|  |
| --- |
| IU |
| Information Security Standards |
| Course Code |

# Learning Objectives

In recent times, it has become impossible to survive in our world without the Internet and interconnectedness. The proliferation of social media platforms, tools and technologies for interactivity is on the rise. Through interactions on each of these digital platforms and media, digital footprints and other means of tracing users has increased, to an extent that, it’s become highly complex, from basic hacking or technical approaches to more subtle, social engineering and non-technical approaches which leverage and deceive the susceptibility of the human mind. Almost all aspects of our lives and interactions are held online. This interconnectedness poses real security challenges to both the individual and the organization. Security of information assets (a collection of organized, managed and valuable knowledge or data) is often overlooked, however, costly.

This course will serve as your guide in navigating the difficult and complex world of information security, its accompanying legal and regulatory requirements and all the relevant standards expected to be implemented to safeguard organizational assets. Most organizations focus on building IT systems but forget the broader management context, including standards which seek to help organizations align their activities and operations to best practices and similar methods of managing information security across the world. The International Standards Organization (ISO) is the body charged with the responsibility of keeping such standards reviewed, improved, and updated.

While touching on basic security concepts and terminology at the very onset, the course delves further into the entire information security framework which must be implemented in and by an organization, more specifically, an information security management system (ISMS). How to initiate an ISMS and then to implement, manage and control the processes during its implementation and beyond, are covered.

# Unit 1 – Introduction to Information Security

**Study Goals**

On completion of this unit, you will be able to…

… recognize basic security terms, information security concepts and objectives.

… understand and describe information security standards and regulatory frameworks.

… identify and discuss information security standards, such as the ISO 27000 Series and BSI standards.

… develop information security management systems (ISMSs), analyze its subtleties, including controls and procedures, and implement measures for continual improvement of such systems.

# 1. Introduction to Information Security

## Introduction

Organizations in contemporary times, are moving towards more deliberate approaches in information security management, contrary to the methodologies employed to deal with information security challenges in the past. This has been necessitated by the ever-growing threats to information security. Risk levels, which would be gathered from analysing vulnerabilities and threats identified, are now becoming more substantial and, in some cases, extremely alarming. Information security measures ought to be commensurate with such heightened activities of malicious persons. Controls, ought to be reviewed, managed, and improved constantly to meet these increasingly complex and sophisticated attacks and threat vectors. The extent and value of information security challenges are growing and so should the measures to curb them, but is that the case?

Companies, whether small, medium or large, have and are still recording, more and more, financial losses in recent years due to information security breaches. Activities of such malicious individuals, such as hacking, ransomware, MITM attacks, etc., for example, seek to cripple organizations and render them powerless. Most companies and organizations have not developed their resilience enough to survive such disruptions to their operations when organizational security is breached. In many cases, large organizations are ill-equipped to fight such activities and are only reactionary and such breaches are often not reported.

IT systems, where information is created, stored, transported and processed, are correspondingly getting more sophisticated, the number of stakeholders and technical aspects are also getting more complex. This complexity introduces a difficulty to customers, in terms of trust. There are security levels that organizations ought to attain to gain trust. Standards such as the ISO 27000 series provide guidance regarding how companies could align their security systems to the level where it offers trust to all stakeholders. Scholars such as Beckers et al. (2014) emphasized that “implementing security standards is difficult, due to the limited support for system development and documentation provided in the standards available”.

To bridge this gap, this unit covers the most important information security terminologies, concepts and objectives, security standards and frameworks and introduces the information security management system (ISMS).

## 1.1 Basic Definitions, Security Concepts, and Information Security Objectives

Organizational assets, which include information assets – such as data and information systems – must be protected from the ever-evolving security threats. It is imperative that organizations incorporate security concepts during the design, acquisition, installation, operation, maintenance, and decommissioning of organizational assets. This section establishes the foundation for understanding the broader field of information security by introducing key terminology and explaining essential information security concepts and objectives.

### History of Information Security

In the view of Whitman and Mattord (2018), the history of information security started with the concept of computer security. The concept of computer security is believed to have arisen during World War II, when the first mainframe computers were developed and used to aid computations for communication code breaking messages, from enemy cryptographic devices like the **Enigma**. During that period, it is reported that multiple levels of security were implemented to protect the devices and the missions they were serving. As a result, processes and methods were needed to maintain data confidentiality. There were restrictions to military locations, some controlled via badges and physical keys, among other measures taken to protect these sensitive devices and systems. The mechanisms to protect national security and resources, at the time, were at best rudimentary. Computer security - or what is now known as information security - was a straightforward process, composed predominantly of physical security and simple document classification schemes. The primary threats to security included physical theft of equipment, espionage, and sabotage. Over time, more complex and technologically sophisticated computer safeguards were needed with the growing need to protect national security, away from the rudimentary approaches. Table…below summarises some of the most important dates in information security.

**Enigma**

This was German code machine, which was first broken by the Poles in the 1930s. The information gained from decrypted transmissions was used to anticipate the actions of the German armed forces.

Keys Dates in Information Security

|  |  |
| --- | --- |
| Date | Document |
| 1968 | Maurice Wilkes discusses Security in *Time-Sharing Computer*. |
| 1970 | Willis H. Ware authors the report *Security Controls for Computer Systems*: *Report of Defense Science Board Task Force on Computer Security-RAND Report R-609,* which was not declassified until 1979. It became known as the seminal work identifying the need for computer security. |
| 1973 | Schell, Downey, and Popek examine the need for additional security in military systems in  *Preliminary Notes on the Design of Secure Military Computer Systems*. |
| 1975 | The Federal Information Processing Standards (FIPS) examines DES (Digital Encryption Standard) in the Federal Register. |
| 1978 | Bisbey and Hollingworth publish their Study “Protection Analysis: Final Report,” which discussed the Protection Analysis project created by ARPA to better understand the vulnerabilities of operating system security and examine the possibility of automated vulnerability detection techniques in existing system software. |
| 1979 | Morris and Thompson author “Password Security: A Case History,” published in the  *Communications of the Association for Computing Machinery* (ACM). The paper examined the design history of a password security scheme on a remotely accessed, time-sharing system. |
| 1979 | Dennis Ritchie publishes “On the Security Of UNIX” and “Protection of Data File Contents,” which discusses secure user IDs, secure group IDs and the problems inherent in the systems. |
| 1982 | The U.S. Department of Defense Computer Security Evaluation Center publishes the first version of the Trusted Computer Security (TCSEC) documents, which came to be known as the Rainbow Series. |
| 1984 | Grampp and Morris write “The UNIX System: UNIX Operating System Security,” In this report, the authors examined four “important handles to computer security”: physical control of premises and computer facilities, management commitment to security Objectives, education of employees, and administrative procedures aimed at increased security. |
| 1984 | Reeds and Weinberger publish “File Security and the UNIX System Crypt Command.” Their premise was: “No can be secure against wiretapping or its equivalent on the computer. Therefore, no technique can be secure against the system administrator or other privileged users...the naive user has no chance.” |
| 1992 | Researchers for the Internet Engineering Task Force, working at the Naval Research Laboratory, develop the Simple Internet protocol plus (SIPP) Security protocols, creating what is now known as IPSEC Security. |

Source: Andrew Sai (2023), based on Whitman and Mattord (2018).

As has been observed earlier in this section, historically, then computer security only focused on protection of devices from attacks. In recent years, the Internet presents millions of threats due to communications, on a massive scale, between many computer systems and networks, some unsecured. Since the 2000s, there has been a growing awareness of the need to improve information security, not only on company level but also a realization that information security is crucial to national security and defence. Governments and companies alike have, and are experiencing the growing threat of **cyber-attacks**, with an increasing need to defend computerized control systems of state utilities and critical national infrastructure. Another growing concern is that threat of nation states engaging in information warfare. A case in point is that of Russia’s alleged hacking of US Democratic Party resources during the 2016 US elections (116th Congress, 2020).

**Cyberattack**

a malicious and deliberate attempt by an individual or organization to breach the information system of another individual or organization

### Basic Security Definitions and Security Concepts

The information security definitions and selected concepts outlined in the following sub-sections are explained in ISO/IEC 27000 or are mentioned in the ISO/IEC 27000:2014. They also come from other ISO standards, where applicable. According to Hintzbergen et al., (2015), the ISO/IEC 27000:2014 is the first volume of the entire ISO 27000 family of standards, containing an overview of the standards and explaining the definitions of terms used in these family of standards, which are all focused on information technology, security techniques and information security management systems. The goal of providing the definitions, according to the ISO is to avoid confusion about terms and definitions while creating a common understanding on terms and definitions. Hintzbergen et al, (2015) in explaining how the framers of the ISO 27000 series seeks to introduce consistency and, create a common understanding on terms and conditions observed that, for example “asset” is defined in the standards as “any item that has value to an organization”. This means that in every standard, notwithstanding the subject, the same definition of asset is referred to (Hintzbergen et al 2015). These same definitions, more specifically, those relevant to this course, are culled and repeated below:

**ISO**

an international standard development organization composed of representative from the national standards organizations of member countries

**Information-related definitions from ISO/IEC 27000 standard**

In the table below, a group of terminologies under the broad umbrella of information-related definitions is presented. These terminologies and concepts start with information, which is to be considered as an asset to an organization or imply information.

Information-Related Definitions from ISO/IEC 27000 standard

|  |  |
| --- | --- |
| Term | Definition |
| Information | Information is data that has meaning in some context for its receiver. |
| Information security | Preservation of confidentiality, integrity, and availability of information. In addition, other properties, such as authenticity, accountability, non-repudiation, and reliability can also be involved. |
| Information security management | Coordinated activities to direct and control an organization with regard to risk. Risk management typically includes risk assessment, risk treatment, risk acceptance and risk communication. |
| Information security management system (ISMS) | Part of the overall management system, based on a business risk approach, to establish, implement, operate, monitor, review, maintain and improve information security. The management system includes organizational structures, policies, planning activities, responsibilities, practices, procedures, processes and resources. |
| Information system | Application, service, information technology asset, or any other information handling component. |

Source: Andrew Sai (2023), based on Hintzbergen et al. (2015).

**Risk-related definitions from ISO/IEC 27000 - Vocabulary**

In the table below, the group of terminologies and concepts which start with risk or are risk-related are presented. These relate to risks and how they are to be interpreted in the context of the course.

Risk-Related Definitions From ISO/IEC 27000

|  |  |
| --- | --- |
| **Term** | **Definition** |
| Residual risk | Risk remaining after risk treatment. Residual risk can contain unidentified risk and can also be known as ‘retained risk.’ |
| Risk | Effect of uncertainty on objectives. |
| Risk acceptance | The decision to accept a risk. |
| Risk analysis | A process to comprehend the nature of risk and to determine the level of risk. A risk analysis provides the basis for risk evaluation and decisions about risk treatment. Risk analysis includes risk estimation. |
| Risk assessment | Risk assessment is the overall process of risk identification, risk analysis and risk evaluation. |
| Risk evaluation | A process of comparing the results of risk analysis with risk criteria to determine whether the risk and/or its magnitude is acceptable or tolerable. |
| Risk identification | The process of finding, recognizing, and describing risks. Risk identification involves the identification of risk sources, events, their causes, and their potential consequences. Risk identification can also involve historical data, theoretical analysis, informed and expert opinions, and stakeholders’ needs. |
| Risk management | Coordinated activities to direct and control an organization with regard to risk. |
| Risk management process | A systematic application of management policies, procedures, and practices to the activities of communicating, consulting, establishing the context and identifying, analysing, evaluating, treating, monitoring, and reviewing risk. ISO/IEC 27005:2011, the ISO standard for information security risk management, uses the term ‘process’ to describe risk management overall. The elements within the risk management process are termed ‘activities’. |
| Risk treatment | The process of selection and implementation of measures to modify risk. |

Source: Andrew Sai (2023), based on Hintzbergen et al. (2015).

Other terminologies and concepts used in this coursebook including control, guideline, asset, attack, policy, preventive action, procedure, process, third-party, threat and vulnerability, which are copiously mentioned in the coursebook can be found on the ISO website. IEC offers the *Electropedia*, which prepares and publishes standards and can be found on the IEC website.

### Information Security Objectives

The reason why information security is important in an organization is to protect information and other organizational assets. Such information could be printed, saved on a computer system, or only living in the mind of a user. The scope of IT security therefore covers all sources including electronically stored information and its processing.

While security incidents could occur or do occur, security controls, when implemented and are effective, are intended to help minimize the level and potency of security threats that an organization may face and assure the continuity of business and its success. Such threats and vulnerabilities cannot be eliminated but their consequences could be minimized with the right security controls in place to ensure fewer security incidents.

To achieve effective information security management, controls ought to be implemented following a risk assessment and management process and then the development and implementation of an information security management system (ISMS). The ISMS is an amalgamation of policies, processes, procedures, organizational structures, software, and hardware intended to protect organizational information assets. The ISMS is expected to be subjected to a periodic review to align with changes and incorporate improvements to systems, also reflecting business objectives, among other strategic objectives of the organization. These controls should be integrated into already existing business processes and should be seamlessly operationalized.

The CIA Triad

Diagram

Description automatically generated

Source: Andrew Sai (2023).

Information can be valuable. This value is based on the characteristics of the information. When such characteristics change, the value changes accordingly. Some of the changes affect the value more significantly, based on the circumstances and the user of that information.

We can infer from the objectives that information must be available, intact and accessible to the intended users without any hindrances. Making information available, accessible, and intact means the user should be able to access information in a timely fashion, without delay or defect. There is, however, a challenge with keeping this triad when managing information. Each of these aspects of the Triad is considered in the following sub-sections:

#### Availability

The ISO/IEC 27001:2013 standards define availability as “property of being accessible and usable upon demand by an authorized entity” Hintzbergen, J., et al (2015). Availability is about ensuring that information is accessible in a timely manner, when needed. It is common knowledge that the other two conditions in the triad are worthless if information is not available. The user, when and where required, with requisite conditions satisfied, should be able to access information.

Information is considered available when authorized users can access it without any obstructions. A simple example is an online library in a university. A user or patron of such online resources requires an identification before accessing the book or materials stack. Such authorized patrons are accepted into the online library system as authorized patrons and the contents of the library are only available to them.

Availability can be compromised through sabotage, denial of service attacks or ransomware. A measure used to counter availability of information threats is backups. The use of redundant networks, servers and applications is also a measure to ensure availability of information.

#### Confidentiality

**MITM attack**

This is an attack in which an attacker is positioned between two communicating parties to intercept and/or alter data traveling between them.

The ISO/IEC 27001:2013 standards define confidentiality as “property that information is not made available or disclosed to unauthorized individuals, entities, or processes.” Hintzbergen, J., et al (2015). Information satisfies the confidentiality requirement when it is protected from disclosure or when information is exposed to individuals and systems without proper authorization. Essentially, authorized users are granted rights and privileges to be able to access information, typically stored, processed, using IT systems. When such information is accessed without proper authorization, there is a breach of confidentiality. A breach of confidentiality can occur in several ways. Some involve direct attacks to gain access to a system or to infiltrate an application or a database. An example of direct attacks uses techniques such as **man-in-the-middle (MITM)** attacks. To protect the confidentiality of information, information assets could be

* classified, such that users with authorization only could access them. For example, information marked as “class A” could mean highly confidential, for only a selected few, say top management.
* stored securely in document storage facilities or with the right tools and resources.
* protected using general and specific security policies which will define access and usage.
* protected through education and training of end users and other stakeholders regarding information security.

Consumers of the Internet and online resources often exchange personal information about themselves for some convenience or value. Signing up on many web portals and online platforms for free, requires that in exchange, such consumers offer as consideration, their personally identifiable information (PII), which are copied, sold, replicated, or distributed by third-party agents within the online chain.

Confidentiality, just like other characteristics of information, does not exist in isolation. It is interdependent. A characteristic is privacy. There are a few measures that could be put in place to curb or better still reduce the spate of confidentiality breaches. Such measures include classifying and restricting data access, implementing access control policies, encrypting data, activating multi-factor authentication (such as 2FA) systems. Another good approach to ensuring confidentiality is training and knowledge readily available to all stakeholders in the information chain.

#### Integrity

Integrity is the third in the triad. The ISO/IEC 27001:2013 standards define integrity as “property of protecting the accuracy and completeness of assets.” Hintzbergen, J., et al (2015). Integrity involves making sure that information is not modified or corrupted. In other words, data is whole, authentic, accurate and reliable.

A breach or violation of the integrity of data or information could occur when an attacker bypasses an intrusion detection system, changes file configurations, and allows unauthorized access, as a first example. A second example is when such an attacker changes system logs and files or thirdly, if an insider, such as an employee violates integrity by accident. For such insider events, a lack of security policies, security controls, processes and procedures have been identified as major triggers.

There are lots of measures that could be implemented to counter information integrity violations. Some of the common ones include hashing or use of hash algorithms, data encryption, use of digital certificates and signatures, and using trustworthy certificate authorities (CAs). A method for verifying the integrity of information is non-repudiation, which is where something cannot be repudiated or denied, ensuring that it is authentic.

Information integrity mechanisms are often grouped into preventive and detective mechanisms. The most common occurrence of integrity breaches is known as unintentional disclosures (Alsmadi I., et al. 2018). With this, users, especially organizational employees lose, misplace, or inadvertently release information in an event not caused by hackers or any electronic attack. For example, some careless organizational employees post pictures of their work monitors with sensitive information openly displayed, among others, on social media. That is an unintentional disclosure. Others take copies of data from their organizations, which might include email addresses, credit card information, ID numbers or important company files and lose them to theft, criminals or for other malicious users to exploit.

### Self-Check Questions

1. Which of the following would be used to ensure that accuracy of information is covered effectively in an organization?

* *Integrity*
* Confidentiality
* Availability
* Authenticity

1. A user logs into a computer system and is required to answer a security question such as “what is your mother’s maiden name” Which of the following is the computer system ensuring?

* Accountability
* *Authentication*
* Authorization
* Applicability

1. Please complete the following sentence.

The *Enigma* was a *German* code machine which was first broken by the *Poles* in the 1930s.

## 1.2 Standards and Regulatory Frameworks

**Standards**

Standards are documents that have been published by a recognized body, such as the International Standards Organization. (ISO), to help communicate a common understanding of the specifications and processes needed to assure the delivery of reliable products and services.

**Standards** are often considered rigid and generally accepted globally. A framework is at best a frame that can be used as a practice. (“Difference Between Standard and Framework”, n.d.) Standards have been developed to harmonize how products and services are delivered to consumers, whether from a government department or agency to a citizen of a country or some new medicine, say for cancer patients, being developed by a pharmaceutical company.

Standards, which are usually not mandatory, spell out the specific protocols and requirements of deliverables, such as an information security management system, such that its integration into an organization will be same around the world. Therefore, the implementation of an ISMS will be consistent globally. They are mostly recommendations about best practices. In the case of the ISMS, for a security manager, the relevant standards serve as a fundamental reference model for the manager to deliver security capabilities and establish ways of delivering security controls which could be applied easily across an organization. Standards help companies to assure that plans, policies, procedures, controls, and other actions taken are consistent with industry and global expectations, are fit for purpose, adding an additional layer of assurance which will satisfy legislative and commercial requirements.

Unlike standards, **regulatory frameworks** are legal mechanisms applicable at both national and international levels, which are mandatory or of a coercive nature. An organization that refuses to satisfy legal or regulatory requirements faces consequences for a lack of compliance. This means if the pharmaceutical company manufacturing the cancer medicines does not follow legal requirements, they risk losing their license or certification which enables them to exist or fines and other penalties, in some cases. On the contrary, standards are not enforceable, but recommendations about best practices. For example, if a standard requires that for a board of directors of a company, some members of the board should understand or have prior working experience in the pharmaceutical industry - is not obligatory but a recommendation.

**Regulatory Framework**

a coercive, mandatory system of rules (instruments, legislation, by-laws, regulation, procedures, degrees)

There are myriad frameworks for information technology. Some of such frameworks are the Federal Information Security Management Act (FISMA), the ISO/IEC 27001 and 27002, the control objectives for information and related technologies (COBIT), among others. It is noteworthy to say that most of these frameworks are subjected to regular review and update. For example, the COBIT framework which define components and design factors to build and sustain a governance system, including information security, in an organization, was recently updated to COBIT 2019, released in 2018, while the ISO/IEC 27001:2022 – *Information security, cybersecurity, and privacy protection – information security management systems – requirements*, was updated and published in 2022. Then, there are those issued by NIST, ENISA, some covering industry-specific areas while others focus on critical infrastructure and how to safeguard same. Others are intended to help protect data and privacy.

According to Landoll (2016), in *Information Security Policies, Procedures and Standards*, page 20-21, “information security standards are a refinement of security requirements in the information security policies that address selected methods, techniques, and devices. These standards are mandatory as they specify required refinements of the information security policies. Standards are typically issued and approved by either senior management or their delegates such as an information security officer or information security manager…. Information security standards are developed to provide greater explanation or specificity for information security policy level statements. For this reason, information security standards should have a direct and clear correlation to the information security policy statement they are refining…”. An example standard statement may read: “The organization should ensure that for password-based authentication, all information systems enforce the following minimum parameter settings: (a) password complexity— 8 characters with both numeric and alphabetic characters, (b) password lifetime—60 days maximum, 1 day minimum, (c) password reuse—6 generations.” (Landoll, 2016, page 20-21)

For the ISMS set up, there are two primary standards, ISO/IEC 27001, and ISO/IEC 27002, which establish the requirements and the necessary procedures for creating an ISMS, which is an important audit and compliance activity. The root ISO/IEC 27000 comprises an overview and the vocabulary which essentially defines the ISMS program to be implemented. The ISO/IEC 27000 series are covered in detail in this Unit.

Aside the primary standards (principally the ISO/IEC 27000 family of standards), there are other related standards and frameworks which work in tandem to satisfy compliance and audit requirements, and in many cases towards certification, in various areas. Such security frameworks often focus on specific industries and sectors. There are tons of such standards, some of which are referred to in this course. A short list of the most common ones is presented below and discussed in the ensuing subunits. It is noteworthy that while the ISO/IEC 27001 allows certification, it is in general not mandatory, however, with some exceptions in certain industries.

The figure below shows some of the most common security standards and frameworks.

Common Security Standards and Frameworks

Shape

Description automatically generated

Source: Andrew Sai (2023).

In no particular order, these common security standards, and regulatory frameworks, available in an enterprise’s arsenal for the safeguarding of security resources, are explained below.

### Common Criteria for Information Technology Security Evaluation

ISO/IEC 15408, also known as the Common Criteria (CC) is an international standard for the security of IT products, including operating systems and firewalls. The current version, released in 2017, is 3.1 revision 5. The CC provides specifications and guidelines for evaluating information security products and systems. It was developed and maintained under an agreement called the **CCRA**. The CC serves as a guide for developing, assessing, and acquiring IT products with security functionality, essentially forming the basis for evaluating the security properties of IT products. Examples of certified products under ISO/IEC 15408 include Microsoft Windows 10, Apple iOS, Samsung Knox, Oracle database, IBM WebSphere Application Server, and many others.

**CCRA**

The Agreement on the Recognition of Common Criteria Certificates in the field of IT Security is an agreement by participating nations.

The CC provides a framework for defining security requirements, evaluating security features and certifying that IT products and systems meet specific standards. The following are six of the most important concepts within CC and how they are applied to secure IT products and systems:

1. **Protection Profile (PP)**: is a document that specifies the required security functionality and assurance requirements for a particular product or system. By defining a set of baseline security requirements, IT product developers can ensure that their products adhere to a specific level of security. Protection profiles can be applied across different industries, allowing for standardization and consistency in secure IT product development.
2. **Security Target** **(ST)**: this is a document that provides a detailed description of a specific product or system’s security features, including its security objectives, threats, and functional requirements. An ST is used to demonstrate that a product or system meets specific security requirements, as defined in the associated protection profile. By reviewing an ST, evaluators can determine if the product or system offers adequate security measures to defend against potential security threats.

**Evaluation Assurance Level** The EAL of an IT product or system is a numerical grade assigned following the completion of a CC evaluation.

1. **Evaluation Assurance Level (EAL)**: is a numerical grade (from EAL1 to EAL7) used to represent the thoroughness and depth of an IT product’s security evaluation. Higher EAL levels indicate greater assurance that the product has been thoroughly tested and is resistant to attack. Through the evaluation process, IT products and systems are granted an EAL based on their degree of adherence to CC standards, allowing customers to make informed decisions about the security of their IT products.
2. **Target of Evaluation (TOE):** refers to the IT product or system being evaluated for its security features, such as software, hardware, or a combination of both. The TOE serves as the focus of the evaluation process and must provide adequate information on the product’s features and functions to facilitate a thorough security assessment.
3. **Assumptions and Threats**: are the conditions that must be satisfied outside the TOE in order for a product or system to achieve its security objectives. Threats are potential events or actions that could compromise the security of an IT product. Identifying and addressing these assumptions and threats is critical to developing a comprehensive security framework for IT products and systems.
4. **Security Functionality (SF) and Security Functional Requirements (SFR)**: SF refers to the features and capabilities of an IT product that contribute to its security objectives. SFRs are specific security capabilities that a product must possess to meet the security objectives defined in the protection profile. Developing well-defined SF and SFR ensures that IT products and systems meet their desired security objectives.

Participating nations have testing organizations that utilize a set of security requirements and evaluation criteria to assess the security of IT products and systems. The certification process involves rigorous evaluation by an accredited evaluation facility, known as an EAL lab. In Germany, for example, the Bundesamt für Sicherheit in der Informationstechnik (BSI) serves as the national approving authority. Agence nationale de la sécurité des systèmes d'information (ANSSI) is the approving authority in France. Outside of the EU, in the United States, it is the National Information Assurance Partnership (NIAP), Communication Security Establishment (CSE) in Canada and Information-technology Promotion Agency (IPA) in Japan.

The ISO/IEC 15408 standards or CC provide a systematic approach to evaluating and ensuring the security of IT products and systems. The concepts and methods within the framework, such as PP, security targets, and EAL contribute to a standardized and consistent process for evaluating and certifying the security of IT products across various industries. As a result, organizations can make informed decisions when choosing products with appropriate security measures to protect against potential threats.

### NIST Security Standards and Guidelines

**Cybersecurity**

This refers to the protection of data found in electronic form from attack or compromise. Information security relates with protection of information and information assets.

The NIST cybersecurity framework (CSF), first published in 2014, is a very popular framework intended to serve as guidance for the management of **cybersecurity** risks. The NIST CSF provides a high-level taxonomy of cybersecurity outcomes and a methodology to evaluate and manage the outcomes. It is one of the over 1300 standard reference materials (SRMs) supplied by the National Institute of Standards and Technology (NIST) of USA to industry, academia, governments and other NIST cybersecurity framework users. The CSF also provides guidance on the protection of privacy and civil rights within the cyber security space. The CSF is divided into three main parts:

1. **Framework core**: This houses activities, outcomes, and references about characteristics and methodologies to cybersecurity.
2. **Framework profile**: this is the list of outcomes selected by an organization from a range of categories and subcategories, following an assessment of risks and its business needs.
3. **Framework implementation tiers**: These are used by organizations to make clear an organization’s perspective of cybersecurity risks and its approach to managing them.

Aside the CSF offering a common language and guidelines for the management of security in an organization, there is the NIST Special Publication (SP) 1800 series which also provides guidance on information security, including risk management, incidence response and supply chain security. Within this NIST SP 1800, some of the specific standards include the NIST SP 800-53 and NIST SP 800-171. They serve as guidance for implementing and applying standards-based security technologies.

### European Union Agency for Cybersecurity (ENISA)

Commonly referred to as the ENISA standards, these are EU standards, frameworks, regulations, and guidelines offering advice and solutions for improving cybersecurity capabilities in the EU. The Agency was created in 2004 by an **EU regulation** No. 460/2004 and is dedicated to the achievement of a common level of cybersecurity across the European region. The Agency contributes to EU cyber policy, maintaining trust in ICT products, services, and processes through cybersecurity certification schemes, and helps member states in the EU to adequately prepare for cybersecurity challenges of the future.

**EU Regulation**

This is a type of legislative act that is directly applicable and binding in all EU countries without the need for national implementing measures.

ENISA offers many tools for measuring maturity levels, self-assessment, and risk management, among others. Some of the most common ENISA tools are the following.

* the Computer Security Incident Response Team (CSIRT) maturity self-assessment tool
* the National Cybersecurity Assessment Framework (NCAF) tool
* SecureSME, which targets small and medium-sized businesses to secure them from cyberattacks
* smartphone Guidelines tools, for developers of smartphones applications
* good practices for the security of healthcare services
* online tool for security of personal data processing
* the Payment Services Directive 2 (PSD2) tool, an interactive map for ensuring security of payments and other financial services’ transactions.

Security regulations and directives have been intentionally developed to protect critical infrastructure, with equal maintenance provided by ENISA, the principal EU agency tasked with ensuring the cybersecurity of member states. Example of such directive include:

#### Security of networks and Information Systems (NIS)

**E**U Directive 2016/1148 aims to increase the levels of cybersecurity and resilience of major systems across the EU region. Introduced in 2016, it is designed to ensure that EU member states have a national framework (including a national security strategy, a competent NIS authority and a CSIRT) in place, which equips them to manage cybersecurity incidents while implementing the directives. These directives are expected to be translated into national laws by each of the EU member states. In Germany, the BSI plays a central role in implementing the NIS directives as a supervisory and enforcement body. The directive also ensures that member states participate in a strategic security cooperation and network group and engage in information exchange.

#### NIS2

**EU Directive**

Is a type of legislative act of the EU that sets out a goal that all EU countries must achieve, but it is up to the individual countries to decide how they will implement it into their national laws.

NIS2 Directive (**EU Directive** 2022/2555) was introduced in 2022 and came into force in 2023. It modernized the existing NIS legal framework to reflect current trends in cyberspace, expanding its scope to cover additional sectors and entities while enhancing incident response and the resiliency of critical infrastructure in the EU region. The primary objectives of NIS2 are to improve cybersecurity across the EU by

* establishing a cyber crises management structure (CyCLONe).
* enhancing the harmonization of security requirements and reporting obligations across member states.
* emphasizing the importance of incorporating areas such as supply chain, vulnerability management, core internet and cyber hygiene into member states’ national security strategies.
* encouraging innovative approaches, such as peer reviews, to promote collaboration and information sharing among EU member states.
* broadening coverage to include more entities and sectors not initially covered by the original nis.

The introduction of NIS2 also assigns several responsibilities to ENISA, the EU agency for cybersecurity. Key tasks include the development and maintenance of an EU vulnerability registry, acting as the secretariat for CyCLONe, publishing annual reports on the state of cybersecurity in the EU, supporting peer reviews among members states, and maintaining a register of entities that provide cross-border services such as domain name registration, cloud computing, and data center service providers. Member states are expected to incorporate these changes into their national legislation.

#### Resilience of Critical Entities (RCE) Directive

The RCE is part of a legislative package with measures intended to improve the protection of cybersecurity and critical infrastructure in the EU, incident response capabilities of entities, and competent authorities. Proposed in the European Commission in 2020, the RCE directive seeks to establish a common cybersecurity certification framework, promote cybersecurity research and innovation and strengthen the cyber security industry in the EU.

Other frameworks, standards and guidelines developed and managed by ENISA include the following:

* The European Cybersecurity Certification Framework
* Cybersecurity Culture in Organizations
* The Baseline Security Recommendations for Internet of Things (**IoT**)
* Cloud Security Guide for SMEs

### Industry-Specific Standards

Various standards, frameworks, regulations, and guidelines ensure quality, safety, and consistency across different sectors and industries. Organizations within specific industries and sectors must adhere to these precise requirements. When setting up an ISMS, relevant standards and frameworks should be considered alongside primary ISO/IEC standards for the establishment and management of the ISMS to ensure collective compliance. Although numerous standards and frameworks exist, the most common ones include:

* **ISO/IEC 13485:2016 (medical devices quality management system**): This is a comprehensive list of requirements that should be followed to ensure the quality of the design and manufacturing of medical devices.
* **AS9100 (aerospace quality management system):** This is a standard specific to the aerospace industry. It provides a framework for managing quality within that sector, addressing safety, reliability, and regulatory compliance and risk management.
* **Hazard analysis and critical control points (HACCP):** This is used in the food industry to ensure the safety of food products; identifying potential hazards, implementing control measures, and monitoring the effectiveness of systems.
* **Good manufacturing practice (GMP):** This is a standard used by the pharmaceutical and medical device industries to ensure that products are produced consistently and meet quality standards. It covers all aspects in manufacturing, from raw materials to the final finished products.
* **FSSC 22000 (food safety systems certification):** This is a standard for the food safety management system certification scheme, covering the entire supply chain. It integrates with the HACCP and other food-related safety requirements such as ISO/IEC 22000 and ISO/TS 22002-1.
* **ISO/SAE 21434 (cyber security for road vehicles):** This is a new standard that sets the requirements for security in the automotive industry. It was developed by the ISO and Society for Automotive Engineers (SAE), offering a unified framework for the industry to address security risks. The standards focus on cybersecurity of road vehicles.
* **EN 50128 - railway applications (communication, signaling and processing systems):** These are standards set for the development of software for railway control and protection systems. By applying these standards, safety and reliability of railway operations is ensured through the development of dependable software. The standards help to ensure the security and operations of critical infrastructure sectors in the EU.
* **IEC 62443:** This is a standard published by the International Electrotechnical Commission (IEC), providing a framework for securing industrial automation and control systems, commonly used in securing critical infrastructure of the energy and transportation sectors.
* **ISO/IEC 27017:** This is a security framework for using cloud services. ISO/IEC 27017 is part of the ISO/IEC 27000 family of standards, which is intended to help keep cloud services providers in compliance to keep their customers and users safe.
* **SOC (service organization controls) for cybersecurity:** This is a cybersecurity-specific framework developed to provide a standardized approach to assessing and reporting the risk management program of an organization. It was developed by the American Institute of Certified Public Accountants (AICPA).

### Other Standards and Frameworks

The following standards and frameworks are not necessarily industry specific. They do have some relationship with IT security even though they do not always address IT security explicitly. They are applied across industries and sectors, where relevant.

* **OHSAS 18001/ISO/IEC 45001 (occupational health and safety management system):** This standard helps organizations to establish a systematic approach to managing occupational health and safety risks. They are intended to help prevent work-related injuries and promote a safety culture overall.
* **ISO/IEC 9001 (quality management system):** This is used by a wide range of industries to establish and maintain quality systems. Its focus is customer satisfaction, continuous improvement and adhering to statutory and regulatory requirements.
* **ISO/IEC 14001 (environmental management system):** This standard provides a framework for organizations to manage their environmental obligations responsibly and sustainably, emphasizing how organizations should minimize environmental impact, comply with respective regulations, and improve their performance.
* **ISO/IEC 22301 (business continuity management system**): Organizations that implement a business continuity management system (BCMS) using the ISO/IEC 22301 can go through a formal evaluation process to obtain accreditation against this standard. It demonstrates that the organization adheres to good practices in BCMS**.**
* **Control objectives for information and related technologies (COBIT):** This is a framework for best practices in IT governance and management. It is developed and managed by the Information systems Audit and Control Association (ISACA). COBIT information security framework creates an enterprise-wide IT governance system implementing several security controls, through a strict set of policies and rules that strengthen enterprise security overall.
* **Information Technology Infrastructure Library (ITIL)**: This is a globally adopted service management framework that has a devoted part known as information security management (ISM) intended to align IT and business security in an enterprise to ensure it is managed across the board.
* **Committee of Sponsoring Organizations (COSO) framewor**k: is a widely used framework for the internal control of financial reporting. COSO recently developed a framework specifically for cybersecurity risk management.

In summary, the standards and frameworks mentioned in this subsection have several things in common, including:

* **They are not industry-specific**: They can be applied across industries and sectors, depending on their relevance and applicability.
* **They have a relationship with IT security**: While they do not address IT security explicitly, they have some connection to it. For example, COBIT and ITIL have specific components related to information security management.
* **They promote a systematic approach**: Each of them provides a structured methodology for managing various aspects of an organization, such as occupational health and safety, quality, environmental impact, business continuity, IT governance, and financial reporting.
* **They emphasize continuous improvement**: They focus on the ongoing enhancement of an organization’s processes, systems, and overall performance.
* **They encourage compliance with statutory and regulatory requirements**: Adhering to these standards and frameworks helps organizations maintain compliance with relevant laws, regulations and industry best practices.
* **They demonstrate a commitment to excellence**: Organizations that choose to adopt and obtain accreditation against these standards and frameworks illustrate their dedication to upholding high professional standards and delivering quality goods and services.

#### To what extent are these standards and frameworks consistent?

Although each standard and framework has its unique focus and application, they do often share certain core principles such as risk management, process improvement, and regulatory compliance. These, as common grounds, allow them to be compatible and complementary to each other in various ways. For example, organizations that implement an environmental management system (ISO/IEC 14001) can easily integrate an occupational health and safety management system (OHSMS) following the OHSAS 18001/ISO/IEC 45001. In the same vein, an organization that uses COBIT for IT governance can align it with ITIL’s information security management (ISM) practices for robust cybersecurity protocols. Further, these standards and frameworks share a similar structure, often adhering to the PDCA cycle for continual improvement. Such an approach allows organizations to assess their current state, set objectives and targets, implement actions, and monitor progress for each of the standard’s respective areas.

It is essential to recognize that each of these standards and frameworks have their unique scope, objective, and requirement. Organizations need to understand the individual aspects of each framework and the proper way to implement them in their operations. While adopting multiple standards and frameworks can be advantageous, it can also be challenging to navigate overlapping areas and requirements, ensuring consistent application across all levels of an organization. Regardless of the specific standards or frameworks used, organizations must prioritize a comprehensive understanding of their security, compliance, and risk management needs. This way, they can adopt the right combination of standards and frameworks, enabling a secure environment for employees, customers and stakeholders.

### Data Protection/Privacy Standards, Laws, and Regulations

In many industries, data protection and privacy standards overlap with other regulations and frameworks. The most commonly incorporated data protection and privacy standards are crucial, as they establish the organization’s requirements for safeguarding data and privacy when providing services or delivering goods and products. Ensuring compliance with these standards often reduces the risk of data breaches and cyberattacks, effectively decreasing the organization’s risk level concerning data protection and privacy. Additionally, these standards and frameworks are vital when implementing an ISMS, as they align with the primary standards for the comprehensive management of the organization’s security practices:

* **GDPR (General Data Protection Regulations):** The GDPR is a regulation which governs the collection, storage, processing and sharing of personal data of EU citizens, regardless of whether the organization is based in the EU. It imposes strict requirements for the protection of data, including the need for express consent, data security measures and the right of data subjects to have their data deleted, among other things.
* **ePrivacy Directive:** are a set of rules for how electronic communications, such as emails, text messaging and voice over IP (VoIP) services, should be used. Organizations need the consent of users to collect and use their personal data, providing clearly how the data will be used.
* **Directive on data protection in law enforcement**: this is a directive for the processing of personal data by law enforcement authorities, with the aim to ensure that the rights of individuals are respected, and their personal data are only used for legitimate purposes. This directive is specific to the processing of personal data by law enforcement authorities. It ensures that the rights of individuals citizens are respected, with their personal data used solely for legitimate purposes.

In closing this section, data protection and privacy standards such as GDPR, ePrivacy Directive and Directive on Data Protection in Law Enforcement provide essential guidelines for organizations to follow when handling sensitive data. Adherence to these standards reduces the risk of data breaches and unauthorized access while ensuring that both businesses and individual citizens are protected. Proper implementation of these standards results in a secure environment, ultimately fostering trust and customer confidence in the organization’s ability to protect and maintain the privacy of their data.

### Self-Check Questions

1. How should senior managers view the use of international standards for information security within an organization?

* *As implementing best practice*.
* If there was the right business environment to implement, as a good idea.
* As a solution when there is a security breach or serious problem in the organization
* As the sole job of the IT director.

1. Please complete the following sentence.

A framework is at best a frame that can be used as a *practice.*

## 1.3 Security Standards: ISO/IEC 27000 Family and BSI Standards

Standards can be described as documents published by internationally recognized bodies, such as the ISO, to assist in dissemination of a common framework, provide assurance, and understanding of specifications and processes required to deliver reliable products and services. The purpose of standards is to address the challenges organizations experience in the delivery of goods and services to consumers. Standards are specific requirements that support high-level policies. (Campbell, 2016). They define what an organization will do to achieve its policy objectives.

### The ISO/IEC 27000 Series of Standards

The ISO/IEC 27001 belongs to a wider family of ISO 27000 series. It is regarded as the source for a whole numbered series, all of which provide a globally accepted framework for effective information security management. The series was developed by a joint committee of the International Standards Organization (ISO) in Geneva and the International Electrotechnical Commission (IEC). The naming convention of the standards in the series is an ISO/IEC prefix, followed by suffix, which is also their publication date. For example, the ISO 27001:2013 was published in 2013. Corrections and updates are made and applied over the years, during which revisions are made and the document is updated accordingly. Meanwhile, ISO/IEC 27001:2022 was published in 2022, which revised previous versions. Clauses are particular and separate articles, stipulations, or provisions specified in the standards. For example, Clause 5.2 of the ISO/IEC 27001 is a provision which requires the top management of an organization to establish an information security policy.

**ISO 27001:2013 Certified**

This means the organization’s ISO 27001 ISMS has been certified in compliance with the standards by an accredited certification body, following an external audit.

If an organization was **certified ISO 27001:2013**, that organization must upgrade to ISO/IEC 27001:2022 before the recertification surveillance or audit. It is important that based on the ISMS scope of the organization, some new controls may have to be implemented.

The ISMS family of standards are organized as follows:

* **the root standard**, ISO/IEC 27000, considered the vocabulary standard: Clause 5.2
* **requirement standards**: Clause 5.3 (27001, 27006 and 27009)
* **guidelines standards:** Clause 5.4 (ISO/IEC 27002-8, 270013-14, TR27016, 27021)
* **sector-specific guidelines standards**: Clause 5.5 (ISO/IEC 27010-11, 27017-19)
* **control-specific guidelines standards:** ISO2703x, ISO2704x

Three of the most common standards are described below.

#### Root standard: ISO/IEC 27000

The root standard ISO/IEC 27000 titled: *Information technology – security techniques – information security management systems – overview and vocabulary*, can be described as the overview and terminology document. For scope, this document provides an overview of the ISMS family of standards, introduces the ISMS, terms, and definitions relevant to the ISMS.

#### Requirement standards: ISO/IEC 27001

ISO/IEC 27001 titled: *Information technology – security techniques – information security management systems – requirements*, is one of the standards specifying requirements. There are other standards within that category, as outlined earlier. In terms of scope, the root standard specifies requirements for establishing, implementing, operating, monitoring, reviewing, maintaining, and improving the formalized ISMS within an organization. The purpose of the ISO/IEC 27001 is to provide the normative requirements towards the development and operations of an ISMS within an organization, notwithstanding its size, type, or nature.

#### Guidelines standards: ISO/IEC 27002

**Guideline**

a description that clarifies what should be done and how, to achieve the objectives set out in policies

An example of **guidelines** standards is the ISO/IEC 27002, titled: *Information technology – security techniques – code of practice for information security controls*. The ISO/IEC 27002 houses a list of commonly accepted control objectives and best practice controls which serve as implementation guidance for the selection and implementation of controls towards attaining effective information security in an organization. It is also a document which provides guidance on the implementation of security controls (specifically clauses 5 to 18) which offer organizations of all sizes, types and nature implementation advice and guidance on best practices, to support security controls in the organization.

The course book frequently refers to the ISO/IEC 27001:2013 standard. In certain cases, the updated ISO/IEC 27001:2022 version is also mentioned as needed. Do note that if the IEC or the suffix is omitted from the name in this coursebook, it does not affect the meaning or significance of the standard. The missing parts are assumed to be implied, and the reference still corresponds to the appropriate standards.

### BSI Standards

In Germany, there exists a Federal Office for Information Security or Bundesamt für Sicherheit in der Informationstechnik (BSI). This entity is the upper-level government agency charged with the responsibility of managing computer and communication security. It is also the central certification body for IT system’s security assurance, computer and data security and data protection in Germany. Its responsibilities include securing computer applications, critical infrastructure, internet security, cryptography, as well as certification of security products and accreditation of test laboratories for security in Germany. The BSI Germany issues guidelines known as the BSI standards. They provide baseline recommendations, technical guidance, methods, processes, and procedures for effective information security within Germany. Government and state authorities, companies, manufacturers, and service providers all use the BSI standards. The BSI standards 200-1, 200-2 and 200-3 have replaced the BSI standards of the 100-x series since October 2017.

#### BSI standard 200-x series

The BSI standard 200-1 defines the requirements for an ISMS. It is developed in tandem with the prescriptions of the ISO/IEC 27001, while taking into consideration recommendations from other standards such as the ISO/IEC 27002.

The BSI standard 200-2 serves as the foundation for the BSI approach for establishing an ISMS, with three procedures for implementing the needed baseline IT protection in an organization. It explains how an ISMS can be built using the three different methodologies.

The BSI standard 200-3 houses risk-related steps and tasks for the implementation of an effective IT security framework within an organization to achieve the desired level of security.

The BSI standard 200-4 is the modernised standard which provides practical instructions for setting up and establishing business continuity management systems in an organization.

It is instructive to note that users of the BSI standards will find them ideal if they are already working with the IT-Grunschutz methodology and wish to add risk analysis as another layer.

The transition to the modernized IT baseline protection has an impact on an ISMS, which is based on the previous IT baseline protection method in accordance with the BSI standard BSI 100-2 and the IT baseline protection catalogues. This means that the conversion primarily affects both ISO certified and non-certified institutions.

For the sake of transparency, organizations can be certified according to the ISO/IEC 27001 with the IT-Grundschutz as the base for it. That sort of certificate in Germany validates that the IT security concepts implemented in the organization conforms with the requirements of the globally accepted ISO/IEC 27001.

### British Standards Institution and BSI standards

The British Standards Institution (BSI group), hereinafter referred to as the BSI-UK, is responsible for the publication of standards in the United Kingdom (UK). The BSI-UK first published the BS 7799. The first publication was developed by the UK government’s department of trade and industry. In 1998, the first part, which contained best practices for information security management, underwent a revision. The ISO adopted the BSI-UK standards in 2000, as ISO/IEC 17799, which was titled: “*Information Technology: Code of Practice for Information Security Management*”. The newly adopted BSI standards were revised in June 2005 and incorporated into the ISO 27000 series family of standards in 2007 as ISO/IEC 27002 (one of the standards in the family describing guidelines, more specifically, code of practice for information security controls).

### Self-Check Questions

1. The task of the German BSI includes all the following, except,

* *Protection of company networks, detection, and defense of attacks on private networks.*
* Testing, certification and accreditation of IT products and services
* Warning of malware or security holes in IT products and services
* IT security consulting for the federal administration and other target groups
* Information and raising awareness of the public and the economy on IT and Internet security.

1. Which of the following is the organization responsible for the maintenance of ISO/IEC 27001?

* *The International Organization for Standardization*.
* The British Standards Institute
* The German Federal Office for Information Security
* The European Union Standards Committee

## 1.4 Information Security Management System (ISMS)

A “management system” comprises all the policies relating to the supervision and management within an organization, for the purposes of achieving organizational objectives. The part of this system that deals with information security is the ISMS. The ISMS specifies the instruments and methods that organization should engage for planning, adoption, implementation, supervision, and improvement of systems within an organization.

The ISMS typically comprises the following essential components:

* ISMS implementation and management systems and tools: The right processes, systems and tools are needed to guide the implementation of the ISMS.
* Policies and controls: Policies and controls must be clearly defined and available to all stakeholders.
* Supply chain management systems and tools: Third parties and suppliers with access to valuable data must be managed to ensure compliance.
* Implementation resources: A clearly defined qualified manager, team, and budget to implement the ISMS is essential.
* Continual improvement resources: The ISMS and the organization must respond and adjust to changes from various sources, internal and external.
* Communication and engagement resources: Effective communication and engagement, and security training is needed to implement the ISMS.

These components are the most important things needed to implement the ISMS.

Components of an ISMS

Source: Andrew Sai (2023).

### Self-Check Questions

1. Please complete the following sentence.

To implement effectively an ISMS, the six components needed are*: ISMS implementation and management systems and tools*, *policies and controls*, *supply chain management systems and tools*, *implementation resources*, *continual improvement resources* and *communication and engagement resources*.

Summary

This unit covered basic definitions which are required to understand information security and its management within an organization. For both private individuals and companies, these security concepts remain useful.

The integrity, confidentiality and availability of data is one of the primary objectives of information security.

The ISO 27000 family of standards provides the needed framework in the form of best practice guidance for the implementation of ISMSs in an organization.

The ISMS is a set of policies, actions and more which should be integrated seamlessly into organizational processes, procedures, and practices.

Several standards and regulatory frameworks exist. Some interface directly with the primary ISMS standards, ISO/IEC 27001 and ISO/IEC 27002. Others are industry-specific or cover specific areas. The key point to note is that they all work towards ensuring a safe and conducive environment for organizations to thrive, when adhered to, hence should be incorporated into the ISMS process and rollout.

When successfully implemented, the ISMS offers a lot of advantages to organizations, both now and into the future.

# Unit 2 – Initiating an Information Security Management System

**Study Goals**

On completion of this unit, you will be able to …

… identify and describe the processes required for the initial set up of the ISMS.

… analyze an organization’s context for ISMS implementation.

… discuss existing ISMSs, determine their maturity level and areas for continual process improvement.

… define the ISMS scope and formulate security policies.

# 2. Initiating an Information Security Management System

## Introduction

Organizations often use IT systems to collect, process, store or transmit information. Such information and information assets are susceptible to threats of attack, human and other errors, natural events, and inherent vulnerabilities while using them.

The information systems audit and control association, ISACA (2016) defines an information security management system as “a comprehensive set of policies and processes that an organization creates and maintains to manage risk to information assets” (ISACA, 2016). The purpose of the ISMS is to help organizations detect security control gaps and to prevent security events or minimize their impact when they do occur. The ISMS is intended to be a main one-stop-shop for all information pertinent to the assurance of information security within an organization.

Management of information security within an organization based on the prescriptions of the ISO 27000 family of standards, more especially the ISO/IEC 27001 and 27002, is not intended to be an end by itself. The aim of the protection in terms of the CIA is to support business processes towards the attainment of organizational objectives.

This unit covers the initial actions to take to prepare for execution of an ISMS in an organization.

## 2.1 Initial Setup for the ISMS

Setting up an ISMS could be for several reasons, such as to obtain International Standards Organization (ISO) certification or just to remain compliant. Organizations wishing to set up an ISMS will need to consider several perspectives: governance, risk, and compliance. Whichever reason is at play, the three perspectives are only a few of the vital areas required to focus attention on, towards the initial set up and eventual implementation of an ISMS in an organization.

Some challenges have been noted in the guidelines developed to operationalize the ISMS in organizations. Of note is the challenge associated with establishing a certification-ready ISMS in small and medium enterprises. Implementation of the ISMS is a very complex exercise, in which activities and resource utilization could span months. Typically, to set up an effective ISMS, the following three tasks are important:

**TARA framework**

a tool that helps to assess risks and manage them. The strategies include transfer, avoid, reduce and Accept risk

1. Identify information assets, taking cognizance of the CIA triad.
2. Assess risks, including vulnerabilities, threats, scenarios, and probabilities.
3. Treat the risks using the **transfer, avoid, reduce, and accept (TARA) framework**.

### Self-Check Questions

1. TARA is a framework that helps to assess risks and manage them within organizations. The strategies include *Transfer*, *Avoid*, *Reduce* and *Accept* risk.

## 2.2 Analysis of the Organization

In accordance with the ISO standards for information security management, the organizational context is to be defined. Clause 5.3.1 of the **ISO/IEC 31000** specifies that both internal and external issues should be considered when setting up the ISMS.

**ISO 31000**

This is a family of standards by the ISO that provides principles and generic guidelines on managing risks faced by an organization.

Various ISMS practitioners have suggested that even though the process is complicated, it is possible to get around the ISMS set up by following the suggestions below. It is important to note that the suggestions are numerous, however the following are essential:

### Understanding the Internal Organizational Context

When considering the implementation of an ISMS, understanding the internal organizational context is a crucial aspect of the process, which involves gaining insight into the organization’s objectives, values, culture, and risk tolerance, as well as developing a clear understanding of the legal, regulatory and contractual requirements that apply to the organization’s information security. Some of the key factors to consider during these initial stages are as follows:

* **scope and objectives of the ISMS:** Define the scope of the ISMS, including the specific areas of the organization that will be covered by the ISMS, and what it aims to achieve. As an example, the ISMS may be focused on protecting customer data, ensuring business continuity, or achieving compliance with specific regulations. They will influence greatly the choice of the policies and procedures to be incorporated into the ISMS.
* **stakeholder identification and communication:** Identify the critical stakeholders in your organization, such as employees, management, customers, and suppliers and considering their specific concerns and requirements, means engaging these stakeholders early in the process to ensure that their needs are taken into account and addressed in the design and implementation of the ISMS.
* **organizational culture:** Understand the culture of the organization, which is vital for the successful implementation of an ISMS. This will include aspects such as leadership styles, decision-making processes, and attitudes in general towards risk-taking. A strong culture that values information security may contribute to the effectiveness of an ISMS when implemented.
* **resources and capabilities:** Evaluate resources and capabilities available in the organization that could support the successful implementation of the ISMS, which could include human resources, such as skilled information security professionals, as well as financial, technological, and other resources. Where there are resource and capability gaps, these should be identified, to ensure that adequate resources are allocated to support the ISMS implementation.
* **Legal, regulatory, and contractual requirements:** Identify legal, regulatory, and contractual obligations that apply to the organization in the context of information security. These may include laws and regulations covering data protection and privacy, cybersecurity, and industry-specific requirements. Ensuring that the ISMS aligns to these requirements helps to ensure compliance and reduce the risk of fines and penalties.
* **risk appetite and tolerance**: Evaluate the organization’s risk appetite and tolerance levels towards the implementation of the ISMS. This will serve as a guide when selecting the appropriate risk assessment and management methodologies as well as the level of investment in information security measures to implement.
* **review of existing policies, procedures and controls**: Identify any existing policies, procedures and controls related to information security and assess their effectiveness and use this information to inform the development of the ISMS. This will typically involve updating or replacing existing policies and procedures or supplementing some with additional controls.
* **integration of the ISMS with other management systems**: The ISMS must align with and integrate into any existing management systems, such as a quality management system, environmental management system, or occupational health and safety management system, just to name a few. This alignment will help to streamline processes, reduce duplication of effort, and create synergies between the different systems. Do not forget, the ISMS is not one-off or just one policy, but a set of policies, systems, processes and more.

An important aspect of setting up initially for the ISMS implementation is assessment of business needs. Understanding why a business exists is crucial to assessing what the business needs and being able to adequately strategize for the ISO/IEC 27001 implementation. From a business standpoint it is crucial, and the business need is a subset of the internal context analysis. When this step is skipped or neglected, this could lead to ISMS scope planning and analysis challenges, which are difficult to resolve later in the process. It is imperative to get this right at the very onset.

Understanding the internal business context is an important first step towards re-configuring the organizational culture, such that the ISMS will be embedded in the organization. This includes understanding the kind of products and services offered to customers and the risk associated with their provision so that processes and assets that support these products and services that need to be controlled, are not left out from a security point of view. This also includes assessing the resources available to the organization, such as the technologies, systems, equipment, and personnel available to help guide the process.

Taking time to understand the internal organizational context during the initial set up of the ISMS ensures that the system is tailored to specific needs and designed to effectively address the risks and challenges an organization may be facing, which will ultimately improve the effectiveness of the ISMS and also contribute to the achievement of the organization’s information security objectives.

### Understanding the External Organizational Context

With the internal organizational context understood, the external context, including the kind of legislation which applies to the business, what threats and risks could emanate from the external environment are worthy of a review and understanding to set up an effective ISMS. This understanding of the external context equally contributes to better definition of the ISMS scope. Requirement and situational analysis are important to the ISMS scope definition.

The ISMS scope is very critical, therefore, clause 4.3 of the ISO/IEC 27001 specifies how it should be defined so that stakeholders such as customers, auditors, staff of an organization and its senior management are aware of the scope covered by the ISMS.

Some important areas to analyze include

* legal and regulatory requirements, such as legal, safety, and regulatory requirements, as well as labor laws and IT-related safety requirements.
* political and economic environmental considerations, such as monitoring government policy changes and changes in currency rates, along with other economic indicators and social considerations.

### Establishment of an Information Security Policy

Once the internal and external organizational contexts have been clearly understood, it is the responsibility of senior or **top management** to establish an information security policy in accordance with the requirements of clause 5.2 of ISO 27001. The information security policy must be documented. This means that management commitment is needed to put the document together and ensure its availability to, and relevance for all stakeholders. The policy must be approved by the board and published so that the key stakeholders, staff, customers, and suppliers are aware of it. In the information security policy document, what the ISMS is expected to achieve (for example, the objectives) should be clearly defined.

**Top Management**

the person or people who directs and controls an organization

Establishing an information security policy is a crucial step towards implementing an effective ISMS in compliance with the ISO/IEC 27001. The policy sets the foundation for the organization’s risk management approach and helps to foster a culture of security awareness and accountability. Organizations can ensure that their information security policy is comprehensive and robust by focusing on factors such as management commitment, alignment with organizational objectives, a risk-based approach, clear roles and responsibilities, continuous improvement, effective communication, incident management, business continuity, and review and updates. In the following, a roadmap is provided on what to look for when establishing an information security policy following the ISO/IEC 27001 standard. Some of the items on the list to check for are - that information security policy should be aligned to the organizational objectives, and that roles and responsibilities ought to be clearly defined, which are covered in some detail later in the Unit. A few of the most important are as follows:

* **management commitment and top-down approach**: Organizations must have a top-level commitment, which should include providing the needed resources, setting organizational priorities, and fostering a security-conscious culture. The management should establish an interdisciplinary team of stakeholders to develop and maintain the information security policy.
* **aligning with objectives and legal requirements:** This alignment of the information security policy with the strategic objectives, legal and regulatory requirements and risk appetite of the organization are important to ensure that the policy is relevant and effective in addressing the organization’s security needs. It is therefore important to identify all relevant legal, regulatory, and contractual requirements related to information security, data privacy, and data protection and ensure compliance.
* **risk-based approach**: ISO/IEC 27001 advocates for a risk-based approach to information security management. Therefore, a robust information security policy should be based on a comprehensive risk assessment, which identifies and assesses threats and vulnerabilities which might impact information assets. Organizations can allocate resources and implement controls more effectively if risk mitigation efforts are prioritized based on their likelihood and potential impact.
* **baseline controls and continuous improvement**: ISO/IEC 27001:2013 provides a catalog of 114 controls in 14 control domains, known as Annex A. These controls serve as a starting point for organizations to develop their unique set of baseline security controls based on their risk assessment process. An information security policy should include the baseline security controls and their implementation, monitoring, and maintenance procedures should be clarified. Further, the policy should promote a continuous improvement process through regular review, monitoring and evaluation of the effectiveness of the ISMS.
* **communication strategy**: This will ensure that the information security policy is understood and adopted by all stakeholders. Regular communication and feedback mechanisms in place means a consistent understanding of the information security policy at all times.

### Roles and Responsibilities Definitions

Management buy-in and approval are important steps in the journey to the ISMS implementation. The approval indicates that the ISMS is driven from the top of the organization. Another step is the definition of roles and responsibilities and competencies. Clause 5.3 of the ISO/IEC 27001 standards specify the needed roles, responsibilities and competencies and the organization needs to define such roles for the effective implementation of the ISMS, including clearly establishing responsibilities of each of the roles defined towards the ISMS setup, its maintenance and continuous improvement. Senior or top management is important during this step. Without top management commitment, an already difficult process becomes far more complicated.

Implementing an ISMS requires assigning specific roles and responsibilities to ensure effective management and control of information security. Some of the main roles needed for an ISMS under the ISO/IEC 27001 are covered below.

#### Top management

Top management sets the overall direction for the organization’s information security efforts and ensuring that necessary resources are allocated to implement the ISMS. Important responsibilities include

* establishing the ISMS policy.
* ensuring legal and regulatory requirements are met.
* supporting the design, implementation, and improvement of the ISMS, and
* reviewing the effectiveness of the ISMS.

#### Chief Information Security Officer (CISO)

The CISO oversees the entire information security program and ensure security is integrated into every aspect of the organization. The responsibilities of the CISO include the following:

* ensuring that policies and procedures are aligned with organizational objectives and the ISO requirements
* coordinating with stakeholders to ensure that they are informed about the ISMS and its performance
* monitoring security risks and ensuring the ISMS is always updated
* overseeing incident response and reporting

#### Data Protection Officer (DPO)

The DPO oversees the organization’s data privacy-related matters and ensures compliance with privacy regulations. The most important responsibilities of the DPO include the following:

* maintaining a thorough understanding of privacy laws and regulations
* advising on data protection requirements and potential privacy risks
* ensuring data protection assessment are conducted
* facilitating privacy-related training and awareness initiatives

#### ISMS Manager

This manager is responsible for the day-to-day management and maintenance of the ISMS. This manager is responsible for the following:

* ensuring that the ISMS is effectively implemented and maintained.
* coordinating with key stakeholder to ensure their roles in relation to the ISMS areunderstood
* reviewing and updating the ISMS to ensure it remains effective and compliant with ISO/IEC 27001 requirements
* providing guidance and support during ISMS audits and assessments

#### Computer Emergency Response Team (CERT)

**T**his team is responsible for handling and responding to security incidents and ensuring they are resolved effectively. Some of their key responsibilities include the following:

* monitoring information systems for potential security incidents
* identifying, analyzing, and responding to security incidents
* communicating with affected parties and coordinating incident response efforts
* documenting and reporting security incidents, including lessons learned to improve the ISMS processes

A mechanism which helps to define these roles and responsibilities more clearly is the responsible, accountable, consulted, and informed (RACI) matrix. For the roles defined above, a RACI matrix could look like the table below.

Example RACI Matrix for ISMS Role and Responsibilities

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Role/Responsibility | Top Management | CISO | DPO | ISMS Manager | CERT |
| Establish ISMS policy | A | C | C | R | I |
| Ensure legal compliance | A | R | R | C | I |
| Review ISMS effectiveness | A | C | I | R | I |
| Coordinate with stakeholders | R | A | R | R | I |
| Monitor risks and update ISMS | I | A | C | R | R |
| Incident response and reporting | I | R | I | C | A |

Source: Andrew Sai (2023)

### Risk Assessment

Clause 6 of the ISO/IEC 27001 specifies that organizations must assess risk and develop actions to be taken to address information security risks according to the following steps:

1. Planning: This involves agreeing the process of risk assessment, maintaining documentation for risks identified, assessed, and treated, and flagging significant risks, weighting, and scoring them. This initial stage is captured in clause 6.1.1 under “Planning” of the ISO/IEC 27001.
2. Risk assessment: In this step, a risk assessment methodology is defined and applied and documented accordingly. Clause 6.1.2 specifies that the risk assessment process should:
   1. Be able to establish and maintain information security risk criteria.
   2. Repeated risk assessments generated should be consistent, valid and the results comparable.
   3. Be able to identify risks connected with losses due to confidentiality, integrity, and availability breaches within the scope of the ISMS.
   4. Clearly specify ownership of the risks, and
   5. Be able to assess information security risks according to laid down criteria.
3. Documentation: The entire information security risk assessment process should be documented.
4. Risk Treatment: After the risk assessment process is exhausted, a risk treatment should be developed, which should outline the steps needed to mitigate the effects of the identified risks and to manage residual risks, where they do exist. The options available for treatment include the transfer, avoidance, reduction, or acceptance of information security risks (TARA) framework.
5. Risk measures: After the risk treatment plan is in place, the actions that are to be taken are to be specified. Annex A of the ISO/IEC 27001:2013 outlines 114 controls. These controls are categorized into 14 groupings. It is noteworthy that organizations are not obligated to implement entirely all the controls outlined in Annex A, but only those that are relevant, following the risk assessment.

As part of the risk treatment steps, a statement of applicability (SoA) is to be completed in accordance with Clause 6.1.3d of ISO/IEC 27001:2013. The SoA shows the controls that are implemented and why, which controls are not implemented and why. In accordance with the ISO/IEC 27001 **Technical Corrigendum** 2, the SoA that organizations produce must reflect necessary controls in place, the justification for the inclusion of those controls, whether those controls are implemented or otherwise, and justification for the exclusion of any of the controls specified in Annex A of the ISO/IEC 27001. It is striking that these requirements have been updated in the ISO/IEC 27001:2022 version of the standards.

**Technical Corrigendum**

These are issued to correct a technical error or ambiguity in the standards, mistakenly introduced during the drafting or printing of the publication. They are not issued for errors assumed to have no consequences in the application of the publication, however.

### Perform Internal Audit

Organizations are required as per Clause 9.2 of ISO/IEC 27001:2013, to carry out an internal audit within scheduled intervals to assess whether the ISMS implementation corresponds to the organizational needs and to the standards. Whether from the internal organizational set up or from outside the organization, an independent review of the ISMS by a competent auditor is essential. It is important that the one performing the audit is outside of the ISMS operationalization. It is advised that this independent review be done by an ISO/IEC 27001 lead auditor or certified.

Internal audit is a systematic, independent, and documented process to evaluate and assess the effectiveness of the organization’s ISMS in accordance with the ISO/IEC 27001 standard. It is intended to identify non-conformities, gaps, and opportunities for improvement of the ISMS. The scope of such audits includes all aspects of the ISMS, covering policies, procedures, controls, risks assessments, and the overall security posture of the organization. The parties involved are internal auditors, who carry out the internal audit or could be external professionals, if necessary. They are typically independent from the day-to-day management of the ISMS. Internal auditors report their findings to top management and or relevant stakeholders.

### Management Review

Management of an organization implementing an ISMS are charged with the responsibility of conducting a management review for the ISO/IEC 27001. The reviews are expected to be pre-planned and seek to ensure that the ISMS is effective and helps to achieve the business objectives. This is considered the final step in the process chain.

To explain, management review is a periodic evaluation of the ISMS conducted by the top management of the organization to assess its continuing suitability, adequacy, and effectiveness in meeting the security objectives of the organization and the requirements of the ISO/IEC 27001 standard.

The purpose of management review is to make informed decisions about the ISMS and provide resources for continual improvement. Its scope includes a high-level review of the ISMS, focusing on its objectives, achievements, resource allocation and overall performance. The parties involved are top management or their representatives, usually with input from the ISMS manager, CISO or relevant stakeholders.

Now, to distinguish management review from internal audit, do note that their objectives, scope, and participants make the separation between the two. Internal audit is a more detailed evaluation focused on identifying non-conformities and opportunities for improvement, while management review is a high-level evaluation of the ISMS to ensure it remains effective and aligned with organizational objectives. Finally, internal audit is performed by independent auditors while management review is conducted by top management.

### Self-Check Questions

1. The implementation of an information security assurance system should be seen within an organization as

* An IT department problem
* A problem for senior managers
* A problem for external experts
* *A problem for the whole organization*

1. Please list three processes in the steps which should be analyzed and considered in setting up an ISMS.

*Understanding the internal organizational context*

*Understanding the external organizational context*

*Establishing an information security policy*

*Defining roles and responsibilities*

*Risk assessment*

*Performing internal audits*

*Management review*

## 2.3 Analysis of the Existing ISMS and Determination of the Maturity

The maturity of an ISMS refers to its level of development, effectiveness, and ability to adapt to changing threats and business requirements. This section discusses a few typical factors to consider when evaluating an existing ISMS to determine it maturity level, as well as some commonly used maturity models.

### Factors to Consider When Evaluating and ISMS Maturity Level

Evaluating an ISMS’s maturity level allows organizations to identify areas that may require improvement, prioritize investments, and demonstrate progress to stakeholders. There are many factors that should be considered when evaluating the maturity level of an ISMS, which can not only enhance the organization’s security posture but also help to meet regulations, standards, and industry best practices. The list of factors are exhaustive and includes an organization’s approach to internal and external audits, integration of the ISMS with other management systems, third-party and supply chain security, compliance with legal and regulatory requirements, incident management and response processes, clearly defined roles and responsibilities for information security in an organisation, employee training and awareness, continuous improvement, in that there is a structured approach to reviewing and monitoring the performance of the existing ISMS, among others.

* **reviewing the ISMS framework and policy implementation**: This is often the first step in analysing an existing ISMS and involves reviewing the ISMS’s scope, objectives, and policies to ensure they align with the organization’s goals and adequately address information security risks. How well policies are enforced, communicated, and updated to reflect changes in the threat landscape and business environment is helpful in establishing maturity level of the ISMS.
* **a robust risk assessment and management process**: This involves identifying and mitigating risks requires a robust risk assessment and management. This process should be comprehensible, repeatable, and aligned with the organization’s risk appetite. Evaluating the existing risk assessment methodology can help to determine the maturity of the ISMS. A mature ISMS uses a systematic approach to identifying, analysing, and prioritizing risks, followed by the implementation of the appropriate risk treatments and controls to maintain risks at acceptable levels.
* **metrics and performance Indicators**: If an organization should be able to measure the success and maturity of an ISMS, relevant metrics and performance indicators ought to be established. These metrics could include the number of security incidents, time to detect and response to incidents, employee training completion rates, and effectiveness of the risk management measures.
* **information security culture**: The overall maturity of an ISMS is influenced greatly by the security culture that exists within an organization. A mature ISMS fosters a proactive, security-minded culture, which can be nurtured through regular communication from leadership, effective employee training and awareness programs and the integration of security considerations into day-to-day decision-making.

Understanding and assessing the maturity level of an organization’s ISMS is a vital aspect of strengthening the overall security posture and protecting information assets. By considering the above factors, organizations can gain insights into the strengths and weaknesses of the ISMS. Gaps identified could be prioritized and improved and help to move organizations towards optimal ISMS maturity levels.

### Maturity Models

Maturity models are designed to assist organizations assess their ISMS maturity levels. They serve as a benchmarking tool, enabling organizations to compare their progress with others and identify which elements should be implemented based on their success. The adoption of best practice standards is promoted using these models to evaluate ISMSs. A crucial aspect highlighted by ISMS maturity models is the importance of a security culture in safeguarding an organisation’s information assets.

Several well-known maturity models exist, with some employing five level, while others use six. Regardless the number of levels in a specified model, a common goal is shared, which is to achieve similar or identical objectives.

#### NIST CSEAT IT Security Maturity Model

This model features five progressive maturity levels that focus on documentation. The five levels are as follows (NIST, 2016):

1. Policies
2. Procedures
3. Implementation
4. Test
5. Integration

**Citigroup’s Information Security Evaluation Model (CITI-ISEM)**

This model consists of five progressive maturity levels, with a focus on organizational awareness and adoption. The five levels are as follows (Citigroup, 2000):

1. Complacency
2. Acknowledgement
3. Integration
4. Common Practice
5. Continuous Improvement

#### COBIT Maturity Model

The COBIT maturity model has six progressive maturity levels that focus on auditing specific procedures. The six levels (starting from zero) are as follows (CEWebS, 2009):

1. Non-existent
2. Initial/Ad-hoc
3. Repeatable but intuitive
4. Defined process
5. Managed and measurable
6. Optimized

#### Systems Security Engineering Capability Maturity Model (SSE-CMM)

This model has six levels of progressive maturity focused on measuring security engineering and software design. It serves as a general framework for executing security engineering within an organization. The ISO/IEC 21827:2008 recommends the SSE-CMM for describing essential characteristics of security engineering processes for organizations. The six levels starting with level 0 as the least developed maturity level are as follows (ISO, 2008).

1. Not performed
2. Performed Informally
3. Planned and tracked
4. Well defined
5. Quantitatively controlled
6. Continuously improving

#### CERT/CSO Security capability Assessment

This model features five progressive maturity levels that focus on documentation. The five levels are:

1. Exists
2. Repeatable
3. Designated person
4. Documented
5. Reviewed and updated

### ISMS Maturity Assessment Methodology Phases

Based on the ISO/IEC 27001 standards, organizations that have implemented an ISMS are required to measure its effectiveness and continuously improve the ISMS. A standard holistic methodology is not available for the measurement of the performance of an ISMS, however, best practices and the prescriptions of the standards provide practical methodologies for the conduct of a maturity assessment. While the ISO/IEC 27001 provides compliance requirements, ISO/IEC 27002 provides guidelines to help design an ISMS and implement ISMS best practices. Against this backdrop, the ISMS Maturity Assessment Methodology Phases are as follows (Monev, 2020).

#### Phase 1: Assessment initiation

A competent individual should initiate the assessment of an existing ISMS. This individual should obtain support from top or senior management and other departments and stakeholders and lay down the foundations for an ongoing ISMS maturity assessment.

#### Phase 2: Appointing an assessment team

In the second phase of the assessment of the existing ISMS, an assessment team should be appointed. Typically, the team should have information security and compliance experts. External consultants can be involved if needed and formal management mandate is needed of the assessment, as a recommendation.

#### Phase 3: Assessment tool creation

An assessment tool for the existing ISMS is the next step, and one should be created. This is often managed through Microsoft Excel templates or some other commercially available templates. For the ISO/IEC 27001 controls, (114 in the Annex A of the ISO/IEC 27001:2013), together with the 25 sub-clauses (totalling about 139), the assessment tool is used to enter information during the assessment of the ISMS and remains the primary document of the final report about the ISMS maturity level.

#### Phase 4: Document review and interviews

In accordance with the best practice guidance, relevant information security documents in the organisation and other sources of information should be reviewed. Interviews with individuals in relation to established processes should be conducted to help get a better understanding of the procedures with reduced maturity levels and to describe the current situation of the security controls.

#### Phase 5: Evaluation and recommendations

It is recommended that during the document review and interviewing stages, the maturity level of every one of the 139 controls (as far as the ISO/IEC 27001:2013 NS 27002:2013 are concerned) is evaluated using a scale based on a maturity reference table. Recommendations can be made for every control after consulting the ISO/IEC 27002 as well as other references and best practices.

#### Phase 6: Reporting

It is recommended that the maturity assessment should end with an assessment report which should include the metrics about the performance of the existing ISMS. One section should cover compliance level with the ISO/IEC 27001. The assessment report should also contain an explanation of the assessment findings, centred on the interviews conducted, evaluation of documents and the recommendations for improving the existing ISMS.

### Self-Check Questions

1. The ISO/IEC 27001 provides guidelines to help design an ISMS and implement ISMS best practices, while ISO/IEC 27002 provides compliance requirements. True or False?

* True
* *False*

1. Please list three notable information security maturity models.

*NIST CSEAT IT Security Maturity Model*

*Citigroup’s Information Security Evaluation Model*

*(CITI-ISEM)*

*COBIT Maturity Model*

*Systems Security Engineering Capability Maturity Model*

*(SSE-CMM)*

*CERT/CSO Security Capability Assessment*

## 2.4 Defining the Scope of the ISMS and Security Policies

The scope definition should be done very early, typically as part of the initial set up of the ISMS, after which it could be adapted iteratively.

The limits and suitability of the ISMS constitutes its scope, which should be established after reviewing internal and external contexts, requirements analysis outcome (ISO/IEC/IEC 27001:2013, clause 4.1), the interfaces and dependencies between activities performed by an organization and those outside which could impact the scope definition. The ISMS scope should be available as documented information (Hintzbergen, et al., 2015).

The scope can cover all part of the organization; therefore, boundaries must be clearly defined if the ISMS scope is limited to only a part of an organization. Management should decide on the size of the ISMS scope based on the business aims and objectives as well as the motivation for a particular choice of ISMS scope. These can include activities of a business unit, department, or project activity, a set of functions or services as depicted in the figure below.

ISMS Scope Scenarios

Diagram

Description automatically generated

Source: Andrew Sai (2023).

### Object of ISMS Scope Definition

A well-defined ISMS scope offers several advantages. Organizations implementing the ISMS route and particular scope of application achieve the following:

* minimizing business impact and financial costs of security incidents in one or more business areas
* reducing the number and frequency of incidents
* complying with laws and regulations such as data privacy directives of the European Union (EU), SOX or HIPPA regulations in the US
* a business enabler and enhancing the corporate value of the business

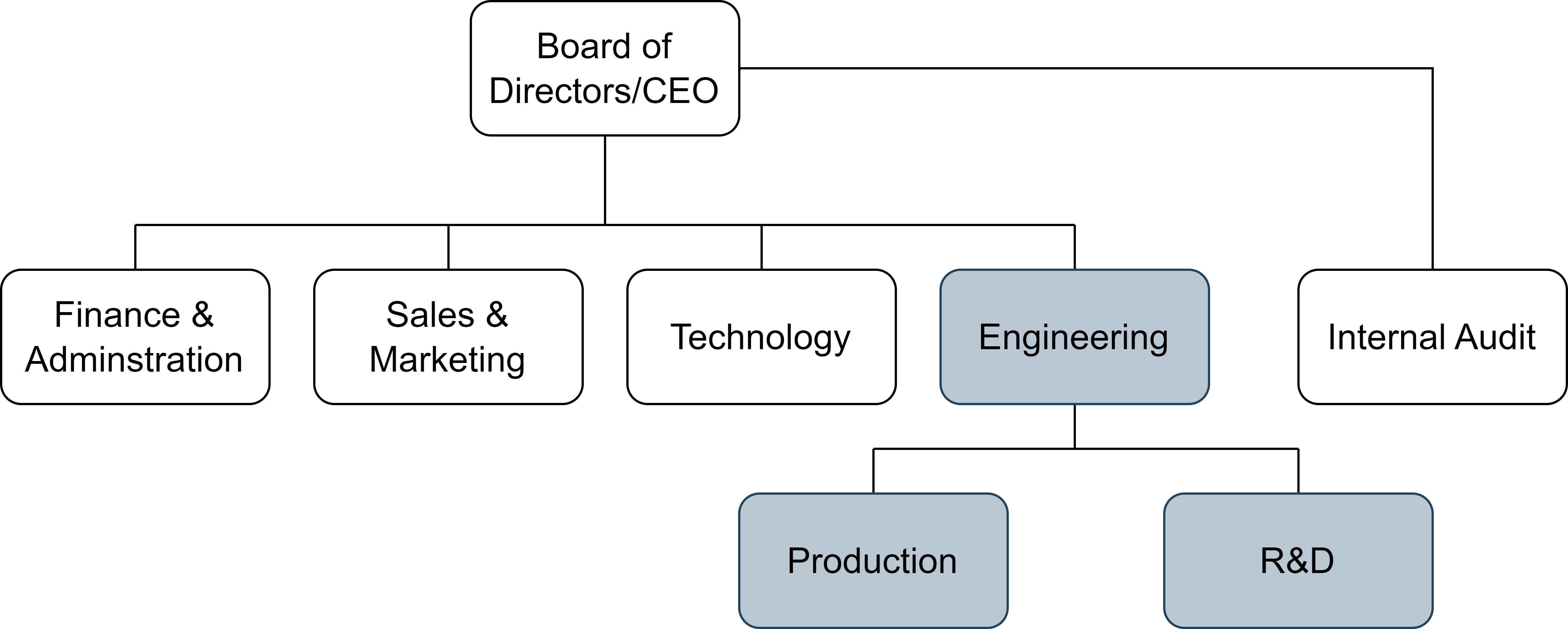
### Defining the ISMS Scope

The scope of the ISMS might include staff and or employees involved in the area of work of the ISMS operationally; processes and services engaged within the areas of work of the ISMS; information assets and systems required to conduct daily business; policies, procedures and necessary documentation required to complete the business of the ISMS; interfaces and dependencies of the ISMS; ICT infrastructure and where the ISMS is located physically. The ISMS scope should reflect the following:

* procedures used by the personnel, such as company policies and procedures, operating manuals, security policies and procedures
* sales and customer service information, such as customer details, customer orders, invoices, internal customer data and data from other companies
* business processes, applications, and services, such as sales order processes, e-commerce, customer enquires processes and IT services
* technical and non-technical Interfaces and dependencies
* technology in use, such as desktop computers and other IT equipment, networks, telephones, mobiles, and tablets
* the physical location of the sales and services department (e.g., Berlin)

In the figure below, the ISMS scope is an Engineering department of a company. This is one department in a larger organization, which is an example of an ISMS scope narrowed to only part of a company and not the entire company.

Example Organization Structure Reflecting ISMS Scope



Source: Andrew Sai (2023).

There are three main steps that could be followed to detect the implementation scope of an ISMS for an organization:

1. Identifying the spaces, structures, and places where relevant information is stored such as document files, both physical and digital
2. Identifying all possible methods by which information will be made accessible to users
3. Identifying scope boundaries, what is within the ISMS scope such as likely areas an organization may not have control over (e.g., outsourced products or services)

The PDCA model is recommended as a useful framework for determining, implementing, monitoring, controlling, and maintaining an ISMS.

PDCA Model and ISMS

Diagram

Description automatically generated

Source: Andrew Sai (2023).

Previously, under the ISO/IEC 27001:2005, the Plan-Do-Check-Act model (also known as Deming’s Quality Circle) was required as the basis for determining, implementing, monitoring, controlling and maintaining the ISMS in an organization. This was updated in the ISO/IEC 27001:2013 by making it an obligation for organizations to establish, implement, maintain, and continually improve the ISMS, in accordance with the standards, as a recommendation, and the PDCA requirement removed. Therefore, it is a recommendation.

The PDCA cycle is a recommended approach for ensuring continuous improvement of the ISMS over the long term and it forms the foundation of numerous management systems. It is important to indicate that the PDCA model serves the purpose of helping to align the ISMS scope on an ongoing basis. For instance, in our example of the Engineering department, there could be specific aspects of the ISMS implementation which are out of scope (e.g., the Sales and marketing departments are included in the implementation mistakenly) and using the PDCA, could be identified. Once identified, the scope could be realigned to the Engineering department only, where it is required.

### PDCA Phases

In the ensuing subsections, each of the PDCA phases depicted in the previous figure is explained.

#### Plan (design the ISMS)

In this “plan” phase, an information security policy is developed and documented, the information security objectives, processes and procedures are defined. These include

* selecting a security maturity model or framework,
* identifying assessment tool or tools, and
* conducting security assessments.

#### Do (implement the ISMS)

In the context of the ISMS, “Do” phase is where the information security policies and relevant procedures are implemented. During this phase, responsibilities are allocated for each process, system, processes, or procedures. This includes

* implementing security controls,
* developing security policies, and
* training personnel.

#### Check (monitor and check the ISMS)

The “Check” phase is where controls are deployed via self-assessment such as internal auditing and possible checks are undertaken to ensure the ISMS is being implemented correctly. The activities in this phase include

* the verification of security controls,
* self-assessment, and
* third party verification, where required.

#### Act (maintain and adjust the ISMS)

In the final phase, the “Act” phase, corrections are made to the ISMS or the defective aspects of its implementation, preventative measures are included, based on the findings of the assessment of the correctness of the ISMS towards the organizational objective and needs. Some activities or actions that could be taken include the following:

* develop lessons learned
* establish baselines
* adjust as needed
* repeat cycle

The PDCA model has proven to be a useful guide in aligning the ISMS scope.

### Self-Check Questions

1. Please list three possible boundaries of an ISMS.

*Activities of a business unit within an organization*

*Activities of a department within an organization*

*Project activity*

*A set of functions or services*

1. Please mark the incorrect statement(s).

* Implementing an ISMS in an organization minimizes business impact and financial costs of security incidents.
* Implementing an ISMS in an organization reduces the number and frequency of incidents.
* Implementing an ISMS in an organization complies with laws and regulations.
* *Implementing an ISMS in an organization increases revenue.*

1. Please complete the following sentence.

The Plan-Do-Check-Act model (Demings’s Quality Circle) was previously required under the *ISO/IEC 27001:2005*, however was updated under the *ISO/IEC 27001:2013*.

Summary

The risks associated with IT systems in organizations are on the ascendency. Companies and individuals alike would have to change their approach to information security, with more and more exposure, particularly, over the Internet. For companies, to start on the right footing means to get the ISMS scope right, aligned correctly with the organizational objectives and with the commitment of top management.

The ISO/IEC 27000 family of standards offers the necessary guidance, which is based on best and globally accepted practices, to manage threats and vulnerabilities and help to mitigate the risks surrounding the IT systems.

In principle, it should be possible for organizations of all sizes, types, and nature to implement an ISMS. The ISMS is not a one-stop shop but a set of policies that are expected to be integrated into existing business processes and set ups. The requirements are laid out in the standards. It is, however, cumbersome to implement and therefore requires skilled and experienced ISO security experts to help top management to implement.

The most significant issue in the implementation of the ISMS is documentation.

# Unit 3 – Implementation of the Information Security Management System

**Study Goals**

On completion of this unit, you will be able to…

… describe the steps to be taken to implement an ISMS in an organization in accordance with the specifications of ISO/IEC 27001 and 27002 standards.

… formulate a statement of applicability (SoA) and offer justification for the inclusion and or exclusion of security controls.

…define an organizational structure, including roles and responsibilities for information security.

… develop and manage documentation and communication in accordance with the relevant ISOs.

… evaluate security controls, design, and implement pertinent controls and procedures for the execution of the ISMS.

# 3. Implementation of the Information Security Management System

## Introduction

The information security management system (ISMS) is considered as difficult to implement. This is largely because, the ISOs provide a general guidance about how to implement it and contextual factors might differ across organizations, since organizations seeking to implement an ISMS might differ in size and type, and therefore, there is no one hard and fast rule for implementation.

On every level, organizations of all sizes and types are faced with some amount of risk. These emanate from threats and vulnerabilities that often cannot be addressed adequately and a lack of effective control mechanisms. The deciding factor often between an effective organization and an ineffective one is commonly, risk management. Organizations that can assess risks, manage, and in many cases mitigate the effects of risks likely to impact their systems and processes, have a higher chance of being successful.

This unit will outline, in accordance with the ISO/IEC 27001, how to implement an ISMS: including the objectives and the scope of the ISMS which would have to be defined. The unit covers inventory of assets, definition of risk management framework, risk identification and scoring, plus risk treatment plans, verification of risk treatment plan against the provision of the Annex A controls and procedures of the ISO/IEC 27001 and 27002, and documentation and communication management as part of the ISMS operationalization. The Unit further covers statement of applicability (SoA) as well and why it is relevant in the execution of the ISMS, roles and responsibilities’ definition, documentation and other controls that ought to be in place to ensure that the ISMS implementation is successful.

## 3.1 Risk Assessment

There are risks associated with implementing the ISMS. Risks are a function of threats and vulnerabilities. In other words, mathematically, risks equal threats multiplied by vulnerabilities. Early identification of risks is good, a step in the right direction, however, a lot could change about an organization and such changes have the propensity to introduce new risks to an organization and its ISMS implementation. Possible changes could emanate from

* changes to the business environment (legal, regulatory, other external factors).
* the risk profile, which could be impacted because of multiple variables affecting the nature and level of threats faced by an organization, internal and external factors.
* business objectives, where the organization or enterprise varies it business goals.
* business strategy, which affects the overall direction of the business or organization.
* operating conditions, which impact day-to-day activities of an organization.
* market conditions, such as competition or changes to the specific industry or economy in which an organization operates.
* hard or infrastructural changes (internal and external), such as changes to information systems and physical location, as well as hardware updates.

In the risk management process or chain, risk assessment (clause 5.4) of ISO/IEC 31000, begins after the organizational context (both internal and external) have been established (clause 5.3), risks have been identified (5.4.2), risks analyzed (clause 5.4.3), evaluated (clause 5.4.4) and treated (clause 5.5) accordingly.

The figure below shows the steps schematically in the risk management process as far as the ISMS implementation is concerned. It is important to note that the first order of business is establishment of the context. It is equally important to note that communication and consultation (clause 5.2) as well as monitoring and review (clause 5.6) of the processes are a necessary part of the entire process as prescribed **by ISO/IEC 31000** (risk management).

**ISO 31000**

This is a family of standards relating to risk management and codified in the International Organization for Standards (ISO).

Risk Management Process

Diagram

Description automatically generated

Source: Andrew Sai (2023). Text based on ISO/IEC 31000. Source (ISACA, 2016, based ISO/IEC 31000 risk management framework)

**Risk**

The ISO 27001:2013 defines risk as “the effect of uncertainty (on objectives).

The ISO/IEC 27001:2013 provides a definition for **risk**, which can be understood as the potential for events and consequences that could adversely affect an organization’s information security objectives. Although various interpretations can be derived from the definition, the core concept revolves around the consequences or impacts of an event. For instance, in the case of a system hacking event, the consequence would be a compromised system that is vulnerable to the hacker’s malicious actions.

Risk management involves a deliberate effort to manage uncertainty related to the attainment of risk objectives, outcomes, targets, and the deliverables of the ISMS. The process of risk management typically begins with risk assessment. According to ISACA (2016), risk management is a “a comprehensive process within a management system; in an ISMS, it is intended to contribute to the systematic identification, assessment, and transparent presentation of risks in the context of information security and to ensure an acceptable/long term improvement in the level of security within the scope of the ISMS” (ISACA, 2016, page 19).

Some specific risk management goals include the following:

* identifying and mitigating information security risks early
* developing an assessment method for identified risks
* assigning responsibility for managing identified risks
* documenting risks, including their assessment
* implementing appropriate treatment for identified risks

Risk management can proceed through the following steps, though the list is not exhaustive:

* identifying risks
* analyzing risks
* assessing risks
* treating risks

Let’s now examine each of these steps, starting with Step 1.

### Risk Identification

Identifying risks involves detecting, describing, and cataloging potential risks that could impact business outcomes adversely, such as performance, quality, damage, loss, or reputation of the organization. Risks are often looked at as an inherent outcome of using IT systems and technologies (be they new and or old). The ISO/IEC 27001:2013 recommends the consideration of information security as a holistic exercise, and not just limited to aspects of the organization. There are myriad sources of security risks to an organization’s information assets. Such risks typically stem from threats and vulnerabilities. Security risks could emanate from

* within and outside the organization, often through the exchange of data across networks.
* internal organizational changes.
* old, legacy, and unreplaced systems and applications.
* cooperation with vendors and third-party organizations.
* access to company networks (possibly through BYOD, insecure connections or third parties).
* natural disasters (earthquakes and natural occurrences which disrupt systems).
* sabotage and criminal activities.
* social engineering and insider threats.

Risk identification typically arises from audits (both internal and external) and audit reports, investigations of similar nature or inquiry into specific aspects of an organization’s operations, which review the organization and its security setup and offer recommendations on how to address the risks identified. Risks could also be identified through explicit risk analysis, which is initiated for specific projects, business processes, etc. Risks are also identified through day-to-day operations. For example, a security vulnerability could be identified while using a CRM, by staff of the customer accounts department and reported to the IT department for action. This type of risk reveals vulnerabilities in the overall organizations’ IT systems and how customer data could easily be leaked for malicious purposes, when they get into the wrong hands.

### Risk Analysis

This is considered step two, after the risk(s) has/have been identified. In analyzing risks, the probability of occurrence and likely impact if the risk materializes, should be clearly determined, and documented.

**Risk Criteria**

Terms of reference against which the significance of a risk is evaluated. (NIST)

Analysis of risk is based on the **risk criteria** established and accepted, particularly with top management. Some of these include organizational objectives, internal/external contexts, and other mandatory requirements such as standards, laws, and policies.

The approach to risk analysis is typically quantitative or qualitative or a combination of both approaches. The ISOs tilt towards the qualitative approach, where risk calculations are not that vital, but rather employing methodologies which assist to identify, in a form of a risk log, with assets, risk owners, threats identified, vulnerabilities and impact.

### Risk Evaluation/Assessment

Risk assessment is the systematic study of organizational assets, threats, vulnerabilities and impact, to measure the likelihood (or probability) and outcomes (or impact) of risks. The assessment process often leads to risk categorization or matrix and eventually scoring. Risk scoring is a process of calculating a number or a score which demonstrates the level of risk associated with an event, or entity.

Risk assessment is stated in clause 6.1.2 of the ISO standards and requires the organization to “define and apply information security risk assessment process” (clause 6 of ISO/IEC 27001:2013) appropriate to the organization, the security objectives, and other requirements such as business, legal and regulatory concerns. There is a lot of flexibility in assessing risks, notwithstanding the guidance provided by ISO/IEC 31000 (is a family of the standards which relate to risk management) and ISO/IEC 27005 (focuses on information security risk management). The methodology must aid in the detection of risks, risk owners, risk acceptance criteria and be able to help to analyze risks in terms of their likelihood and impact. The assessment is a formal process: which means it must be planned and the outcome recorded or documented.

### Risk Treatment

Organizations must implement risk treatment measures according to the recommendation in Annex A of the ISO/IEC 27001 standard and develop an SoA as part of the ISMS implementation process. Annex A provides a comprehensive list of 114 security controls organized into 14 categories, which were later restructured in the 2022 version into 93 security controls across four main domains: organizational, people, physical and technological.

**Risk Appetite**

The level of risk that an organization is willing to accept in the pursuit of its objectives before any actions to reduce risks.

The main control categories in Annex A of ISO 27001:2013 includes the following. Do note that these have been re-organized in the 2022 edition of the standard:

1. A.5 information security policies
2. A.6 Organization of information security
3. A.7 Human resource security
4. A.8 Asset management
5. A.9 Access control
6. A.10 Cryptography
7. A.11 Physical and environmental security
8. A.12 Operations security
9. A.13 communications security
10. A.14 System acquisition, development, and maintenance
11. A.15 Supplier relations
12. A.16 Information security incident management
13. A.17 Information security aspects of business continuity management
14. A.18 Compliance.

The main objective of Annex A is to offer guidance to organizations in selecting and implementing suitable controls based on the outcomes of their risk assessment and risk treatment processes. By this action, organizations could address unique risks posed by their information assets and processes, demonstrate compliance with industry standards, legal and regulatory requirement and enhance overall security posture.

It is important to note that organizations do not have to implement all 114 controls or their reduced version of 93 in Annex A. Instead, they can choose what is relevant based on their risk assessment and business needs. Implementing relevant controls from Annex A helps organizations build a strong security foundation and manage risks effectively.

The SoA is the core connector between risk assessment and its treatment in an organization, making it key in the ISMS implementation process. Additionally, there should be risk ownership clearly defined for each risk type and class identified, based on the risk criteria established.

An underlying principle concerning how organizations treat risks is founded in their **risk appetite**. This is often defined in a risk policy or some other management policy document, to guide the organization in its risk assessment and management. ISO/IEC 27005:2011 provides a starting point for a risk treatment model. Some of the typical types of risk treatment options according to the ISO/IEC 27005 include the following:

* **risk reduction**: This is using preventive, deterrent, or detective types of control methods to reduce risk identified.
* **risk avoidance**: This includes decisions to not address risks identified or that could cause risk, but rather terminate activities that could cause them, postpone or cancel plans or projects which are associated with such high risks, depending on the risk criteria and appetite of the organization.
* **risk transfer**: This involves engaging another party such as an insurance company, supplier, external or some other third party to share the risk identified. Organizations typically insure their assets and by that transfer the risks to the third party. For individuals, when you buy a car, and own it, you are responsible for it, however, subscribing to and paying insurance premiums to an insurance company relieves an individual of any burdens, in the event of an accident, certainly based on the type of insurance option selected.
* **risk acceptance**: This involves seeing risks identified or potential risks as openings to take up. This means that within the organization’s strategy, objectives or risk appetite often, no other options exist to cater to such risks. Risks accepted by organizations are often small and within the containment of management of the organization.

Risk management options are based on the outcome of the risk assessment exercise. The figure below shows an example risk matrix for assessing the impact and likelihood of risk. A risk matrix (or categorization) helps the organization to distinguish which risks should be prioritized and treatment options to address them.

Risk Matrix Example in MS Excel

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | | **Impact** | | | | |
| **Insignificant** | **Minor** | **Moderate** | **Major** | **Severe** |
| **Likelihood** | **Almost certain** | Medium | High | Very High | Very High | Very High |
| **Likely** | Medium | High | High | Very High | Very High |
| **Possible** | Low | Medium | High | High | Very High |
| **Unlikely** | Low | Low | Medium | Medium | High |
| **Rare** | Low | Low | Low | Low | Medium |

Source: Andrew Sai (2023).

To sum up, risk treatment options refer to the measures taken to address risks identified through a risk matrix. This matrix, illustrated in the figure above, serves as a tool for evaluating the likelihood and impact of potential risks. As a result, organizations can prioritize and make well-informed decisions on how to handle these risks. Some of the common risk treatment options include avoiding high-impact, high-likelihood risks, mitigating or transferring risks to another party; and accepting low-impact, low-likelihood risks without any specific action. For instance, even after securing a building with comprehensive physical and logical controls, there may still be residual risks, such as the possibility of internal staff engaging in malicious activities. Though unlikely, such risks could be accepted without taking any specific action and noted for management. As another example, managing such a risk would involve implementing staff training and awareness programs which could help prevent such risks from materializing, though accepted, if within the organization’s risk appetite framework.

### Self-Check Questions

1. Please list all the steps in the risk management process

*Step 1: Identifying risks.*

*Step 2: Analyzing risks.*

*Step 3: Assessing risks.*

*Step 4: Treating risks.*

1. Please complete the following sentence.

*STRIDE* and *Delphi method* are two of the methods and techniques that can be used as tools in risk identification process.

## 3.2 Statement of Applicability (SoA)

A **Statement of Applicability (SoA)** is a crucial component when implementing an ISMS, as it serves as the link between risk assessment and risk treatment within an organization. The SoA is addressed in clause 6.1.3 of the ISO/IEC 27001:2013 standard and contains a checklist that acts as a guide for the ISMS implementation. Same is addressed in the updated 2022 version. This checklist assists in identifying all relevant regulatory, legal, and contractual requirements as well as necessary controls that ensure that the organization’s business needs are met. The SoA is a vital document for organizations seeking ISO/IEC 27001 certification. It is important to note that the SoA is not a mandatory requirement but is strongly recommended. The purpose of the SoA is to identify which of the controls in Annex A of the standard are applicable to the organization’s information security risks, and to explain how these controls are implemented.

**Statement of Applicability (SoA)**

Is a document formed by the complete list of assessable information security controls indicated in the Annex A of ISO 27001 and detailed in ISO 27002.

The ISO/IEC 27001:2013 includes a documented SoA which contains 35 control objectives, each of which has one or more associated controls, and 114 comprehensive controls for the implementation of the ISMS. The controls cover a range of information security areas, such as access control, asset management, cryptography, incident management, and physical security. The SoA should list each of the applicable controls from Annex A together with a brief description of how each control is implemented. If any controls are to be excluded from the implementation, the organization must provide justification for the exclusion. The SoA documents the rationale for the exclusion of specific controls as well as the implementation status of controls implemented. It is worthy of note that not all organizations need to implement every control as some may not be relevant to their specific needs.

Creating an SoA demands significant coordination, time, and effort, with management commitment and involvement crucial to its success. Although various approaches to the SoA development exists, the following process is recommended when implementing an ISMS:

1. Activities to be carried out must follow a method, which is to be documented.
2. Every process must have a corresponding control or controls, such as audits and some level of review or reviews.
3. At the organizational level, a security goal is needed. This goal should be stated clearly in an information security policy document and available to stakeholders.
4. All processes and controls must be continually improved.

The SoA is like a registry of security controls that are applicable to a specified organization. Security controls and which will be most suitable go after a risk analysis, evaluation, and treatment. The SoA development can be mapped in five steps:

1. Risks must be identified and analyzed.
2. Security controls are selected to treat the risks, based on the earlier evaluation and treatment options mapped to the risks.
3. Risk treatment planning is carried out.
4. Security controls are then implemented.
5. The SoA is then maintained.

Documentation is an important aspect of maintaining the SoA. Table… below shows an example of a Statement of Applicability table. In the table, the relevant controls accompanying processes and actions are outlined and described and it is indicated whether these were applied, the justification for applying or otherwise.

Example Statement of Applicability (SoA) Table

|  |  |  |  |
| --- | --- | --- | --- |
| Control | | Applied  (Y/N) | Justification |
| Reference | **Description** |
| A.5.1.0 | Information security policies | Y | ISO/IEC 27001 Requirement |

Source: Andrew Sai (2023)

### Self-Check Questions

1. Please mark the incorrect statement(s).

* An SoA houses a checklist which serves as a map in the implementation of the ISMS.
* An SoA helps to identify all relevant regulatory and legal requirements.
* Developing an SoA requires a lot of coordination, time, and effort.
* *There is no need to exclude controls not implemented in an SoA.*

## 3.3 Definition of the Organizational Structure for Information Security

It is considered rational and practical to develop an information security management composition and structure for the ISMS implementation at the initial phases of the ISMS execution. An effective organizational structure enables better risk assessment. Depending on the size of the organization, roles and responsibilities must be clearly defined for the information security apparatus and controls to work effectively. It is recommended that information security activities in an organization is coordinated by a cross-functional management forum (i.e., representatives from different parts of an organization). For the ISMS implementation, more specifically, a project team chaired by a senior management member is expected to be constituted, to oversee the implementation of the ISMS.

**Information Security Governance Structures**

Just like any other corporate or organizational level control activity, the ISMS starts with governance. The purpose of information security governance is to ensure that all agencies and actors proactively implement appropriate information security controls to achieve the organizational objectives. The governance part also identifies key information security roles and responsibilities as well as the organizational structure needed to implement and continually manage the ISMS.

Bowen et al. (2006, p. 2) define information security governance as:

*“…the process of establishing and maintaining a framework and supporting management structure and processes to provide assurance that information security strategies are aligned with and support business objectives, are consistent with applicable laws and regulations through adherence to policies and internal controls, and provide assignment of responsibility, all in an effort to manage risk.”*

Typically, the regulator of the industry or sector where the organization operates serves as a line of defense in terms of its governance. Enterprises, businesses, or organizations, for example, will have legal and regulatory requirements all defined by such regulators. The next in the governance sequence is external audit. Internally, is the governing board or board of directors and an audit committee. The internal audit department of the organization reports directly as a third line of defense. In the second line of defense is financial control, security, risk management, compliance, and quality control. These departments in the second line of defense serve as an oversight on the activities of the first line of defense, which are management controls and internal control measures.

An organizational structure for information security could be described in the following hierarchical format, starting from the top-level management down to specific teams responsible for carrying out tasks. Some important positions are described briefly below. The roles are recommended as part of the security positions to oversee and manage information security in the organization. It is important to note that, again, these roles may be implemented in their entirety or not, based on the size of the organization, objectives and other factors as may be deemed necessary.

* **board of directors/executive management**: This is top-level management responsible for setting organizational information security strategy and policy objectives. The board of directors has the ultimate decision-making authority on information security matters and ensures that the organization complies with relevant laws, regulations, and standards.
* **Chief Information Officer (CIO)/Chief Information Security Officer (CISO)**: The CIO or CISO plays a critical role in defining and managing information security policies, procedures, and standards in line with the executive management’s directives. The CIO or CISO is responsible for setting the security vision and strategy, managing risks, and ensuring that security policies are effectively implemented and maintained.
* **security steering committee**: In some organizations, a cross-functional team, involving representatives from various departments, such as IT, Legal, HR and Operations provide guidance, support, and oversight for the organization’s information security program. The Steering Committee’s role is to ensure that information security initiatives are aligned with the organization’s overall strategy and objectives.
* **Information Security Manager (ISM)**: While could be referred to differently in various organizations, an ISM oversees day-to-day operations and management of information security programs. The ISM is responsible for implementing and enforcing security policies, managing risks, and ensuring that security controls and processes are working well.
* **information security teams:** Multiple teams or units may be responsible for specific information security tasks based on the size and complexity of an organization. Some of the most common security teams include:
  + **risk assessment and compliance team:** This team is responsible for identifying, assessing and managing information security risks and ensuring compliance with relevant laws, regulations and standards.
  + **security operations center (SOC) team:** This team is responsible for monitoring, detecting and responding to security incidents and threats, while managing the organization’s security infrastructure such as firewalls, intrusion detection and prevention systems.
  + **incident response team:** This team is responsible for managing and responding to security incidents, investigation and implementing remediation measures.
  + **security awareness and training team:** This team is responsible for designing and delivering security training and awareness programs to educate employees on security best practices and policies.
  + **information security auditors:** This team is responsible for conducting regular security audits, assessing and testing security controls to ensure they are effective and compliant with relevant standards.

To conclude this section, an effective organizational structure for information security should have clear lines of communication, responsibility, and accountability from the top-level management to individual employees, notwithstanding the positions defined and assigned to tasks, which will depend on how the organization is set up or configured. The structure ensures that information security is integrated into the overall strategy and culture.

### Self-Check Questions

1. Please mark the incorrect statement(s).

* The purpose of information security governance is to ensure that all agencies and actors proactively implement appropriate information security controls to achieve the organizational objectives.
* The governance part also identifies key information security roles and responsibilities as well as the organizational structure needed to implement and continually manage the ISMS.
* Just like any other corporate or organizational level control activity, the ISMS starts with governance.
* *The size of the organization is not relevant in determining roles and responsibilities for the information security apparatus and controls to work effectively.*

## 3.4 Document Management and Communication Plan

Documentation and communication are important requirements in the ISMS implementation process.

### Documentation

Documents must be created, updated, and if needed, published. Documents must be labelled and appropriately classified. Classification is of course dependent on the contents of the document.

The number or type of documents can vary. There is also flexibility in terms of documentation and records, according to the ISO/IEC 27001:2013.

The documentation requirements according to the ISO/IEC 27001:2013 (clauses 4-10) are as follows.

Documentation Requirements According to ISO/IEC 27001:2013

|  |  |
| --- | --- |
| **Documentation Requirement** | **Relevant Clause of ISO/IEC 27001** |
| Scope of the ISMS | clause 4.3 |
| Information security policy | clause 5.2e |
| Description of the risk assessment process | clause 6.1.2 |
| Description of the risk treatment process | clause 6.1.3 |
| Statement of applicability | clause 6.1.3d |
| Information security risk treatment plan | Clause 6.1.3e |
| Information security objectives | clause 6.2 |
| Evidence of competence | clause 7.2d |
| Proof of proper execution of the ISMS processes | clause 8.1 |
| Results of the information security risk assessment | clause 8.2 |
| Results of the information security risk treatment | clause 8.3 |
| Evidence of monitoring and measurement results of the ISMS | clause 9.1 |
| Evidence of audit programs and the audit results | clause 9.2 |
| Evidence of the results of management reviews | clause 9.3 |
| Evidence of the nature of the nonconformities and any subsequent actions taken | clause 10.1f |
| Evidence of the results of any corrective action | clause 10.1g |

Andrew Sai (2023). Text source: based on ISO/IEC 27001 (clauses 4-10)

The onus lies with the respective organization setting up the ISMS to determine which documentation and records it deems necessary, in addition to those required by the standards (clause 8.1). Again, this depends on the type, size and needs of the organization involved.

### Communication

Communication is key in the operationalization of the ISMS. This includes exchanges with both internal and external stakeholders. The stakeholders range from employees and the board of directors to third party vendors, customers, among others. For this, clause 7.4 recommends determining what information is to be communicated, who the recipients are (clause 7.4c), and who should do the communicating (clause 7.4d). When the information should be communicated (clause 7.4b), and which channels to use and processes to do, as specified by clause 7.4e. The figure below shows how to develop the communication plan.

Developing a Communication Plan

Source: Andrew Sai (2023), based on ISACA (2017).

Per the communication plan, communication objectives should be defined, followed by analysis of the target group and determination of the appropriate media to use. Next is to identify the most important communication messages, assign roles and tasks and then develop the communication plan thereafter. The outcome should be a detailed communication plan. The communication plan enables the delivery of information to all stakeholders effectively. The figure below depicts an example communication plan, alternatively called a communication matrix.

Communication Matrix: Internal Communication

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Reason for communication | Initiator | Recipient | Frequency | Medium |
| Management review | Chief Information Security Officer (CISO) | Top management | Annually | Management report according to template via email + presentation |
| Reporting | CISO | Top management | Quarterly | KPI report according to template via email + presentation |
| Awareness training | CISO | All employees within the scope | Annually | Training (classroom or online) |
| IS newsletter | CISO | All employees within the scope | Quarterly and on a case-by-case basis if an acute threat occurs | Email |
| Risk management | CISO | Top management | Quarterly, on a case-by-case basis if an acute threat occurs, on a project basis | Balanced scorecard report, by email if required |
| Security incident | Support | CISO (possibly others, in accordance with SIRP) | Case-by-case basis | Escalation in accordance with SIRP (security incident response process) |
| Security incident | CISO | Top management | Case-by-case basis | Email, possibly verbally |
| Security incident involving personal data | CISO | Data protection officer | Case-by-case basis | Email, possibly also by telephone or verbally |
| Compliance-related security incident | CISO | Legal advisory department | Case-by-case basis | Email, possibly also by telephone or verbally |

Source: Andrew Sai (2023). Text source: ISACA (2017) page 28.

An example external communication matrix appears below.

Communication Matrix: External Communication

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Reason for communication | Initiator | Recipient | Frequency | Medium |
| Operational service provider report | Operational service provider | CISO | Quarterly | SLA report according to template via email |
| Externally commissioned CERT/vulnerability analysis | CERT | CISO/head of IT | Weekly, case-by-case basis | Report in accordance with contract by email |
| Security incident | CISO, possibly top management | All affected customers/partners | Case-by-case basis | in accordance with SIRP, on the website, by mail, email, by telephone |
| Security incident of a criminal nature | CISO | Law enforcement agencies | Case-by-case basis | in accordance with SIRP |

Source: Andrew Sai (2023). Text source: ISACA (2017) page 28.

The communication matrix defines parameters for both internal and external communication, including the purpose, recipient, frequency, and media used for communication. It is important to note however, that ISO/IEC 27001:2013 does not provide specific documentation requirements for ISMS communication. It is the responsibility of the organization to determine its communication approach and ensure that the plan accurately reflects their needs.

### Self-Check Questions

1. Please mark the **correct** statement(s).

* Documentation requirements are stated in clauses 1-5 of the ISO/IEC 27001:2013
* Documentation requirements are stated in clauses 1-3 of the ISO/IEC 27001:2013
* Documentation requirements are stated in clauses 1-11 of the ISO/IEC 27001:2013
* *Documentation requirements are stated in clauses 4-10 of the ISO/IEC 27001:2013*

1. The ISO/IEC 27001:2013 (*clause 7.4)* recommends determining what information is to be communicated, who the recipients are *(clause 7.4c),* and who should do the communicating *(clause 7.4d)*.

## 3.5 Definition of Controls and Procedures

In the context of ISO/IEC 27001, controls are policies, guidelines and technical measures implemented within an organization’s ISMS to manage and mitigate potential risks. Controls serve as a basis for safeguarding information assets from unauthorized access, accidental or intentional damage or other threats that could compromise sensitive data.

Generally, controls can be classified into three main types, according to their nature:

1. **Preventive controls**: These are controls designed to anticipate potential security incidents and breaches before they occur and include firewalls, encryption and employee awareness training programs.
2. **Detective controls**: These are controls that focus on detecting and monitoring security incidents or breaches in progress and include intrusion detection systems, log review and analysis and regular security audits.
3. **Corrective controls**: These controls are usually in response to security incidents or breaches. They are designed to minimize damage, recover from breaches, and prevent recurrence of such events. Some examples of corrective controls are backup and recovery systems, incident response plans and post incident analysis.

Procedures are step-by-step detailed instructions that define how activities related to controls should be executed. They should provide clarity and consistency by specifying who, what, when, where and how of executing control activities. Procedures may document tasks, such as routinely updating system software, performing risk assessment, managing access rights, handling incidents, and dealing with sensitive data securely. Procedures help to ensure that employees responsible for maintaining the ISMS are competent and diligent in implementing the needed controls to guarantee an effective ISMS.

Both controls and procedures are implemented based on the ISO/IEC 27001 and are the backbone of the ISMS in the organization. They provide a framework for effectively managing information security risks.

A set of controls must be implemented after risk treatment options have been selected. These are outlined in Annex A of the ISO/IEC 27001:2013. Existing controls would have to be assessed. This is important to check if new controls planned conflict with the existing ones and whether they can work together seamlessly. Controls can take the form of policies, procedures, plans or techniques. These constitute a control framework. Such controls and procedures are management-oriented controls and not necessarily IT controls. The system of controls is segregated as follows, in accordance with ISO/IEC 27001.

Some examples of policy and procedural controls include information security policy and procedures, acceptable use policies, access control policies and procedures, backup procedures, secure operating procedures, system change, recruitment processes, information security incident management, among others. There are also process controls such as: assignment of roles, responsibilities, risk assessment and treatment procedures, etc.

Policies remain the bedrock of such controls and procedures. Information security policies are high level policies of top management. The ISO/IEC 27001 clause 5.2 specifies a top management information security policy, intended to be a high-level directive and mission statement of an organization. The policy document includes information security objectives, a commitment to satisfy those requirements (clause 4.1 and 4.2) and continual improvement of the ISMS (as prescribed in Clause 10 of the standard). The information security policy should do the following:

* Define the scope of information security, its importance, and objectives.
* Make staff and stakeholders aware of their duties and responsibilities.
* Provide acceptable and unacceptable behaviors and use of organizational resources.
* Clarify obligations regarding compliance with laws and regulations.
* Refer to other policy documents that staff ought to be aware of and comply with.

### Self-Check Questions

1. Please mark the incorrect statement(s).

* A set of controls must be implemented after the risk treatment options have been selected.
* The controls are outlined in Annex A of the ISO/IEC 27001:2013.
* Existing controls would have to be assessed.
* *Controls only take the form of policies, procedures, plans or techniques.*

1. Please complete the following sentence.

Some examples of policy and procedural controls include *information security policy* *and procedures*, *acceptable use policies*, *access control policies and procedures.*

Summary

The boundaries of information security have been expanding and will continue to expand, from the traditional scope it came along with, which included primarily managing patches, firewalls, and other rudimentary security actions. The shift in the scope and focus of information security is in response to the changes in technology, advancements and the interconnectedness now experienced since the Internet became a thing.

Risk management has taken center stage in the information security conversation. Risk management is a core part of the ISMS implementation. While organizations need to provide the needed structure to facilitate the information security management in their organizations, it is important to elevate the security role with representation at board and higher levels and often when information security projects will be implemented, including the ISMS, a senior management officer should chair and coordinate its implementation, also to ensure that proper documents are maintained for ease of reference and tracking. It is vital that when information security groups are formed, it is cross functional.

This unit covered the risk management process, from risk identification to treatment and actions needed beyond, why an SoA is crucial to an ISMS implementation, when it should be created and why, and what goes into it, and how it interfaces with security controls in an organization. Roles and responsibilities which are constantly changing due to the ever-changing information security landscape were covered as part of defining the security organization structure. Then documentation, including the SoA and developing a communication framework to guide communication with internal and external stakeholders were covered. The Unit ends with a definition of controls and procedures as specified in Annex A of the ISO/IEC 27001.

# Unit 4 – Controlling the Information Security Management System

**Study Goals**

On completion of this unit, you will be able to…

… understand and discuss monitoring, evaluation, and measurement requirements of the ISMS, as part of controlling its implementation process.

… examine the overall ISMS monitoring process and evaluate how changes to the organization impacts its implementation.

…define metrics needed to measure progress of the ISMS, develop and manage an ISMS measurement program.

… recognize and appraise the need for performance evaluation, including internal auditing of the ISMS in conformity with the ISO/IEC 27001 and management review.

# 4. Controlling the Information Security Management System

## Introduction

The information security management system (ISMS) once implemented, must be monitored, and subjected to regular appraisals and updates. The implementation is to be regarded as an ongoing exercise, and not a one-off project. Therefore, monitoring of the ISMS is crucial. Further, measuring and evaluating whether the implementation is on track is another important aspect of staying in control of the ISMS operationalization. Monitoring and reviewing how the ISMS is performing enables an organization to check its suitability, and effectiveness. In this unit, the tools for measuring, analysing, and evaluating ISMS rollout is covered. Example metrics for enabling measurement of the ISMS progress are covered.

Then, there is the evaluation of the performance of the ISMS, when implemented, which is another crucial aspect of the ISMS control mechanism, entailing internal auditing and management reviews. Internal audits must be conducted periodically to ascertain the effectiveness of the ISMS implementation. This internal auditing of the ISMS is expected to be different from the ISO/IEC 27001 certification audits. Internal auditing of the ISMS should be performed by a qualified auditor and the outcome of such an audit is a report, usually outlining and detailing lapses in the implementation; is based on an audit program, audit criteria and plan agreed with the management of the organization. Management review of the ISMS progress is also an important part of the ISMS implementation process. By this management expresses its commitment to the process, validating it and at the same time, checking efficiency, effectiveness, and adequacy of the ISMS implementation.

Performance evaluation of the ISMS and its constituents, as above described, are covered in this unit.

## 4.1 Monitoring, Measurement, Analysis and Evaluation

The ISMS implementation should be monitored, measured, and evaluated. Measurement of performance of the ISMS is not such an easy task, however, feasible and covered in some detail in the following sub-sections.

### ISMS Performance Evaluation

The ISMS, once implemented, should be subjected to ongoing evaluation to determine its effectiveness and whether it adequately meets the organizational objectives and business needs. This means an appraisal of the performance of the ISMS. But how can the ISMS be measured?

Changes occur every now and then. A change management process properly defined would enable the organization to account for updates to the existing framework and the ISMS operationalization. Tracking and reviewing change is an important part of the overall ISMS monitoring process. Paying attention to incidents and new trends and patterns is a great source of information for guaranteeing updates to the ISMS and to account for gaps in the system.

ISO/IEC 27001:2013 makes room for monitoring of the ISMS, which falls under the heading “performance evaluation” (ISO/IEC 27001:2013). Accordingly, those aspects of the ISMS which should be considered in monitoring and review include the following:

* ISMS performance in terms of its effectiveness, adequacy, and suitability
* changes, risks and impact and their effects on the ISMS performance
* ISMS processes and information security controls to check their effectiveness, adequacy, and suitability, which includes processes for incident management, risk assessment/treatment, information processing, access control and human resource management.
* staff awareness, competence, and utilization of the ISMS
* efficiency, efficacy and effectiveness of the IT and network services and infrastructure
* management of supplier relationship, services, and contracts and SLAs
* conformance with organization’s policies, and procedures, contractual obligations, laws and regulations

The ISMS must be monitored and reviewed for effectiveness and adequacy as well as suitability.

### ISMS Measurement Program

An organization needs to define what **metrics** or measure it will use and how, when and by whom or what measures will be taken in measuring the ISMS.

**Metric**

These are predefined standards of measurements or types of measure. A measurement is the result of measuring something against a metric.

The selection of the metric must be situated on checking the ISMS performance in terms of its adequacy, effectiveness, and suitability. Measurement of the performance of the ISMS is a requirement of the ISO/IEC 27001. Conformance indicates that the ISMS is actually doing what it is envisioned to accomplish.

Performance indicators or KPIs are metrics that are used to measure and evaluate progress towards goal or objective achievement. They can be quantitative or qualitative in nature. Effective KPIs should be specific, measurable, achievable, relevant, and time-bound, enabling data-driven decision making to improve performance. Some common performance indicators for measuring information security include the following:

* Security incident response time is the time taken to identify, respond to, and resolve a security incident.
* Mean time between failures (MTBF) measures the average time between security incidents or breaches, showing the effectiveness of an organization in preventing them.
* Mean time to detect (MTTD) measures the average time taken to detect a security incident or breach. A shorter MTTD means the security system is effectively detecting potential threats.
* Mean time to respond (MTTR) measures the average time to respond to and recover from security incidents. A shorter MTTR means faster recovery and less disruption to operations.
* Security training and awareness program effectiveness measures the effectiveness of training and awareness programs by evaluating factors such as employee participation, knowledge retention, and improvement in behavior.
* Patch management efficiency measures the efficiency of patch management processes, including time taken to identify, test and deploy security patches for vulnerabilities in software and hardware.
* Risk assessment coverage measures the percentage of the organization’s critical assets and systems covered by regular risks assessments to ensure that potential risks are identified and mitigated.
* Number of security incidents measures the total number of security incidents or breaches over a given period.
* Percentage of compliance with security policies and standards measures the level of compliance with the organization’s information security policies, procedures and standards by evaluating factors such as audit findings, policy violations and non-compliance reports.
* Security control maturity evaluates security controls by measuring their effectiveness and gauging progress in improving security levels over time in an organization.
* Vulnerability management measures the efficiency of the organization’s vulnerability management processes, tracking the number of identified vulnerabilities, the time taken to remediate and the percentage of vulnerabilities that remain unaddressed.
* Security cost versus budget compares the actual cost of security measures against the budget allocated for information security in a bid to ascertain cost-effectiveness.

The following guides and frameworks are useful in measuring information security:

* **COBIT 5** for information security is a comprehensive framework which helps organizations achieve their objectives for the governance and management of enterprise IT, including information security.

**COBIT 5 for Information Security**

COBIT 5 comes with 7 enablers for the governance and management of IT, one of which is processes (including information security processes)

* Center for Internet Security (CIS) security metrics is a set of recommended metrics for organizations to assess their security posture and track improvements over time.
* Performance measurement guide for information security is a guide which provides a comprehensive approach to performance measurement for information security, including identifying objectives, selecting KPIs and monitoring progress.

Selection of specific key performance indicators is dependent on the organization and its needs and context, which should be assessed at the initial stages of the ISMS implementation process. The selection of the appropriate metric is dependent on the organizational dynamics and requirements. Other KPIs could include integrating information security into projects, deviating from IT security and architecture standards, and incident response and problem management.

To conclude the section, an effective ISMS measurement program is an important component of a robust information security governance system. By selecting and monitoring relevant KPIs, organizations can gain valuable insights into the efficacy of policies, processes, and controls. Using established frameworks such as COBIT, CIS security metrics and performance measurement guide for information security can offer a strong foundation for developing a good measurement program.

### Self-Check Questions

1. Please list three possible KPIs employed to measure the performance of an ISMS.

*COBIT 5 for information security*

*Center for Internet Security (CIS) security metrics*

*Performance measurement guide for information security*

1. Please mark the incorrect statement(s).

* Measurement of the performance of the ISMS is a requirement of the ISO/IEC 27001.
* The selection of the metric must be situated on checking the ISMS performance in terms of its adequacy, effectiveness, and suitability.
* Conformance indicates that the ISMS is actually doing what it is envisioned to accomplish.
* *The selection of the appropriate metric is not dependent on the organizational dynamics and requirements.*

1. Please complete the following sentence.

ISO/IEC 27001:2013 makes room for monitoring of the ISMS, which falls under the heading *“performance evaluation”.*

## 4.2 Internal Auditing

Audits are essential for organizations to ensure compliance, assess the effectiveness of management systems and continuously improve processes. There are three main types of audits - first-party, second-party and third-party audits. Each of these types of audits serves a unique purpose and is conducted by different parties.

### First-Party Audits

First-party audits are also known as internal audits or self-assessments and are often conducted by the organization itself to review their own processes, systems, and activities against a specific set of criteria, such as the ISO/IEC 27001 standard for ISMS. The purpose of such audits is to identify gaps, non-conformities, and opportunities for improvement in the organization’s management system. There are three types of first-party audits, namely

* compliance audits, which focus on assessing the organization’s compliance with applicable laws, regulations, and policies,
* operational audits, which assess the efficiency and effectiveness of internal processes, departments, or systems within an organization, and
* readiness audits, which evaluate an organization’s preparedness for pursuing external certification (such as ISO 27001) and identify areas that require improvements before undergoing a certification audit

### Second-Party Audits

Second-party audits are known as supplier or vendor audits and are typically conducted by a party with a direct interest in the organization, such as a customer, partner or a regulatory authority. Such audits involve evaluating the organization against specific criteria or requirements set by a second-party auditor or as part of a contractual agreement. Its purpose is to ensure trust, mitigate risks and monitor the performance of the audited organization. Some examples of second-party audits include the following:

* Supplier qualification audits: These are used by organizations to evaluate potential suppliers and their ability to meet specific requirements, such as quality, security, and performance.
* Contract compliance audits: These are audits conducted by customers to confirm that an organization is meeting its contractual obligations and delivering the required services or products.
* Regulatory audits: These are audits performed by regulatory authorities to verify an organization’s compliance with the applicable laws, regulations, and standards.

### Third-Party Audits

Third-party audits are typically conducted by independent external organizations or certification bodies. These audits are meant to assess an organization against internationally recognized standards, such as the ISO/IEC 27001, to verify that an organization’s management system meets the requirements of the standards. It is purposed to provide assurance to stakeholders, namely customers, partners, and regulators, that the organization has an effective management system in place. Example of third-party audits include the following:

* certification audits: In this audit, a third-party certification body evaluates an organization’s management system against a specific standard such as ISO/IEC 27001 and if compliant, certification is issued to that effect (e.g., ISO/IEC 27001 certification). There are often two stages in this audit - a documentation review and an on-site assessment.
* surveillance audits: These are regular follow-up audits, usually annually, and conducted by a certification body to verify the organization’s continued compliance with the standards.
* re-certification audits: These are comprehensive audits performed every three years to confirm that an organization is complying on an ongoing basis with the standards and to renew certification.

Now, the objective of internal ISMS audits is to monitor the extent to which the ISMS meets organizational requirements. So essentially, to review processes and sub-processes underlying the ISMS operationalization and to bring to the fore important observations to improve the ISMS implementation. This is a major control activity (conformity control) in accordance with the ISO/IEC 27001. An audit program should be planned and developed. This audit program should indicate audit frequency, procedure, roles and responsibilities, requirements, reporting in addition to ways of definition of corrective and preventive actions. The audits are expected to be conducted or performed at least once in three years, covering all business processes under the ISMS, as defined in the ISMS scope. An audit program should be developed for the audit and should spell out the processes, planning, definition, implementation, monitoring and review and improvement of the audit process.

The ISMS auditors should be experts who will deliver objectively and neutrally as required under the audit process from the beginning of the audit engagement until the reporting phase.

The ISMS audits should be planned such that non-conforming activities, potential as well as unidentified vulnerabilities and threats are identified.

In the planning and conduct of the audits, the following matters apply:

* Audits cannot be commenced until they have been commissioned. The process formally starts with communication and engagement with the audited entity, where the scope and other aspects of the audit delivery are considered and agreed.
* Steps to deal with threats and vulnerabilities identified should be documented during the audit process.
* Events from previous audits, such as inherent risks and unresolved matters, should be logged accordingly.
* The results of the audit must be communicated to the stakeholders, including the ISMS management. Such reports must show what was accessed and or used as the basis for the audit conclusions.

The audit program and audit results should be documented in accordance with clause 9.2g of the standard.

There exists a difference between an organization’s internal control mechanisms and systems, and the ISMS, which is considered an aspect of the overall organizational internal control system (ICS). The ICS is the broader organizational level system of control, while the ISMS audit is a component or subcomponent of the overall ICS. It is important to note that the ISMS could overlap with the ICS.

### Self-Check Questions

1. Please complete the following sentence.

The review of processes and sub-processes underlying the ISMS operationalization to bring to the fore important observations to improve the ISMS implementation is known in the ISO/IEC 27001:2013 as *“conformity control”.*

1. Please complete the following sentence.

The organizational internal control system (ICS) is the broader *organizational level system of control*, while the ISMS audit is a *component of the overall ICS*.

## 4.3 Management Review

Clause 9.3 of ISO/IEC 27001 requires a management review of the ISMS. The review is expected to occur between agreed intervals by a board of directors or when a significant change occasions the risk profile of the organization. While the board of directors or top management are responsible for governance, an information security manager or whoever has been designated by the top management should be responsible for organizing, communicating, and gathering inputs into the process and relaying the outputs or outcomes of the review back to relevant stakeholders.

### Self-Check Questions

1. Please complete the following sentence.

*Clause 9.3* of ISO/IEC 27001 requires a management review of the ISMS.

Summary

In this unit, performance evaluation of the ISMS was covered. The ISMS progress must be analyzed and evaluated, its efficiency and effectiveness monitored on a regular basis, often to adjust for changes in both the internal organizational and external environment. Metrics for measuring the ISMS progress will have to be defined by the organization based on its needs and relevant factors covered in the unit.

Internal audit of the ISMS, which should be clearly distinguished from ISO certification audit, should be performed on a regular basis. It is purposed to check whether the ISMS satisfies the requirements and specifications of the ISO/IEC 27001 requirements, identify weak links, gaps in the ISMS implementation and also possible potential avenues for improvement.

# Unit 5 – Improving the Information Security Management System

**Study Goals**

On completion of this unit, you will be able to…

… understand and explain how challenges and non-conformities that may arise during the ISMS setup in an organization could be addressed.

… develop measures for continual improvement of the ISMS.

… plan and implement corrective measures and preventive action plans to ensure that the ISMS is always functioning properly.

# 5. Improving the Information Security Management System

## Introduction

Up to this point, the ISMS has been put in place. ISMS continual improvement is needed as a check along the implementation journey, which is essentially an ongoing project. Following the PDCA lifecycle, the organization should check if the implementation is on tract and adjust areas not working, re-align scope, if such problems exist, or eliminate nonconformities in the process.

This unit covers how to treat nonconformities, which connects to root cause analysis and determining and uprooting implementation bottlenecks out of the way, and their common causes; continual improvement measures to put in place to ensure that the ISMS is working on an ongoing basis; to also safeguard information assets of the organization, as well as corrective actions and preventive measures which are required to avoid recurrence of problems identified.

## 5.1 Treatment of Challenges and Non-conformities

A **non-conformity** in an ISMS is a non-fulfillment of the requirements specified in the ISO/IEC 27001. It is instructive to note that some of the requirements listed in the standards are mandatory, while others are recommendations. The mandatory ones are those referred to as “shall” requirements, which should be adhered to by an organization in the implementation of an ISMS and in the general protection of their information assets. Most of the requirements in the standards include “shall” and during audits or reviews, are included in the checklist for conformance or not by the implementing entity or organization. In the event that these requirements are not met, there are non-conformities, which should be corrected.

**Non-conformity**

There are major and minor nonconformities, which may be recorded in the process of an organization’s ISO certification audit. Major nonconformities usually result in non-certification.

Non-conformities range from operational to technical and could be caused by several factors or lack of it thereof, including (but not limited to) the following:

* a failure on the part of management (senior or top management) to appreciate the internal and external context and the needs of all stakeholders in the ISMS rollout: This failure on the side of management often impacts the effectiveness of the ISMS implementation and delivery (in accordance with clause 4.1 and 4.2 of the ISO/IEC 27001:2013)
* no clear definition of the scope of the ISMS: Scope definition is specified in clause 4.3 of the ISO/IEC 27001 and is one of the important steps towards the implementation of the ISMS. Without a proper scope definition, the ISMS will lack appropriate boundaries within which they are expected to be delivered and consequently, their effectiveness measured against.
* no proper risk assessment process and treatment mechanisms: Risk assessment and treatment are specified in the clause 6 of the standards.
* continual improvement: This is required to be part of the ISMS implementation process. The ISMS is not a one-off project. Management’s inability to ensure this is considered a nonconformity, is in contravention with clauses 5.2 and 6.1.1 of the standards.
* Smaller enterprises/organizations faced with the problem of lack of resources to manage the ISMS implementation process, which requires resources (both human and material): Clause 7 of the standards specifies making available the needed resources and support towards the implementation of the ISMS, which rests on the shoulders of the management of the organization.
* a failure on the part of management to ensure controls are effective and address the risks identified at the initial phases of the rollout. Clause 6 specifies adequate measures to address risks identified and the implementation of controls.
* a failure on the part of management to ensure evaluation of the performance of the ISMS. Performance evaluation is specified in clause 9 of the standards. These include internal audits and reviews and other investigations which will help to identify challenges fraught with the ISMS implementation and its correction for that matter.

It is the duty of management to ensure through the conduct of audits, investigations, and checks, among other, that nonconformities duly detected are removed to enable a healthy ISMS implementation.

### Self-Check Questions

1. Please list four possible causes of nonconformities in an ISMS implementation.

*A failure on the part of management to ensure controls are effective and address the risks identified at the initial phases of the rollout.*

*No proper risk assessment process and treatment mechanisms*

*No clear definition of the scope of the ISMS*

*A failure on the part management (senior or top management) to appreciate the internal and external context and the needs of all stakeholders in the ISMS rollout.*

1. Please complete the following sentence.

Non-conformities range from *operational* to *technical.*

## 5.2 Continual Improvement

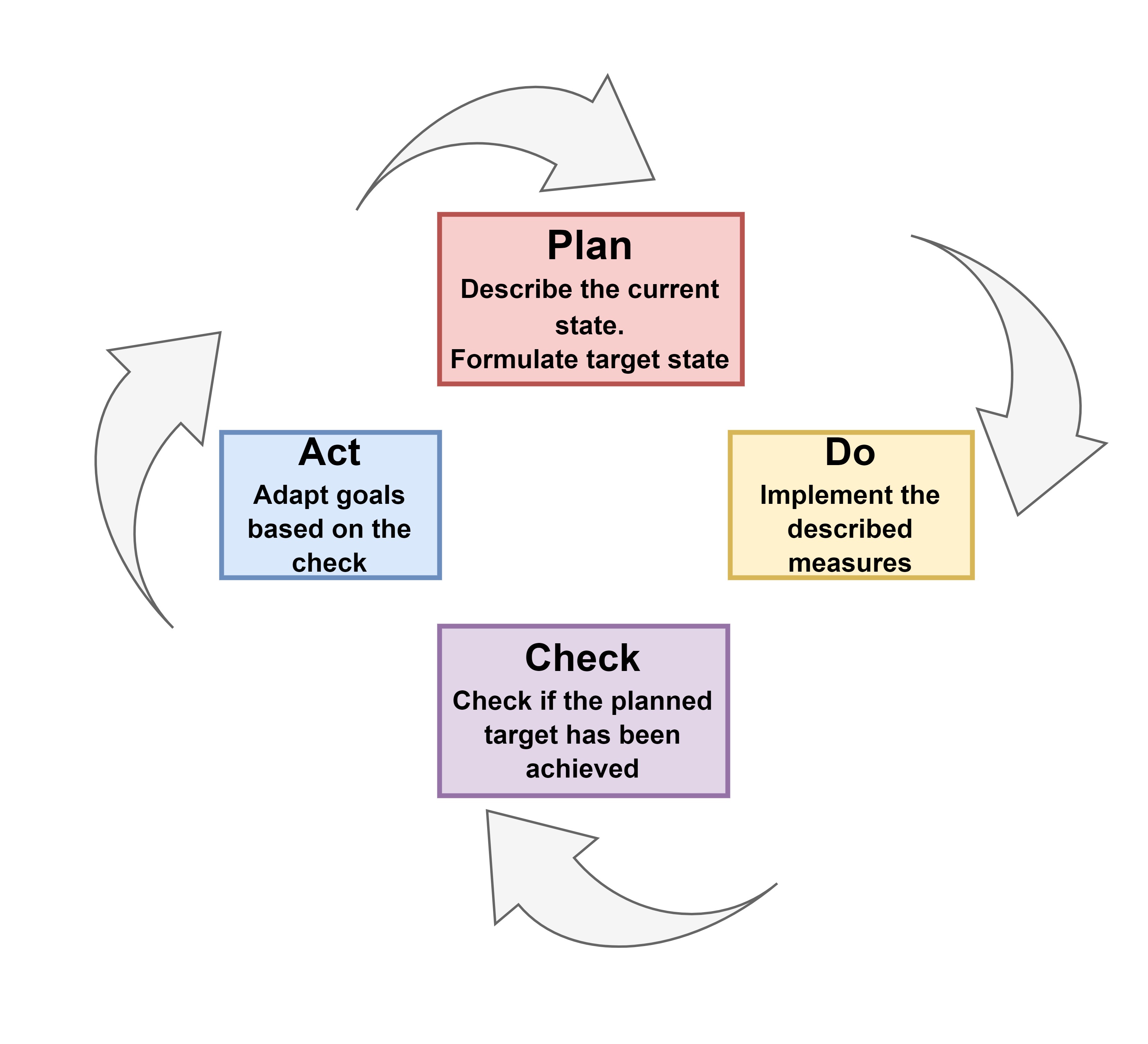
The ISO/IEC 27001:2013 refers to improvement as “continuous improvement” and is mandatory as an aspect of conformance with the standards. (Humphreys, 2016)

The Plan-Do-Check-Act (**PDCA**) cycle (also known as the Deming cycle) is a useful model to ensure continual improvement of the ISMS. *Plan* is for description of the existing state of the ISMS, *Do* is implementing measures to ensure the ISMS is operating effectively. *Check* is to ensure the ISMS is effective and on target to achieve its intended objective, as part of the broader organizational objectives, and finally, *Act*, is making changes to the ISMS following its continual review and checks.

**PDCA**

An iterative design and management method used in business for the control and continuous improvement of processes and products.

Continual Improvement of the ISMS Using PDCA



Source: Andrew Sai (2023).

The question of how to identify which areas to improve has come up severally from organizations intending to set up an ISMS successfully. Practitioners often suggest considering the following areas:

* audit reports (internal and external)
* special and regular investigation reports
* monthly performance reviews and reports
* participation or reporting by employees. E.g., incidents are reported by employees directly who use systems and or processes, when they are defective.
* management review reports
* customers and third parties, other stakeholders
* the outcome of checking compatibility between new tools and technologies and the existing systems and ISMS setup
* external factors such as regulatory and legal updates

While the list above is not exhaustive, success of the improvement steps could be gauged using the template suggested in the figure below. Improvements could be to processes, policies and procedures, awareness, and training improvements. This sample tracker (in MS Excel) is intended to help members of the organization seeking to improve the ISMS to be able to know and track how improvements were implemented in a given period, how much time was spent, responsible persons and priority levels, among others.

Continual Improvement Plan Tracker Template

Table

Description automatically generated with medium confidence

Source: Andrew Sai (2023).

### Self-Check Questions

1. Please complete the following sentence.

According to the Deming Cycle, *Plan* is for description of the existing state of the ISMS, *Do* is implementing measures to ensure the ISMS is operating effectively, *Check* is to ensure the ISMS is effective and on target to achieve its intended objective, and *Act*, is making changes to the ISMS following its continual review and checks.

## 5.3 Corrective and Preventive Action Plans

When nonconformities have been detected, the next important action is correction and further on, preventive measures to avoid recurrence.

For corrective action, it is important to identify the source of the anomaly and to eliminate them. Depending on the complexity of the problem or nonconformity, performing a **root-cause analysis** is paramount. This helps to understand where the problem emanates from, its effects or potential effects and how it could be curbed. Root causes could come from many sources, such as people, processes, technical issues, managerial lapses, method defects, among others.

**Root cause analysis**

This is a method of problem solving used for identifying the root causes of faults or problems and is widely used on IT, and operations. industries

An example of such a nonconformity could be a defective policy, say on asset and device management, this anomaly could be remedied by rolling out a new policy document, with amendments to it, fixing the problem. In the same vein, if the problem is inadequate training or staff awareness regarding a policy or procedure, this nonconformity could be fixed with further training and refresher courses for staff of the organization to bring them up to date, thus an improved training and awareness programme to correct the nonconformity identified.

Preventive action plans usually accompany corrective measures taken and could range from simple training programs to major overhauls in systems, processes or more once the root cause of the problem is identified and fixed. In some cases, where they are not fixed and for example, human error is the main root cause of a problem, a preventive action could be to automate that process, eliminating the human intervention, as a preventive measure.

**ISO 22301 - Security and resilience - BCMS**

This defines business continuity management as part of overall risk management in a company.

As part of preventative measures, cyber-attacks, data breaches and natural disasters could interrupt business and therefore the ISMS execution. The ISO/IEC 22301 is tailored to help organizations manage threats, including their identification and prioritisation. Organizations that implement business continuity management systems (BCMS) effectively are better prepared to deal with any incidents and recover far more quickly with the least of interruption to business, than those that do not work with the BCMS standards.

### Self-Check Questions

1. Please mark the incorrect statement(s).

* When nonconformities have been detected, the next important action is correction.
* Root causes could come from many sources, such as people, processes, technical issues, managerial lapses, method defects.
* Preventive action plans usually accompany corrective measures taken.
* *A defective policy is not an example of nonconformity.*

Summary

In the Unit, nonconformities were first discussed, followed by continual improvement and which corrective and preventive measures are needed to remedy such problems. Nonconformities are basically non-fulfillment of the requirements specified in the standards. The elimination of nonconformities should be a top priority for management of an enterprise or organization. Once nonconformities are detected, steps to ensure an improvement to the ISMS are to be taken and monitored on an ongoing basis. Opportunities exist for management of an enterprise or organization to identify areas for improvement, and this must be done, to ensure that the ISMS implementation is successful.

# Unit 6 – Controls of the Information Security Management System

**Study Goals**

On completion of this unit, you will be able to…

…identify and discuss the general structure of controls listed in the ISO/IEC 27000 series of standards, more specifically, the ISO/IEC 27001 and ISO/IEC 27002.

…understand and describe the groupings and categorizations of the various controls prescribed in Annex A of the ISO/IEC 27001.

…differentiate and manage controls put into effect as part of the ISMS implementation.

…evaluate the effectiveness of controls of the ISMS in an organization and formulate control objectives to meet organizational needs, where required.

# 6. Controls of the Information Security Management System

## Introduction

Annex A of the ISO/IEC 27001 contains a number of controls, which are fundamentally elements of risk treatment, to be selected following a thorough assessment of risks in an organization. Before selecting controls to implement, risks should be assessed, business needs and best practice perused, and legal and contractual obligations analysed.

**ISO certification**

This demonstrates that an organization is committed to continual improvement, development, and protection of information assets and data by implementing risk assessments, policies, and controls.

Annex A of the ISO/IEC 27001 lists the controls, which are categorized. Meanwhile, ISO/IEC 27002, provides a detailed explanation of the controls. The 14 clauses in the ISO/IEC 27001:2013, were revised and replaced with four thematic areas in the 2022 edition, and the 114 controls revised down to 93. These updates are merely re-organizations of the same contents, which do not affect the core structure of the ISO family of standards. For organizations seeking **ISO/IEC 27001 re-certification**, the updates are crucial, however.

In this unit, ISO/IEC 27001:2013 and ISO/IEC 27002:2013 are referenced copiously. Where content from the updated version of the ISO/IEC 27001 or 27002: 2022 are implied, they are explicitly stated.

Controls that are selected from the list offered in Annex A of the ISO/IEC 27001, must be accompanied by detailed justification for their inclusion or exclusion, which is typically informed by factors surrounding the organization implementing the ISMS. The justification for inclusion or exclusion of some controls must be documented in a statement of applicability (SoA). The SOA provides management with a snapshot of risk exposures, levels and status of risk treatment.

The unit covers what controls are generally; summarizes the control categories listed in the ISO/IEC 27001 and their objectives and closes with how controls should be managed and their evaluation to check for suitability and effectiveness.

## 6.1 General Structure of Controls

Controls could be considered as methods, systems and processes by which an organization stimulates its subunits and members to act in accordance with organizational edicts and prescriptions. Controls could range from rules, guidelines, procedures, policies and more intended to guide how things are done.

ISMS controls are typically steps required to mitigate risks and exposures to information assets in an organization. Such controls are often requirements specified in the standards.

Controls are established as part of the risk treatment process. It is noteworthy that ISO/IEC 27001 is to be understood as a management system standard with an objective of protecting information and not necessarily an IT-security standard. They wield a heavy management-oriented concentration mostly.

Some examples of controls in an organization include information security policies, recruitment processes, internet usage policies, access control policies, communications policy, security procedures, standard operating procedures, incident management processes among others.

**Control Framework**

This is a data structure that organizes and categorizes an organization’s internal controls, including practices and procedures established to create business value and reduce risks.

The above controls could be delineated into packets, as a **control framework**, which could consist of the following:

* policies and procedures
* processes
* practices
* plans
* programs

Each of the control elements may exist in one of these packets.

There are four main control domains in the ISO/IEC 27001:2022 standards, as follows.

Organizational controls

People controls

Physical controls

Technological controls

ISO/IEC 27001 Control Domains

Source: Andrew Sai (2023).

These four domains were included in the updated version of ISO/IEC 27001:2022. The themes were introduced to group the controls accordingly. Again, it is an issue of re-organization/rehashing of what already existed in the ISO/IEC 27001:2013:

* organizational controls (37 controls): These are controls for setting up crucial organizational security processes and documenting them, such as organizational information policies, cloud service use, asset use and more.
* people controls (8 controls): These are controls on secure management of human resources in the organization, including remote work, confidentiality, non-disclosures and screening.
* physical controls (14 controls): These are the controls to secure areas and equipment in the organization, including security monitoring, storage media, maintenance, and facilities security.
* technological controls (34 controls): These are controls for the protection of IT and communication systems, including controls on authentication, encryption, and data leakage prevention.

The changes to the ISO/IEC 27000 family of standards can be found on the ISO website (ISO, 2022). In the 2022 edition, 11 new control categories were added, including threat intelligence, information security for use of cloud services, ICT readiness for business continuity, configuration management, information deletion, data masking, data leakage prevention, monitoring activities, web filtering, and secure coding. Additionally, new attributes were introduced to simplify the categorization of controls in the standard:

* control type (preventive, detective, corrective)
* information security properties (confidentiality, integrity, availability)
* cyber security concepts (identify, protect, detect, respond, and recover)
* operational capabilities (governance, asset management etc.)
* security domains (governance and ecosystem, protection, defence, resilience)

### Self-Check Question

1. Please list at least three of the elements that could be contained in a control framework.

* *Policies and Procedures*
* *Processes*
* *Practices*
* *Plans*
* *Programmes*

1. Which of the following is not one of the four domains that were included in the updated version of ISO/IEC 27001:2022?

* *Business controls*
* Technological controls
* Physical controls
* People controls

1. Please complete the following sentence.

Controls could range from *rules*, *guidelines*, *procedures*, *policies* and more intended to guide how things are done.

## 6.2 Controls of the ISO/IEC 27001 - Annex A

**Annex A of ISO/IEC 27001**

This is the most famous of all the ISO standards. It provides an essential tool for managing information security risks, offering a list of security controls required to improve security in an organization.

**Annex A** **of the ISO/IEC 27001** standards contain essential controls for managing information security risks in an organization. It houses a list of controls or safeguards needed to strengthen organizational information security. Annex A provides an outline of all the controls, which elaborate versions and explanations are available in ISO/IEC 27002 in more detail, providing pointers about how to implement them as well. This also answers the question of the connecting tissue between ISO/IEC 27001 and ISO/IEC 27002.

As noted earlier in the Unit, there are 14 control categories into which Annex A of the ISO/IEC 27001:2013 are organized. The controls are 114 according to the ISO/IEC 27001:2013, however revised down to 93 in the more updated version such as ISO/IEC 27001:2022. The organization of the controls into 14 groupings makes it easier to identify the different sets of controls and improve organizational information security. These follow an established structure, with a naming convention. Below, each of the 14 control categories are summarized and described, their category names/numbers are indicated, and the number of objectives and controls under each one stated. The objectives are covered briefly; however, the controls can be gleaned from the ISO website directly, due to its volume. Summaries and descriptions (from Annex A of ISO/IEC 27001:2013) are as follows (ISACA, 2017):

* **information security policies** (control category A.5 - 1 objective and 2 controls): This category of controls is intended to provide management with direction and the needed support to conform organizational requirements, legal and other regulatory requirements.
* **organization of information security** (control category A.6 - 3 objectives and 6 controls): This category of controls is intended to establish a management framework for implementation and operation of information security in an organization. Its second objective is ensuring that remote working and mobile devices are secured.
* **human resource security** (control category A.7 - 3 objectives and 6 controls): This category of controls relates to pre-employment requirements; to ensuring individuals are aware of their responsibilities for information security during employment and finally to protection of an organization’s interests when employees exit or change roles.
* **asset management** (category A.8 - 3 objectives and 10 controls): This category is intended to identify information assets and define appropriate responsibilities to secure them; protection of information; and prevention of unauthorized disclosure, updating or destruction of information.
* **access control** (control category A.9 - 4 objectives and 14 controls):This category of controls is intended to limit access to information and its processing facilities; ensuring that authorized users have access to perform their duties; ensuring that users take steps to protect their passwords and PINs and are accountable for same; and finally, prevention of unsanctioned access to systems and applications.
* **cryptography** (control category A.10 - 1 objective and 2 controls):This category relates to how cryptography is used to protect information assets.
* **physical and environmental security** (control category A.11 - 2 objectives and 15 controls):This category of controls seeks to prevent unauthorized physical access and damage to information assets and facilities which house them; and prevention of loss, theft, or interruptions to operations of an organization.
* **operational security** (control category A.12 - 7 objectives and 14 controls): This category ensures that information assets and physical locations are protected; protection against malware, protection against loss of data, including backups and policies and procedures to safeguard backups; maintaining records of events and providing evidence where required; integrity of operational systems; prevention of exploitation of technical weaknesses; and finally to reduction of the impact of audit activities on operational systems in an organization.
* **communications security** (control category A.13 - 2 objectives and 7 controls): This category relates the maintenance of information transferred internally and externally.
* **system acquisition, development and maintenance** (control category A.14 - 3 objectives and 13 controls): This category relates to the set of controls which ensure that information security is a core part of information systems, including over public networks, design and development of information systems within the development lifecycle and ensuring the protection of data used in testing software in the course of its development, including its anonymization, among others.
* **supplier relationships** (control category A.15 - 2 objectives and 5 controls): This category is intended to protect assets that are accessible to suppliers and third parties and to maintain agreed levels of information security, and service delivery levels per agreement with such suppliers.
* **information Security incident management** (control category A.16 - 1 objective and 7 controls): Intended to ensure the proper management of security incidents, including communication of security events and vulnerabilities.
* **information security aspects of business continuity management** (control category A.17 - 2 objectives and 4 controls): Intended to avoid breaches of legal, statutory, regulatory and contractual requirements about information security and its obligations; ensure availability of information processing locations.
* **compliance** (control category A.18 - 2 objectives and 8 controls): Intended to avoid breaches of legal, statutory, regulatory, and contractual requirements about information security; and ensure that information security practices agree with organizational policies and procedures.

For each of the control categories listed in Annex A of the ISO/IEC 27001:2013, the specific controls are likewise listed with further explanation in ISO/IEC 27002:2013 or their updated versions, such as ISO/IEC 27001:2022 and ISO/IEC 27002:2022.

### Self-Check Questions

1. Annex A of the ISO/IEC 27001:2013 lists:

* *114 controls and 14 control categories*
* 14 controls and 114 control categories
* 37 controls and 93 control categories
* 93 controls and 37 control categories

1. Please list five ISO/IEC 27001:2013 control categories.

*Information security policies*

*Human resource security*

*Access control*

*Cryptography*

*Compliance*

## 6.3 Management of Controls

The effective management of controls is an important aspect of implementing, maintaining and improving any ISMS. When organizations introduce or adapt controls within their ISMS, conducting a gap analysis is highly recommended to assess the adequacy of the controls in meeting the ISMS requirements. The gap analysis outcome is valuable in updating policies, processes and the overall enhancement of the ISMS. The decision-making process regarding which controls to apply heavily depends on the organization’s specific needs, industry and objectives. The section outlines various aspects of control management, including the selection of appropriate controls, documentation, staff training and continuous monitoring and improvement.

### Selecting Appropriate Controls

Organizations must choose the controls that are most relevant to their operations and the implementation of the ISMS. Controls that do not pertain to the organization’s scope of work or industry can be excluded, provided that their exclusion is justified and documented in a SoA - which should detail why the selected control is not necessary based on the organization’s objectives, requirements and specific circumstances. For example, if an organization does not engage in software development, it may opt not to include controls related to designing and developing information systems within a prescribed software development lifecycle (control category A.14 - System acquisition, development and maintenance). However, such an exclusion must be justified and documented in the SoA, clarifying why this particular control is not required.

### Documentation

Proper documentation plays an important role in the management of controls for an ISMS. It should capture essential information regarding analyzed risks, selected controls, justification for inclusion or exclusion of controls, responsibilities, and details about effectiveness of the controls and implementation. Documentation helps management in decision making; to understand the rationale behind each of the controls and their importance in the overall ISMS and as well provides a good foundation for improvement and fine-tuning of the system. Documentation is not only essential for organizational purposes but is also a requirement for obtaining ISO/IEC 27001 certification. Adequate and efficient documentation allows for identification and tracking of controls and taking of appropriate actions to address any non-conformities or challenges.

### Staff training

Staff training is another important aspect of the management of controls. Ensuring that employees who are directly involved in the ISMS implementation or are responsible for overseeing its execution have the needed skills, knowledge and competencies to deliver ensure that the ISMS is effective. Training should be tailored to the needs of the organization and cover topics including the following

* An overview of the ISMS
* specific policies and procedures of the organization
* relevant controls
* incident reporting and response
* security awareness and culture

Staff training is such a vital requirement for attainment of the ISO/IEC certification and maintaining compliance with the standards. Organizations should regularly review and adapt training programs to accommodate evolving information security needs, risks and regulatory requirements.

### Continuous monitoring and improvement

Effective management of controls includes continuous monitoring, evaluation, and improvement of their performance. Establishing and implementing monitoring mechanisms such as regular audit and compliance assessment is important for ensuring that the selected controls remain relevant, adequate, and sufficient in address organizational needs and the ISMS objectives. Including feedback loops within the system to enable continuous learning and improvement goes a long way to ensure the success of the ISMS. Feedback could come from many sources, such as staff, customers, suppliers, auditors, and regulators. The outcome of these monitoring activities should help organizations implement or improve corrective and preventive measures.

To conclude, the management of controls is an important aspect of implementing and maintaining an ISMS. Selecting appropriate controls, ensuring proper documentation, training staff and monitoring and improving the system all go to improve an organization’s security posture and stay compliant with the ISO/IEC 27001 standards.

### Self-Check Questions

1. Please complete the following sentence.

In the management of controls, controls not implemented are expected to be included in *a statement of applicability* or *SoA*.

## 6.4 Evaluating the Effectiveness of Controls

In the sphere of risk management and internal control systems, evaluating the effectiveness of controls plays a vital role in ensuring overall efficiency and reliability of an organization’s operations. As businesses continue to face dynamic challenges and risks, it becomes increasingly important to assess strengths and weaknesses of existing control measures. The subsection aims to explore the various methodologies, criteria, and indicators used in evaluating the effectiveness of controls, for organizations seeking to maintain a robust control environment.

Controls can take many forms, from policies, processes, practices, techniques, methods to technology. Controls are intended to work as preventative measures, detective measures and corrective measures. Controls, when effective help to reduce risk. An organization’s internal control mechanism should be subjected to regular review to ascertain whether they are working effectively or not. How well a control is working could be established by evaluating

* The relevance of the control (Does it address the intended risks?),
* the completeness of the control (Does it address some risks, or all risks intended to be addressed?),
* the reliability of the control (Does it work as expected?), and
* the timeliness of the control (Does it work at the right time?)

When assessing to determine whether the controls are effective or otherwise, it is important to evaluate if the controls help

* reduce the impact of risks.
* reduce the likelihood of risks.
* detect and respond to possible attacks before they materialize.
* implement corrective and preventive actions.

Several methods could be used as a vehicle to check for the suitability, adequacy and effectiveness of an ISMS. It is however important, notwithstanding the method engaged, to ensure that risks are identified, assessed, and mitigated, where they could pose significant concerns to the objectives of the organization.

Data is essential in any evaluation process, and it is not any different for evaluating the effectiveness of controls. Such data, whether qualitative or quantitative could be gathered from sources such as: complaints and survey results, incidents reported, root cause and problem analysis, user testing reports, self-assessment reports, audit reports, among others.

A rating scale is often used to evaluate the effectiveness of controls. Typically, such scales are 3-level or 5-level scales, for example, a three-level scale will look the following:

* effective (Level 3)
* partially effective (Level 2)
* ineffective (level 1)

Level 3 suggests that the controls are effective and working as expected. Meanwhile Level 1 suggests that the controls are not working well, have not been documented or communicated properly, based on the criteria developed. A 5-level scale will also look like the following:

* fully effective (level 5)
* substantially effective (level 4)
* partially effective (level 3)
* largely ineffective (level 2)
* totally ineffective (level 1)

Notwithstanding which of the rating scale is employed, what is important is that there is consistency and a widespread shared understanding regarding how and when to evaluate the effectiveness of controls. Ineffective controls mean greater risks and exposures for the organization.

In conclusion, evaluating the effectiveness of controls is an essential component of maintaining a strong control environment and mitigating risks. By employing a comprehensive, systematic approach that includes all aspects of the control system, it is possible to identify areas for improvement. Ultimately, a well-designed and effectively functioning control system serves as the foundation for a resilient and successful organization.

### Self-Check Questions

1. Please mark the incorrect statement(s).

When assessing to determine whether the controls are effective or otherwise, it is important to evaluate if the controls help:

* Reduce the impact of risks.
* Reduce the likelihood of risks.
* Detect and respond to possible attacks before they materialize.
* *Reduce corrective and preventive actions.*

1. Please complete the following sentence.

On a three-scale controls rating scale, Level 3 suggests that the *controls are effective and working as expected*, while Level 1 suggests that the *controls are not working well*, *have not been documented* or *communicated properly.*

Summary

Controls could be organized into packets based on the control framework developed for an organization as part of the maintenance of its information security apparatus. These range from policies, procedures, down to plans and programs.

Annex A of the ISO/IEC 27001:2013 houses a list of 14 control categories and 114 controls, which were restructured in the updated 2022 version of the standard, to 93 controls with four main control categories. The changes include 11 new controls added. Overall, the different sets of controls are designed to help an organization improve its information security. Each of the control categories and their controls are explained in further detail in ISO/IEC 27002, including the primary objectives and the objectives of each of the categories.

The decision about which controls to implement or otherwise is left to the organization to tailor to its needs and requirements, but with a responsibility to document in an SoA.

The effectiveness of a set of controls when implemented can be gauged in several ways. It is however imperative to ensure that they are helping to manage risks in the implementation of the ISMS.