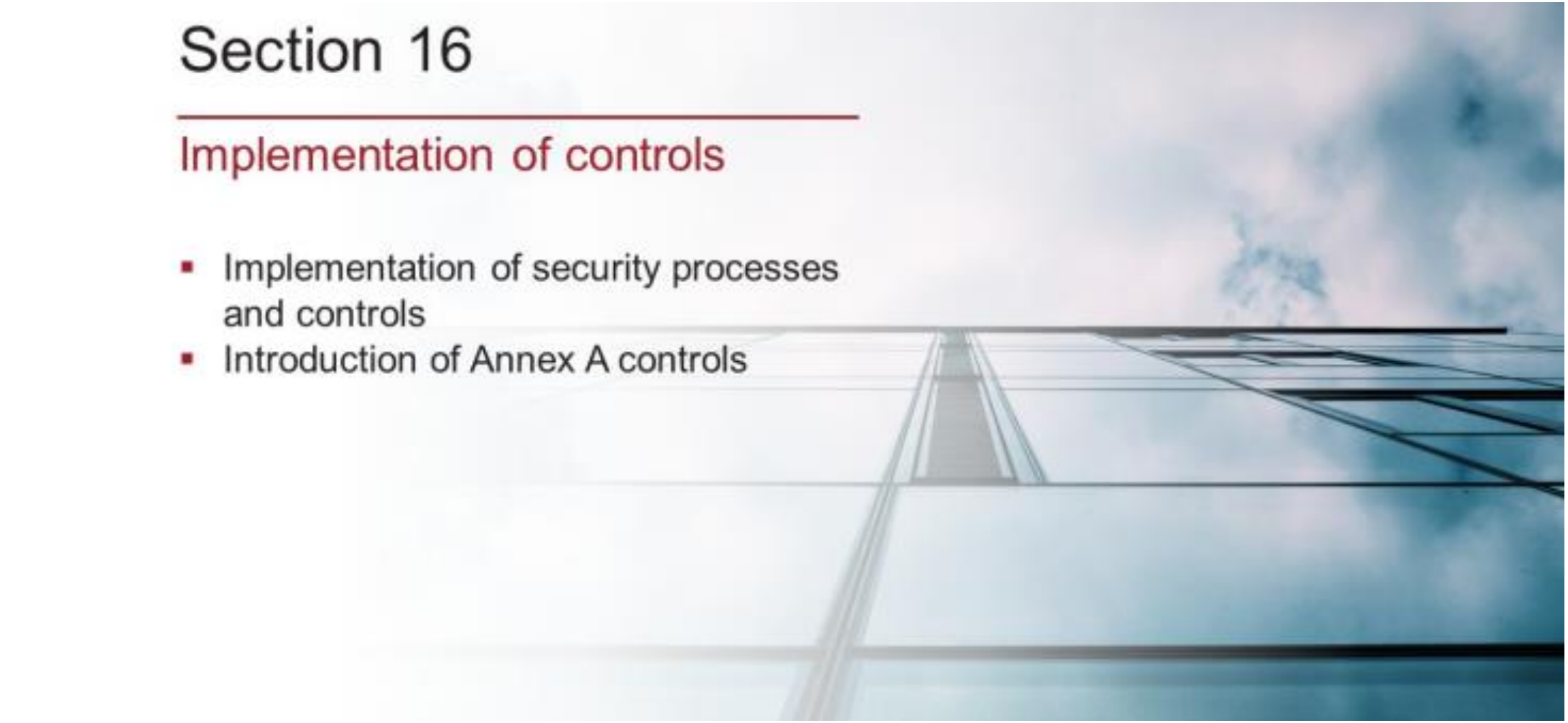
7.ISO/IEC 27001 provides a specific documentation method to be used for designing and describing controls?

A. True
B. False

Section 16

Implementation of controls

- Implementation of security processes and controls
- Introduction of Annex A controls



2.3 Implementation of Controls

ISO/IEC 27001 Requirements

ISO/IEC 27001, clause 6.1.3

The organization shall define and apply an information security risk treatment process to:

a) select appropriate information security risk treatment options, taking account of the risk assessment results;

b) determine all controls that are necessary to implement the information security risk treatment option(s) chosen;

NOTE 1 Organizations can design controls as required, or identify them from any source.

c) compare the controls determined in 6.1.3 b) above with those in Annex A and verify that no necessary controls have been omitted;

NOTE 2 Annex A contains a list of possible information security controls. Users of this document are directed to Annex A to ensure that no necessary information security controls are overlooked.

NOTE 3 The information security controls listed in Annex A are not exhaustive and additional information security controls can be included if needed.

Introduction of Annex A Controls

What has changed in Annex A of ISO/IEC 27001?

- The updated Annex A of ISO/IEC 27001 based on ISO/IEC 27002 controls contains a list of information security controls. Annex A provides only information security controls and does not provide the control purpose and guidance as ISO/IEC 27002:2022.
- Annex A introduces 11 new information security controls, 58 updated controls, and 24 controls that have been merged with the existing controls. These controls are grouped into four categories.

Organizational controls

5.1-5.37

People controls

6.1-6.8

Physical controls

7.1-7.14

Technological controls

8.1-8.34

Organizational Controls

ISO/IEC 27001, Annex A 5

Annex A 5.1 Policies for information security

Information security policy and topic-specific policies shall be defined, approved by management, published, communicated to and acknowledged by relevant personnel and relevant interested parties, and reviewed at planned intervals and if significant changes occur.

Annex A 5.2 Information security roles and responsibilities

Information security roles and responsibilities shall be defined and allocated according to the organization needs.

Annex A 5.3 Segregation of duties

Conflicting duties and conflicting areas of responsibility shall be segregated.

Annex A 5.4 Management responsibilities

Management shall require all personnel to apply information security in accordance with the established information security policy, topic-specific policies and procedures of the organization.

Organizational Controls (Cont'd)

ISO/IEC 27001, Annex A 5

Annex A 5.5 Contact with authorities

The organization shall establish and maintain contact with relevant authorities.

Annex A 5.6 Contact with special interest groups

The organization shall establish and maintain contact with special interest groups or other specialist security forums and professional associations.

Annex A 5.7 Threat intelligence

Information relating to information security threats shall be collected and analysed to produce threat intelligence.

Annex A 5.8 Information security in project management

Information security shall be integrated into project management.

Organizational Controls (Cont'd)

ISO/IEC 27001, Annex A 5

Annex A 5.9 Inventory of information and other associated assets

An inventory of information and other associated assets, including owners, shall be developed and maintained.

Annex A 5.10 Acceptable use of information and other associated assets

Rules for the acceptable use and procedures for handling information and other associated assets shall be identified, documented and implemented.

Annex A 5.11 Return of assets

Personnel and other interested parties as appropriate shall return all the organization's assets in their possession upon change or termination of their employment, contract or agreement.

Annex A 5.12 Classification of information

Information shall be classified according to the information security needs of the organization based on confidentiality, integrity, availability and relevant interested party requirements.

Organizational Controls (Cont'd)

ISO/IEC 27001, Annex A 5

Annex A 5.13 Labelling of information

An appropriate set of procedures for information labelling shall be developed and implemented in accordance with the information classification scheme adopted by the organization.

Annex A 5.14 Information transfer

Information transfer rules, procedures, or agreements shall be in place for all types of transfer facilities within the organization and between the organization and other parties.

Annex A 5.15 Access control

Rules to control physical and logical access to information and other associated assets shall be established and implemented based on business and information security requirements.

Annex A 5.16 Identity management

The full life cycle of identities shall be managed.

Organizational Controls (Cont'd)

ISO/IEC 27001, Annex A 5

Annex A 5.17 Authentication information

Allocation and management of authentication information shall be controlled by a management process, including advising personnel on appropriate handling of authentication information.

Annex A 5.18 Access rights

Access rights to information and other associated assets shall be provisioned, reviewed, modified and removed in accordance with the organization's topic-specific policy on and rules for access control.

Annex A 5.19 Information security in supplier relationships

Processes and procedures shall be defined and implemented to manage the information security risks associated with the use of supplier's products or services.

Annex A 5.20 Addressing information security within supplier agreements

Relevant information security requirements shall be established and agreed with each supplier based on the type of supplier relationship.

Organizational Controls (Cont'd)

ISO/IEC 27001, Annex A 5

Annex A 5.21 Managing information security in the ICT supply chain

Processes and procedures shall be defined and implemented to manage the information security risks associated with the ICT products and services supply chain.

Annex A 5.22 Monitoring, review and change management of supplier service

The organization shall regularly monitor, review, evaluate and manage change in supplier information security practices and service delivery.

Annex A 5.23 Information security for use of cloud services

Processes for acquisition, use, management and exit from cloud services shall be established in accordance with the organization's information security requirements.

Annex A 5.24 Information security incident management planning and preparation

The organization shall plan and prepare for managing information security incidents by defining, establishing and communicating information security incident management processes, roles and responsibilities.

Organizational Controls (Cont'd)

ISO/IEC 27001, Annex A 5

Annex A 5.25 Assessment and decision on information security events

The organization shall assess information security events and decide if they are to be categorized as information security incidents.

Annex A 5.26 Response to information security incidents

Information security incidents shall be responded to in accordance with the documented procedures.

Annex A 5.27 Learning from information security incidents

Knowledge gained from information security incidents shall be used to strengthen and improve the information security controls.

Annex A 5.28 Collection of evidence

The organization shall establish and implement procedures for the identification, collection, acquisition and preservation of evidence related to information security events.

Organizational Controls (Cont'd)

ISO/IEC 27001, Annex A 5

Annex A 5.29 Information security during disruption

The organization shall plan how to maintain information security at an appropriate level during disruption.

Annex A 5.30 ICT readiness for business continuity

ICT readiness shall be planned, implemented, maintained and tested based on business continuity objectives and ICT continuity requirements.

Annex A 5.31 Legal, statutory, regulatory and contractual requirements

Legal, statutory, regulatory and contractual requirements relevant to information security and the organization's approach to meet these requirements shall be identified, documented and kept up to date.

Annex A 5.32 Intellectual property rights

The organization shall implement appropriate procedures to protect intellectual property rights.

Organizational Controls (Cont'd)

ISO/IEC 27001, Annex A 5

Annex A 5.33 Protection of records

Records shall be protected from loss, destruction, falsification, unauthorized access and unauthorized release.

Annex A 5.34 Privacy and protection of personal identifiable information (PII)

The organization shall identify and meet the requirements regarding the preservation of privacy and protection of PII according to applicable laws and regulations and contractual requirements.

Annex A 5.35 Independent review of information security

The organization's approach to managing information security and its implementation including people, processes and technologies shall be reviewed independently at planned intervals, or when significant changes occur.

Organizational Controls (Cont'd)

ISO/IEC 27001, Annex A 5

Annex A 5.36 Compliance with policies, rules and standards for information security

Compliance with the organization's information security policy, topic-specific policies, rules and standards shall be regularly reviewed.

Annex A 5.37 Documented operating procedures

Operating procedures for information processing facilities shall be documented and made available to personnel who need them.

People Controls

ISO/IEC 27001, Annex A 6

Annex A 6.1 Screening

Background verification checks on all candidates to become personnel shall be carried out prior to joining the organization and on an ongoing basis taking into consideration applicable laws, regulations and ethics and be proportional to the business requirements, the classification of the information to be accessed and the perceived risks.

Annex A 6.2 Terms and conditions of employment

The employment contractual agreements shall state the personnel's and the organization's responsibilities for information security.

People Controls (Cont'd)

ISO/IEC 27001, Annex A 6

Annex A 6.3 Information security awareness, education and training

Personnel of the organization and relevant interested parties shall receive appropriate information security awareness, education and training and regular updates of the organization's information security policy, topic-specific policies and procedures, as relevant for their job function.

Annex A 6.4 Disciplinary process

A disciplinary process shall be formalized and communicated to take actions against personnel and other relevant interested parties who have committed an information security policy violation.

People Controls (Cont'd)

ISO/IEC 27001, Annex A 6

Annex A 6.5 Responsibilities after termination or change of employment

Information security responsibilities and duties that remain valid after termination or change of employment shall be defined, enforced and communicated to relevant personnel and other interested parties.

Annex A 6.6 Confidentiality or non-disclosure agreements

Confidentiality or non-disclosure agreements reflecting the organization's needs for the protection of information shall be identified, documented, regularly reviewed and signed by personnel and other relevant interested parties.

Annex A 6.7 Remote working

Security measures shall be implemented when personnel are working remotely to protect information accessed, processed or stored outside the organization's premises.

Annex A 6.8 Information security event reporting

The organization shall provide a mechanism for personnel to report observed or suspected information security events through appropriate channels in a timely manner.

Physical Controls

ISO/IEC 27001, Annex A 7

Annex A 7.1 Physical security perimeter

Security perimeters shall be defined and used to protect areas that contain information and other associated assets.

Annex A 7.2 Physical entry

Secure areas shall be protected by appropriate entry controls and access points.

Annex A 7.3 Securing offices, rooms and facilities

Physical security for offices, rooms and facilities shall be designed and implemented.

Annex A 7.4 Physical security monitoring

Premises shall be continuously monitored for unauthorized physical access.

Physical Controls (Cont'd)

ISO/IEC 27001, Annex A 7

Annex A 7.5 Protecting against physical and environmental threats

Protection against physical and environmental threats, such as natural disasters and other intentional or unintentional physical threats to infrastructure shall be designed and implemented.

Annex A 7.6 Working in secure areas

Security measures for working in secure areas shall be designed and implemented.

Annex A 7.7 Clear desk and clear screen

Clear desk rules for papers and removable storage media and clear screen rules for information processing facilities shall be defined and appropriately enforced.

Annex A 7.8 Equipment siting and protection

Equipment shall be sited securely and protected.

Physical Controls (Cont'd)

ISO/IEC 27001, Annex A 7

Annex A 7.9 Security of assets off-premises

Off-site assets shall be protected.

Annex A 7.10 Storage media

Storage media shall be managed through their life cycle of acquisition, use, transportation and disposal in accordance with the organization's classification scheme and handling requirements.

Annex A 7.11 Supporting utilities

Information processing facilities shall be protected from power failures and other disruptions caused by failures in supporting utilities.

Annex A 7.12 Cabling security

Cables carrying power, data or supporting information services shall be protected from interception, interference or damage.

Physical Controls (Cont'd)

ISO/IEC 27001, Annex A 7

Annex A 7.13 Equipment maintenance

Equipment shall be maintained correctly to ensure availability, integrity and confidentiality of information.

Annex A 7.14 Secure disposal or re-use of equipment

Items of equipment containing storage media shall be verified to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal or re-use.

Technological Controls

ISO/IEC 27001, Annex A 8

Annex A 8.1 User end point devices

Information stored on, processed by or accessible via user end point devices shall be protected.

Annex A 8.2 Privileged access rights

The allocation and use of privileged access rights shall be restricted and managed.

Annex A 8.3 Information access restrictions

Access to information and other associated assets shall be restricted in accordance with the established topic-specific policy on access control.

Annex A 8.4 Access to source code

Read and write access to source code, development tools and software libraries shall be appropriately managed.

Technological Controls (Cont'd)

ISO/IEC 27001, Annex A 8

Annex A 8.5 Secure authentication

Secure authentication technologies and procedures shall be implemented based on information access restrictions and the topic-specific policy on access control.

Annex A 8.6 Capacity management

The use of resources shall be monitored and adjusted in line with current and expected capacity requirements.

Annex A 8.7 Protection against malware

Protection against malware shall be implemented and supported by appropriate user awareness.

Annex A 8.8 Management of technical vulnerabilities

Information about technical vulnerabilities of information systems in use shall be obtained, the organization's exposure to such vulnerabilities shall be evaluated and appropriate measures shall be taken.

Technological Controls (Cont'd)

ISO/IEC 27001, Annex A 8

Annex A 8.9 Configuration management

Configurations, including security configurations, of hardware, software, services and networks shall be established, documented, implemented, monitored and reviewed.

Annex A 8.10 Information deletion

Information stored in information systems, devices or in any other storage media shall be deleted when no longer required.

Annex A 8.11 Data masking

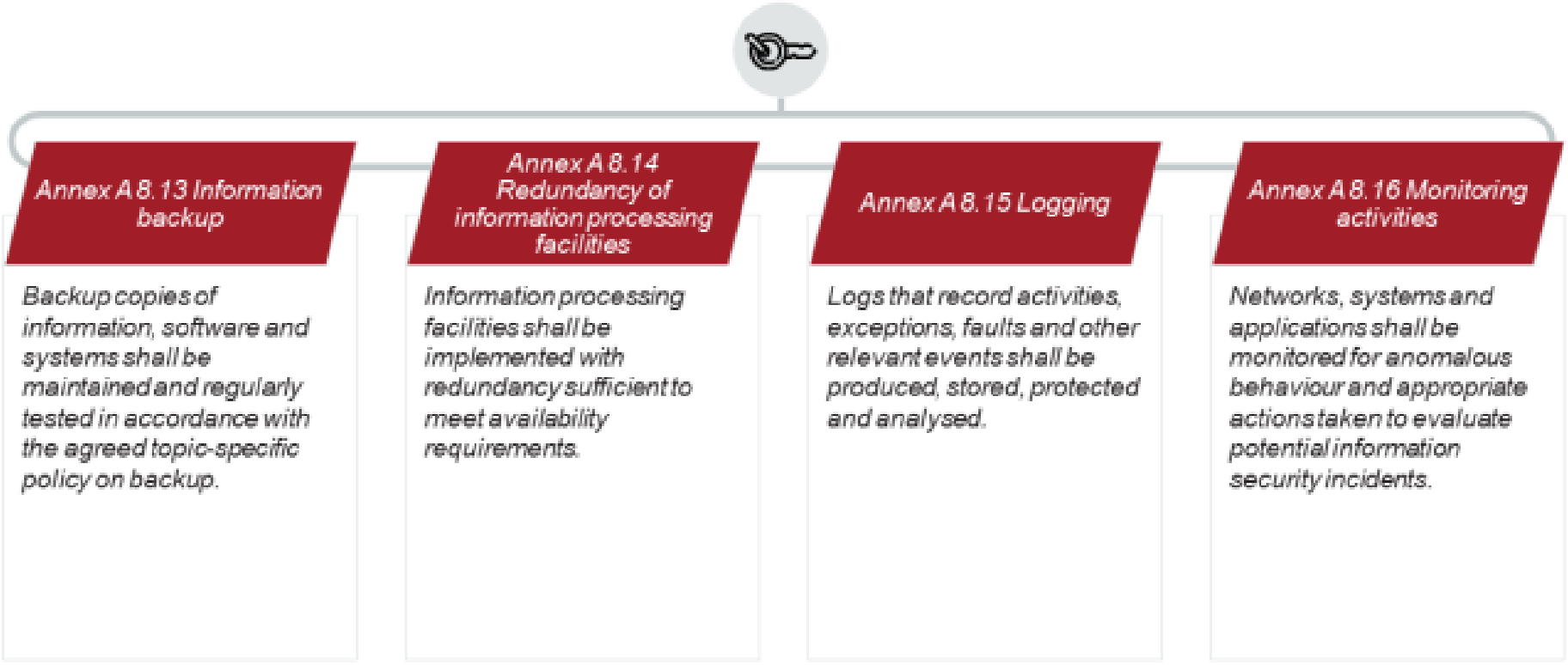
Data masking shall be used in accordance with the organization's topic-specific policy on access control and other related topic-specific policies, and business requirements, taking applicable legislation into consideration.

Annex A 8.12 Data leakage prevention

Data leakage prevention measures shall be applied to systems, networks and any other devices that process, store or transmit sensitive information.

Technological Controls (Cont'd)

ISO/IEC 27001, Annex A 8



Technological Controls (Cont'd)

ISO/IEC 27001, Annex A 8

Annex A 8.17 Clock synchronization

The clocks of information processing systems used by the organization shall be synchronized to approved time sources.

Annex A 8.18 Use of privileges utility programs

The use of utility programs that can be capable of overriding system and application controls shall be restricted and tightly controlled.

Annex A 8.19 Installation of software on operational systems

Procedures and measures shall be implemented to securely manage software installation on operational systems.

Annex A 8.20 Networks security

Networks and network devices shall be secured, managed and controlled to protect information in systems and applications.

Technological Controls (Cont'd)

ISO/IEC 27001, Annex A 8

Annex A 8.21 Security of network services

Security mechanisms, service levels and service requirements of network services shall be identified, implemented and monitored.

Annex A 8.22 Segregation of networks

Groups of information services, users and information systems shall be segregated in the organization's networks.

Annex A 8.23 Web filtering

Access to external websites shall be managed to reduce exposure to malicious content.

Annex A 8.24 Use of cryptography

Rules for the effective use of cryptography, including cryptographic key management, shall be defined and implemented.

Technological Controls (Cont'd)

ISO/IEC 27001, Annex A 8

Annex A 8.25 Secure development life cycle

Rules for the secure development of software and systems shall be established and applied.

Annex A 8.26 Application security requirements

Information security requirements shall be identified, specified and approved when developing or acquiring applications.

Annex A 8.27 Secure system architecture and engineering principles

Principles for engineering secure systems shall be established, documented, maintained and applied to any information system development activities.

Annex A 8.28 Secure coding

Secure coding principles shall be applied to software development.

Technological Controls (Cont'd)

ISO/IEC 27001, Annex A 8

Annex A 8.29 Security testing in development and acceptance

Security testing processes shall be defined and implemented in the development life cycle.

Annex A 8.30 Outsourced development

The organization shall direct, monitor and review the activities related to outsourced system development.

Annex A 8.31 Separation of development, test and production environments

Development, testing and production environments shall be separated and secured.

Annex A 8.32 Change management

Changes to information processing facilities and information systems shall be subject to change management procedures.

Technological Controls (Cont'd)

ISO/IEC 27001, Annex A 8

Annex A 8.33 Test information

Test information shall be appropriately selected, protected and managed.

Annex A 8.34 Protection of information systems during audit testing

Audit tests and other assurance activities involving assessment of operational systems shall be planned and agreed between the tester and appropriate management.

Section 17

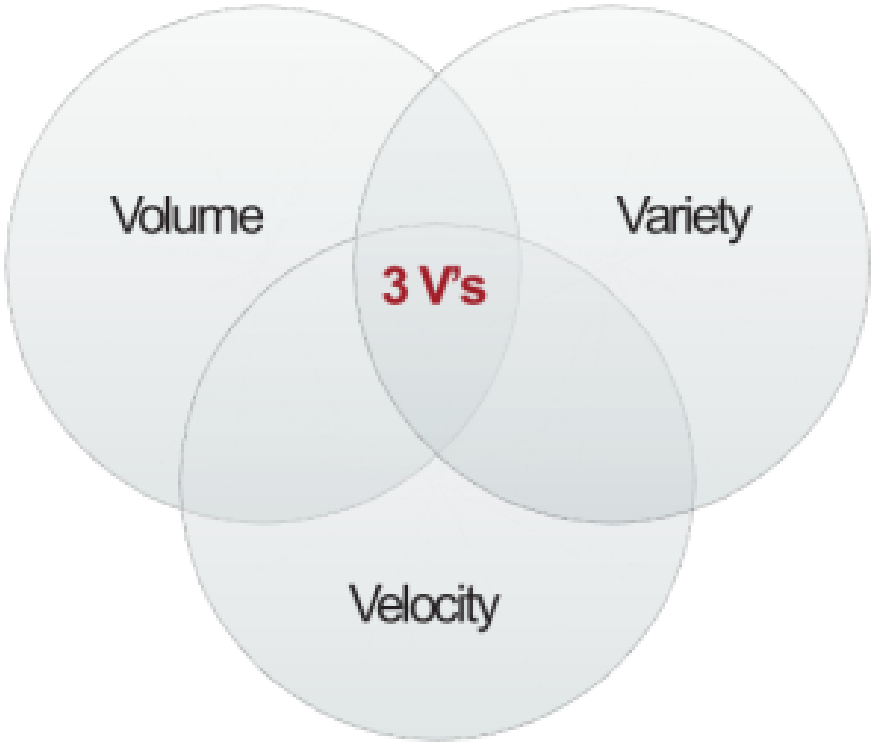
Trends and technologies

- Big data
- The three V's of big data
- Artificial intelligence
- Machine learning
- Cloud computing
- Outsourced operations
- The impact of new technologies in information security

Big Data

- The dictionary of Merriam-Webster defines big data as “an accumulation of data that is too large and complex for processing by traditional database management tools.”
- Big data includes a large number of structured and unstructured data.
- Structured data are organized and easily reachable.
- Unstructured data cannot be organized in relational databases and are not easily reachable.

The Three V's of Big Data



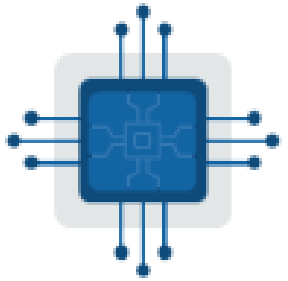
Volume of data refers to the amount of data generated through websites, online applications, transactions, data saved in records, tables, files, etc.

Variety refers to the different types of data, including structured and unstructured data, online images and videos, human-generated texts, machine-generated readings, etc.

Velocity refers to the speed of data processing generated in real time, online and offline, in streams, batches, or bits.

Artificial Intelligence (AI)

- The Oxford English Dictionary defines Artificial Intelligence (AI) as “the theory and development of computer systems able to perform tasks usually requiring human intelligence, such as visual perception, speech recognition, decision-making, and translation between languages.”
- The interconnectivity and fast data transfers that are made possible through the usage of 5G will allow for AI applications to become integral parts of our lives.
- Common application of AI are in:
  - Banking
  - Marketing
  - Healthcare
  - Autonomous vehicles



Artificial Intelligence (AI) (Cont'd)

Weak and strong AI

- Weak AI is also known as narrow AI.
- Weak AI is focused on a specific task and outperforms humans when conducting technical and automated tasks. However, when weak AI has to conduct a task that it does not recognize, it will not be able to complete it unless it is specifically programmed to do so.
- The benefit of weak AI is the automation of tasks.
- Examples of weak AI include Apple's Siri, Alexa, AlphaGo, etc.

- Strong AI is also known as artificial general intelligence (AGI).
- AGI has the capacity to understand newly presented problems and derive solutions based on prior knowledge.
- The benefit of strong AI is problem-solving.
- Examples of strong AI include AI that can communicate in natural language, use critical thinking, etc.

Machine Learning (ML)

- Machine learning and artificial intelligence are sometimes mistakenly used interchangeably, but they do not represent the same thing.
- As previously mentioned, AI encompasses a broader concept of machines that have the capacity to mimic a human being, whereas the main purpose of ML is to enable computers to learn automatically.
- In machine learning, the processor is given the entry data and the machine solves the problems by applying various methodologies.
- Some of the essential algorithms that are utilized by machine learning are:
  - Linear regression
  - Logistic regression
  - Decision tree

Machine Learning — Example

Google photos machine learning algorithm

- The Google Photos application has recently provided a new search feature that recognizes things and items within photos. It allows its users to search by generic terms such as dog, beach, sunset, etc.
- This feature is powered by Google's machine learning algorithms and operators due to the large amount of photos that are uploaded in Google Photos by users.
- The algorithm processes all of the photos and then tags what it can recognize in that photo. These tags can then be used as search inputs.
- Firstly, the algorithm attaches a score to each of the tags, then the photo that contains the tag with the highest score is displayed first when searched, and so on.

Cloud Computing

Cloud computing is the delivery of computing services such as servers, storage, databases, networking, and processing power. In general, cloud computing includes delivering hosted services over the internet. These services are:

Infrastructure as a service (IaaS)

- It includes the delivery of services such as software, hardware, networking, storage services, etc.
- IaaS can be public or private.
- Advantages of the IaaS:
  - Better security
  - Improvement of business continuity
  - Focus on the organization's core business
  - Infrastructure flexibility

Platform as a service (PaaS)

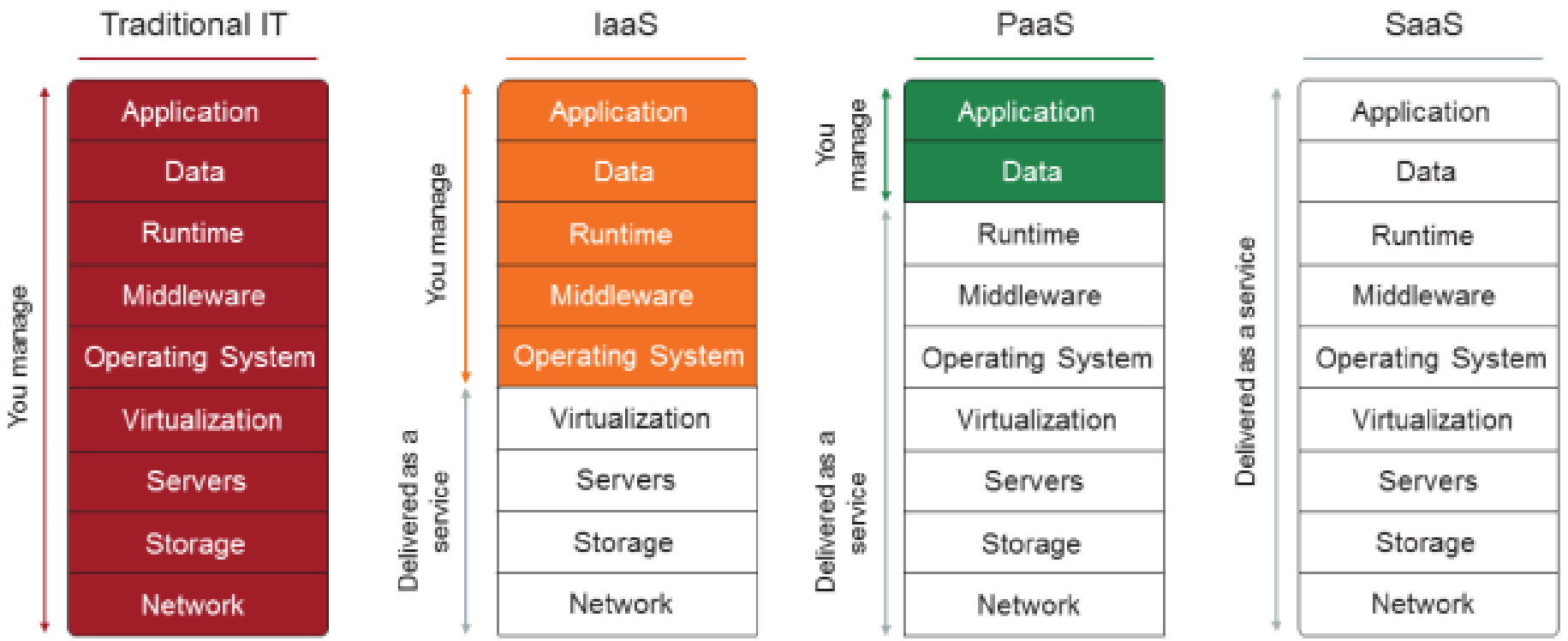
- It is related to IaaS services.
- It is a complete development and deployment environment in the cloud.
- Advantages of PaaS:
  - Reduction of coding time
  - Usage of sophisticated tools
  - Efficient management of the application life cycle

Software as a service (SaaS)

- It includes cloud-based apps that are accessed through the web or an API.
- By logging into your account, you are using SaaS.
- Advantages of SaaS:
  - You pay only for what you use.
  - You use open source software.
  - Apps are accessible from anywhere.
  - No data is lost because they are stored in the cloud.

Cloud Computing (Cont'd)

Levels of integration



Outsourced Operations

- Outsourcing is the practice of hiring a third party (an organization or a person) to perform activities, tasks, or provide services. Organizations practice this with the purpose of focusing more on their crucial activities.
- Nowadays, organizations can outsource different kinds of services such as payroll, technical support, human resource activities, and so forth.
- Organizations outsource in order to reduce their costs, become more efficient, and focus on key business operations.

The Impact of New Technologies in Information Security

- The new technological advancements, such as Artificial Intelligence (AI), Machine Learning (ML), and Blockchain, are becoming part of almost every business. They are advantageous in that they create new opportunities.
- The fast evolution of technology is greatly impacting the security of information and the way data are analyzed. As such, information security should evolve at the same pace of innovation as technology is.
- Among the greatest impacts of new technology in information security are:
  - Predictive information security is improved with AI.
  - Applications can protect themselves through AI and ML.
  - Organizations will need to continually improve and update their information security controls as the three V's of big data are increased exponentially.
  - Passwords will not be used any longer, as new technology requires the use of more secure authentication methods such as the use of biometrics, Identity as a Service (IDaaS), Fast Identity Online (FIDO), etc.
  - Organizations will need to implement new information security and privacy controls to protect their could services, as the usage of the virtual infrastructure is enormously increasing.

1. **Which of the options below is NOT part of the three V's of big data?**
    A. Volume
    B. Velocity
    C. Voltage
2. **Structured data are based on binary data and do not have a data model.**
    A. True
    B. False
3. **Which of the following is an example of unstructured data?**
    A. MongoDB
    B. SQL (Structured Query Language)
    C. Microsoft Excel files
4. **Which of the following is a benefit of weak artificial intelligence?**
    A. Automated tasks
    B. Problem-solving
    C. Critical thinking improvement
5. **Linear regression and logistic regression are algorithms utilized by:**
    A. Machine learning
    B. Outsources operations
    C. Cloud computing

6.Which cloud computing service ensures an efficient management of the application life cycle?

A. Infrastructure as a service (IaaS)
B. Platform as a service (PaaS)
C. Software as a service (SaaS)

7.Which of the statements below regarding cloud computing is NOT true?

A. Cloud computing reduces the costs needed to manage and maintain the network system
B. Cloud computing promotes security of information because data can be accessed no matter what happens to the machine
C. Cloud computing requires too many tasks, such as software patching, hardware setup, and "racking and stacking"

8.Which services are delivered by the cloud provider when using Infrastructure as a Service (IaaS)?

A. Virtualization, servers, storage, network
B. Virtualization, servers, application, data, network
C. Application, data, runtime, middleware, operating system

9.New technologies do not require the use of more secure authentication methods since passwords are good enough to guarantee information security.

A. True
B. False

10.Which of the statements below is correct?

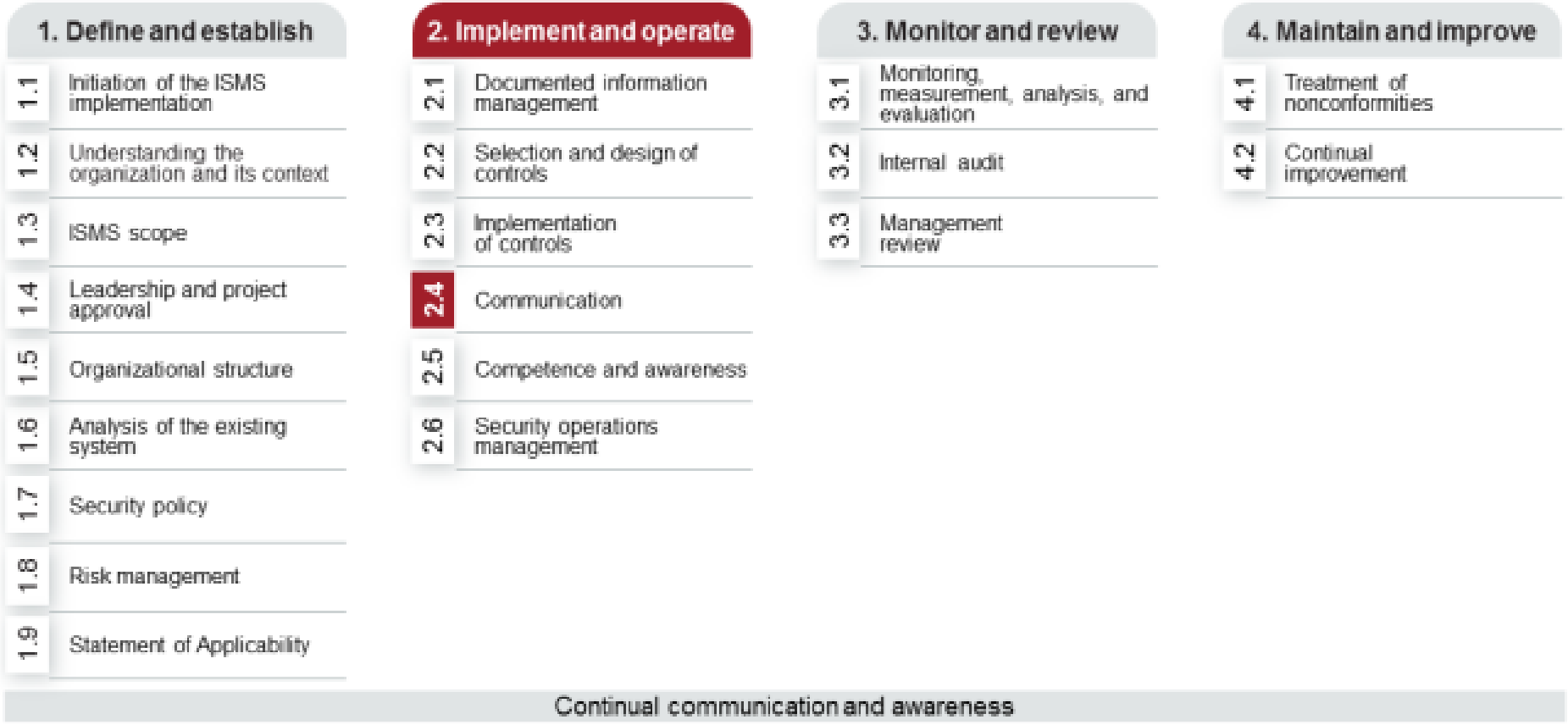
A. Machine learning is synonymous to artificial intelligence and the terms can be used interchangeably
B. Machine learning includes the delivery of hosted services over the internet
C. There are two types of machine learning: supervised machine learning and unsupervised machine learning

Section 18

Communication

- Principles of an efficient communication strategy
- Information security communication process
- Establishing communication objectives
- Identifying interested parties
- Planning communication activities
- Performing a communication activity
- Evaluating communication

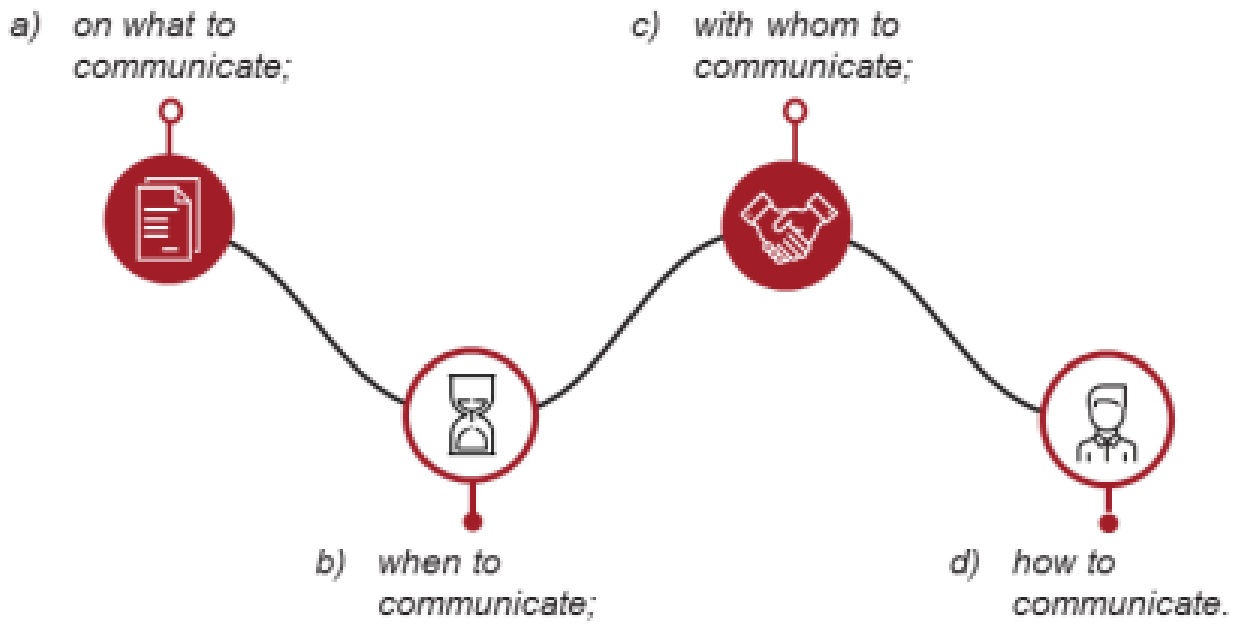
2.4 Communication



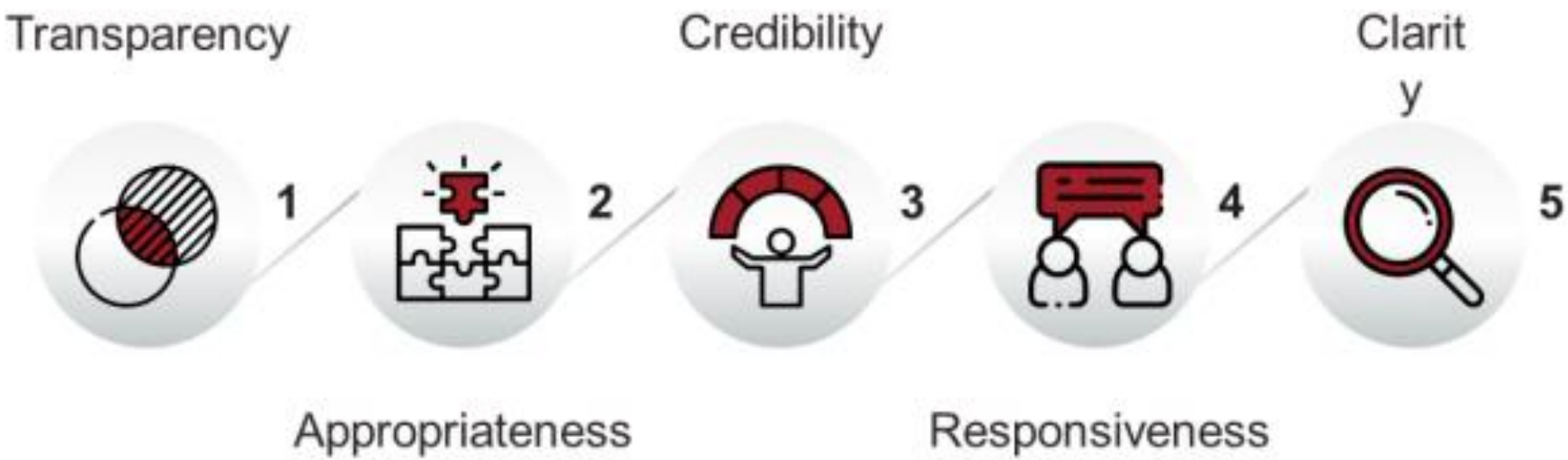
ISO/IEC 27001 Requirements

ISO/IEC 27001, clause 7.4

The organization shall determine the need for internal and external communications relevant to the information security management system including:

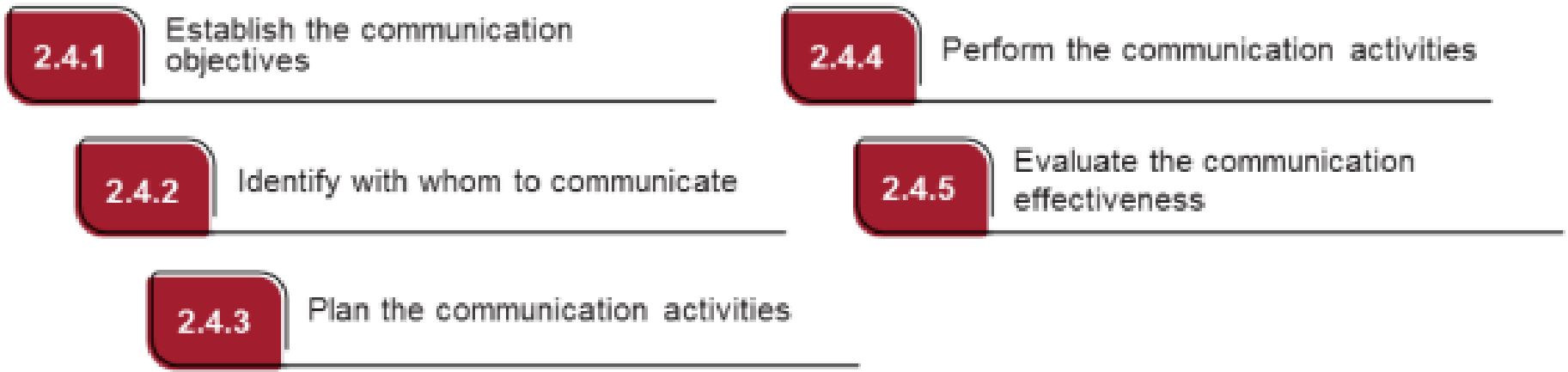


Principles of an Efficient Communication Strategy

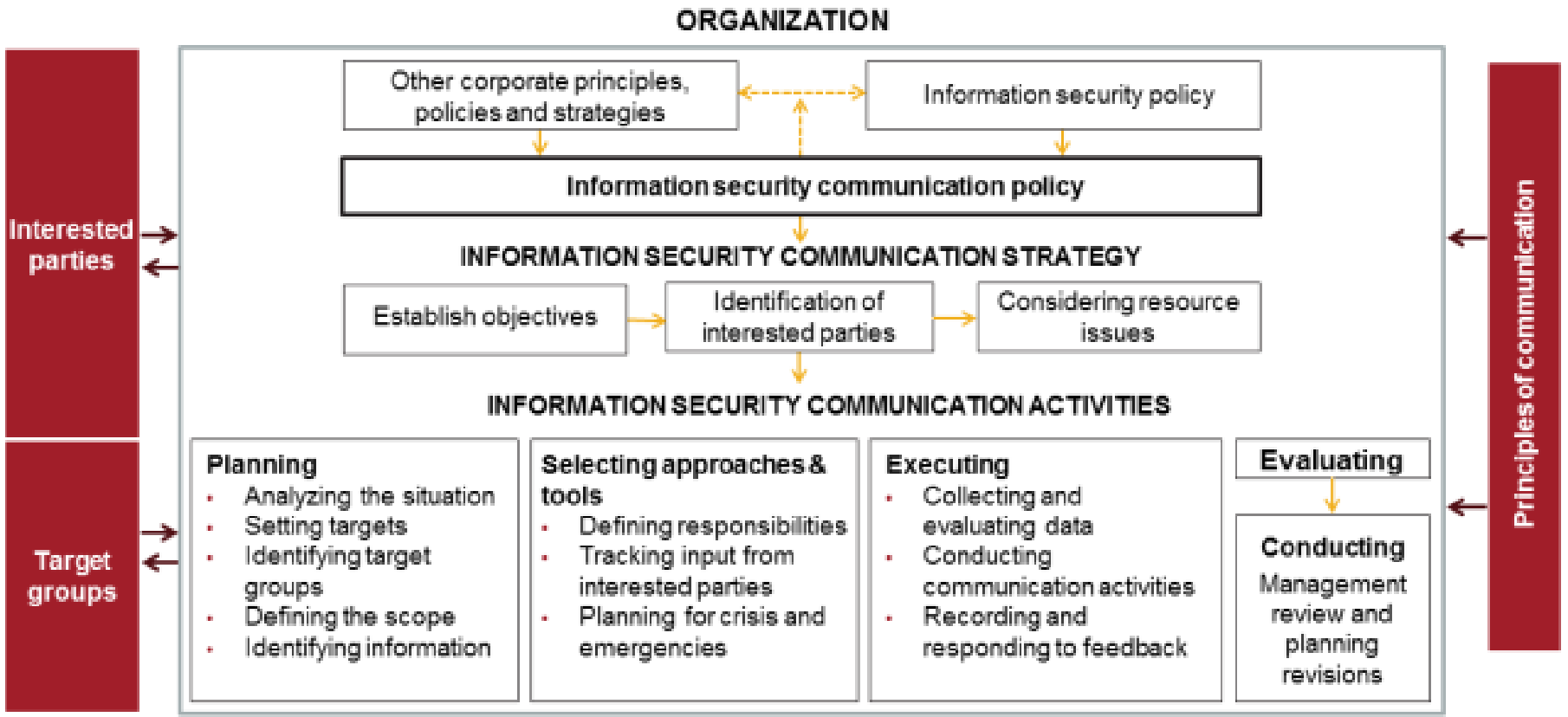


2.4 Communication

List of activities



Information Security Communication Process



2.4.1 Establish the Communication Objectives

Examples

- Improving the organization's credibility and reputation
- Establishing ongoing dialogue on information security matters with interested parties
- Complying with applicable legal requirements and with other requirements to which the organization subscribes
- Influencing public policy on information security issues
- Providing information and encouraging the understanding of information security activities by interested parties
- Meeting the expectations of interested parties in terms of information security

Communication is crucial in achieving the ISMS objectives.

2.4.2 Identify with Whom to Communicate

Adaptation of the communication plan

2.4.3 Plan the Communication Activities

Key for success

- An organization should decide its goals and intentions by means of information security communication activities.
- The established targets should be specific, measurable, achievable, realistic, time-bound, and consistent with the information security communication objectives.
- The organization should anticipate information security issues of concern and communicate them with the interested parties.

This will allow the organization to evaluate the information security communication activity and determine whether the targets have been met or not.

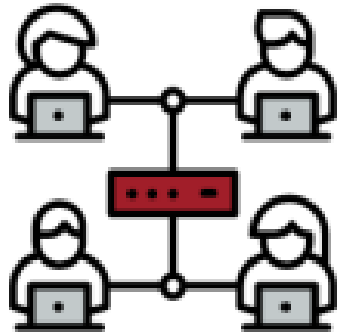
2.4.4 Perform the Communication Activities

Communication approaches and tools

Communication can be carried out using the following approaches and tools:

- Websites
- Reports
- Brochures and newsletters
- Posters
- Emails
- Newspaper articles
- Press releases
- Advertisements

- Public meetings
- Focus groups
- Surveys
- Workshops and conferences
- Media interviews
- Group presentations



2.4.5 Evaluate the Communication Effectiveness

- The organization should allow the necessary time for the information security communication to be effective.
- The time needed depends on the nature of the communication, the number of interested parties and their concerns, and the type of media used.
- The organization should review and assess the effectiveness of its information security communication.

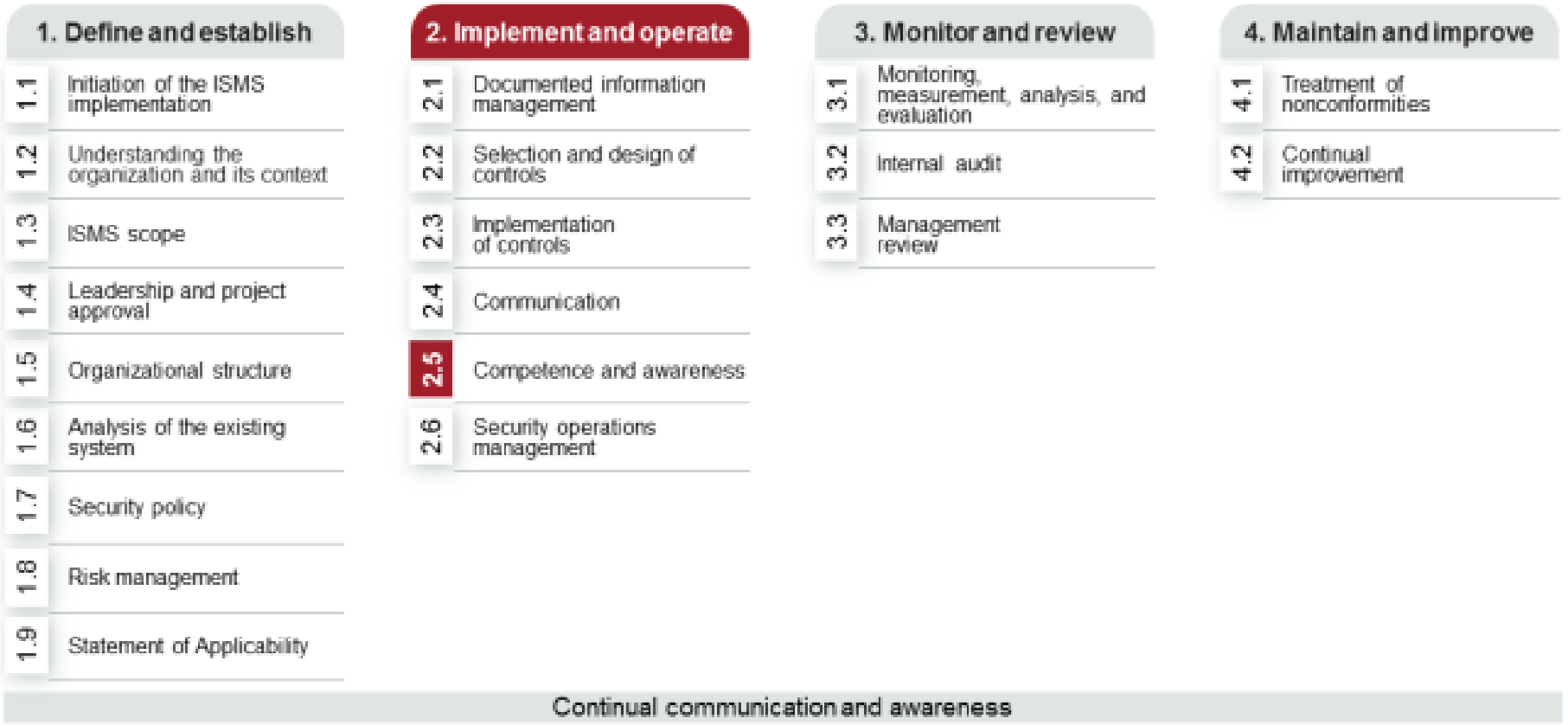
1. **What information aspect can transparency compromise in an efficient communication strategy, if not done properly?**
    A. Ambiguity
    B. Confidentiality
    C. Accuracy
2. **What do communication objectives reflect?**
    A. The information security objectives
    B. The organizational structure objectives
    C. The ISMS scope objectives
3. **The information security communication approach is impacted by whether it wants to consult, understand, inform, or involve target groups.**
    A. True
    B. False
4. **Why should an organization provide a communication program?**
    A. To integrate the ISMS into existing processes
    B. To obtain management support for the ISMS
    C. To inform all interested parties about the ISMS and the changes that may affect them
5. **Which of the following is NOT an information security communication objective?**
    A. Improving the credibility and reputation of the organization
    B. Enhancing information security risks
    C. Influencing public policy on information security issues

Section 19

Competence and awareness

- Competence and people development
- Difference between training, awareness, and communication
- Determine competence needs
- Plan the competence development activities
- Define the competence development program type and structure
- Training and awareness programs
- Provide the trainings

2.5 Competence and Awareness



ISO/IEC 27001 Requirements

ISO/IEC 27001, clauses 7.2 and 7.3

The organization shall:

a) determine the necessary competence of person(s) doing work under its control that affects its information security performance;

b) ensure that these persons are competent on the basis of appropriate education, training, or experience;

c) where applicable, take actions to acquire the necessary competence, and evaluate the effectiveness of the actions taken; and

d) retain appropriate documented information as evidence of competence.

> *NOTE Applicable actions can include, for example: the provision of training to, the mentoring of, or the reassignment of current employees; or the hiring or contracting of competent persons.*

Persons doing work under the organization's control shall be aware of:

a) the information security policy;

b) their contribution to the effectiveness of the information security management system, including the benefits of improved information security performance; and

c) the implications of not conforming with the information security management system requirements.

Competence and People Development

ISO 9000, clause 3.10.4 and ISO 10015, clause 3.2

Competence

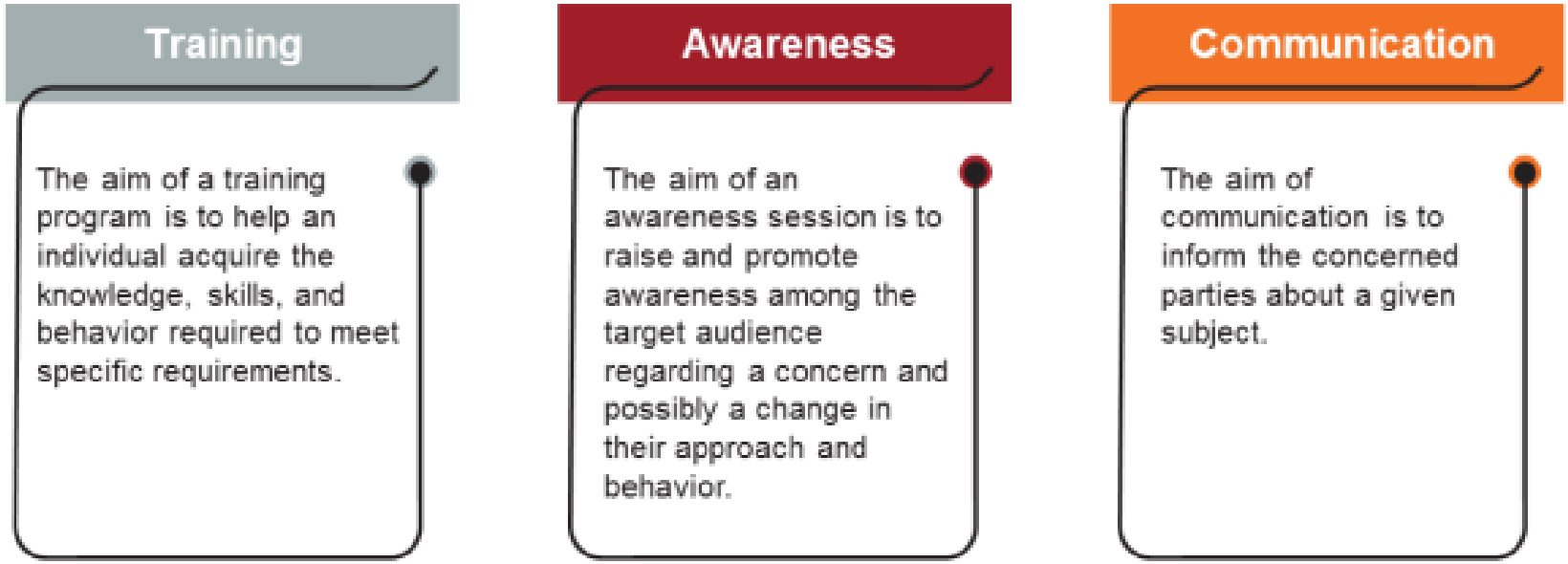
Ability to apply knowledge and skills to achieve intended results

People development

Encouragement of employees to acquire new or advanced competence by creating learning and training opportunities with circumstances to deploy the outcomes that have been acquired

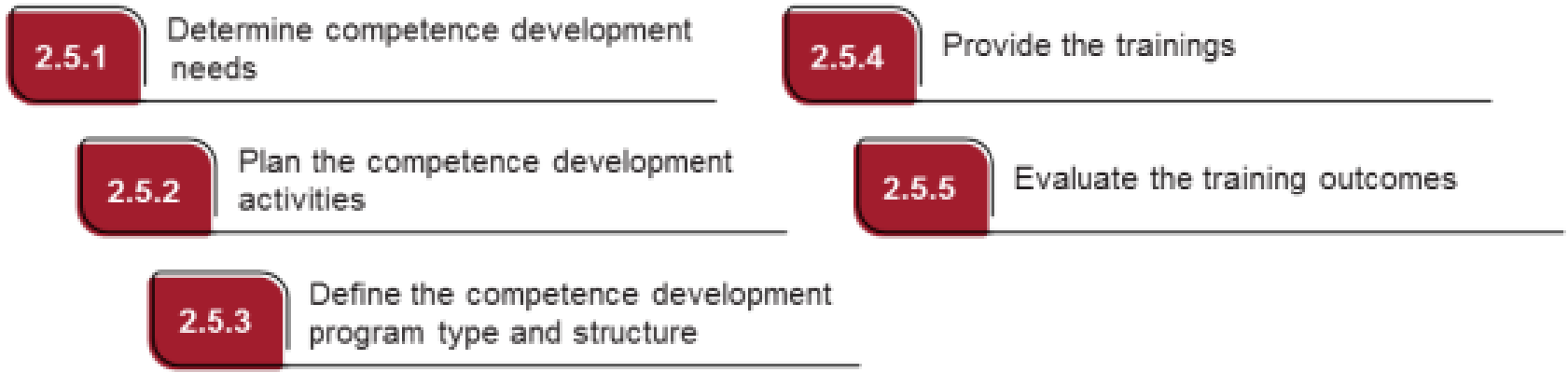
Training, Awareness, and Communication

Differences



2.5 Competence and Awareness

List of activities



Assess Current Competence and Development Needs

ISO 10015, clause 4.3

The organization should review its current competence levels against required competence needs as determined in 4.2 at the organizational, team, group and individual level to establish if or where action needs to be taken to meet competence needs.

The organization should:

a) *consider existing competence levels;*

b) *compare these with required competence levels;*

c) *use risk-based thinking to prioritize actions to address competence gaps.*

2.5.2 Plan the Competence Development Activities

ISO 10015, clause 5.2

When planning competence development activities, the organization should:

a) *determine specific development objectives (to address a competence gap or personal development need);*
b) *consider relevant development activities;*
c) *determine criteria to monitor and evaluate the development outputs;*
d) *consider risks and opportunities that can affect effective delivery of the development activities;*
e) *consider statutory and regulatory requirements;*
f) *determine organizational resources, including financial considerations;*
g) *determine organizational policies;*
h) *determine contractual arrangements with external providers;*
i) *determine planning and scheduling requirements;*
j) *determine an appropriate provider;*
k) *determine individual (or team/group) availability, motivation and ability.*

2.5.3 Define the Competence Development Program Type and Structure

Depending on the results of the assessment of employee competencies, the organization must select the type of activities needed to address those competence gaps, including:

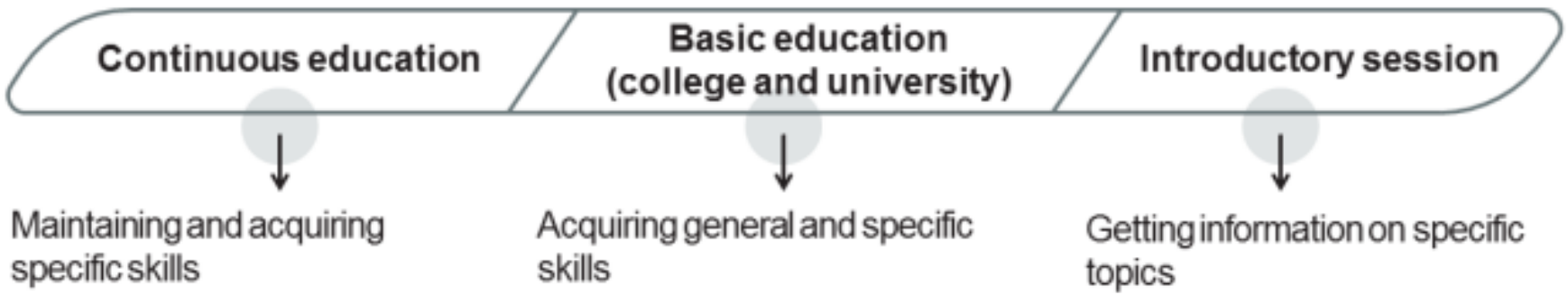
- Training programs
- Awareness programs
- Conferences, professional forums, and other networking events
- Workshops
- Self-studies

The competence development program structure should focus on the following key points:

- The target audience
- The objective of the competence development program
- The program details (place, time, etc.)
- Closing program activities (tests, awards, certifications)

Training Program

Types of training programs and their objectives

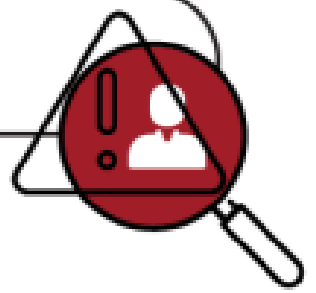


Awareness Program

An awareness program allows the organization to:

- Raise awareness regarding information security threats and how to protect from potential risks
- Ensure consistency in information security practices
- Contribute to the dissemination and implementation of its policies, guidelines, and procedures

An employee who is neither aware nor trained represents a potential risk.



Awareness Program

Main areas that should be addressed

- Information security policy
- Use of passwords
- Protection against viruses
- Proper use of the internet
- Risks associated with emails (spam, phishing, malicious code)
- Backup and data storage
- Social engineering
- Security incidents
- Use of encryption
- Security of laptops and smartphones
- Use of private files or systems at work
- Respect for intellectual property
- Problems related to access control
- Individual roles and responsibilities

2.5.4 Provide the Trainings

- The training provider is responsible for fulfilling the requirements specified in the training plan.
- However, the organization has also an important role, that is to provide the necessary resources for the successful delivery of the training, to support both the trainer and the trainee, as well as to ensure that the training is qualitative and achieves its intended results.

Before the training: In this phase, the organization is responsible for providing the necessary information to the training provider such as the nature of the training and the competence gaps that have been identified during the training needs assessment.

During the training: In this phase, the organization is responsible for providing the resources needed to successfully deliver the training, such as the relevant tools, the documentation, and the required equipment.

After the training: In this phase, the organization receives feedback from the trainee and the training provider regarding the training. In addition, after the training, the person responsible within the organization should provide feedback to the managers and employees involved in the training

2.5.5 Evaluate the Training Outcomes

- The purpose of evaluating a training program is to acquire knowledge on whether its objectives have been accomplished or not.
- The evaluation of the training includes getting feedback from the trainer, trainee, and other people involved to improve the quality of the training and ensure that the training objectives have been met.

1. **How can an organization ensure employee competence for the proper functioning of the ISMS?**
    A. Through appropriate education, training, or experience
    B. Through understanding the information security policy
    C. Through personal behavior
2. **What is the main objective of an ISMS training program?**
    A. To inform the interested parties about information security
    B. To promote the importance of information security within an organization
    C. To enable individuals to acquire general and specific skills related to the implementation of an ISMS.
3. **How can competence gap be identified?**
    A. Based on statutory and regulatory requirements
    B. By comparing current and required competence levels
    C. Based on the training and awareness programs output
4. **Which of the options below should be included in an awareness program?**
    A. The implementation of antivirus software
    B. Documented information required by the ISMS
    C. The use of passwords
5. **An employee has received an email with a link that, when clicked, redirects to a malicious website. The IT manager identifies the issue and immediately blocks the email forward system. What action should the organization take to prevent similar situations from recurring?**
    A. Conduct an awareness program to address social engineering and risks associated with emails
    B. Conduct a training program to inform the employees about the risks associated with phishing and spams
    C. Conduct an awareness program to address problems related to access control

Section 20

Security operations management

- Change management planning
- Management of operations
- Resource management
- ISO/IEC 27035-1 and ISO/IEC 27035-2
- ISO/IEC 27032
- Information security incident management policy
- Process and procedure for incident management
- Incident response team
- Incident management security controls
- Forensics process
- Records of information security incidents
- Measure and review of the incident management process

2.6 Security Operations Management

1. Define and establish		2. Implement and operate		3. Monitor and review		4. Maintain and improve	
1.1	Initiation of the ISMS implementation	2.1	Documented information management	3.1	Monitoring, measurement, analysis, and evaluation	4.1	Treatment of nonconformities
1.2	Understanding the organization and its context	2.2	Selection and design of controls	3.2	Internal audit	4.2	Continual improvement
1.3	ISMS scope	2.3	Implementation of controls	3.3	Management review		
1.4	Leadership and project approval	2.4	Communication				
1.5	Organizational structure	2.5	Competence and awareness				
1.6	Analysis of the existing system	2.6	Security operations management				
1.7	Security policy						
1.8	Risk management						
1.9	Statement of Applicability						

Continual communication and awareness

ISO/IEC 27001 Requirements

ISO/IEC 27001, clause 8.1

The organization shall plan, implement and control the processes needed to meet requirements, and to implement the actions determined in Clause 6, by:

- *establishing criteria for the processes;*
- *implementing control of the processes in accordance with the criteria.*

Documented information shall be available to the extent necessary to have confidence that the processes have been carried out as planned.

The organization shall control planned changes and review the consequences of unintended changes, taking action to mitigate any adverse effects, as necessary.

The organization shall ensure that externally provided processes, products or services that are relevant to the information security management system are controlled.

ISO/IEC 27003, clause 8.1 Operational planning and control

Processes to meet information security requirements include:

a. *ISMS processes (e.g. management review, internal audit); and*
b. *processes required for implementing the information security risk treatment plan.*

Implementation of plans results in operated and controlled processes.

The organization ultimately remains responsible for planning and controlling any outsourced processes in order to achieve its information security objectives. Thus the organization needs to:

ISO/IEC 27001 Requirements

ISO/IEC 27001, clause 8.2 and 8.3

Information security risk assessment

- *The organization shall perform information security risk assessments at planned intervals or when significant changes are proposed or occur, taking account of the criteria established in 6.1.2 a).*
- *The organization shall retain documented information of the results of the information security risk assessments.*

Information security risk treatment

- *The organization shall implement the information security risk treatment plan.*
- *The organization shall retain documented information of the results of the information security risk treatment.*

ISO/IEC 27001 Requirements

ISO/IEC 27001, clause 5.1 and 7.1

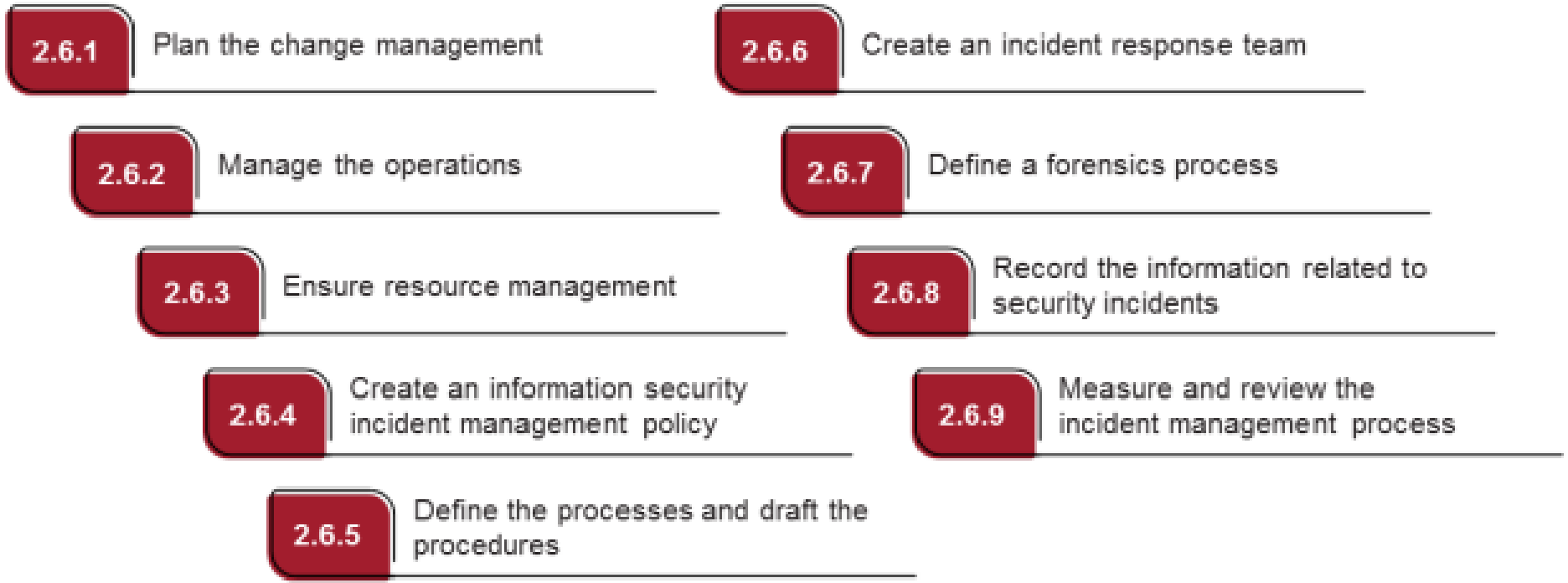
Top management shall demonstrate leadership and commitment with respect to the information security management system by:

c) ensuring that the resources needed for the information security management system are available;

The organization shall determine and provide the resources needed for the establishment, implementation, maintenance and continual improvement of the information security management system.

2.6 Security Operations Management

List of activities



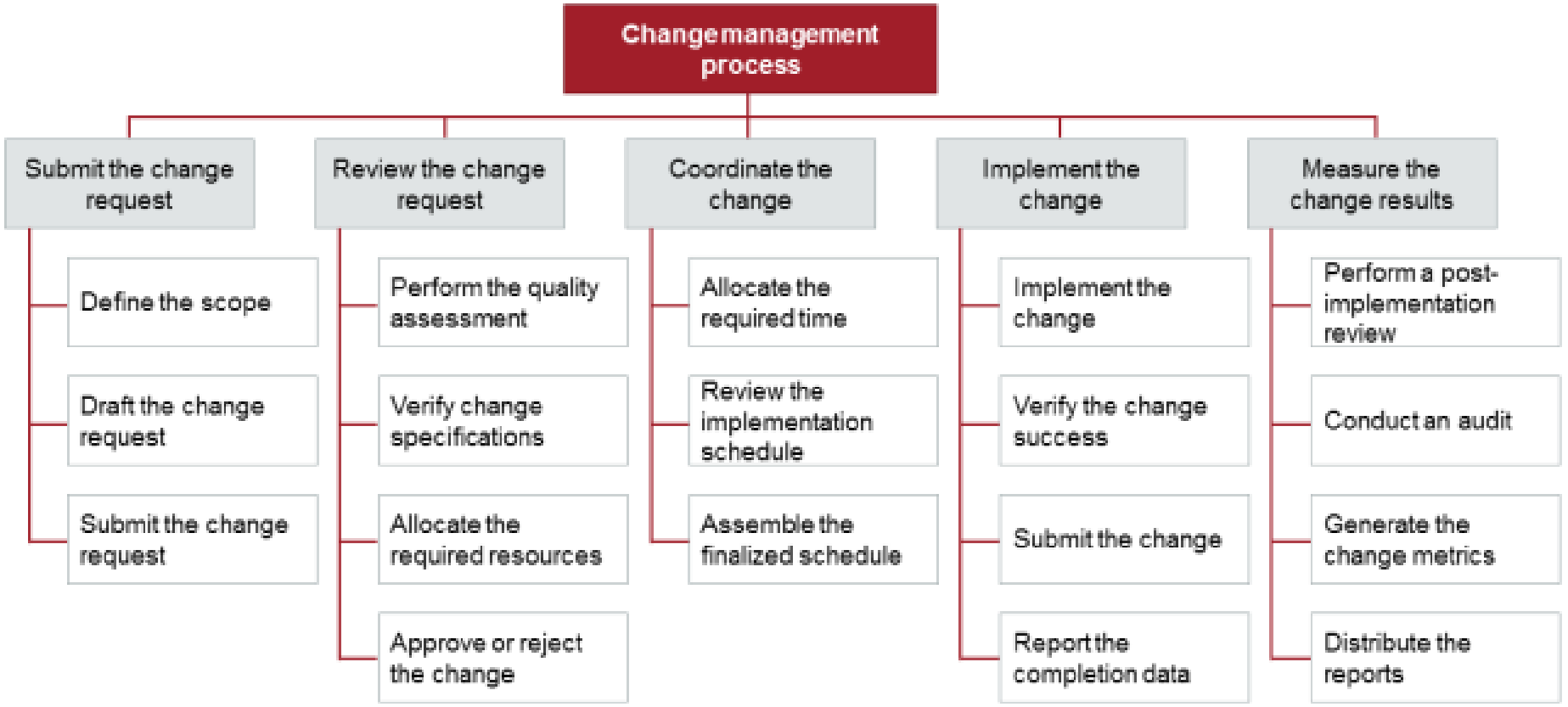
2.6.1 Plan the Change Management

Provide a communication plan for users before transferring to normal operations

Avoid implementing too many new processes at the same time

Where required, conduct staff training before transferring to an operational mode

Change Management Process



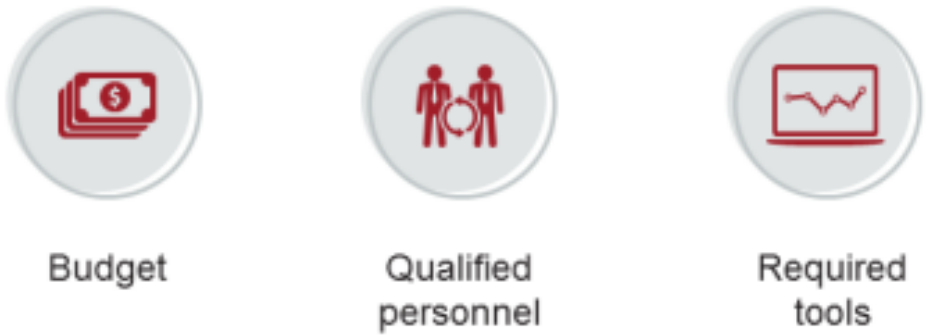
2.6.2 Manage the Operations

Management of operations

When the implementation of the ISMS has been completed, be it a first implementation or the modification of an existing ISMS, the transition to daily operations should be smooth and not interrupt the main business processes.

2.6.3 Ensure Resource Management

To ensure the maintenance and continual improvement of the information security management system, the organization must allocate sufficient resources for its operation.



ISO/IEC 27035-1

- The standard presents basic concepts and phases for managing information security incidents.
- It also provides combined concepts with principles in a structured approach.
- It is a document to be used as a reference to ISO/IEC 27001 and ISO/IEC 27002.
- Organizations cannot get certified against this standard.


INTERNATIONAL STANDARD

ISO/IEC 27035-1

Information technology — Security techniques — Information security incident management —

Part 1:

Principles of incident management

ISO/IEC 27035-2

- The standard provides guidelines to plan and prepare for incident response.
- It is a document to be used as a reference to ISO/IEC 27001 and ISO/IEC 27002.
- The guidelines are based on a new model: “Plan and prepare,” “Lessons learned,” and “Information security incident management phases.”
- Organizations cannot get certified against this standard.

ISO/IEC 27032

- The standard provides guidelines for security practices for stakeholders in the cyberspace.
- It provides an explanation of the relationship between cybersecurity and other types of security.
- It is a framework to enable stakeholders to collaborate on resolving cybersecurity issues.
- Organizations cannot obtain certification against this standard.

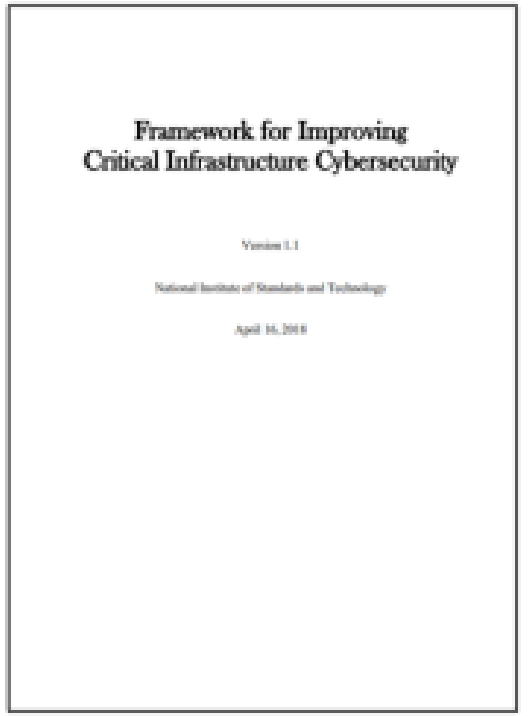

INTERNATIONAL STANDARD

ISO/IEC 27032

Information technology — Security techniques — Guidelines for cybersecurity

NIST Cybersecurity Framework

- It is a framework created by NIST.
- It is designed for the US Federal Government, but can be used by any organization worldwide.
- It follows a phased modeling approach.
- Organizations cannot obtain certification against this standard.



Security Operations Center (SOC)

- The Security Operations Center is the facility of the information security team responsible for detecting, analyzing, responding, reporting, monitoring, and preventing organizations from cybersecurity incidents.
- The SOC team is a group of expert individuals, security analysts, engineers, and managers who supervise security operations. This team works closely with other teams and departments of the organization to ensure that security issues are addressed prior to discovery.
- The primary benefit of correctly implementing the SOC is the improvement of security incident detection through continual monitoring and analysis of the organization's activities.

1. **What does the measurement of change results include?**
    A. Generating the change metrics
    B. Verifying the change success
    C. Approving or rejecting the change
2. **Which of the statements below is NOT true?**
    A. Organizations cannot get certified against ISO/IEC 27032
    B. Organizations cannot get certified against ISO/IEC 27035-2
    C. Organizations can get certified against ISO/IEC 27035-1
3. **Which standard provides guidelines for security practices in the Cyberspace?**
    A. ISO/IEC 27032
    B. ISO/IEC 27035-1
    C. ISO/IEC 27035-2
4. **What is a Security Operations Center (SOC) team?**
    A. A group of information security program coordinators
    B. A group of expert individuals, security analysts, engineers, and managers who supervise security operations
    C. A group of internal auditors who uninterruptedly manage operational activities of the organization
5. **The top management must ensure that all members within the ISMS scope understand the value and importance of an effective information security incident management policy.**
    A. True
    B. False

ISO/IEC 27035-1

ISO/IEC 27035-1, Figure 3

PLAN AND PREPARE

- *information security incident management policy, and commitment of top management*
- *information security policies, including those related to risk management, updated at both corporate level and system, service, and network levels*
- *information security incident management plan*
- *IRT establishment*
- *relationships and connections with internal and external organizations*
- *technical and other support (including organizational and operational support)*
- *information security incident management awareness briefings and training*
- *information security incident management plan testing*

DETECTION AND REPORTING

- *collecting situational awareness information from local environment and external data sources and news feeds*
- *monitoring of constituency systems and networks*
- *detection and alerting of anomalous, suspicious or malicious activities*
- *collection of information security event reports from constituents, vendors, other IRTs or security organizations and automated sensors*
- *reporting information security events*

ISO/IEC 27035-1

ISO/IEC 27035-1, Figure 3 (cont'd)

2.6.4 Create an Information Security Incident Management Policy

The information security incident management policy should include the following:

- Top management's commitment
- Definition of an information security incident
- Roles and responsibilities
- Collection and preservation of records
- Training and awareness
- Reference to legal, regulatory, and contractual requirements

2.6.6 Create an Incident Response Team

ISO/IEC 27035-2, clause 7.1

- *The aim of establishing the IRT is to provide the organization with appropriate capability for assessing, responding to and learning from information security incidents, and providing the necessary coordination, management, feedback and communication.*
- *An IRT contributes to the reduction in physical and monetary damage, as well as the reduction of the damage to the organization's reputation that is sometimes associated with information security incidents.*
- *IRTs can be structured differently depending on the organization size, its staff members and industry type.*

Implement Incident Management Security Controls

Examples of preventive controls

- Training sessions, user awareness, demilitarized zone (DMZ), virtual private network (VPN), personnel selection, etc.

Examples of detective controls

- Intrusion detection system (IDS), security guard, security alerts, etc.

Examples of corrective controls

- Incident response group, incidents handling process, forensics process, etc.

ISO/IEC 27001 emphasizes the need to implement controls to detect and respond (e.g., correction) to security incidents. It is also requires to establish a number of preventive measures, such as training of key stakeholders and user awareness.

Here are the main security controls related to incident management:

Examples of preventive controls

- Proper training of staff
- Controlling of physical access to the equipment
- Well-designed documents
- Authentication and authorization (password)
- Cryptography

Examples of detective controls

- Telecommunications equipment with built-in alarm systems
- Intrusion detection systems (IDS)
- Alarms for the detection of heat, smoke, fire, or risk to water
- Checking of duplicate calculations
- Video cameras

Examples of corrective controls

- Establishment of emergency plans with all the necessary training, awareness, test, and maintenance activities
- Creation of an incident response team
- Incidents investigation process

2.6.7 Define a Forensics Process

ISO/IEC 27002, clause 5.28

- *Internal procedures should be developed and followed when dealing with evidence related to information security events for the purposes of disciplinary and legal actions. The requirements of different jurisdictions should be considered to maximize chances of admission across the relevant jurisdictions.*
- *In general, these procedures for the management of evidence should provide instructions for the identification, collection, acquisition and preservation of evidence in accordance with different types of storage media, devices and status of devices (i.e. powered on or off).*

2.6.8 Record the Information Related to Security Incidents

All relevant information related to the incident should be recorded, including:

- Unique record identifier
- Category and priority
- Date and time of the recording
- Identification of the person who reported the incident
- Identification of the person who created the incident record
- Description of the symptoms
- Incident status (active, pending, closed)
- Assets affected
- Closing information (resolution, date, and time of the closure)
- Groups or individuals affected by the incident
- Activities undertaken to resolve the incident and their results
- Approvals of actions taken and incident closure

2.6.9 Measure and Review the Incident Management Process

The performance of the incident management process should be regularly:

Measured

using performance indicators

Re-evaluated

to identify corrective and preventive actions

Business Continuity and Disaster Recovery

Differences

Business continuity (BC)

- Defines the dangers that threaten an organization
- Defines an effective response
- Prioritizes recovery efforts
- Protects the interests of various interested parties

Disaster recovery (DR)

- Deals with the direct impact of an event, such as server outages, security breaches, or hurricanes
- Involves stopping the disaster's effects as quickly as possible and immediately addressing its consequences

1. **Upon receiving an event report, the operations support group should complete the information security event ticket, analyze it (triage), and assign a priority. What process is this?**
    A. Initial assessment and decision
    B. Detection and reporting
    C. Response
2. **A team where the responsibility for dealing with incidents is typically assigned to a specifically qualified group of individuals is known as:**
    A. Security team
    B. Internal computer security incident response team (Internal CSIRT)
    C. Management team
3. **What type of control is cryptography?**
    A. Preventive control
    B. Detective control
    C. Corrective control
4. **What are the steps of a forensic analysis?**
    A. Prepare, review, and analyze
    B. Prepare, collect, archive, and report
    C. Prepare, collect and archive, review and analyze, and report
5. **The performance of the incident management process should be regularly _____.**
    A. Measured using imperial units
    B. Evaluated to identify corrective actions
    C. Re-evaluated to identify corrective and preventive actions

6.Disaster recovery (DR) defines the dangers that threaten an organization and protects the interests of various interested parties.

A. True
B. False