TECHNICAL SPECIFICATION

ISO/IEC TS 17021-6

First edition
2014-12-01

Conformity assessment — Requirements for bodies providing audit and certification of management systems —

Part 6: Competence requirements for auditing and certification of business continuity management systems

Évaluation de la conformité — Exigences pour les organismes procédant à l'audit et à la certification des systèmes de management —

Partie 6: Exigences de compétence pour l'audit et la certification des systèmes de management de la continuité d'activité

Reference number
ISO/IEC TS 17021-6:2014(E)

COPYRIGHT PROTECTED DOCUMENT

ISO copyright office
Case postale 56 • CH-1211 Geneva 20
Tel. + 41 22 749 01 11
Fax + 41 22 749 09 47
E-mail copyright@iso.org
Web www.iso.org

Published in Switzerland

Contents

Page

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 conformity assessment, the ISO Committee on conformity assessment (CASCO) is responsible for the development of International Standards and Guides.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2.

Draft International Standards are circulated to the national bodies for voting. Publication as an International Standard requires approval by at least 75 % of the national bodies casting a vote.

In other circumstances, particularly when there is an urgent market requirement for such documents, a technical committee may decide to publish other types of document:

— an ISO/IEC Publicly Available Specification (ISO/IEC PAS) represents an agreement between technical experts in an ISO working group and is accepted for publication if it is approved by more than 50 % of the members of the parent committee casting a vote;

— an ISO/IEC Technical Specification (ISO/IEC TS) represents an agreement between the members of a technical committee and is accepted for publication if it is approved by 2/3 of the members of the committee casting a vote.

An ISO/PAS or ISO/TS is reviewed after three years in order to decide whether it will be confirmed for a further three years, revised to become an International Standard, or withdrawn. If the ISO/PAS or ISO/TS is confirmed, it is reviewed again after a further three years, at which time it must either be transformed into an International Standard or be withdrawn.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO shall not be held responsible for identifying any or all such patent rights.

ISO/IEC/TS 17021-6 was prepared by the *ISO Committee on conformity assessment* (CASCO).

ISO/IEC 17021 consists of the following parts, under the general title *Conformity assessment — Requirements for bodies providing audit and certification of management systems:*

— *Part 2: Competence requirements for auditing and certification of environmental management systems* [Technical Specification]

— *Part 3: Competence requirements for auditing and certification of quality management systems* [Technical Specification]

— *Part 4: Competence requirements for auditing and certification of event sustainability management systems* [Technical Specification]

— *Part 5: Competence requirements for auditing and certification of asset management systems* [Technical Specification]

— *Part 6: Competence requirements for auditing and certification of business continuity management systems* [Technical Specification]

— *Part 7: Competence requirements for auditing and certification of road traffic safety management* systems [Technical Specification]

The next revision of ISO/IEC 17021:2011 will reflect the different parts and will become ISO/IEC 17021-1.

Introduction

This Technical Specification complements ISO/IEC 17021:2011. In particular, it clarifies the requirements for the competence of personnel involved in the certification process set out in ISO/IEC 17021:2011, Annex A.

The guiding principles in ISO/IEC 17021:2011, Clause 4, are the basis for the requirements in this Technical Specification.

Certification bodies have a responsibility to interested parties, including their clients and the customers of the organizations whose management systems are certified, to ensure that business continuity management system (BCMS) certification is credible by only using certification personnel that have demonstrated relevant competence.

BCMS certification personnel need to have the generic competencies described in ISO/IEC 17021:2011, as well as the specific BCMS competencies described in this Technical Specification.

Certification bodies will need to identify the specific audit team competence needed for the scope of each BCMS audit.

In this Technical Specification, the following verbal forms are used:

— “shall” indicates a requirement;

— “should” indicates a recommendation;

— “may” indicates a permission;

— “can” indicates a possibility or a capability.

Further details can be found in the ISO/IEC Directives, Part 2.

For the purposes of research, users are encouraged to share their views on this Technical Specification and their priorities for changes to future editions. Click on the link below to take part in the online survey:

https://www.surveymonkey.com/s/TPTVJCL

Conformity assessment — Requirements for bodies providing audit and certification of management systems —

Part 6: Competence requirements for auditing and certification of business continuity management systems

1 Scope

This Technical Specification complements the existing requirements of ISO/IEC 17021:2011. It includes specific competence requirements for personnel involved in the certification process for business continuity management systems (BCMS).

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 17000, *Conformity assessment — Vocabulary and general principles*

ISO/IEC 17021:2011, *Conformity assessment — Requirements for bodies providing audit and certification of management systems*

ISO 22301, *Societal security — Business continuity management systems --- Requirements*

ISO 22300, *Societal security — Terminology*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO 22300, ISO 22301, ISO/IEC 17000 and ISO/IEC 17021:2011 apply.

4 Generic competence requirements

The certification body shall define the competence requirements for each certification function as referenced in ISO/IEC 17021:2011, Table A.1. When defining these competence requirements, the certification body shall take into account all the requirements specified in ISO/IEC 17021:2011, as well as those specified in Clauses 5 and 6 of this Technical Specification.

NOTE 1 Annex A provides an informative summary of the competence requirements for personnel involved in specific certification functions.

NOTE 2 Information on the principles of auditing is provided in ISO 19011.

5 Competence requirements for BCMS auditors and personnel reviewing audit reports and making certification decisions

5.1 General

All personnel involved in BCMS auditing and personnel reviewing audit reports and making certification decisions shall have a level of competence that includes the generic competencies described in ISO/IEC 17021:2011, as well as the BCMS knowledge described in 5.2 to 5.11.

NOTE 1 It is not necessary for each auditor in the audit team to have the same competence, however, the collective competence of the audit team needs to be sufficient to achieve the audit objectives.

NOTE 2 Although the elements of the knowledge requirements are the same, it is recognized that the level of detail can be different for auditors and personnel reviewing audit reports and making certification decisions. It is the responsibility of each individual certification body to define this.

5.2 Business continuity management (BCM) terminology

The audit team and those reviewing the audit reports and making certification decisions shall have knowledge of BCM and risk terms, definitions and concepts.

5.3 Context of an organization

The audit team and those reviewing the audit reports and making certification decisions shall have knowledge of the context in which an organization operates.

5.4 Applicable laws, regulations and other requirements

The audit team and those reviewing the audit reports and making certification decisions shall have knowledge to determine whether an organization has identified and evaluated its compliance with applicable legal and other requirements.

NOTE 1 Statutory and regulatory requirements can be expressed as legal requirements.

NOTE 2 Other requirements can include voluntary national, international and sector-specific protocols.

5.5 Relationships within the business continuity management process

The audit team and those reviewing the audit reports and making certification decisions shall have knowledge of the interrelationships between BCM elements.

5.6 Business impact analysis and risk assessment

The audit team and those reviewing the audit reports and making certification decisions shall have knowledge of business impact analysis (BIA), including:

— methodologies and techniques;

— identification of activities that deliver products and services;

— assessment of impacts over time, and identifying when these become unacceptable;

— setting prioritized timescales for resumption;

— identifying dependencies and supporting resources.

The audit team and those reviewing the audit reports and making certification decisions shall have knowledge of risk assessment and risk management, including:

— methodologies and techniques;

— identification, analysis and evaluation of risks related to disruptive incidents;

— effectiveness of the existing controls;

— identification of appropriate risk treatments.

5.7 Business continuity strategies

The audit team and those reviewing the audit reports and making certification decisions shall have knowledge of strategies and methodologies for reducing the impact and the likelihood of disruptive incidents, including:

— strategy development;

— preparedness measures;

— selection of alternative strategies;

— cost/benefit analysis of continuity strategies;

— coordination approaches with external stakeholders;

— incident response;

— communications;

— command and control;

— coordination of responding organizations;

— recovery and restoration.

5.8 Incident management

The audit team and those reviewing the audit reports and making certification decisions shall have knowledge of incident management measures to determine whether an organization has identified appropriate responses to disruptive incidents, including warning and communication needs.

They shall have knowledge to evaluate an organization's effectiveness in testing its incident management capability.

5.9 Business continuity plans

The audit team and those reviewing the audit reports and making certification decisions shall have knowledge of business continuity plans, their establishment, development, maintenance, purpose, formats, structure and procedural detail.

5.10 Business continuity exercises

The audit team and those reviewing the audit reports and making certification decisions shall have knowledge of planning and implementing exercise types, processes, techniques and criteria to evaluate the capability of an organization to meet its recovery priorities and objectives.

5.11 BCMS performance evaluation

The audit team and those reviewing the audit reports and making certification decisions shall have knowledge of BCMS performance evaluation, including indicators and performance metrics, to determine whether an organization's BCMS performance is meeting the objectives and targets established by its management.

6 Competence requirements for personnel conducting the application review to determine audit team competence required, to select the audit team members, and to determine the audit time

6.1 General

The group or individual involved in other certification functions shall have competence that includes the generic competence described in ISO/IEC 17021:2011, and the BCMS knowledge described in 6.2 and 6.3 below.

6.2 BCM terminology

The group or individual involved in other certification functions shall have knowledge of BCM terms.

6.3 Context of an organization

The group or individual involved in other certification functions shall have knowledge of the context in which the organization operates.

6.4 Relationships within the business continuity management process

The group or individual involved in other certification functions shall have knowledge of the interrelationships between BCM elements.

Annex A
(informative)

Knowledge for BCMS auditing and certification

Table A.1 provides a summary of the knowledge required for BCMS auditing and certification but is informative because it only identifies the areas of knowledge for specific certification functions.

The competence requirements for each function are stated in the main text of this Technical Specification.

In Table A.1, "X" indicates that the certification body should define the criteria and depth of knowledge.

Table A.1 — Table of knowledge

Knowledge	Certification functions		
	Conducting the application review to determine audit team competence required, to select the audit team members, and to determine the audit time	Reviewing audit reports and making certification decisions	Auditing and leading the audit team
BCM terminology	X (see 6.2)	X (see 5.2)	X (see 5.2)
Context of an organization	X (see 6.3)	X (see 5.3)	X (see 5.3)
Applicable laws, regulations and other requirements		X (see 5.4)	X (see 5.4)
Relationships within the business continuity management process	X (see 6.4)	X (see 5.5)	X (see 5.5)
Business impact analysis and risk assessment		X (see 5.6)	X (see 5.6)
Continuity and recovery strategies		X (see 5.7)	X (see 5.7)
Incident management		X (see 5.8)	X (see 5.8)
Business continuity plans		X (see 5.9)	X (see 5.9)
Business continuity exercises		X (see 5.10)	X (see 5.10)
BCMS performance evaluation		X (see 5.11)	X (see 5.11)

Expertise should exist within the audit team or should be supplemented by a technical expert when necessary. Where any audit is conducted by a team, the level of skills required should be held within the team as a whole and not by every individual member of the team.

Bibliography

[1] ISO 19011, *Guidelines for auditing management systems*

[2] ISO 22313, *Societal security — Business continuity management systems — Guidance*

[3] ISO 22398, *Societal security — Guidelines for exercises*

[4] ISO 31000, *Risk management — Principles and guidelines*

[5] ISO Guide 73, *Risk management — Vocabulary*

[6] IEC 31010, *Risk management — Risk assessment techniques*

ICS 03.100.01;03.120.20

Price based on 6 pages