INTERNATIONAL STANDARD

ISO/IEC 27006

Third edition
2015-10-01

AMENDMENT 1
2020-03

Information technology — Security techniques — Requirements for bodies providing audit and certification of information security management systems

AMENDMENT 1

Technologies de l'information — Techniques de sécurité — Exigences pour les organismes procédant à l'audit et à la certification des systèmes de management de la sécurité de l'information

AMENDEMENT 1

Reference number
ISO/IEC 27006:2015/Amd.1:2020(E)

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

Published in Switzerland

Foreword

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

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

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

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

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

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

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

Information technology — Security techniques — Requirements for bodies providing audit and certification of information security management systems

AMENDMENT 1

7.2.1.1 d)

Replace the text by the following:

d) has gained experience of auditing ISMS prior to acting as an auditor performing ISMS audits. This experience shall be gained by performing as an auditor-in-training monitored by an ISMS evaluator (see ISO/IEC 17021-1:2015, 9.2.2.1.4) in at least one ISMS initial certification audit (stage 1 and stage 2) or re-certification and at least one surveillance audit. This experience shall be gained in at least 10 ISMS on-site audit days and performed in the last 5 years. The participation shall include review of documentation and risk assessment, implementation assessment and audit reporting.

7.2.1.1

Add a new bullet point g) as follows:

g) has competence in auditing an ISMS in accordance with ISO/IEC 27001.

8.2.1

Replace the last paragraph by the following:

The certification documents may reference national and international standards as source(s) of control set for controls that are determined as necessary in the organization's Statement of Applicability in accordance with ISO/IEC 27001:2013, 6.1.3 d). The reference on the certification documents shall be clearly stated as being only a control set source for controls applied in the Statement of Applicability and not a certification thereof.

9.3.1.1

Replace the third paragraph by the following:

The results of stage 1 shall be documented in a written report. The certification body shall review the stage 1 audit report before deciding on proceeding with stage 2 and shall confirm if the stage 2 audit team members have the necessary competence; this may be done by the auditor leading the team that conducted the stage 1 audit if deemed competent and appropriate.

NOTE Independent review (i.e. by a person from the certification body not involved in the audit) is one measure to mitigate the risks involved when deciding if and with whom to proceed to stage 2. However, other risk mitigation measures can already be in place achieving the same goal.

B.2.1

Replace the first paragraph by the following:

The total number of persons doing work under the organization's control for all shifts within the scope of the certification is the starting point for determination of audit time.

B.3.6

Replace the first paragraph by the following:

It is expected that the time calculated for planning and report writing combined should not typically reduce the total on-site "audit time" to less than 70 % of the time calculated in accordance with B.3.3 and B.3.4. Where additional time is required for planning and/or report writing, this shall not be a justification for reducing on-site audit time. Auditor travel time is not included in this calculation and is additional to the audit time referenced in the chart.

B.6

Replace the first paragraph by the following:

The number of total on-site auditor days – as calculated for the scope following the procedure stated in B.3.3 – shall be distributed amongst the different sites based on the relevance of the site for the management system and the risks identified. The justification for the distribution shall be recorded by the certification body.

The total time expended on initial audit and surveillance is the total sum of the time spent at each site plus the central office and shall never be less than that which would have been calculated for the size and complexity of the operation if all the work had been undertaken at a single site (i.e. with all the employees of the company in the same site).