TECHNICAL SPECIFICATION

ISO/IEC TS 27022

First edition

Information technology — Guidance on information security management system processes

PROOF/ÉPREUVE

Reference number
ISO/IEC TS 27022:2021(E)

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

Contents

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular, the different approval criteria needed for the different types of document should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO and IEC shall not be held responsible for identifying any or all such patent rights. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents) or the IEC list of patent declarations received (see patents.iec.ch).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation of the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT), see www.iso.org/iso/foreword.html.

This document was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *Information security, cybersecurity and privacy protection*.

Any feedback or questions on this document should be directed to the user’s national standards body. A complete listing of these bodies can be found at www.iso.org/members.html.

Introduction

An information security management system (ISMS) includes a collection of interacting processes and is operated by performing those processes. This document provides a process reference model (PRM) for information security management, which differentiates between ISMS processes and measures/controls initiated by them.

A PRM is a model comprising definitions of processes described in terms of process purpose and results, together with an architecture describing the relationships between the processes. Using the PRM in a practical application can require additional elements suited to the environment and circumstances.

The PRM specified in this document describes the ISMS processes implied by ISO/IEC 27001. The PRM is intended to be used as a process implementation and operation guide.

Any organization can define processes with additional elements in order to tailor it to its specific environment and circumstances. Some processes cover general management aspects of an organization. These processes have been identified in order to support organizations in addressing the requirements of ISO/IEC 27001.

Information technology — Guidance on information security management system processes

1 Scope

This document defines a process reference model (PRM) for the domain of information security management, which is meeting the criteria defined in ISO/IEC 33004 for process reference models (see Annex A). It is intended to guide users of ISO/IEC 27001 to:

— incorporate the process approach as described by ISO/IEC 27000:2018, 4.3, within the ISMS;

— be aligned to all the work done within other standards of the ISO/IEC 27000 family from the perspective of the operation of ISMS processes

— support users in the operation of an ISMS – this document is complementing the requirements-oriented perspective of ISO/IEC 27003 with an operational, process-oriented point of view.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO/IEC 27000, *Information technology — Security techniques — Information security management systems — Overview and vocabulary*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 27000 and the following apply.

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

— ISO Online browsing platform: available at https://www.iso.org/obp

— IEC Electropedia: available at http://www.electropedia.org/

3.1
core process
process that delivers apparent and direct customer value and is derived from the *core competencies* (3.1) of the management systems

Note 1 to entry: This definition relies on and extends the definitions in ISO 9000:2015 and ISO 38500:2015.

Note 2 to entry: In this definition, "core competency" is understood as the set of skills and know-how present within a management system, directly aligned with the objectives of the management system, supporting the achievement of the objectives and not elsewhere present within the organization at a competitive level.

3.2
integrated management system
IMS
management system that integrates all of an organization’s systems – like information security management and business continuity management – and processes in to one complete framework, enabling an organization to work as a single unit with unified objectives

3.3
key goal indicator
indicator that is an ex-post measure for the achievement of a goal/objective

3.4
key performance indicator
indicator that is an ex-ante measure, which allow a prediction if a goal/objective is achieved in the future

3.5
management process
process that defines the objectives of the management system to achieve the strategic objectives set by the organization's governing body

Note 1 to entry: This definition relies on and extends the definitions in ISO 9000:2015 and ISO/IEC 38500:2015.

3.6
support process
process that supports core processes by providing and managing necessary resources without delivering direct customer value

Note 1 to entry: This definition relies on and extends the definitions in ISO 9000:2015 and ISO/IEC 38500:2015.

4 Structure and usage of this document

The objective of this document is to guide the users of ISO/IEC 27001 on the operation of the ISMS. No additional requirements are defined within this document.

It is not intended to be used "out of the box" without adapting it to the implementing organization and it should not be used as requirements within ISMS certification audits.

The model architecture specifies a process architecture for the domain and comprises a set of processes, with each described in terms of process purpose and results. The PRM is closely aligned to the information security requirements as contained in ISO/IEC 27001:2013. Processes are differentiated in core, management and supporting processes. The PRM is also meeting the criteria defined in ISO/IEC 33004 for process reference models.

Each process of this PRM is described in terms of:

- process category;
- brief description;
- process flowchart;
- objective/purposes;
- input and results;
- activities/functions;
- references.

The PRM does not attempt to place the processes in any specific environment nor does it pre-determine any level of process capability/maturity required to fulfil the ISO/IEC 27001 requirements.

The PRM provides a detailed but generic blueprint regarding the core processes of an ISMS. The PRM is applicable to all organizations independent of their size, objectives, business model, location, etc. The ISMS PRM should be used as a prototype for an ISMS, which needs to be tailored to the objectives, needs and individual requirements of the implementing organization. The tailoring of the PRM can include omission of some of the listed processes, where they are inapplicable or would be reduced to vestigial form.

The process orientation of the PRM also supports the transition from designing and implementing an ISMS (project phase) to the operation of the ISMS (performing the processes). The process orientation also supports and allows the integration of the ISMS processes in further domains of an integrated management system, described within the ISO handbook "The Integrated Use of Management System Standards (IUMSS)".

5 Overview

The fundamental elements of a PRM are the descriptions of the processes within the scope of the model. The process descriptions in the PRM incorporate a statement of the purpose of the process, which describes at a high level the overall objectives of performing the process.

An ISMS incorporates processes, for example shown in Figure 1. The listed processes illustrate key topics that should be considered during the process design phase when implementing an ISMS.

The PRM should not be used "out of the box" without adapting it to the objectives, needs and individual requirements of the implementing organization. For every ISMS process, the individually necessary maturity level should be determined, implemented and operated. A possible result of determining the necessary maturity level of a process can be, that the process is not needed at all (maturity level zero).

ISMS processes should be individually integrated into existing management systems and processes. This is not displayed in the figure to ensure readability and due to existing management systems differing too much in praxis.

Interfaces to the ISMS processes are described within the detailed process profiles and process flow charts. Interfaces to the records control process and to the security policy management process are only described within the detailed process profiles to ensure readability of the process flow charts.

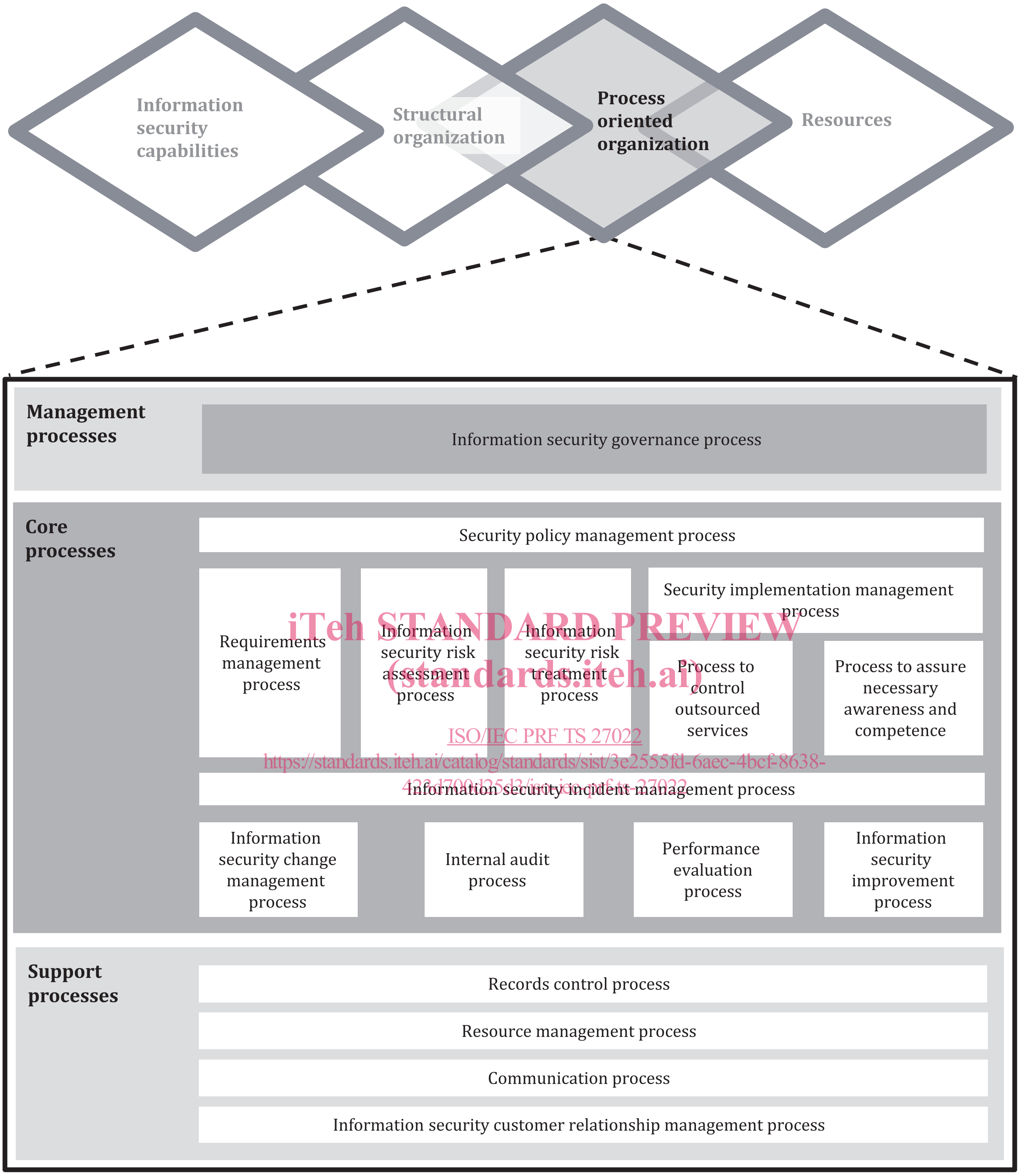
Information security capabilities
Structural organization
Process oriented organization
Resources
Management processes
Information security governance process
Core processes
Security policy management process
Requirements management process
Information security risk assessment process
Information security risk treatment process
Security implementation management process
Process to control outsourced services
Process to assure necessary awareness and competence
Information security incident management process
Information security change management process
Internal audit process
Performance evaluation process
Information security improvement process
Support processes
Records control process
Resource management process
Communication process
Information security customer relationship management process

Figure 1 — ISMS process reference model

The **information security governance/management interface process** should ensure an alignment of the ISMS with the objectives and needs of the overall organization and its stakeholders.

The **security policy management process** should be the process for the development, maintenance and retention of information security policies, standards, procedures and guidelines –referred to as “IS policies”.

Key to satisfying the ISMS objectives is an up-to-date understanding of the needs and expectations of interested parties relevant to information security and the ISMS. This should be realized within the **requirements management process**, which should identify legal, statutory, regulatory and contractual requirements for the risk assessment process, the internal audit process and the process to control outsourced processes.

In the **risk assessment process**, risks should be identified, analysed and evaluated. The results of this process should be documented and evaluated risks in a list of prioritized risks (list) and risk owners, which should be input for the communication process and the information security risk treatment process.

In the **information security risk treatment process**, risk treatment options should be identified and selected, and control objectives/controls should be determined necessary for the chosen risk treatment options. The results of this process should be lists with determined controls and control objectives, a risk treatment plan including acceptance of residual risks, a control implementation plan and requests for changes for the information security change management process, which are used as input in various ISMS processes.

The **security implementation management process** should be the process to initiate and verify the implementation of the risk treatment plan and necessary changes.

As services are outsourced, these services need to be determined and controlled, which should be realized within the **process to control outsourced services**.

Within the **information security awareness process**, an information security awareness, training and education program should be developed and implemented to ensure that all personnel receive the necessary security training and/or education.

The **information security incident management process** should be for detecting, reporting, assessing, responding to, dealing with and learning from information security incidents. The results of this process are identified incidents, which should be used in various ISMS processes including the information security change management process and the process to ensure necessary awareness and competence.

The implementation of controls always constitutes changes, which should be managed within a general change management process of the implementing organization or – if the change focuses on an ISMS element – within the **information security change management process**. The information security change management process is the process to control changes of ISMS elements and review the consequences of unintended changes. This process only focusses on change management of the ISMS. The results of this process should be necessary changes (for records control process), proposed and necessary changes as well as results of changes (for and from risk assessment process), initiation of risk assessment when significant changes are proposed or occur, and the results of changes to information security incident management process, as that process initiated them.

The **performance evaluation process** should contain monitoring, measurement, analysis and evaluation of two main criteria. First, the performance of the security controls and second the performance of the ISMS processes. Performance measurement differs from performance audit (within the **internal audit process** where effectiveness and efficiency of the ISMS and implemented controls are audited), which should be performed independently.

Results from the performance evaluation process, the internal audit process as well as results from the service provider audits from the process to control outsourced services should be used to improve effectiveness, efficiency, suitability and adequacy of the ISMS and the controls. This should be realized within the **information security improvement process.**

Within the **records control process** information determined to be necessary for the effectiveness and/or the demonstration/provision of documented evidence of the effectiveness of the ISMS should be identified, created, updated and controlled.

To implement the controls as well as to run the ISMS processes resources are needed which should be identified, allocated and monitored in the **resource management process**. Results of the resource management process should be planned/documented resources to implement and run determined controls, categorization of controls regarding who funds the control, planned and documented resources to run the ISMS core processes, reports regarding resource usage of ISMS core processes, and for the information security customer relationship management process: reports on resource usage.

Results of nearly all ISMS processes should be centrally communicated within the **communication process** to interested parties outside the ISMS. This should include the communication of risks and information security management reports. Those reports as well as identified requirements should serve as input for the information security governance/management interface process.

The information security governance/management interface process forms the interface between the ISMS and its interested parties. Beside this, the operational management of the customer satisfaction level as well as the continuous demonstration of the added value of investments in information security should be realized. This should be done within the **information security customer relationship management process.**

All processes have the potential to be designed and implemented as integrated processes within an IMS. Synergy effects resulting from the integration of processes into an IMS should be identified and realized wherever possible as suitable.

The processes are described in more detail in Clause 6 and Tables 1 to 17.

6 Management processes

6.1 General

This clause describes management processes of an ISMS. The concepts and purposes embodied in these example processes should be considered during the process planning phase of an ISMS implementation project.

6.2 Information security governance/management interface process

Table 1 — Process profile — Information security governance/management interface process

Process name	Information security governance/management interface process
Process category	Management process
Brief description	This process ensures that information security is managed in a way that meets the needs of the organization.
Objective/purposes	Objective of this process should be to ensure an alignment of the ISMS with the objectives and needs of the organization.
Input	— From requirements management process: Requirements for approval. — From communication process: Information security management reports containing: — former management reports; — status of actions from former management reports; — changes in requirements (external and internal issues as they are relevant for the ISMS); — audit reports (including feedback on the information security performance, including trends in nonconformities and corrective actions, monitoring and measurement results, audits results and fulfilment of information security objectives); — feedback from interested parties; — results of risk assessment and status of risk treatment plan; — opportunities for continual improvement; and — incident reports.
Results	— For requirements management process: — strategic objectives, goals, vision, restrictions, approved requirements; — list of interested parties of the ISMS; — risk criteria; — existing management systems; — approved requirements. — For records control process: Decisions related to the governance of the ISMS. — For information security change management: Change requests.
Activities/functions	— Initiate the ISMS. — Review reports (measurement, audit reports, results of risk assessment and status of risk treatment plan and feedback from interested parties). — Generate and provide feedback to top management, decisions and, if necessary, change requests.
References	— ISO/IEC 27001:2013, 5.1 and 9.3 — ISO/IEC 27003:2017, 8.4

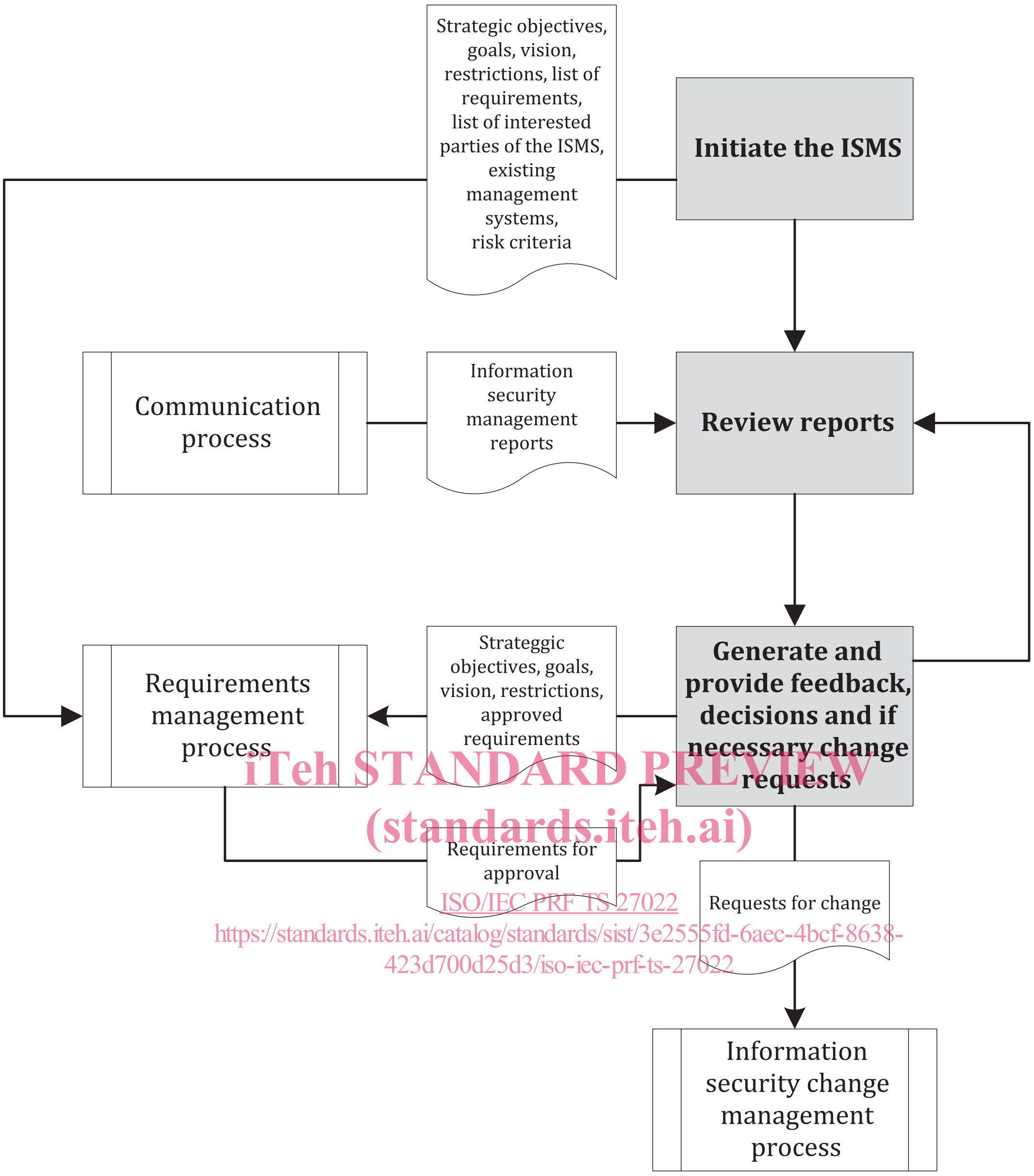
Strategic objectives, goals, vision, restrictions, list of requirements, list of interested parties of the ISMS, existing management systems, risk criteria
Initiate the ISMS
Communication process
Information security management reports
Review reports
Requirements management process
Strateggic objectives, goals, vision, restrictions, approved requirements
Generate and provide feedback, decisions and if necessary change requests
Requirements for approval
Requests for change
Information security change management process

Figure 2 — Process flow chart — Information security governance/management interface process

7 Core processes

7.1 General

This clause describes example core processes that can be found in an ISMS. The concepts and purposes embodied in these example processes should be considered during the process planning phase of an ISMS implementation project.

7.2 Security policy management process

Table 2 — Process profile — Security policy management process

Process name	Security policy management process
Process category	Core process
Brief description	The security policy management process should be the process to develop, maintain and retention of information security policies, standards, procedures and guidelines (referred to as “IS policies”).
Objective/purposes	Ensure that appropriate policies, standards, procedures and guidelines (IS policies) regarding information security are developed, maintained, available and understood by the target group.
Input	— From all other information security processes (as basis for policies): Results of the processes. — From change management process: Necessary changes of policies in form of change requests.
Results	— For communication process, internal audit process, performance evaluation process, records control process and the process to assure necessary awareness and competence: Appropriate IS policies.
Activities/functions	— Obtain input from ISMS processes and develop IS policies. — Obtain formal approval of IS policies. — Distribution of IS policies (via communication process). — Storage and preservation, including preservation of legibility. — Control of changes/version control. — Obtain replaced versions of IS policies. — Deletion or disposal of IS policies after retention period.
References	— ISO/IEC 27001:2013, 5.2, 7.4 and 7.5 — ISO/IEC 27003:2017, 5.2, 7.4, 7.5 and Annex A