PD ISO/IEC TS 33052:2016

BSI Standards Publication

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

Documents
Document Sharing Hub

Full document details: PD ISO/IEC TS 33052:2016

National foreword

This Published Document is the UK implementation of ISO/IEC TS 33052:2016.

The UK participation in its preparation was entrusted to Technical Committee IST/15, Software and systems engineering.

A list of organizations represented on this committee can be obtained on request to its secretary.

This publication does not purport to include all the necessary provisions of a contract. Users are responsible for its correct application.

© The British Standards Institution 2016.
Published by BSI Standards Limited 2016

ISBN 978 0 580 92221 3
ICS 35.080

Compliance with a British Standard cannot confer immunity from legal obligations.

This Published Document was published under the authority of the Standards Policy and Strategy Committee on 30 June 2016.

Amendments/corrigenda issued since publication

Date	Text affected

Documents
Document Sharing Hub

Full document details: PD ISO/IEC TS 33052:2016

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)

Documents
Document Sharing Hub
© ISO/IEC 2016

Full document details: PD ISO/IEC TS 33052:2016

COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2016, Published in Switzerland

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized otherwise in any form or by any means, electronic or mechanical, including photocopying, or posting on the internet or an intranet, without prior written permission. Permission can be requested from either ISO at the address below or ISO's member body in the country of the requester.

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

© ISO/IEC 2016 – All rights reserved

Documents
Document Sharing Hub

Full document details: PD ISO/IEC TS 33052:2016

Contents

Page

Foreword ..... **iv**

Introduction ..... **v**

1 Scope **1**

2 Normative references **1**

3 Terms and definitions **1**

4 Overview of the PRM **1**

5 Process descriptions **2**

5.1 Introduction 2
5.2 ORG.1 Asset management 3
5.3 TEC.01 Capacity management 3
5.4 TEC.02 Change management 4
5.5 COM.01 Communication management 4
5.6 TEC.03 Configuration management 5
5.7 COM.02 Documentation management 5
5.8 ORG.2 Equipment management 6
5.9 ORG.3 Human resource employment management 7
5.10 COM.03 Human resource management 8
5.11 COM.04 Improvement 9
5.12 TEC.04 Incident management 9
5.13 ORG.4 Infrastructure and work environment 9
5.14 COM.05 Internal audit 11
5.15 TOP.1 Leadership 11
5.16 COM.06 Management review 12
5.17 COM.07 Non-conformity management 13
5.18 COM.09 Operational implementation and control 13
5.19 COM.08 Operational planning 15
5.20 COM.10 Performance evaluation 17
5.21 TEC.05 Product/service release 18
5.22 TEC.08 Product/Service/System requirements 18
5.23 COM.11 Risk and opportunity management 19
5.24 TEC.06 Service availability management 19
5.25 TEC.07 Service continuity management 20
5.26 ORG.5 Supplier management 20
5.27 TEC.09 Technical data preservation and recovery 21

Annex A (informative) **The relationship between management system requirements and a process reference model** **22**

Annex B (informative) **Statement of conformity to ISO/IEC 33004** **58**

Bibliography **60**

© ISO/IEC 2016 – All rights reserved

Documents
Document Sharing Hub
Full document details: PD ISO/IEC TS 33052:2016

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*.

© ISO/IEC 2016 – All rights reserved
Documents
Document Sharing Hub
Full document details: PD ISO/IEC TS 33052:2016

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.

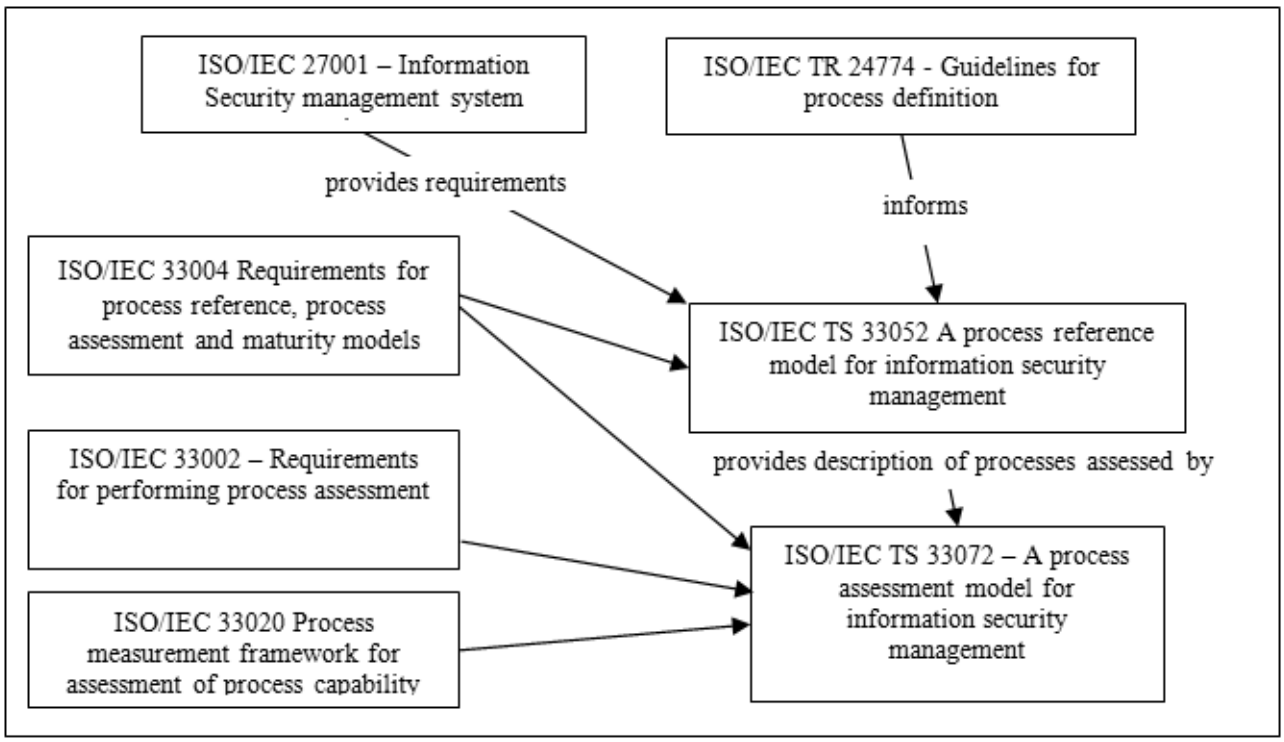

Figure 1 — Relationships between relevant standards

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.

© ISO/IEC 2016 – All rights reserved

Documents
Document Sharing Hub
Full document details: PD ISO/IEC TS 33052:2016

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.

© ISO/IEC 2016 – All rights reserved
Documents
Document Sharing Hub
Full document details: PD ISO/IEC TS 33052:2016

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.

© ISO/IEC 2016 – All rights reserved

Documents
Document Sharing Hub

Full document details: PD ISO/IEC TS 33052:2016

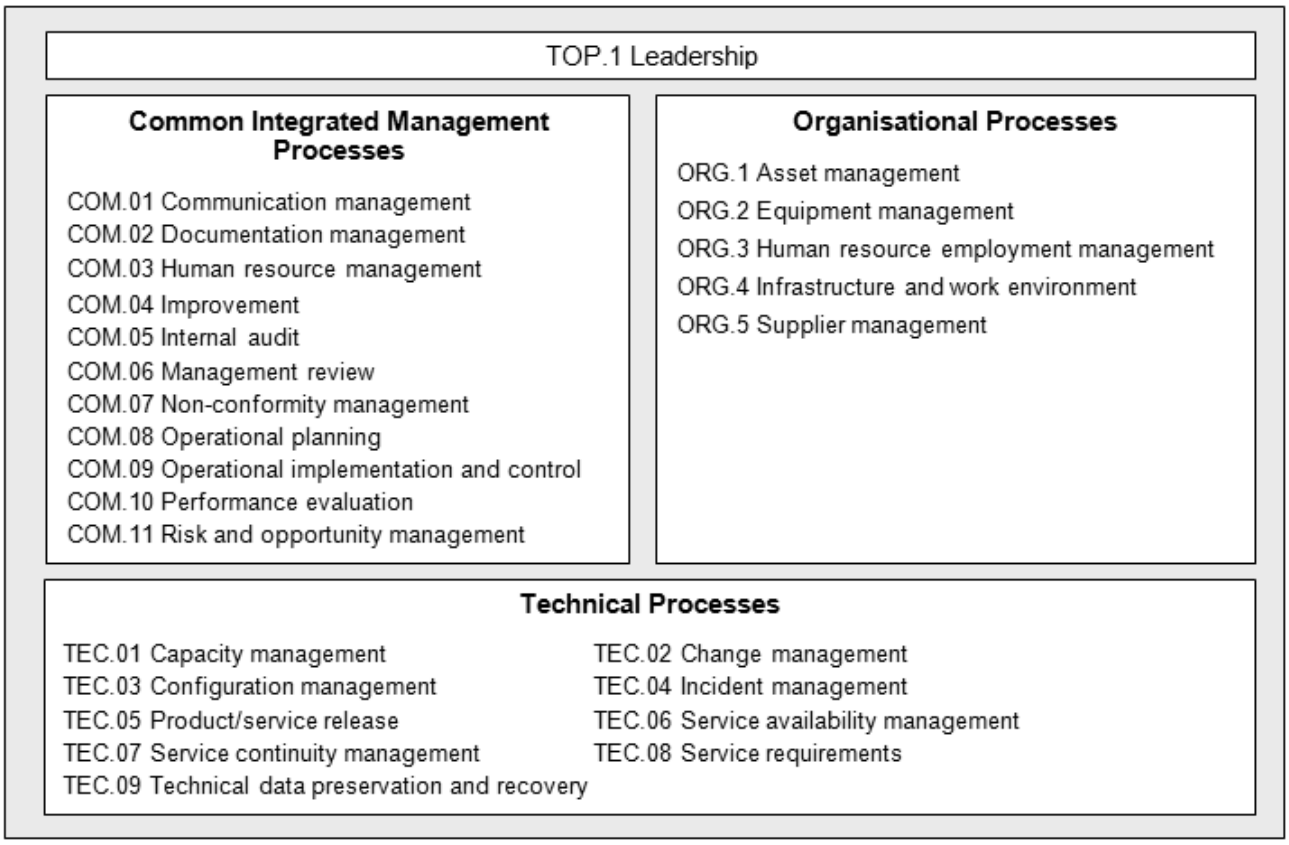

Figure 2 — Processes in the process reference model

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.

© ISO/IEC 2016 – All rights reserved
Documents
Document Sharing Hub
Full document details: PD ISO/IEC TS 33052:2016

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]

© ISO/IEC 2016 – All rights reserved

AVA Documents
Document Sharing Hub
Full document details: PD ISO/IEC TS 33052:2016

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]

© ISO/IEC 2016 – All rights reserved
Documents
Document Sharing Hub
Full document details: PD ISO/IEC TS 33052:2016

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.

© ISO/IEC 2016 – All rights reserved

Documents
Document Sharing Hub
Full document details: PD ISO/IEC TS 33052:2016

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.

© ISO/IEC 2016 – All rights reserved
Documents
Document Sharing Hub
Full document details: PD ISO/IEC TS 33052:2016

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.

© ISO/IEC 2016 – All rights reserved

Documents
Document Sharing Hub
Full document details: PD ISO/IEC TS 33052:2016

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]

© ISO/IEC 2016 – All rights reserved
Documents
Document Sharing Hub
Full document details: PD ISO/IEC TS 33052:2016

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.

© ISO/IEC 2016 – All rights reserved

Documents
Document Sharing Hub
Full document details: PD ISO/IEC TS 33052:2016

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]

© ISO/IEC 2016 – All rights reserved
Documents
Document Sharing Hub
Full document details: PD ISO/IEC TS 33052:2016

	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.

© ISO/IEC 2016 – All rights reserved

Documents
Document Sharing Hub
Full document details: PD ISO/IEC TS 33052:2016

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]

© ISO/IEC 2016 – All rights reserved
Documents
Document Sharing Hub
Full document details: PD ISO/IEC TS 33052:2016

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.]

© ISO/IEC 2016 – All rights reserved

Documents
Document Sharing Hub
Full document details: PD ISO/IEC TS 33052:2016