TECHNICAL SPECIFICATION

ISO/IEC TS 33052

First edition
2016-06-15

Information technology — Process reference model (PRM) for information security management

Technologies de l'information — Modèle de référence des procédés pour le management de la sécurité de l'information

Reference number
ISO/IEC TS 33052:2016(E)

ISO copyright office
Ch. de Blandonnet 8 • CP 401
CH-1214 Vernier, Geneva, Switzerland
Tel. +41 22 749 01 11
Fax +41 22 749 09 47
copyright@iso.org
www.iso.org

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. In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1.

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).

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

For an explanation on the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the WTO principles in the Technical Barriers to Trade (TBT) see the following URL: Foreword - Supplementary information

The committee responsible for this document is ISO/IEC JTC 1, *Information technology*, Subcommittee SC 7, *Software and systems engineering*.

Introduction

The purpose of this Technical Specification is to facilitate the development of a process assessment model (PAM) described in ISO/IEC TS 33072.

ISO/IEC 33002 describes the requirements for the conduct of an assessment. ISO/IEC 33020 describes the measurement scale for assessing the process quality characteristic of process capability. ISO/IEC 33001 describes the concepts and terminology used for process assessment.

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

The PRM specified in this Technical Specification describes the processes including the information security management system (ISMS) processes implied by ISO/IEC 27001. Each process of this PRM is described in terms of a purpose and outcomes and provides traceability to requirements. The PRM does not attempt to place the processes in any specific environment nor does it pre-determine any level of process capability required to fulfil the ISO/IEC 27001 requirements. The PRM is not intended to be used for a conformity assessment audit or as a process implementation reference guide.

The relationships between ISO/IEC TR 24774, ISO/IEC 27001, ISO/IEC 33002, ISO/IEC 33004, ISO/IEC 33020, ISO/IEC TS 33052 and ISO/IEC TS 33072 are shown in Figure 1.

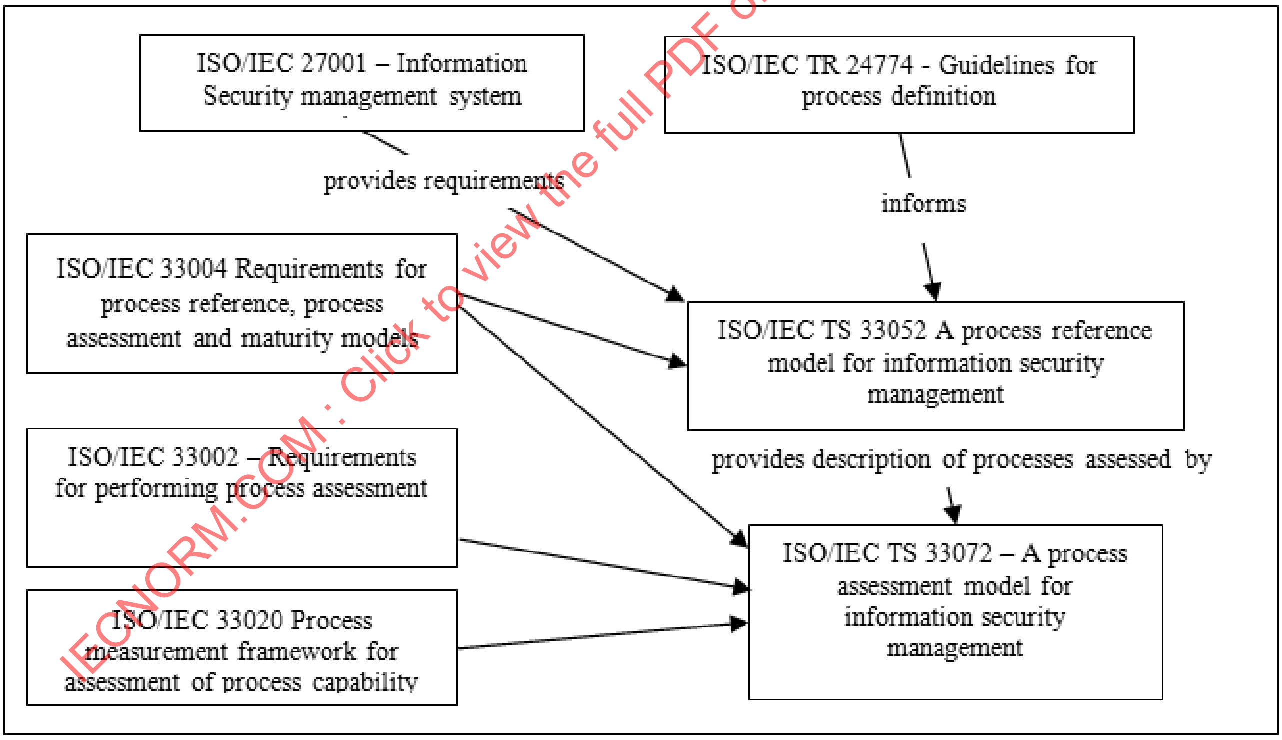

ISO/IEC 27001 – Information Security management system
ISO/IEC TR 24774 - Guidelines for process definition
provides requirements
informs
ISO/IEC 33004 Requirements for process reference, process assessment and maturity models
ISO/IEC TS 33052 A process reference model for information security management
provides description of processes assessed by
ISO/IEC 33002 – Requirements for performing process assessment
ISO/IEC TS 33072 – A process assessment model for information security management
ISO/IEC 33020 Process measurement framework for assessment of process capability

Figure 1 — Relationships between relevant standards

Any organization may define processes with additional elements in order to suit it to its specific environment and circumstances. Some processes cover general management aspects of an organization. These processes have been identified in order to give coverage to the requirements of ISO/IEC 27001.

The PRM does not provide the evidence required by ISO/IEC 27001. The PRM does not specify the interfaces between the processes.

This Technical Specification describes a PRM for information security management with descriptions of processes in Clause 5. Annex A provides the statement of conformity in accordance with ISO/IEC 33002.

Information technology — Process reference model (PRM) for information security management

1 Scope

This Technical Specification defines a process reference model (PRM) for the domain of information security management. 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 outcomes.

2 Normative references

The following documents, in whole or in part, are normatively referenced in this document and are indispensable for its application. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO/IEC 27001:2013, *Information technology — Security techniques — Information security management systems — Requirements*

ISO/IEC 33001, *Information technology — Process assessment — Concepts and terminology*

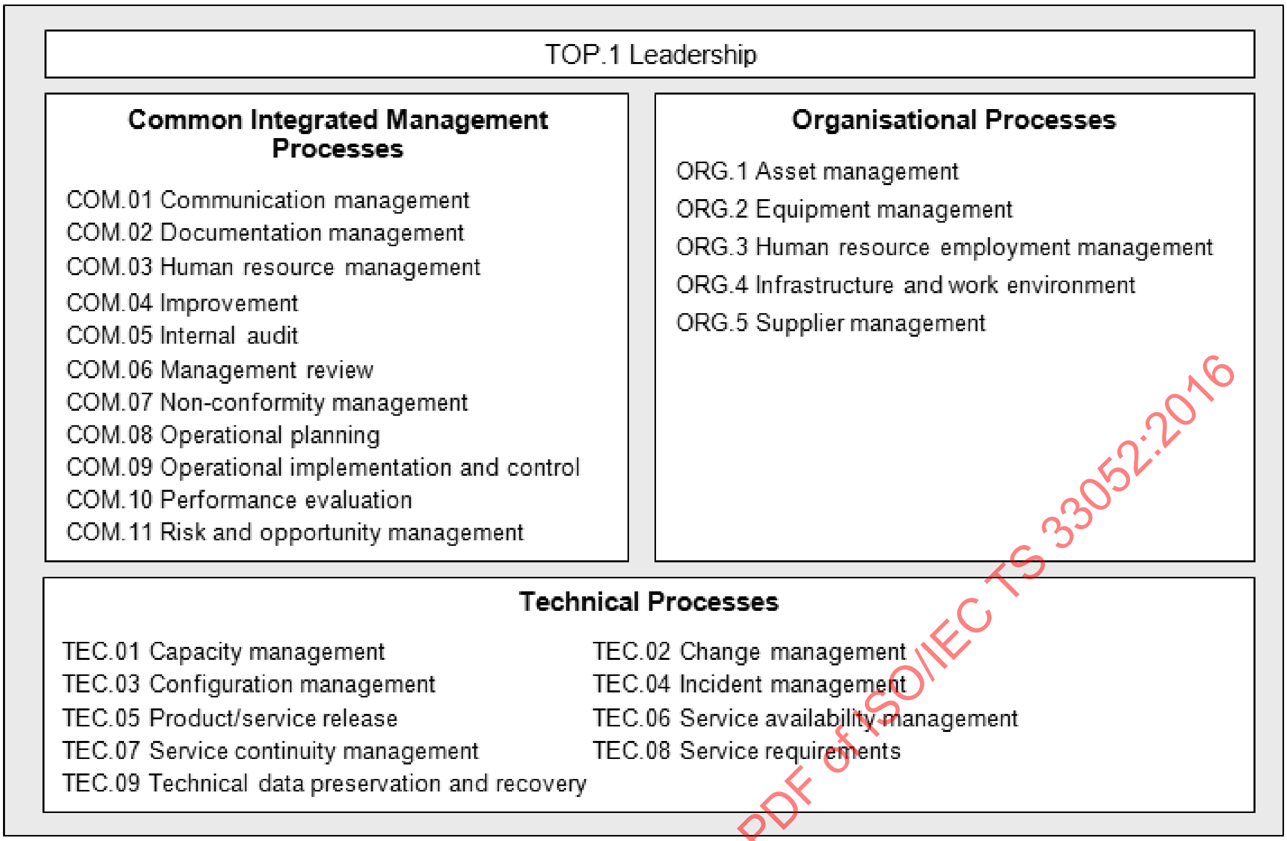
3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 27001 and ISO/IEC 33001 apply.

4 Overview of the PRM

This Clause describes the structure of a process reference model to support information security management. The process reference model includes processes, which can already exist in the context of a management system of a service provider.

Figure 2 identifies the processes derived from ISO/IEC 27001 requirements.



TOP.1 Leadership

Common Integrated Management Processes

COM.01 Communication management
COM.02 Documentation management
COM.03 Human resource management
COM.04 Improvement
COM.05 Internal audit
COM.06 Management review
COM.07 Non-conformity management
COM.08 Operational planning
COM.09 Operational implementation and control
COM.10 Performance evaluation
COM.11 Risk and opportunity management

Organisational Processes

ORG.1 Asset management
ORG.2 Equipment management
ORG.3 Human resource employment management
ORG.4 Infrastructure and work environment
ORG.5 Supplier management

Technical Processes

TEC.01 Capacity management
TEC.02 Change management
TEC.03 Configuration management
TEC.04 Incident management
TEC.05 Product/service release
TEC.06 Service availability management
TEC.07 Service continuity management
TEC.08 Service requirements
TEC.09 Technical data preservation and recovery

Figure 2 — Processes in the process reference model

5 Process descriptions

5.1 Introduction

Each process in the PRM has the following descriptive elements:

a) Process ID: Each process belonging to a Group is identified with a Process Identifier [ID] consisting of the Group abbreviated name and a sequential number of the process in that Group.

b) Name: The name of a process is a short phrase that summarizes the scope of the process, identifying the principal concern of the process, and distinguishes it from other processes within the scope of the process reference model.

c) Context: For each process, a brief overview describes the intended context of the application of the process.

d) Purpose: The purpose of the process is a high-level, overall goal for performing the process.

e) Outcomes: An outcome is an observable result of the successful achievement of the process purpose. Outcomes are measurable, tangible, technical or business results that are achieved by a process. Outcomes are observable and assessable.

f) Requirements traceability: The outcomes are based on the requirements of ISO/IEC 27001. The references identify the applicable subclauses of ISO/IEC 27001, the subclause heading, and the outcomes that are supported.

In 5.2 to 5.27, all entries in the requirements traceability row end with numbers in square brackets, (i.e. [n]). Each number in the square brackets is a reference to a numbered outcome. These outcomes are directly linked to the requirements of ISO/IEC 27001.

Some outcomes are shown in square brackets. These are only indirectly linked to requirements of ISO/IEC 27001. The outcomes in square brackets are not referenced by any of the entries in the requirements traceability row. These additional outcomes have been included because they are considered necessary in order for this type of PRM to serve as the basis of the PAM (ISO/IEC TS 33072). With these additional outcomes, the process is complete and the process purpose can be achieved.

5.2 ORG.1 Asset management

Process ID	ORG.1
Name	Asset management
Purpose	The purpose of Asset Management is to establish and maintain the integrity of all identified product assets.
Context	This process is concerned with establishing and maintaining the identity of the products and their configuration information to enable effective control of the products. The scope of assets may include physical assets (e.g. infrastructure, hardware, software) and intangible assets (e.g. intellectual property).
Outcomes	As a result of successful implementation of this process: 1. Items requiring asset management are identified. 2. Asset items are classified. 3. Assets are inventoried. 4. [The status of assets is identified.] 5. Changes to assets under management are controlled.
Requirements traceability	27001 2ED A.08.1.1 Inventory of assets [1,3,5] 27001 2ED A.08.2.1 Classification of information [2] 27001 2ED A.08.3.2 Disposal of media [5] 27001 2ED A.08.3.3 Physical media transfer [5]

5.3 TEC.01 Capacity management

Process ID	TEC.01
Name	Capacity management
Purpose	The purpose of Capacity Management is to ensure that the organization has the capacity to meet current and future system performance requirements.
Context	This process ensures that there are sufficient resources and capacity to meet current and future agreed requirements in a cost-effective and timely manner. The process enables a service provider to provide sufficient resources across an entire service in order to deliver the agreed service performance and meet the service-level targets.
Outcomes	As a result of successful implementation of this process: 1. [Current and future capacity and performance requirements are identified.] 2. [Capacity is provided to meet current capacity and performance requirements.] 3. Capacity usage is monitored, analysed and performance is tuned. 4. [Capacity is prepared to meet future capacity and performance needs.]
Requirements traceability	27001 2ED A.12.1.3 Capacity management [3]

5.4 TEC.02 Change management

Process ID	TEC.02
Name	Change management
Purpose	The purpose of Change Management is to provide the focus for all activities associated with changes associated with product, services, processes and systems used to produce a product or deliver a service.
Context	Changes to products, services and systems, their applications and infrastructure, are planned and controlled to ensure timeliness without unnecessary disruption.
Outcomes	As a result of successful implementation of this process: 1. [Change requests are classified.] 2. Change requests are analysed and assessed using defined criteria. 3. [Changes are approved or rejected using defined criteria.] 4. [Changes are implemented, as appropriate.]
Requirements traceability	27001 2ED A.15.2.2 Managing changes to supplier services [2]

5.5 COM.01 Communication management

Process ID	COM.01	
Name	Communication management	
Purpose	The purpose of Communication Management is to produce timely and accurate information products to support effective communication and decision making.	
Context	This process represents the focus for all communication activities associated with the management system processes.	
Outcomes	As a result of successful implementation of this process: 1. Information content is defined in terms of identified communication needs and requirements. 2. Parties to communicate with are identified. 3. The party responsible for the communication is identified. 4. Events that require communication actions are identified. 5. The channel for the communication is selected. 6. Information products are communicated to interested parties.	
Requirements traceability	27001 2ED 05.1	Leadership and commitment [6]
	27001 2ED 05.2	Policy [6]
	27001 2ED 05.3	Organizational roles, responsibilities and authorities [6]
	27001 2ED 06.2	Information security objectives and plans to achieve them [6]
	27001 2ED 07.4	Communication [1 to 5]
	27001 2ED 09.2	Internal audit [6]
	27001 2ED A.05.1.1	Policies for information security [6]
	27001 2ED A.06.1.3	Contact with authorities[2]
	27001 2ED A.06.1.4	Contact with special interest groups [2]
	27001 2ED A.07.2.3	Disciplinary process [6]
	27001 2ED A.07.3.1	Termination or change of employment responsibilities [6]

5.6 TEC.03 Configuration management

Process ID	TEC.03
Name	Configuration management
Purpose	The purpose of Configuration Management is to identify, control, record, track, report and verify all identified product/service components.
Context	This process is concerned with establishing and maintaining the integrity of product/service components to enable effective control of the products/services.
Outcomes	As a result of successful implementation of this process: 1. [Items requiring configuration management are identified.] 2. [The status of configuration items and modifications is identified.] 3. Changes to items under configuration management are controlled. 4. [The integrity of systems, products/services and product/service components is assured.] 5. [The configuration of released items is controlled.]
Requirements traceability	27001 2ED A.14.2.4 Restrictions on changes to software packages [3] 27001 2ED A.14.3.1 Protection of test data [3]

5.7 COM.02 Documentation management

Process ID	COM.02
Name	Documentation management
Purpose	The purpose of Document Management is to provide relevant, timely, complete, valid and, if required, confidential documented information to designated parties.
Context	This process consists of ensuring that the required documented information (e.g. procedures, instructions and templates) is available to designated parties for achieving the information security objectives.
Outcomes	As a result of successful implementation of this process: 1. Documented information to be managed is identified. 2. The forms of documented information representation are defined. 3. The documented information content status is known. 4. Documented information is current, complete and valid. 5. Documented information is released according to defined criteria. 6. Documented information is available to designated parties. 7. Documented information is archived, or disposed of, as required.

Requirements traceability	27001 2ED 04.3	Determining the scope of the information security management system [1]
	27001 2ED 05.2	Policy [1,6]
	27001 2ED 06.1.2	Information security risk assessment [1]
	27001 2ED 06.1.3	Information security risk treatment [1,5]
	27001 2ED 06.2	Information security objectives and plans to achieve them [1,3]
	27001 2ED 07.2	Competence [1]
	27001 2ED 07.5.2	Creating and updating [2,5]
	27001 2ED 07.5.3	Control of documented information [2-4,6,7]
	27001 2ED 08.1	Operational planning and control [7]
	27001 2ED 08.2	Information security risk assessment [1]
	27001 2ED 08.3	Information security risk treatment [1]
	27001 2ED 09.1	Monitoring, measurement, analysis and evaluation [1]
	27001 2ED 09.2	Internal audit [1]
	27001 2ED 09.3	Management review [1]
	27001 2ED 10.1	Nonconformity and corrective action [1]
	27001 2ED A.05.1.1	Policies for information security [5,6]
	27001 2ED A.08.1.3	Acceptable use of assets [1]
	27001 2ED A.09.1.1	Access control policy [1]
	27001 2ED A.12.1.1	Documented operating procedures [1,6]
	27001 2ED A.12.4.1	Event logging [1]
	27001 2ED A.13.2.4	Confidentiality or nondisclosure agreements [1]
	27001 2ED A.14.2.5	Secure system engineering principles [1,3]
	27001 2ED A.15.1.1	Information security policy for supplier relationships [1,5]
	27001 2ED A.16.1.5	Response to information security incidents [1]
	27001 2ED A.16.1.7	Collection of evidence [1]
	27001 2ED A.17.1.2	Implementing information security continuity [1,3]
	27001 2ED A.18.1.1.01	Applicable statutory and regulatory requirements [1,3]
	27001 2ED A.18.1.1.02	Applicable contractual requirements [1,3]
	27001 2ED A.18.1.3	Protection of records [4]

5.8 ORG.2 Equipment management

Process ID	ORG.2
Name	Equipment management
Purpose	The purpose of Equipment Management is to ensure integrity of the performance and behaviour of equipment and associated software.

Context	This process is concerned with actions to be taken to protect equipment from changes to settings (i.e. calibration) or changes in environment that might invalidate those settings.
Outcomes	As a result of successful implementation of this process: 1. Equipment is sited to minimize risk of environmental or other damage. 2. Continuity in the provision of utilities and services to equipment is assured. 3. Equipment is maintained to ensure its continued availability and integrity. 4. Equipment used offsite is managed to ensure integrity of operation. 5. The integrity of information is assured when equipment is withdrawn from service. 6. Equipment relocation is controlled.
Requirements traceability	27001 2ED A.11.2.1 Equipment siting and protection [1] 27001 2ED A.11.2.2 Supporting utilities [2] 27001 2ED A.11.2.3 Cabling security [1] 27001 2ED A.11.2.4 Equipment maintenance [3] 27001 2ED A.11.2.5 Removal of assets [6] 27001 2ED A.11.2.6 Security of equipment and assets off-premises [4] 27001 2ED A.11.2.7 Secure disposal or re-use of equipment [5] 27001 2ED A.13.1.1 Network controls [3]

5.9 ORG.3 Human resource employment management

Process ID	ORG.3
Name	Human resource employment management
Purpose	The purpose of Human Resource Employment Management is to prevent threats to information security by employees, before hiring, during employment and after termination of employment.
Context	This process addresses security precautions related to employment of individuals. These precautions refer to actions prior to employment, when employment is in progress, and once employment is terminated.

Outcomes	As a result of successful implementation of this process: 1. Roles and responsibilities of employees, contractors and third-party users are defined. 2. Prospective employees are screened in accordance with relevant laws, regulations and ethics, and in proportional to the business requirements and the perceived risks. 3. Prospective employees agree to the terms and conditions of their employment contract. 4. The terms and conditions of employment are applied. 5. [Employees are equipped to apply relevant organizational policies and procedures as relevant for their job function.] 6. Disciplinary measures are applied to employees that have committed a breach of the agreed conditions of employment. 7. Responsibilities for performing employment termination or change of employment are defined and assigned. 8. Employees return all of the organization's assets in their possession upon termination of employment. 9. Employee access to information resources is removed upon termination of their employment.
Requirements traceability	27001 2ED A.07.1.1 Screening [2] 27001 2ED A.07.1.2 Terms and conditions of employment [1,3] 27001 2ED A.07.2.1 Management responsibilities [4] 27001 2ED A.07.2.3 Disciplinary process [6] 27001 2ED A.07.3.1 Termination or change of employment responsibilities [7] 27001 2ED A.08.1.4 Return of assets [8] 27001 2ED A.09.2.6 Removal or adjustment of access rights [9] 27001 2ED A.09.3.1 Use of secret authentication information [3]

5.10 COM.03 Human resource management

Process ID	COM.03
Name	Human resource management
Purpose	The purpose of Human Resource Management is to provide the organization with necessary competent human resources and to improve their competencies in alignment with business needs.
Context	This process consists of identifying and developing the competence of individuals in relation to their activities and the process needs of the organization.
Outcomes	As a result of successful implementation of this process: 1. The competencies required by the organization to produce products and services are identified. 2. Identified competency gaps are filled through training or recruitment. 3. Understanding of role and activities in achieving organizational objectives in product and service provision is demonstrated by each individual.
Requirements traceability	27001 2ED 07.2 Competence [1 to 3] 27001 2ED 07.3 Awareness [3] 27001 2ED A.07.2.2 Information security awareness, education and training [3]

5.11 COM.04 Improvement

Process ID	COM.04
Name	Improvement
Purpose	The purpose of Improvement is to continually improve the management system, its processes and products.
Context	This process enables an organization to improve the management system, its processes and products and services. It includes the identification, evaluation, approval, prioritization, management, measurement and review of improvements.
Outcomes	As a result of successful implementation of this process: 1. Opportunities for improvement are identified. 2. [Opportunities for improvement are evaluated against defined criteria.] 3. [Improvements are prioritised.] 4. [Improvements are implemented.] 5. [The effectiveness of implemented improvements is evaluated.]
Requirements traceability	27001 2ED 09.3 Management review [1]

5.12 TEC.04 Incident management

Process ID	TEC.04
Name	Incident management
Purpose	The purpose of Incident Management is to identify and resolve information security events and incidents within agreed service levels.
Context	The objective of incident management is to restore the service within agreed service levels. The focus is on reducing the duration and consequences of the service outage from a business and customer perspective and not on finding the root cause of the incident.
Outcomes	As a result of successful implementation of this process: 1. Incidents are identified. 2. Incidents are classified, prioritised and analysed. 3. Incidents are resolved and closed. 4. [Incidents are reported and escalated according to agreed service levels.]
Requirements traceability	27001 2ED A.16.1.2 Reporting information security events [1] 27001 2ED A.16.1.3 Reporting information security weaknesses [1] 27001 2ED A.16.1.4 Assessment of and decision on information security events [2] 27001 2ED A.16.1.5 Response to information security incidents [3]

5.13 ORG.4 Infrastructure and work environment

Process ID	ORG.4
Name	Infrastructure and work environment
Purpose	The purpose of Infrastructure and Work Environment is to provide the enabling infrastructure and services to projects to support organization and project objectives throughout the life cycle.

Context	The infrastructure refers to those physical elements associated with physical plant within which individuals can be accommodated. The work environment refers to the arrangements within the infrastructure that facilitate and promote effective human interactions and activities.
Outcomes	As a result of successful implementation of this process: 1. The requirements for infrastructure and work environment to support processes are defined. 2. Access rights to the information resource are defined. 3. [The infrastructure and work environment elements are identified and specified.] 4. [The infrastructure and work environment elements are acquired and commissioned.] 5. The infrastructure and work environment is controlled and maintained. 6. Access to the information resource is controlled. 7. The information resource is protected from abuse.
Requirements traceability	27001 2ED A.09.1.2 Access to networks and network services [6] 27001 2ED A.09.2.3 Management of privileged access rights [6] 27001 2ED A.09.2.5 Review of user access rights [6] 27001 2ED A.09.4.1 Information access restriction [2] 27001 2ED A.09.4.2 Secure log-on procedures [6] 27001 2ED A.09.4.3 Password management system [6] 27001 2ED A.09.4.4 Use of privileged utility programs [7] 27001 2ED A.09.4.5 Access control to program source code [6] 27001 2ED A.11.1.1 Physical security perimeter [1,5] 27001 2ED A.11.1.2 Physical entry controls [1] 27001 2ED A.11.1.3 Securing offices, rooms and facilities [1,5] 27001 2ED A.11.1.4 Protecting against external and environmental threats [1,5] 27001 2ED A.11.1.6 Delivery and loading areas [5] 27001 2ED A.11.2.8 Unattended user equipment [5] 27001 2ED A.12.1.4 Separation of development, testing and operational environments [2]

	27001 2ED A.12.4.1	Event logging [7]
	27001 2ED A.12.4.2	Protection of log information [7]
	27001 2ED A.12.4.3	Administrator and operator logs [6]
	27001 2ED A.12.4.4	Clock synchronisation [1]
	27001 2ED A.12.6.1	Management of technical vulnerabilities [7]
	27001 2ED A.13.1.2	Security of network services [1]
	27001 2ED A.13.1.3	Segregation in networks [2]
	27001 2ED A.13.2.3	Electronic messaging [7]
	27001 2ED A.14.1.3	Protecting application services transactions [7]
	27001 2ED A.14.2.6	Secure development environment [1]
	27001 2ED A.18.1.4	Privacy and protection of personally identifiable information [7]
	27001 2ED A.18.1.5	Regulation of cryptographic controls [7]

5.14 COM.05 Internal audit

Process ID	COM.05	
Name	Internal audit	
Purpose	The purpose of Internal Audit is to independently determine conformity of the management system, services, and processes to the requirements, policies, plans and agreements, as appropriate.	
Context	This process consists of conducting audits to independently determine whether the management system and business processes conform to the requirements established by the organization.	
Outcomes	As a result of successful implementation of this process: 1. The scope and purpose of each audit are defined. 2. The objectivity and impartiality of the conduct of audits and selection of auditors are assured. 3. Conformity of selected services, products and processes with requirements, plans and agreements is determined.	
Requirements traceability	27001 2ED 09.2	Internal audit [1 to 3]
	27001 2ED A.15.2.1	Monitoring and review of supplier services [3]
	27001 2ED A.18.2.1	Independent review of information security [3]
	27001 2ED A.18.2.2	Compliance with security policies and standards [3]
	27001 2ED A.18.2.3	Technical compliance review [1]

5.15 TOP.1 Leadership

Process ID	TOP.1
Name	Leadership
Purpose	The purpose of Leadership is to direct the organization in the achievement of its vision, mission, strategy and goals, through the definition and implementation of a management system, a management system policy, and management system objectives.

Context	This process consists in defining the scope of the management system as well as the policy and objectives.
Outcomes	As a result of successful implementation of this process: 1. The context of the organization, including the expectations of its interested parties, is understood and analysed. 2. The scope of management system activities is defined, taking the context of the organization into consideration. 3. The management system policy and objectives are defined. 4. The management system and operational process strategy are determined. 5. Commitment and leadership with respect to the management system are demonstrated.
Requirements traceability	27001 2ED 04.1 Understanding the organization and its context [1] 27001 2ED 04.2 Understanding the needs and expectations of interested parties [1] 27001 2ED 04.3 Determining the scope of the information security management system [2] 27001 2ED 04.4 Information security management system [4] 27001 2ED 05.1 Leadership and commitment [5] 27001 2ED 05.2 Policy [3] 27001 2ED 06.2 Information security objectives and plans to achieve them [3] 27001 2ED 07.5.1 General [4] 27001 2ED 07.5.3 Control of documented information [4] 27001 2ED 08.1 Operational planning and control [4] 27001 2ED 10.2 Continual improvement [4] 27001 2ED A.05.1.1 Policies for information security [3]

5.16 COM.06 Management review

Process ID	COM.06
Name	Management review
Purpose	The purpose of Management Review is to assess the performance of the management system and to identify and make decisions regarding potential improvements.
Context	This process checks the management system at planned intervals to ensure its continuing suitability, adequacy and effectiveness. A review may include any undertaking, ranging in scope from a complete organization down to a single process and its outcomes and product delivered. It takes into account the results of audits, the performance of the processes conformance to product requirements, services, reports, incidents, known errors, risks, suggestions and feedback from interested parties.
Outcomes	As a result of successful implementation of this process: 1. The objectives of the review are established. 2. The status and performance of an activity or process are assessed in terms of the established objectives. 3. Risks, problems and opportunities for improvement are identified.
Requirements traceability	27001 2ED 09.3 Management review [1 to 3]

5.17 COM.07 Non-conformity management

Process ID	COM.07
Name	Non-conformity management
Purpose	The purpose of the Non-conformity Management process is to resolve non-conformities and to eliminate their causes when appropriate.
Context	This process establishes that where a non-conformity occurs, a review may indicate that only correction is required. Alternatively, the causes of the non-conformity are investigated, with a view to removing the possibility the non-conformity re-occurring.
Outcomes	As a result of successful implementation of this process: 1. Non-conformities are identified. 2. Non-conformities are resolved and closed. 3. The cause(s) of selected non-conformities is determined. 4. The need for action to eliminate the causes of non-conformities is evaluated. 5. A selected action proposal is implemented. 6. The effectiveness of changes to eliminate the non-conformities is confirmed.
Requirements traceability	27001 2ED 10.1 Non-conformity and corrective action [1-5,6]

5.18 COM.09 Operational implementation and control

Process ID	COM.09
Name	Operational implementation and control
Purpose	The purpose of the Process Implementation and Control process is to deploy and control the execution and performance of operational and organizational processes.
Context	This process consists in supporting the efficient, timely and quality day-to-day operations by optimizing resource allocation, and by directing execution of operating policies to support overall company policies and objectives.
Outcomes	As a result of successful implementation of this process: 1. The required roles, responsibilities and authorities are allocated. 2. The required resources are allocated and applied. 3. Actions required to achieve the management system objectives are implemented. 4. Suitability and effectiveness of the actions taken to achieve the management system objectives are reviewed. 5. Deviations from planned arrangements are corrected when targets are not achieved. 6. [Data is collected and analysed as a basis for understanding the behaviour of and to demonstrate the suitability and effectiveness of the processes.]

Requirements traceability	27001 2ED 05.3	Organizational roles, responsibilities and authorities [1]
	27001 2ED 06.1.2	Information security risk assessment [3,4]
	27001 2ED 06.1.3	Information security risk treatment [3]
	27001 2ED 07.1	Resources [2]
	27001 2ED 07.2	Competence [4]
	27001 2ED 08.1	Operational planning and control [3-5]
	27001 2ED 09.2	Internal audit [3,4]
	27001 2ED A.05.1.2	Review of the policies for information security [4]
	27001 2ED A.06.1.1	Information security roles and responsibilities [1]
	27001 2ED A.06.2.1	Mobile device policy [3]
	27001 2ED A.06.2.2	Teleworking [3]
	27001 2ED A.08.1.3	Acceptable use of assets [3]
	27001 2ED A.08.2.2	Labelling of information [3]
	27001 2ED A.08.2.3	Handling of assets [3]
	27001 2ED A.08.3.1	Management of removable media [3]
	27001 2ED A.09.1.1	Access control policy [4]
	27001 2ED A.09.2.1	User registration and deregistration [3]
	27001 2ED A.09.2.2	User access provisioning [3]
	27001 2ED A.09.2.4	Management of secret authentication information of users [3]
	27001 2ED A.10.1.1	Policy on the use of cryptographic controls [3]
	27001 2ED A.10.1.2	Key management [3]
	27001 2ED A.11.1.5	Working in secure areas [3]
	27001 2ED A.11.2.9	Clear desk and clear screen policy [3]
	27001 2ED A.12.1.2	Change management [4,5]
	27001 2ED A.12.2.1	Controls against malware [3]
	27001 2ED A.12.4.1	Event logging [4]
	27001 2ED A.12.4.3	Administrator and operator logs [4]
	27001 2ED A.12.5.1	Installation of software on operational systems [3]
	27001 2ED A.12.6.2	Restrictions on software installation [3]
	27001 2ED A.12.7.1	Information systems audit controls [4]
	27001 2ED A.13.2.4	Confidentiality or nondisclosure agreements [4]

	27001 2ED A.14.2.3	Technical review of applications after operating platform changes [4]
	27001 2ED A.14.2.7	Outsourced development [4]
	27001 2ED A.15.2.1	Monitoring and review of supplier services [4]
	27001 2ED A.16.1.7	Collection of evidence [3]
	27001 2ED A.17.1.2	Implementing information security continuity [3]
	27001 2ED A.17.1.3	Verify, review and evaluate information security continuity [4]
	27001 2ED A.17.2.1	Availability of information processing facilities [3]
	27001 2ED A.18.1.2	Intellectual property rights [3]
	27001 2ED A.18.2.1	Independent review of information security [4]
	27001 2ED A.18.2.2	Compliance with security policies and standards [4]
	27001 2ED A.18.2.3	Technical compliance review [4]

5.19 COM.08 Operational planning

Process ID	COM.08
Name	Operational planning
Purpose	The purpose of Operational Planning is to define the characteristics of all operational and organizational processes and to plan their execution.
Context	The scope of this process includes the creation of all policies, procedures, process descriptions, and plans required by the organizational and operational processes of the organization. Roles and responsibilities associated with the oversight of business processes are also identified. Resource needs are identified. The methods for monitoring process effectiveness are described.
Outcomes	As a result of successful implementation of this process: 1. Process needs and requirements are identified. 2. [Process input and output products are determined.] 3. The set of activities that transform the inputs into outputs is determined. 4. [The sequence and interaction of the process with other processes are determined.] 5. The required competencies and roles for performing the process are identified. 6. The required resources for performing the process are identified. 7. Methods for monitoring the effectiveness and suitability of the process are determined. 8. Plans for the deployment of the process are developed.

Requirements traceability	27001 2ED 05.3	Organizational roles, responsibilities and authorities [5]
	27001 2ED 06.1.1	General [1,8]
	27001 2ED 06.1.2	Information security risk assessment [1]
	27001 2ED 06.1.3	Information security risk treatment [1]
	27001 2ED 06.2	Information security objectives and plans to achieve them [1,5,6,7,8]
	27001 2ED 07.1	Resources [6]
	27001 2ED 07.2	Competence[5]
	27001 2ED 08.2	Information security risk assessment [8]
	27001 2ED 09.1	Monitoring, measurement, analysis and evaluation [5,8]
	27001 2ED 09.2	Internal audit [8]
	27001 2ED 09.3	Management review [8]
	27001 2ED A.05.1.2	Review of the policies for information security [8]
	27001 2ED A.06.1.1	Information security roles and responsibilities [5]
	27001 2ED A.06.1.2	Segregation of duties [5]
	27001 2ED A.06.1.5	Information security in project management [1]
	27001 2ED A.06.2.1	Mobile device policy [1]
	27001 2ED A.06.2.2	Teleworking [1,3]
	27001 2ED A.08.1.2	Ownership of assets [5]
	27001 2ED A.08.1.3	Acceptable use of assets [1]
	27001 2ED A.08.2.2	Labelling of information [3]
	27001 2ED A.08.2.3	Handling of assets [3]
	27001 2ED A.08.3.1	Management of removable media [3]
	27001 2ED A.08.3.2	Disposal of media[3]
	27001 2ED A.09.1.1	Access control policy [1]
	27001 2ED A.09.2.1	User registration and deregistration [1]
	27001 2ED A.09.2.4	Management of secret authentication information of users [1]
	27001 2ED A.09.2.5	Review of user access rights [8]
	27001 2ED A.10.1.1	Policy on the use of cryptographic controls [1]
	27001 2ED A.10.1.2	Key management [1]
	27001 2ED A.11.1.5	Working in secure areas [3]
	27001 2ED A.11.2.9	Clear desk and clear screen policy [1]

	27001 2ED A.12.1.1	Documented operating procedures [3]
	27001 2ED A.12.3.1	Information backup [1,8]
	27001 2ED A.12.5.1	Installation of software on operational systems [3]
	27001 2ED A.12.6.2	Restrictions on software installation [1]
	27001 2ED A.12.7.1	Information systems audit controls [8]
	27001 2ED A.13.2.1	Information transfer policies and procedures [1,3]
	27001 2ED A.13.2.4	Confidentiality or nondisclosure agreements [1]
	27001 2ED A.14.2.1	Secure development policy [1]
	27001 2ED A.14.2.2	System change control procedures [1]
	27001 2ED A.14.2.5	Secure system engineering principles [1]
	27001 2ED A.14.2.8	System security testing [1]
	27001 2ED A.15.1.1	Information security policy for supplier relationships [1]
	27001 2ED A.15.2.1	Monitoring and review of supplier services [8]
	27001 2ED A.16.1.1	Responsibilities and procedures [3,5]
	27001 2ED A.16.1.5	Response to information security incidents [3]
	27001 2ED A.16.1.7	Collection of evidence [3]
	27001 2ED A.17.1.2	Implementing information security continuity [1]
	27001 2ED A.17.1.3	Verify, review and evaluate information security continuity [8]
	27001 2ED A.18.1.2	Intellectual property rights [3]
	27001 2ED A.18.2.1	Independent review of information security [8]
	27001 2ED A.18.2.2	Compliance with security policies and standards [8]
	27001 2ED A.18.2.3	Technical compliance review [8]

5.20 COM.10 Performance evaluation

Process ID	COM.10
Name	Performance evaluation
Purpose	The purpose of Performance Evaluation is to collect and analyse data that will be used to evaluate the performance of the management system and the business processes in terms of the defined objectives.

Context	This process consists of monitoring the achievement of the information security objectives as well as the execution and performance of operational and organizational processes.
Outcomes	As a result of successful implementation of this process: 1. Performance monitoring and measurement needs are defined. 2. [Performance measures, derived from the performance measurement needs, are identified.] 3. Performance measurement methods, supportive of the performance measures, are identified. 4. [Data is collected using the identified performance measurement methods.] 5. The collected performance data is analysed.
Requirements traceability	27001 2ED 06.2 Information security objectives and plans to achieve them [1] 27001 2ED 09.1 Monitoring, measurement, analysis and evaluation [1,3,5] 27001 2ED A.16.1.6 Learning from information security incidents [5]

5.21 TEC.05 Product/service release

Process ID	TEC.05
Name	Product/service release
Purpose	The purpose of Product/service Release is to control the availability of a product/service to the intended customer.
Context	This process is responsible for creation of release packages, i.e. the assembly of product/service and associated components with deployment in mind.
Outcomes	As a result of successful implementation of this process: 1. [The contents of the release are determined.] 2. [Release and acceptance criteria are determined.] 3. [The release is assembled from the product/service/system elements.] 4. [Tests are defined for the release.] 5. The release is tested in accordance with defined criteria. 6. [Products/services/systems are released to the intended customer according to defined criteria.]
Requirements traceability	27001 2ED A.14.2.3 Technical review of applications after operating platform changes [5]

5.22 TEC.08 Product/Service/System requirements

Process ID	TEC.08
Name	Product/Service/System requirements
Purpose	The purpose of Product/Service/System Requirements is to establish and agree to the requirements for products/services and systems.

Context	This process gathers requirements for products, services and systems. The product/service/system may originate from within the service provider (build from catalogue), or requests from one or more clients (build to order). The requirements may relate to a new product/service/system or changes to existing products/services/systems.
Outcomes	As a result of successful implementation of this process: 1. [The required characteristics and context of use of products/services/systems are identified.] 2. [The constraints for a product/service/system solution are defined.] 3. The requirements for the product/service/system are defined. 4. The requirements for validating the product/service/system are defined.
Requirements traceability	27001 2ED A.14.1.1 Information security requirements analysis and specification [3] 27001 2ED A.14.1.2 Securing application services on public networks [3] 27001 2ED A.14.2.3 Technical review of applications after operating platform changes [3] 27001 2ED A.14.2.9 System acceptance testing [4] 27001 2ED A.18.1.1.01 Applicable statutory and regulatory requirements [3] 27001 2ED A.18.1.1.02 Applicable contractual requirements [3]

5.23 COM.11 Risk and opportunity management

Process ID	COM.11
Name	Risk and opportunity management
Purpose	The purpose of Risk and Opportunity Management is to identify, analyse, evaluate, treat and monitor risks.
Context	This process consists of continually identifying, evaluating and reacting to the risks and opportunities encountered by the organization.
Outcomes	As a result of successful implementation of this process: 1. Risks are identified. 2. Identified risks are analysed. 3. Risks are evaluated against defined criteria. 4. Risks are selected for treatment. 5. Selected risks are treated.
Requirements traceability	27001 2ED 06.1.1 General [1] 27001 2ED 06.1.2 Information security risk assessment [1 to 3] 27001 2ED 06.1.3 Information security risk treatment [4] 27001 2ED 08.2 Information security risk assessment [1] 27001 2ED 08.3 Information security risk treatment [5]

5.24 TEC.06 Service availability management

Process ID	TEC.06
Name	Service availability management
Purpose	The purpose of the Service Availability Management is to ensure that agreed service levels will be met in foreseeable circumstances.

Context	This process is responsible for safeguarding the interests of the customers and interested parties by ensuring that agreed service levels will be met. It includes defining, analysing, planning, measuring and improving all aspects of service availability.
Outcomes	As a result of successful implementation of this process: 1. Service availability requirements are identified. 2. [A service availability plan is developed using the service availability requirements.] 3. [Service availability is tested against the service availability requirements.] 4. [Service availability is monitored.] 5. [Causes of unplanned service non-availability are identified and analysed.] 6. [Corrective actions are taken to address identified causes for unplanned non-availability.]
Requirements traceability	27001 2ED A.17.2.1 Availability of information processing facilities [1]

5.25 TEC.07 Service continuity management

Process ID	TEC.07
Name	Service continuity management
Purpose	The purpose of Service Continuity Management is to ensure that agreed service continuity commitments can be met within agreed targets and disrupted services can be resumed.
Context	This process is responsible for safeguarding the interests of the customers and interested parties by ensuring that agreed service levels will be met. It includes defining, analysing, planning, measuring and improving all aspects of service continuity. The process involves reducing risks to an acceptable level and planning for the recovery of service if a disruption occurs.
Outcomes	As a result of successful implementation of this process: 1. Service continuity requirements are identified. 2. [Service continuity is planned to meet the service continuity requirements.] 3. Service continuity is evaluated against the service continuity requirements. 4. [Changes in service continuity requirements are monitored.] 5. [Service continuity is ensured by activating the continuity plan in cases of major loss of service.]
Requirements traceability	27001 2ED A.17.1.1 Planning information security continuity [1] 27001 2ED A.17.1.3 Verify, review and evaluate information security continuity [3]

5.26 ORG.5 Supplier management

Process ID	ORG.5
Name	Supplier management
Purpose	The purpose of Supplier Management is to ensure supplier products, services or systems are managed and integrated into the delivered products, services or systems to meet the agreed requirements.

Context	Suppliers are participants in the supply of a product, service or system, either through horizontal or vertical integration. The process ensures that the organization establishes commitments with its suppliers that support the integration and alignment of products or services and agreements between the organization and customers. It verifies that suppliers are able to demonstrate that they can manage their subcontracted suppliers to meet their obligations and contractual requirements. Note: This process does not deal with supply to, for example, a warehouse, nor intermittent supply arrangements that are not directly involved in one or more services.
Outcomes	As a result of successful implementation of this process: 1. [Suppliers are identified.] 2. Products or services to be provided are negotiated and defined with each supplier. 3. [Roles and relationships between suppliers are determined.] 4. [The capability of subcontracted suppliers to meet obligations is confirmed.] 5. [Supplier obligations to meet requirements are monitored.] 6. [Supplier performance against agreed criteria is monitored.]
Requirements traceability	27001 2ED A.13.2.2 Agreements on information transfer [2] 27001 2ED A.15.1.2 Addressing security within supplier agreements [2] 27001 2ED A.15.1.3 Information and communication technology supply chain [2]

5.27 TEC.09 Technical data preservation and recovery

Process ID	TEC.09
Name	Technical data preservation and recovery
Purpose	The purpose of Technical Data Preservation and Recovery is to back up and preserve data and to recover data from archive media.
Context	This process addresses actions taken to preserve electronic data, and those actions to restore data, under controlled conditions, from archive media.
Outcomes	As a result of successful implementation of this process: 1. [Data backup requirements are identified.] 2. [Data restore requirements are identified.] 3. Data backups are executed. 4. Data restoration is performed. 5. [Backup media are preserved under controlled conditions.] 6. [Restored data is verified.]
Requirements traceability	27001 2ED A.12.3.1 Information backup [3,4]

Annex A
(informative)

The relationship between management system requirements and a process reference model

A.1 Introduction

This Annex examines the similarities, differences and relationships between an information security management system used in ISO/IEC 27001, a process reference model (PRM) in this Technical Specification and the assessment of the process quality characteristic of process capability.

ISO/IEC 27001 defines an information security management system as that part of the overall management system, based on a business risk approach, to establish, implement, operate, monitor, review, maintain and improve information security.

Process reference models are used as a basis for developing process assessment models that are used to assess process capability. A consistent description of processes within and across process reference models allows the combination of processes from different reference models that can ease the development of new models and facilitate comparison of models.

A.2 Processes and process models

A.2.1 Process seen in terms of inputs and outputs

For an organization to function effectively, it has to determine and manage numerous linked activities. An activity or set of activities using resources, and managed in order to enable the transformation of inputs into outputs, can be considered a process. Often the output from one process forms the input to the next as shown in Figure A.1.

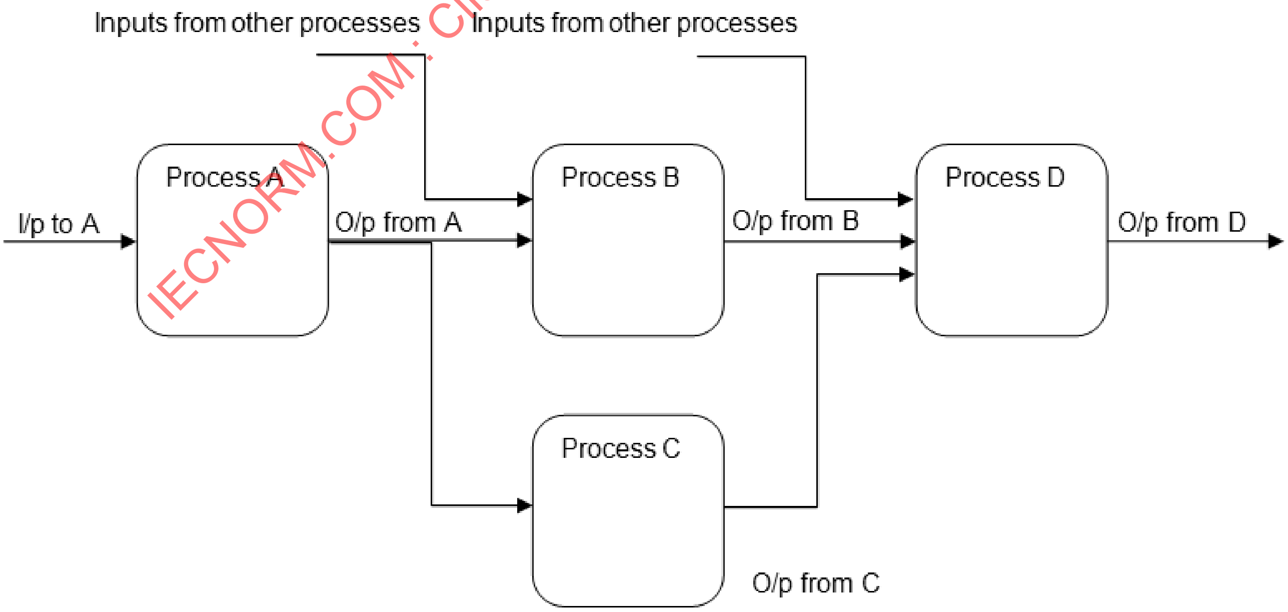


Figure A.1 — Process seen as a transformation of inputs to outputs

A.2.2 Using a Process Reference Model as a basis for understanding capability

Capability is defined in ISO 9000 as the “ability of an organization, system or process to realize a product (or service) that will fulfil the requirements for that product (or service).” In ISO/IEC 33020, process capability is considered to be “characterization of the ability of a process to meet current or projected business goals.”

Whereas the view of ISO 9000 is on customer satisfaction, process outputs and outcomes, ISO/IEC 33002 focuses on process outcomes, which are defined to be “observable results of a process.” ISO/IEC TR 24774 elaborates the definition of an outcome as “observable result of the successful achievement of the process purpose.” Outcomes are measurable, tangible, technical or business results that are achieved by a process, for example, the results that are used by other processes. Outcomes are observable and assessable for a specific process.

A.3 The nature of requirements for a management system

The requirements for management systems are generic and applicable to organizations in any industry or economic sector. ISO 9000 identifies requirements as a “need or expectation that is stated, generally implied or obligatory.”

A.4 The relationship of requirements to a process reference model

The PRM describes individual processes whereas ISO/IEC 27001 is that part of the overall management system, based on a business risk approach, to establish, implement, operate, monitor, review, maintain and improve information security.

Processes are instantiated within an organization — often within a quality management system (e.g. ISO 9001 or ISO/IEC 27001).

ISO/IEC 27001 defines the requirements for an information security management system. Some of the requirements in ISO/IEC 27001 are broader than the requirements for individual processes that can be represented in a process reference model.

Some requirements are general requirements for an ISMS that are applicable across all processes.

For example, ISO/IEC 27001 states in 5.1, Leadership and commitment:

5.1 Management commitment

> Top management shall demonstrate leadership and commitment with respect to the information security management system by:
>
> a) ensuring the information security policy and the information security objectives are established and are compatible with the strategic direction of the organization;
>
> b) ensuring the integration of the information security management system requirements into the organization’s processes;
>
> c) ensuring that the resources needed for the information security management system are available,
>
> d) communicating the importance of effective information security management and of conforming to the information security management system requirements;
>
> e) ensuring that the information security management system achieves its intended outcome(s);
>
> f) directing and supporting persons to contribute to the effectiveness of the information security management system;
>
> g) promoting continual improvement; and
>
> h) supporting other relevant management roles to demonstrate their leadership as it applies to their areas of responsibility.

Management system standards include general requirements and specific requirements. They include specific requirements for a process including requirements for the interaction of processes.

Most of the specific requirements in ISO/IEC 27001 are contained in Annex A (Reference control objectives and controls).

A.5 Illustrative example

An example is presented to explain the relationship between the requirements perspective of processes (i.e. from the viewpoint of ISO/IEC 27001) and the process perspective of ISO/IEC 33002. The example is that of the Audit process. This process is well understood in terms of its expected outcomes (i.e. in terms of the needs of conformity assessment), and it also has a comprehensive set of requirements in ISO/IEC 27001.

A.5.1 Audit requirements and the Audit process

Each process in 5.2 to 5.27 is supported by a Requirements traceability section. This section provides information about requirements that are supported by the process outcomes in this Technical Specification. In most cases, the process outcomes are supported by requirements from several subclauses, indicating that requirements for a process that is implemented within an ISMS are generally wider than the headline subclause associated with it.

Table A.1 illustrates the relationship between the PRM process perspective (i.e. as indicated by the outcomes) and the requirements perspective, as indicated by the defined requirements.

Table A.1 — The Internal Audit process: Process outcome and requirements perspective

PRM process perspective		ISO/IEC 27001 requirements perspective	
Process outcome	Process outcome description	Reference	Requirement definition
1	the scope and purpose of each audit is defined;	9.2	a) conforms to 1) the organization’s own requirements for its information security management system; and 2) the requirements of this International Standard;
		A.18.2.3	Information systems shall be [regularly] reviewed for compliance with the organization’s information security policies and standards.
2	the objectivity and impartiality of the conduct of audits and selection of auditors are assured;	9.2	The organization shall: e) select auditors and conduct audits that ensure objectivity and the impartiality of the audit process;

Table A.1 *(continued)*

PRM process perspective		ISO/IEC 27001 requirements perspective	
Process outcome	Process outcome description	Reference	Requirement definition
3	conformity of selected services, products and processes with requirements, plans and agreements is determined;	9.2	The organization shall conduct internal audits [at planned intervals] to provide information on whether the information security management system:
		A.15.2.1	Organizations shall regularly [monitor, review] and audit supplier service delivery.
		A.18.2.1	The organization's approach to managing information security and its implementation (i.e. control objectives, controls, policies, processes and procedures for information security) shall be reviewed independently [at planned intervals or when significant changes occur.]
		A.18.2.2	Managers shall [regularly] review the compliance of information processing and procedures within their area of responsibility with the appropriate security policies, standards and any other security requirements. Managers shall regularly [review] the compliance of information processing and procedures within their area of responsibility with the appropriate security policies, standards and any other security requirements.
4	Audit results are produced.	9.2	The organization shall: g) [retain documented information as evidence of the audit programme(s)] and the audit results.

A.6 Associations of requirements with process outcomes

Table A.2 identifies subclauses and singular requirements and associated outcomes.

Table A.2 — Association of ISO/IEC 27001 requirements with process outcomes

ISO/IEC 27001:2013		**Common Integrated Management Processes**	
Understanding the organization and its context 1. The organization shall determine external and internal issues that are relevant to its purpose and that affect its ability to achieve the intended outcome(s) of its information security management system.	04.1	TOP.1	**Leadership** 1. The context of the organization, including the expectations of its interested parties, are understood and analysed.
Understanding the needs and expectations of interested parties 1. The organization shall determine: a) interested parties that are relevant to the information security management system;	04.2	TOP.1	**Leadership** 1. The context of the organization, including the expectations of its interested parties, are understood and analysed.
Understanding the needs and expectations of interested parties 2. The organization shall determine: b) the requirements of these interested parties relevant to information security.	04.2	TOP.1	**Leadership** 1. The context of the organization, including the expectations of its interested parties, are understood and analysed.
Determining the scope of the information security management system 1. The organization shall determine the boundaries and applicability of the information security management system to establish its scope.	04.3	TOP.1	**Leadership** 2. The scope of management system activities is defined, taking the context of the organization into consideration.

Table A.2 *(continued)*

ISO/IEC 27001:2013		**Common Integrated Management Processes**	
Determining the scope of the information security management system 2. When determining this scope, the organization shall consider: a) the external and internal issues referred to in 4.1; b) the requirements referred to in 4.2; and c) interfaces and dependencies between activities performed by the organization, and those that are performed by other organizations.	04.3	TOP.1	**Leadership** 2. The scope of management system activities is defined, taking the context of the organization into consideration.
Determining the scope of the information security management system 3. The scope shall be available as documented information.	04.3	COM.02	**Documentation management** 1. Documented information to be managed is identified.
Information security management system 1. The organization shall establish, implement, maintain and continually improve an information security management system, in accordance with the requirements of this International Standard.	04.4	TOP.1	**Leadership** 4. The management system and operational process strategy is determined.
Leadership and commitment 1. Top management shall demonstrate leadership and commitment with respect to the information security management system by: a) ensuring the information security policy and the information security objectives are established and are compatible with the strategic direction of the organization; b) ensuring the integration of the information security management system requirements into the organization's processes; c) ensuring that the resources needed for the information security management system are available; d) communicating the importance of effective information security management and of conforming to the information security management system requirements; e) ensuring that the information security management system achieves its intended outcome(s); f) directing and supporting persons to contribute to the effectiveness of the information security management system; g) promoting continual improvement; and h) supporting other relevant management roles to demonstrate their leadership as it applies to their areas of responsibility.	05.1	TOP.1	**Leadership** 5. Commitment and leadership with respect to the management system is demonstrated.
Leadership and commitment 2. Top management shall demonstrate leadership and commitment with respect to the information security management system by: d) communicating the importance of effective information security management and of conforming to the information security management system requirements;	05.1	COM.01	**Communication management** 6. Information products are communicated to interested parties.

Table A.2 *(continued)*

ISO/IEC 27001:2013		**Common Integrated Management Processes**	
Policy 1. Top management shall establish an information security policy that: a) is appropriate to the purpose of the organization; b) includes information security objectives (see 6.2) or provides the framework for setting information security objectives; c) includes a commitment to satisfy applicable requirements related to information security; and d) includes a commitment to continual improvement of the information security management system.	05.2	TOP.1	**Leadership** 3. The management system policy and objectives are defined.
Policy 2. The information security policy shall: e) be available as documented information;	05.2	COM.02	**Documentation management** 1. Documented information to be managed is identified.
Policy 3. The information security policy shall: f) be communicated within the organization;	05.2	COM.01	**Communication management** 6. Information products are communicated to interested parties.
Policy 4. The information security policy shall: g) be available to interested parties, as appropriate.	05.2	COM.02	**Documentation management** 6. Documented information is available to designated parties.
Organizational roles, responsibilities and authorities 1. Top management shall ensure that the responsibilities and authorities for roles relevant to information security are assigned [and communicated.]	05.3	COM.09	**Operational implementation and control** 1. The required roles, responsibilities and authorities are allocated.
Organizational roles, responsibilities and authorities 2. Top management shall ensure that the responsibilities and authorities for roles relevant to information security are [assigned and] communicated.	05.3	COM.01	**Communication management** 6. Information products are communicated to interested parties.
Organizational roles, responsibilities and authorities 3. Top management [shall assign] the responsibility and authority for: a) ensuring that the information security management system conforms to the requirements of this International Standard; and b) reporting on the performance of the information security management system to top management.	05.3	COM.08	**Operational planning** 5. The required competencies and roles for performing the process are identified.
General 1. When planning for the information security management system, the organization shall consider the issues referred to in 4.1 and the requirements referred to in 4.2 [and determine the risks and opportunities that need to be addressed to: a) ensure the information security management system can achieve its intended outcome(s); b) prevent, or reduce, undesired effects; and c) achieve continual improvement.]	06.1.1	COM.08	**Operational planning** 1. Process needs and requirements are identified.

Table A.2 *(continued)*

ISO/IEC 27001:2013		**Common Integrated Management Processes**	
General 2. [When planning for the information security management system, the organization shall consider the issues referred to in 4.1 and the requirements referred to in 4.2 and] determine the risks and opportunities that need to be addressed to: a) ensure the information security management system can achieve its intended outcome(s); b) prevent, or reduce, undesired effects; and c) achieve continual improvement.	06.1.1	COM.11	**Risk and opportunity management** 1. Risks are identified.
General 3. The organization shall plan: d) actions to address these risks and opportunities; and e) how to 1) integrate and implement these actions into its information security management system processes; and 2) evaluate the effectiveness of these actions.	06.1.1	COM.08	**Operational planning** 8. Plans for the deployment of the process are developed.
Information security risk assessment 1. The organization shall define [and apply] an information security risk assessment process that: a) establishes and maintains information security risk criteria that include: 1) the risk acceptance criteria; and 2) criteria for performing information security risk assessments;	06.1.2	COM.08	**Operational planning** 1. Process needs and requirements are identified.
Information security risk assessment 2. [The organization shall define [and apply] an information security risk assessment process that: a) establishes and maintains information security risk criteria that include:] 1) the risk acceptance criteria; [and 2) criteria for performing information security risk assessments;]	06.1.2	COM.08	**Operational planning** 1. Process needs and requirements are identified.
Information security risk assessment 3. [The organization shall define [and apply] an information security risk assessment process that: a) establishes and maintains information security risk criteria that include: 1) the risk acceptance criteria; and] 2) criteria for performing information security risk assessments;	06.1.2	COM.08	**Operational planning** 1. Process needs and requirements are identified.
Information security risk assessment 4. The organization shall [define and] apply an information security risk assessment process that: a) establishes and maintains information security risk criteria that include: 1) the risk acceptance criteria; and 2) criteria for performing information security risk assessments;	06.1.2	COM.09	**Operational implementation and control** 3. Actions required to achieve the management system objectives are implemented.
Information security risk assessment 5. b) ensures that repeated information security risk assessments produce consistent, valid and comparable results;	06.1.2	COM.09	**Operational implementation and control** 4. Suitability and effectiveness of the actions taken to achieve the management system objectives are reviewed.

Table A.2 *(continued)*

ISO/IEC 27001:2013		**Common Integrated Management Processes**	
Information security risk assessment 6. c) identifies the information security risks: 1) apply the information security risk assessment process to identify risks associated with the loss of confidentiality, integrity and availability for information within the scope of the information security management system; and 2) identify the risk owners;	06.1.2	COM.11	**Risk and opportunity management** 1. Risks are identified.
Information security risk assessment 7. d) analyses the information security risks: 1) assess the potential consequences that would result if the risks identified in 6.1.2 c) 1) were to materialize; 2) assess the realistic likelihood of the occurrence of the risks identified in 6.1.2 c) 1); and 3) determine the levels of risk;	06.1.2	COM.11	**Risk and opportunity management** 2. Identified risks are analysed.
Information security risk assessment 8. e) evaluates the information security risks: 1) compare the results of risk analysis with the risk criteria established in 6.1.2 a); and 2) prioritise the analysed risks for risk treatment.	06.1.2	COM.11	**Risk and opportunity management** 3. Risks are evaluated against defined criteria.
Information security risk assessment 9. The organization shall retain documented information about the information security risk assessment process.	06.1.2	COM.02	**Documentation management** 1. Documented information to be managed is identified.
Information security risk treatment 1. The organization shall define [and apply] an information security risk treatment process to: a) select appropriate information security risk treatment options, taking account of the risk assessment results; b) determine all controls that are necessary to implement the information security risk treatment option(s) chosen; c) compare the controls determined in 6.1.3 b) above with those in Annex A and verify that no necessary controls have been omitted; d) produce a Statement of Applicability that contains the necessary controls [see 6.1.3 b) and c)] and justification for inclusions, whether they are implemented or not, and the justification for exclusions of controls from Annex A; e) formulate an information security risk treatment plan; and f) obtain risk owners' approval of the information security risk treatment plan and acceptance of the residual information security risks.	06.1.3	COM.08	**Operational planning** 1. Process needs and requirements are identified.
Information security risk treatment 2. The organization shall [define and] apply an information security risk treatment process to...	06.1.3	COM.09	**Operational implementation and control** 3. Actions required to achieve the management system objectives are implemented.
Information security risk treatment 3. e) formulate an information security risk treatment plan; and	06.1.3	COM.11	**Risk and opportunity management** 4. Risks are selected for treatment.

Table A.2 *(continued)*

ISO/IEC 27001:2013		**Common Integrated Management Processes**	
Information security risk treatment 4. f) obtain risk owners' approval of the information security risk treatment plan and acceptance of the residual information security risks.	06.1.3	COM.02	**Documentation management** 5. Documented information is released according to defined criteria.
Information security risk treatment 5. The organization shall retain documented information about the information security risk treatment process	06.1.3	COM.02	**Documentation management** 1. Documented information to be managed is identified.
Information security objectives and plans to achieve them 1. The organization shall establish information security objectives at relevant functions and levels.	06.2	TOP.1	**Leadership** 3. The management system policy and objectives are defined.
Information security objectives and plans to achieve them 2. The information security objectives shall: a) be consistent with the information security policy; b) be measurable (if practicable); c) take into account applicable information security requirements, and risk assessment and risk treatment results; d) be communicated; and e) be updated as appropriate.	06.2	TOP.1	**Leadership** 3. The management system policy and objectives are defined.
Information security objectives and plans to achieve them 3. The information security objectives shall: b) be measurable (if practicable);	06.2	COM.10	**Performance evaluation** 1. Performance monitoring and measurement needs are defined.
Information security objectives and plans to achieve them 4. The information security objectives shall: d) be communicated;	06.2	COM.01	**Communication management** 6. Information products are communicated to interested parties.
Information security objectives and plans to achieve them 5. The information security objectives shall: e) be updated as appropriate.	06.2	COM.02	**Documentation management** 3. The documented information content status is known.
Information security objectives and plans to achieve them 6. The organization shall retain documented information on the information security objectives.	06.2	COM.02	**Documentation management** 1. Documented information to be managed is identified.
Information security objectives and plans to achieve them 7. When planning how to achieve its information security objectives, the organization shall determine: f) what will be done;	06.2	COM.08	**Operational planning** 1. Process needs and requirements are identified.
Information security objectives and plans to achieve them 8. When planning how to achieve its information security objectives, the organization shall determine: g) what resources will be required;	06.2	COM.08	**Operational planning** 6. The required resources for performing the process are identified.

Table A.2 *(continued)*

ISO/IEC 27001:2013		**Common Integrated Management Processes**	
Information security objectives and plans to achieve them 9. When planning how to achieve its information security objectives, the organization shall determine: h) who will be responsible;	06.2	COM.08	**Operational planning** 5. The required competencies and roles for performing the process are identified.
Information security objectives and plans to achieve them 10. When planning how to achieve its information security objectives, the organization shall determine: i) when it will be completed; and	06.2	COM.08	**Operational planning** 8. Plans for the deployment of the process are developed.
Information security objectives and plans to achieve them 11. When planning how to achieve its information security objectives, the organization shall determine: j) how the results will be evaluated.	06.2	COM.08	**Operational planning** 7. Methods for monitoring the effectiveness and suitability of the process are determined.
Resources 1. The organization shall determine [and provide] the resources needed for the establishment, implementation, maintenance and continual improvement of the information security management system.	07.1	COM.08	**Operational planning** 6. The required resources for performing the process are identified.
Resources 2. The organization shall [determine and] provide the resources needed for the establishment, implementation, maintenance and continual improvement of the information security management system.	07.1	COM.09	**Operational implementation and control** 2. The required resources are allocated and applied.
Competence 1. The organization shall: a) determine the necessary competence of person(s) doing work under its control that affects its information security performance;	07.2	COM.08 COM.03	**Operational planning** 5. The required competencies and roles for performing the process are identified. **Human resource management** 1. The competencies required by the organization to produce products and services are identified.
Competence 2. The organization shall: b) ensure that these persons are competent on the basis of appropriate education, training, or experience;	07.2	COM.03	**Human resource management** 3. Understanding of role and activities in achieving organizational objectives in product and service provision is demonstrated by each individual.
Competence 3. The organization shall: c) where applicable, take actions to acquire the necessary competence, [and evaluate the effectiveness of the actions taken; and]	07.2	COM.03	**Human resource management** 2. Identified competency gaps are filled through training or recruitment.
Competence 4. The organization shall: c) [where applicable, take actions to acquire the necessary competence, and] evaluate the effectiveness of the actions taken; and	07.2	COM.09	**Operational implementation and control** 4. Suitability and effectiveness of the actions taken to achieve the management system objectives are reviewed.

Table A.2 *(continued)*

ISO/IEC 27001:2013		**Common Integrated Management Processes**	
Competence 5. The organization shall: d) retain appropriate documented information as evidence of competence.	07.2	COM.02	**Documentation management** 1. Documented information to be managed is identified.
Awareness 1. Persons doing work under the organization's control shall be aware of: a) the information security policy; b) their contribution to the effectiveness of the information security management system, including the benefits of improved information security performance; and c) the implications of not conforming to the information security management system requirements.	07.3	COM.03	**Human resource management** 3. Understanding of role and activities in achieving organizational objectives in product and service provision is demonstrated by each individual.
Communication 1. The organization shall determine the need for internal and external communications relevant to the information security management system including: a) on what to communicate;	07.4	COM.01	**Communication management** 1. Information content is defined in terms of identified communication needs and requirements.
Communication 2. The organization shall determine the need for internal and external communications relevant to the information security management system including: b) when to communicate;	07.4	COM.01	**Communication management** 4. Events that require communication actions are identified.
Communication 3. The organization shall determine the need for internal and external communications relevant to the information security management system including: c) with whom to communicate;	07.4	COM.01	**Communication management** 2. Parties to communicate with are identified.
Communication 4. The organization shall determine the need for internal and external communications relevant to the information security management system including: d) who shall communicate;	07.4	COM.01	**Communication management** 3. The party responsible for the communication is identified.
Communication 5. The organization shall determine the need for internal and external communications relevant to the information security management system including: e) the processes by which communication shall be effected.	07.4	COM.01	**Communication management** 5. The channel for the communication is selected.
General 1. The organization's information security management system shall include: a) documented information required by this International Standard; and b) documented information determined by the organization as being necessary for the effectiveness of the information security management system.	07.5.1	TOP.1	**Leadership** 4. The management system and operational process strategy is determined.

Table A.2 *(continued)*

ISO/IEC 27001:2013		**Common Integrated Management Processes**	
Creating and updating 1. When creating and updating documented information the organization shall ensure appropriate: a) identification and description (e.g. a title, date, author, or reference number);	07.5.2	COM.02	**Documentation management** 2. The forms of documented information representation are defined.
Creating and updating 2. When creating and updating documented information the organization shall ensure appropriate: b) format (e.g. language, software version, graphics) and media (e.g. paper, electronic); and	07.5.2	COM.02	**Documentation management** 2. The forms of documented information representation are defined.
Creating and updating 3. When creating and updating documented information the organization shall ensure appropriate: c) review [and approval] for suitability and adequacy.	07.5.2	COM.02	**Documentation management** 2. The forms of documented information representation are defined.
Creating and updating 4. When creating and updating documented information the organization shall ensure appropriate: c) [review and] approval for suitability and adequacy.	07.5.2	COM.02	**Documentation management** 5. Documented information is released according to defined criteria.
Control of documented information 1. Documented information required by the information security management system and by this International Standard shall be controlled to ensure: a) it is available and suitable for use, where and when it is needed; and b) it is adequately protected (e.g. from loss of confidentiality, improper use, or loss of integrity).For the control of documented information, the organization shall address the following activities, as applicable: c) distribution, access, retrieval and use; d) storage and preservation, including the preservation of legibility; e) control of changes (e.g. version control); and f) retention and disposition.	07.5.3	TOP.1	**Leadership** 4. The management system and operational process strategy is determined.
Control of documented information 2. a) it is available and suitable for use, where and when it is needed; and	07.5.3	COM.02	**Documentation management** 6. Documented information is available to designated parties.
Control of documented information 3. b) it is adequately protected (e.g. from loss of confidentiality, improper use, or loss of integrity)	07.5.3	COM.02	**Documentation management** 4. Documented information is current, complete and valid.
Control of documented information 4. c) distribution, access, retrieval and use;	07.5.3	COM.02	**Documentation management** 6. Documented information is available to designated parties.
Control of documented information 5. d) storage and preservation, including the preservation of legibility;	07.5.3	COM.02	**Documentation management** 7. Documented information is archived, or disposed of, as required.
Control of documented information 6. e) control of changes (e.g. version control); and	07.5.3	COM.02	**Documentation management** 3. The documented information content status is known.

Table A.2 *(continued)*

ISO/IEC 27001:2013		**Common Integrated Management Processes**	
Control of documented information 7. f) retention and disposition.	07.5.3	COM.02	**Documentation management** 7. Documented information is archived, or disposed of, as required.
Control of documented information 8. Documented information of external origin, determined by the organization to be necessary for the planning and operation of the information security management system, shall be identified as appropriate, and controlled.	07.5.3	COM.02	**Documentation management** 2. The forms of documented information representation are defined.
Operational planning and control 1. The organization shall plan, implement and control the processes needed to meet information security requirements, and to implement the actions determined in 6.1.	08.1	TOP.1	**Leadership** 4. The management system and operational process strategy is determined.
Operational planning and control 2. The organization shall also implement plans to achieve information security objectives determined in 6.2.	08.1	COM.09	**Operational implementation and control** 3. Actions required to achieve the management system objectives are implemented.
Operational planning and control 3. The organization shall keep documented information to the extent necessary to have confidence that the processes have been carried out as planned.	08.1	COM.02	**Documentation management** 7. Documented information is archived, or disposed of, as required.
Operational planning and control 4. The organization shall [control planned changes] and review the consequences of unintended changes, taking action to mitigate any adverse effects, as necessary.	08.1	COM.09	**Operational implementation and control** 4. Suitability and effectiveness of the actions taken to achieve the management system objectives are reviewed.
Operational planning and control 5. The organization shall control planned changes [and review] the consequences of unintended changes, taking action to mitigate any adverse effects, as necessary.	08.1	COM.09	**Operational implementation and control** 4. Suitability and effectiveness of the actions taken to achieve the management system objectives are reviewed.
		COM.09	**Operational implementation and control** 5. Deviations from planned arrangements are corrected when targets are not achieved.
Operational planning and control 6. The organization shall ensure that outsourced processes are determined and controlled.	08.1	TOP.1	**Leadership** 4. The management system and operational process strategy is determined.
Information security risk assessment 1. The organization shall perform information security risk assessments [at planned intervals or when significant changes are proposed or occur], taking account of the criteria established in 6.1.2 a).	08.2	COM.11	**Risk and opportunity management** 1. Risks are identified.
Information security risk assessment 2. [The organization shall perform information security risk assessments] at planned intervals or when significant changes are proposed or occur, [taking account of the criteria established in 6.1.2 a).]	08.2	COM.08	**Operational planning** 8. Plans for the deployment of the process are developed.

Table A.2 *(continued)*

ISO/IEC 27001:2013		**Common Integrated Management Processes**	
Information security risk assessment 3. The organization shall retain documented information of the results of the information security risk assessments.	08.2	COM.02	**Documentation management** 1. Documented information to be managed is identified.
Information security risk treatment 1. The organization shall implement the information security risk treatment plan.	08.3	COM.11	**Risk and opportunity management** 5. Selected risks are treated.
Information security risk treatment 2. The organization shall retain documented information of the results of the information security risk treatment.	08.3	COM.02	**Documentation management** 1. Documented information to be managed is identified.
Monitoring, measurement, analysis and evaluation 1. The organization shall evaluate the information security performance and the effectiveness of the information security management system.	09.1	COM.10	**Performance evaluation** 5. The collected performance data is analysed.
Monitoring, measurement, analysis and evaluation 2. The organization shall determine: a) what needs to be monitored and measured, including information security processes and controls;	09.1	COM.10	**Performance evaluation** 1. Performance monitoring and measurement needs are defined.
Monitoring, measurement, analysis and evaluation 3. b) the methods for monitoring, measurement, analysis and evaluation, as applicable, to ensure valid results;	09.1	COM.10	**Performance evaluation** 3. Performance measurement methods, supportive of the performance measures, are identified.
Monitoring, measurement, analysis and evaluation 4. c) when the monitoring and measuring shall be performed;	09.1	COM.08	**Operational planning** 8. Plans for the deployment of the process are developed.
Monitoring, measurement, analysis and evaluation 5. d) who shall monitor and measure;	09.1	COM.08	**Operational planning** 5. The required competencies and roles for performing the process are identified.
Monitoring, measurement, analysis and evaluation 6. e) when the results from monitoring and measurement shall be analysed and evaluated; and	09.1	COM.08	**Operational planning** 8. Plans for the deployment of the process are developed.
Monitoring, measurement, analysis and evaluation 7. f) who shall analyse and evaluate these results.	09.1	COM.08	**Operational planning** 5. The required competencies and roles for performing the process are identified.
Monitoring, measurement, analysis and evaluation 8. The organization shall retain appropriate documented information as evidence of the monitoring and measurement results.	09.1	COM.02	**Documentation management** 1. Documented information to be managed is identified.
Internal audit 1. The organization shall conduct internal audits [at planned intervals] to provide information on whether the information security management system:	09.2	COM.05	**Internal audit** 3. Conformity of selected services, products and processes with requirements, plans and agreements is determined.

Table A.2 *(continued)*

ISO/IEC 27001:2013		**Common Integrated Management Processes**	
Internal audit 2. [The organization shall conduct internal audits] at planned intervals [to provide information on whether the information security management system:]	09.2	COM.08	**Operational planning** 8. Plans for the deployment of the process are developed.
Internal audit 3. a) conforms to 1) the organization’s own requirements for its information security management system; and 2) the requirements of this International Standard;	09.2	COM.05	**Internal audit** 1. The scope and purpose of each audit is defined.
Internal audit 4. b) is effectively implemented [and maintained].	09.2	COM.09	**Operational implementation and control** 3. Actions required to achieve the management system objectives are implemented.
Internal audit 5. b) is [effectively implemented] and maintained.	09.2	COM.09	**Operational implementation and control** 4. Suitability and effectiveness of the actions taken to achieve the management system objectives are reviewed.
Internal audit 6. The organization shall: c) plan, establish, [implement and maintain] an audit programme(s), including the frequency, methods, responsibilities, planning requirements and reporting.	09.2	COM.08	**Operational planning** 8. Plans for the deployment of the process are developed.
Internal audit 7. The organization shall: c) [plan, establish,] implement and maintain an audit programme(s), including the frequency, methods, responsibilities, planning requirements and reporting.	09.2	COM.09	**Operational implementation and control** 3. Actions required to achieve the management system objectives are implemented.
Internal audit 8. The organization shall: The audit programme(s) shall take into consideration the importance of the processes concerned and the results of previous audits;	09.2	COM.08	**Operational planning** 8. Plans for the deployment of the process are developed.
Internal audit 9. The organization shall: d) define the audit criteria and scope for each audit;	09.2	COM.05	**Internal audit** 1. The scope and purpose of each audit is defined.
Internal audit 10. The organization shall: e) select auditors and conduct audits that ensure objectivity and the impartiality of the audit process;	09.2	COM.05	**Internal audit** 2. The objectivity and impartiality of the conduct of audits and selection of auditors are assured.
Internal audit 11. The organization shall: f) ensure that the results of the audits are reported to relevant management; and	09.2	COM.01	**Communication management** 6. Information products are communicated to interested parties.
Internal audit 12. The organization shall: g) retain [documented] information as evidence [of the audit programme(s) and the audit results.	09.2	COM.05	**Internal audit** 3. Conformity of selected services, products and processes with requirements, plans and agreements is determined.

Table A.2 *(continued)*

ISO/IEC 27001:2013		**Common Integrated Management Processes**	
Internal audit 13. [The organization shall: g) retain] documented [information as evidence [of the audit programme(s) and the audit results.]	09.2	COM.02	**Documentation management** 1. Documented information to be managed is identified.
Management review 1. Top management shall review the organization's information security management system [at planned intervals] to ensure its continuing suitability, adequacy and effectiveness.	09.3	COM.06	**Management review** 2. The status and performance of an activity or process are assessed in terms of the established objectives.
Management review 2. [Top management shall review the organization's information security management system] at planned intervals [to ensure its continuing suitability, adequacy and effectiveness.]	09.3	COM.08	**Operational planning** 8. Plans for the deployment of the process are developed.
Management review 3. The management review shall include consideration of: a) the status of actions from previous management reviews; b) changes in external and internal issues that are relevant to the information security management system; c) feedback on the information security performance, including trends in: 1) non-conformities and corrective actions; 2) monitoring and measurement results; 3) audit results; and 4) fulfilment of information security objectives; d) feedback from interested parties; e) results of risk assessment and status of risk treatment plan; and f) opportunities for continual improvement.	09.3	COM.06	**Management review** 1. The objectives of the review are established.
Management review 4. The outputs of the management review shall include decisions related to continual improvement opportunities and any needs for changes to the information security management system.	09.3	COM.04 COM.06	**Improvement** 1. Opportunities for improvement are identified. **Management review** 3. Risks, problems and opportunities for improvement are identified.
Management review 5. The organization shall retain documented information as evidence of the results of management reviews.	09.3	COM.02	**Documentation management** 1. Documented information to be managed is identified.
Nonconformity and corrective action 1. When a nonconformity occurs...	10.1	COM.07	**Non-conformity management** 1. Non-conformities are identified.
Nonconformity and corrective action 2. [When a nonconformity occurs], the organization shall: a) react to the nonconformity, and as applicable: 1) take action to control and correct it; and	10.1	COM.07	**Non-conformity management** 2. Non-conformities are resolved and closed.

Table A.2 *(continued)*

ISO/IEC 27001:2013		**Common Integrated Management Processes**	
Nonconformity and corrective action 3. [When a nonconformity occurs], the organization shall: b) evaluate the need for action to eliminate the causes of nonconformity, in order that it does not recur or occur elsewhere, [by: 1) reviewing the nonconformity; 2) determining the causes of the nonconformity; and 3) determining if similar nonconformities exist, or could potentially occur;]	10.1	COM.07	**Non-conformity management** 4. The need for action to eliminate the causes of non-conformities is evaluated.
Nonconformity and corrective action 4. [When a nonconformity occurs, the organization shall: b) evaluate the need for action to eliminate the causes of nonconformity, in order that it does not recur or occur elsewhere, by: 1) reviewing the nonconformity;] 2) determining the causes of the non-conformity; and 3) determining if similar nonconformities exist, or could potentially occur;	10.1	COM.07	**Non-conformity management** 3. The cause(s) of selected non-conformities is determined.
Nonconformity and corrective action 5. [When a non-conformity occurs], the organization shall: c) implement any action needed;	10.1	COM.07	**Non-conformity management** 5. A selected action proposal is implemented.
Nonconformity and corrective action 6. [When a nonconformity occurs], the organization shall: d) review the effectiveness of any corrective action taken; and	10.1	COM.07	**Non-conformity management** 6. The effectiveness of changes to eliminate the non-conformities is confirmed.
Nonconformity and corrective action 7. [When a nonconformity occurs], the organization shall: e) make changes to the information security management system, if necessary.	10.1	COM.07	**Non-conformity management** 5. A selected action proposal is implemented.
Nonconformity and corrective action 8. Corrective actions shall be appropriate to the effects of the nonconformities encountered.	10.1	COM.07	**Non-conformity management** 4. The need for action to eliminate the causes of non-conformities is evaluated.
Nonconformity and corrective action 9. The organization shall retain documented information as evidence of: f) the nature of the nonconformities and any subsequent actions taken, and g) the results of any corrective action.	10.1	COM.02	**Documentation management** 1. Documented information to be managed is identified.
Continual improvement 1. The organization shall continually improve the suitability, adequacy and effectiveness of the information security management system.	10.2	TOP.1	**Leadership** 4. The management system and operational process strategy is determined.
Policies for information security 1. A set of policies for information security shall be defined, [approved by management, published and communicated to employees and relevant external parties.]	A.05.1.1	TOP.1	**Leadership** 3. The management system policy and objectives are defined.

Table A.2 *(continued)*

ISO/IEC 27001:2013		**Common Integrated Management Processes**	
Policies for information security 2. A set of policies for information security shall be [defined,] approved by management, [published and communicated to employees and relevant external parties.]	A.05.1.1	COM.02	**Documentation management** 5. Documented information is released according to defined criteria.
Policies for information security 3. A set of policies for information security shall be [defined, approved by management,] published [and communicated to employees and relevant external parties.]	A.05.1.1	COM.02	**Documentation management** 6. Documented information is available to designated parties.
Policies for information security 4. A set of policies for information security shall be [defined, approved by management, published and] communicated to employees and relevant external parties.	A.05.1.1	COM.01	**Communication management** 6. Information products are communicated to interested parties.
Review of the policies for information security 1. The policies for information security shall be reviewed [at planned intervals] or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.	A.05.1.2	COM.09	**Operational implementation and control** 4. Suitability and effectiveness of the actions taken to achieve the management system objectives are reviewed.
Review of the policies for information security 2. The policies for information security [shall be reviewed] at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.	A.05.1.2	COM.08	**Operational planning** 8. Plans for the deployment of the process are developed.
Information security roles and responsibilities 1. All information security responsibilities shall be defined [and allocated].	A.06.1.1	COM.08	**Operational planning** 5. The required competencies and roles for performing the process are identified.
Information security roles and responsibilities 2. All information security responsibilities shall be [defined and] allocated.	A.06.1.1	COM.09	**Operational implementation and control** 1. The required roles, responsibilities and authorities are allocated.
Segregation of duties 1. Conflicting duties and areas of responsibility shall be segregated to reduce opportunities for unauthorized or unintentional modification or misuse of the organization's assets.	A.06.1.2	COM.08	**Operational planning** 5. The required competencies and roles for performing the process are identified.
Contact with authorities 1. Appropriate contacts with relevant authorities shall be maintained.	A.06.1.3	COM.01	**Communication management** 2. Parties to communicate with are identified.
Contact with special interest groups 1. Appropriate contacts with special interest groups or other specialist security forums and professional associations shall be maintained.	A.06.1.4	COM.01	**Communication management** 2. Parties to communicate with are identified.
Information security in project management 1. Information security shall be addressed in project management, regardless of the type of the project.	A.06.1.5	COM.08	**Operational planning** 1. Process needs and requirements are identified.

Table A.2 *(continued)*

ISO/IEC 27001:2013		**Common Integrated Management Processes**	
Mobile device policy 1. A policy and supporting security measures [shall be adopted] to manage the risks introduced by using mobile devices.	A.06.2.1	COM.08	**Operational planning** 1. Process needs and requirements are identified.
Mobile device policy 2. A policy and supporting security measures shall be adopted to manage the risks introduced by using mobile devices.	A.06.2.1	COM.09	**Operational implementation and control** 3. Actions required to achieve the management system objectives are implemented.
Teleworking 1. A policy [and supporting security measures] shall be implemented to protect information accessed, processed or stored at teleworking sites.	A.06.2.2	COM.08	**Operational planning** 1. Process needs and requirements are identified.
Teleworking 2. A [policy and] supporting security measures [shall be implemented to protect information accessed, processed or stored at teleworking sites.]	A.06.2.2	COM.08	**Operational planning** 3. The set of activities that transform the inputs into outputs is determined.
Teleworking 3. A [policy and supporting security measures] shall be implemented to protect information accessed, processed or stored at teleworking sites.	A.06.2.2	COM.09	**Operational implementation and control** 3. Actions required to achieve the management system objectives are implemented.
Screening 1. Background verification checks on all candidates for employment shall be carried out in accordance with relevant laws, regulations and ethics and shall be proportional to the business requirements, the classification of the information to be accessed and the perceived risks.	A.07.1.1	ORG.3	**Human resource employment management** 2. Prospective employees are screened in accordance with relevant laws, regulations and ethics, and in proportional to the business requirements and the perceived risks.
Terms and conditions of employment 1. The contractual agreements with employees and contractors shall state their and the organization’s responsibilities for information security.	A.07.1.2	ORG.3 ORG.3	**Human resource employment management** 3. Prospective employees agree to the terms and conditions of their employment contract. **Human resource employment management** 1. Roles and responsibilities of employees, contractors and third-party users are defined.
Management responsibilities 1. Management shall require all employees and contractors to apply information security in accordance with the established policies and procedures of the organization.	A.07.2.1	ORG.3	**Human resource employment management** 4. The terms and conditions of employment are applied.
Information security awareness, education and training 1. All employees of the organization and, where relevant, contractors shall receive appropriate awareness education and training and regular updates in organizational policies and procedures, as relevant for their job function.	A.07.2.2	COM.03	**Human resource management** 3. Understanding of role and activities in achieving organizational objectives in product and service provision is demonstrated by each individual.

Table A.2 *(continued)*

ISO/IEC 27001:2013		**Common Integrated Management Processes**	
Disciplinary process 1. There shall be a formal [and communicated] disciplinary process in place to take action against employees who have committed an information security breach.	A.07.2.3	ORG.3	**Human resource employment management** 6. Disciplinary measures are applied to employees that have committed a breach of the agreed conditions of employment.
Disciplinary process 2. There shall be a [formal and] communicated disciplinary process in place to take action against employees who have committed an information security breach.	A.07.2.3	COM.01	**Communication management** 6. Information products are communicated to interested parties.
Termination or change of employment responsibilities 1. Information security responsibilities and duties that remain valid after termination or change of employment shall be defined, [communicated to the employee or contractor and enforced.]	A.07.3.1	ORG.3	**Human resource employment management** 7. Responsibilities for performing employment termination or change of employment are defined and assigned.
Termination or change of employment responsibilities 2. Information security responsibilities and duties that remain valid after termination or change of employment shall be [defined,] communicated to the employee or contractor and enforced.	A.07.3.1	COM.01	**Communication management** 6. Information products are communicated to interested parties.
Inventory of assets 1. Assets associated with information and information processing facilities shall be identified [and an inventory of these assets shall be drawn up and maintained.]	A.08.1.1	ORG.1	**Asset management** 1. Items requiring asset management are identified.
Inventory of assets 2. [Assets associated with information and information processing facilities shall be identified] and an inventory of these assets shall be drawn up [and maintained.]	A.08.1.1	ORG.1	**Asset management** 3. Assets are inventoried.
Inventory of assets 3. [Assets associated with information and information processing facilities shall be identified] and an inventory of these assets shall be drawn up] and maintained.	A.08.1.1	ORG.1	**Asset management** 5. Changes to assets under management are controlled.
Ownership of assets 1. Assets maintained in the inventory shall be owned.	A.08.1.2	COM.08	**Operational planning** 5. The required competencies and roles for performing the process are identified.
Acceptable use of assets 1. Rules for the acceptable use of information and of assets associated with information and information processing facilities shall be identified, [documented and implemented.]	A.08.1.3	COM.08	**Operational planning** 1. Process needs and requirements are identified.
Acceptable use of assets 2. Rules for the acceptable use of information and of assets associated with information and information processing facilities shall be [identified,] documented [and implemented.]	A.08.1.3	COM.02	**Documentation management** 1. Documented information to be managed is identified.

Table A.2 *(continued)*

ISO/IEC 27001:2013		**Common Integrated Management Processes**	
Acceptable use of assets 3. Rules for the acceptable use of information and of assets associated with information and information processing facilities shall be [identified, documented and] implemented.	A.08.1.3	COM.09	**Operational implementation and control** 3. Actions required to achieve the management system objectives are implemented.
Return of assets 1. All employees and external party users shall return all of the organizational assets in their possession upon termination of their employment, contract or agreement.	A.08.1.4	ORG.3	**Human resource employment management** 8. Employees return all of the organization's assets in their possession upon termination of employment.
Classification of information 1. Information shall be classified in terms of legal requirements, value, criticality and sensitivity to unauthorised disclosure or modification.	A.08.2.1	ORG.1	**Asset management** 2. Asset items are classified.
Labelling of information 1. An appropriate set of procedures for information labelling shall be developed [and implemented] in accordance with the information classification scheme adopted by the organization.	A.08.2.2	COM.08	**Operational planning** 3. The set of activities that transform the inputs into outputs is determined.
Labelling of information 2. An appropriate set of procedures for information labelling shall be [developed and] implemented in accordance with the information classification scheme adopted by the organization.	A.08.2.2	COM.09	**Operational implementation and control** 3. Actions required to achieve the management system objectives are implemented.
Handling of assets 1. Procedures for handling assets shall be developed and [implemented] in accordance with the information classification scheme adopted by the organization.	A.08.2.3	COM.08	**Operational planning** 3. The set of activities that transform the inputs into outputs is determined.
Handling of assets 2. Procedures for handling assets shall be [developed and] implemented in accordance with the information classification scheme adopted by the organization.	A.08.2.3	COM.09	**Operational implementation and control** 3. Actions required to achieve the management system objectives are implemented.
Management of removable media 1. Procedures shall be [implemented] for the management of removable media in accordance with the classification scheme adopted by the organization.	A.08.3.1	COM.08	**Operational planning** 3. The set of activities that transform the inputs into outputs is determined.
Management of removable media 2. [Procedures shall be] implemented [for the management of removable media in accordance with the classification scheme adopted by the organization.]	A.08.3.1	COM.09	**Operational implementation and control** 3. Actions required to achieve the management system objectives are implemented.
Disposal of media 1. Media [shall be disposed of securely when no longer required,] using formal procedures.	A.08.3.2	COM.08	**Operational planning** 3. The set of activities that transform the inputs into outputs is determined.
Disposal of media 2. Media shall be disposed of securely when no longer required, [using formal procedures.]	A.08.3.2	ORG.1	**Asset management** 5. Changes to assets under management are controlled.

Table A.2 *(continued)*

ISO/IEC 27001:2013		**Common Integrated Management Processes**	
Physical media transfer 1. Media containing information shall be protected against unauthorized access, misuse or corruption during transportation.	A.08.3.3	ORG.1	**Asset management** 5. Changes to assets under management are controlled.
Access control policy 1. An access control policy shall be established, [documented and reviewed based on business and information security requirements.]	A.09.1.1	COM.08	**Operational planning** 1. Process needs and requirements are identified.
Access control policy 2. An access control policy shall be [established,] documented [and reviewed based on business and information security requirements].	A.09.1.1	COM.02	**Documentation management** 1. Documented information to be managed is identified.
Access control policy 3. An access control policy shall be [established, documented and] reviewed based on business and information security requirements.	A.09.1.1	COM.09	**Operational implementation and control** 4. Suitability and effectiveness of the actions taken to achieve the management system objectives are reviewed.
Access to networks and network services 1. Users shall only be provided with access to the network and network services that they have been specifically authorized to use.	A.09.1.2	ORG.4	**Infrastructure and work environment** 6. Access to the information resource is controlled.
User registration and deregistration 1. A formal user registration and de-registration process shall be [implemented] to enable assignment of access rights.	A.09.2.1	COM.08	**Operational planning** 1. Process needs and requirements are identified.
User registration and deregistration 2. A formal user registration and de-registration process shall be implemented to enable assignment of access rights.	A.09.2.1	COM.09	**Operational implementation and control** 3. Actions required to achieve the management system objectives are implemented.
User access provisioning 1. A formal user access provisioning process shall be implemented to assign or revoke access rights for all user types to all systems and services.	A.09.2.2	COM.09	**Operational implementation and control** 3. Actions required to achieve the management system objectives are implemented.
Management of privileged access rights 1. The allocation and use of privileged access rights shall be restricted and controlled.	A.09.2.3	ORG.4	**Infrastructure and work environment** 6. Access to the information resource is controlled.
Management of secret authentication information of users 1. The allocation of secret authentication information [shall be controlled through] a formal management process.	A.09.2.4	COM.08	**Operational planning** 1. Process needs and requirements are identified.
Management of secret authentication information of users 2. [The allocation of secret authentication information] shall be controlled [through a formal management process.]	A.09.2.4	COM.09	**Operational implementation and control** 3. Actions required to achieve the management system objectives are implemented.
Review of user access rights 1. Asset owners shall review users' access rights [at regular intervals.]	A.09.2.5	ORG.4	**Infrastructure and work environment** 6. Access to the information resource is controlled.

Table A.2 *(continued)*

ISO/IEC 27001:2013		**Common Integrated Management Processes**	
Review of user access rights 2. Asset owners [shall review users' access rights] at regular intervals.	A.09.2.5	COM.08	**Operational planning** 8. Plans for the deployment of the process are developed.
Removal or adjustment of access rights 1. The access rights of all employees and external party users to information and information processing facilities shall be removed upon termination of their employment, contract or agreement, or adjusted upon change.	A.09.2.6	ORG.3	**Human resource employment management** 9. Employee access to information resources is removed upon termination of their employment.
Use of secret authentication information 1. Users shall be required to follow the organization's practices in the use of secret authentication information.	A.09.3.1	ORG.3	**Human resource employment management** 3. Prospective employees agree to the terms and conditions of their employment contract.
Information access restriction 1. Access to information and application system functions shall be restricted in accordance with the access control policy.	A.09.4.1	ORG.4	**Infrastructure and work environment** 2. Access rights to the information resource are defined.
Secure log-on procedures 1. Where required by the access control policy, access to systems and applications shall be controlled by a secure log-on procedure.	A.09.4.2	ORG.4	**Infrastructure and work environment** 6. Access to the information resource is controlled.
Password management system 1. Password management systems shall be interactive and shall ensure quality passwords.	A.09.4.3	ORG.4	**Infrastructure and work environment** 6. Access to the information resource is controlled.
Use of privileged utility programs 1. The use of utility programs that might be capable of overriding system and application controls shall be restricted and tightly controlled.	A.09.4.4	ORG.4	**Infrastructure and work environment** 7. The information resource is protected from abuse.
Access control to program source code 1. Access to program source code shall be restricted.	A.09.4.5	ORG.4	**Infrastructure and work environment** 6. Access to the information resource is controlled.
Policy on the use of cryptographic controls 1. A policy on the use of cryptographic controls for protection of information shall be developed [and implemented.]	A.10.1.1	COM.08	**Operational planning** 1. Process needs and requirements are identified.
Policy on the use of cryptographic controls 2. A policy on the use of cryptographic controls for protection of information shall be [developed and] implemented.	A.10.1.1	COM.09	**Operational implementation and control** 3. Actions required to achieve the management system objectives are implemented.
Key management 1. A policy on the use, protection and lifetime of cryptographic keys shall be developed [and implemented] through their whole lifecycle.	A.10.1.2	COM.08	**Operational planning** 1. Process needs and requirements are identified.
Key management 2. A policy on the use, protection and lifetime of cryptographic keys shall be [developed and] implemented through their whole lifecycle.	A.10.1.2	COM.09	**Operational implementation and control** 3. Actions required to achieve the management system objectives are implemented.

Table A.2 *(continued)*

ISO/IEC 27001:2013		**Common Integrated Management Processes**	
Physical security perimeter 1. Security perimeters shall be defined [and used] to protect areas that contain either sensitive or critical information and information-processing facilities.	A.11.1.1	ORG.4	**Infrastructure and work environment** 1. The requirements for infrastructure and work environment to support processes are defined.
Physical security perimeter 2. Security perimeters shall be [defined and] used to protect areas that contain either sensitive or critical information and information-processing facilities.	A.11.1.1	ORG.4	**Infrastructure and work environment** 5. The infrastructure and work environment is controlled and maintained.
Physical entry controls 1. Secure areas shall be protected by appropriate entry controls to ensure that only authorized personnel are allowed access.	A.11.1.2	ORG.4	**Infrastructure and work environment** 1. The requirements for infrastructure and work environment to support processes are defined.
Securing offices, rooms and facilities 1. Physical security for offices, rooms and facilities shall be designed [and applied].	A.11.1.3	ORG.4	**Infrastructure and work environment** 1. The requirements for infrastructure and work environment to support processes are defined.
Securing offices, rooms and facilities 2. Physical security for offices, rooms and facilities shall be [designed and] applied.	A.11.1.3	ORG.4	**Infrastructure and work environment** 5. The infrastructure and work environment is controlled and maintained.
Protecting against external and environmental threats 1. Physical protection against natural disasters, malicious attack or accidents shall be designed [and applied].	A.11.1.4	ORG.4	**Infrastructure and work environment** 1. The requirements for infrastructure and work environment to support processes are defined.
Protecting against external and environmental threats 2. Physical protection against natural disasters, malicious attack or accidents shall be [designed and] applied.	A.11.1.4	ORG.4	**Infrastructure and work environment** 5. The infrastructure and work environment is controlled and maintained.
Working in secure areas 1. Procedures for working in secure areas shall be designed [and applied.]	A.11.1.5	COM.08	**Operational planning** 3. The set of activities that transform the inputs into outputs is determined.
Working in secure areas 2. Procedures for working in secure areas shall be [designed and] applied.	A.11.1.5	COM.09	**Operational implementation and control** 3. Actions required to achieve the management system objectives are implemented.
Delivery and loading areas 1. Access points such as delivery and loading areas and other points where unauthorized persons could enter the premises shall be controlled and, if possible, isolated from information-processing facilities to avoid unauthorized access.	A.11.1.6	ORG.4	**Infrastructure and work environment** 5. The infrastructure and work environment is controlled and maintained.
Equipment siting and protection 1. Equipment shall be sited and protected to reduce the risks from environmental threats and hazards and opportunities for unauthorized access.	A.11.2.1	ORG.2	**Equipment management** 1. Equipment is sited to minimize risk of environmental or other damage.
Supporting utilities 1. Equipment shall be protected from power failures and other disruptions caused by failures in supporting utilities.	A.11.2.2	ORG.2	**Equipment management** 2. Continuity in the provision of utilities and services to equipment is assured.

Table A.2 *(continued)*

ISO/IEC 27001:2013		**Common Integrated Management Processes**	
Cabling security 1. Power and telecommunications cabling carrying data or supporting information services shall be protected from interception, interference or damage.	A.11.2.3	ORG.2	**Equipment management** 1. Equipment is sited to minimize risk of environmental or other damage.
Equipment maintenance 1. Equipment shall be correctly maintained to ensure its continued availability and integrity.	A.11.2.4	ORG.2	**Equipment management** 3. Equipment is maintained to ensure its continued availability and integrity.
Removal of assets 1. Equipment, information or software shall not be taken off-site without prior authorization.	A.11.2.5	ORG.2	**Equipment management** 6. Equipment relocation is controlled.
Security of equipment and assets off-premises 1. Security shall be applied to off-site assets taking into account the different risks of working outside the organization's premises.	A.11.2.6	ORG.2	**Equipment management** 4. Equipment used offsite is managed to ensure integrity of operation.
Secure disposal or reuse of equipment 1. All items of equipment containing storage media shall be verified to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal or reuse.	A.11.2.7	ORG.2	**Equipment management** 5. The integrity of information is assured when equipment is withdrawn from service.
Unattended user equipment 1. Users shall ensure that unattended equipment has appropriate protection.	A.11.2.8	ORG.4	**Infrastructure and work environment** 5. The infrastructure and work environment is controlled and maintained.
Clear desk and clear screen policy 1. A clear desk policy for papers and removable storage media and a clear screen policy for information processing facilities [shall be adopted.]	A.11.2.9	COM.08	**Operational planning** 1. Process needs and requirements are identified.
Clear desk and clear screen policy 2. A clear desk policy for papers and removable storage media and a clear screen policy for information processing facilities shall be adopted.	A.11.2.9	COM.09	**Operational implementation and control** 3. Actions required to achieve the management system objectives are implemented.
Documented operating procedures 1. Operating procedures [shall be documented and made available to all users who need them.]	A.12.1.1	COM.08	**Operational planning** 3. The set of activities that transform the inputs into outputs is determined.
Documented operating procedures 2. [Operating procedures] shall be documented [and made available to all users who need them.]	A.12.1.1	COM.02	**Documentation management** 1. Documented information to be managed is identified.
Documented operating procedures 3. [Operating procedures shall be documented] and made available to all users who need them.	A.12.1.1	COM.02	**Documentation management** 6. Documented information is available to designated parties.
Change management 1. Changes to the organization, business processes, information processing facilities and systems that affect information security shall be controlled.	A.12.1.2	COM.09	**Operational implementation and control** 4. Suitability and effectiveness of the actions taken to achieve the management system objectives are reviewed.

Table A.2 *(continued)*

ISO/IEC 27001:2013		Common Integrated Management Processes	
		COM.09	**Operational implementation and control** 5. Deviations from planned arrangements are corrected when targets are not achieved.
Capacity management 1. The use of resources shall be monitored, tuned and projections made of future capacity requirements to ensure the required system performance.	A.12.1.3	TEC.01	**Capacity management** 3. Capacity usage is monitored, analysed and performance is tuned.
Separation of development, testing and operational environments 1. Development, testing, and operational environments shall be separated to reduce the risks of unauthorized access or changes to the operational environment.	A.12.1.4	ORG.4	**Infrastructure and work environment** 2. Access rights to the information resource are defined.
Controls against malware 1. Detection, prevention and recovery controls to protect against malware shall be implemented, combined with appropriate user awareness.	A.12.2.1	COM.09	**Operational implementation and control** 3. Actions required to achieve the management system objectives are implemented.
Information backup 1. Backup copies of information, software and system images shall be taken [and tested regularly in accordance with an agreed backup policy.]	A.12.3.1	TEC.09	**Technical data preservation and recovery** 3. Data backups are executed.
Information backup 2. Backup copies of information, software and system images shall be [taken and] tested [regularly in accordance with an agreed backup policy.]	A.12.3.1	TEC.09	**Technical data preservation and recovery** 4. Data restoration is performed.
Information backup 3. [Backup copies of information, software and system images shall be taken and tested] regularly [in accordance with an agreed backup policy].	A.12.3.1	COM.08	**Operational planning** 8. Plans for the deployment of the process are developed.
Information backup 4. [Backup copies of information, software and system images shall be taken and tested regularly in accordance with an agreed] backup policy.	A.12.3.1	COM.08	**Operational planning** 1. Process needs and requirements are identified.
Event logging 1. Event logs recording user activities, exceptions, faults and information security events shall be produced, [kept and regularly reviewed.]	A.12.4.1	ORG.4	**Infrastructure and work environment** 7. The information resource is protected from abuse.
Event logging 2. Event logs recording user activities, exceptions, faults and information security events shall be [produced,] kept [and regularly reviewed].	A.12.4.1	COM.02	**Documentation management** 1. Documented information to be managed is identified.
Event logging 3. Event logs recording user activities, exceptions, faults and information security events shall be [produced, kept and] regularly reviewed.	A.12.4.1	COM.09	**Operational implementation and control** 4. Suitability and effectiveness of the actions taken to achieve the management system objectives are reviewed.

Table A.2 *(continued)*

ISO/IEC 27001:2013		**Common Integrated Management Processes**	
Protection of log information 1. Logging facilities and log information shall be protected against tampering and unauthorized access.	A.12.4.2	ORG.4	**Infrastructure and work environment** 7. The information resource is protected from abuse.
Administrator and operator logs 1. System administrator and system operator activities shall be logged [and the logs protected and regularly reviewed.]	A.12.4.3	ORG.4	**Infrastructure and work environment** 6. Access to the information resource is controlled.
Administrator and operator logs 2. [System administrator and system operator activities shall be logged] and the logs protected [and regularly reviewed.]	A.12.4.3	ORG.4	**Infrastructure and work environment** 6. Access to the information resource is controlled.
Administrator and operator logs 3. [System administrator and system operator activities shall be logged and the logs protected] and regularly reviewed.	A.12.4.3	COM.09 ORG.4	**Operational implementation and control** 4. Suitability and effectiveness of the actions taken to achieve the management system objectives are reviewed. **Infrastructure and work environment** 6. Access to the information resource is controlled.
Clock synchronisation 1. The clocks of all relevant information processing systems within an organization or security domain shall be synchronised to a single reference time source.	A.12.4.4	ORG.4	**Infrastructure and work environment** 1. The requirements for infrastructure and work environment to support processes are defined.
Installation of software on operational systems 1. Procedures shall be [implemented] to control the installation of software on operational systems.	A.12.5.1	COM.08	**Operational planning** 3. The set of activities that transform the inputs into outputs is determined.
Installation of software on operational systems 2. Procedures shall be implemented to control the installation of software on operational systems.	A.12.5.1	COM.09	**Operational implementation and control** 3. Actions required to achieve the management system objectives are implemented.
Management of technical vulnerabilities 1. Information about technical vulnerabilities of information systems being used shall be obtained in a timely fashion, the organization's exposure to such vulnerabilities evaluated and appropriate measures taken to address the associated risk.	A.12.6.1	ORG.4	**Infrastructure and work environment** 7. The information resource is protected from abuse.
Restrictions on software installation 1. Rules governing the installation of software by users shall be [established and] implemented.	A.12.6.2	COM.09	**Operational implementation and control** 3. Actions required to achieve the management system objectives are implemented.
Restrictions on software installation 2. Rules governing the installation of software by users shall be established [and implemented].	A.12.6.2	COM.08	**Operational planning** 1. Process needs and requirements are identified.