INTERNATIONAL STANDARD

ISO/IEC 19770-11

First edition

Information technology — IT asset management —

Part 11: Requirements for bodies providing audit and certification of IT asset management systems

Technologies de l'information — Gestion de biens de logiciel — Partie 11: Exigences pour les organismes procédant & l'audit et & la certification des systèmes de management de la gestion des actifs logiciels

PROOF/ÉPREUVE

Reference number
ISO/IEC 19770-11:2021(E)

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

Published in Switzerland

Contents

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.

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 or www.iec.ch/members_experts/refdocs).

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

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

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

This document was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, subcommittee SC 7, *Software and systems engineering*.

A list of all parts in the ISO/IEC 19770 series can be found on the ISO and IEC websites.

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 and www.iec.ch/national-committees.

Introduction

This document is for use by certification bodies for auditing and certifying a management system for IT asset management (ITAM), referred to as an "IT asset management system" (ITAMS) in accordance with ISO/IEC 19770-1. It can also be used by accreditation bodies when assessing certification bodies. It is intended to be used in conjunction with ISO/IEC 17021-1, which sets out criteria for certification bodies providing audit and certification of management systems. This document provides requirements additional to those in ISO/IEC 17021-1.

Correct application of this document enables certification bodies to harmonize their application of ISO/IEC 17021-1 for audits against ISO/IEC 19770-1. It will also enable accreditation bodies to harmonize their application of the standards they use to audit certification bodies.

This document follows the structure of ISO/IEC 17021-1, as far as possible. The requirements additional to those in ISO/IEC 17021-1 are identified by subclauses titles that include "SMxxx".

ISO/IEC 17021-1 and this document use the term "client" for the organization seeking certification.

Information technology — IT asset management —

Part 11: Requirements for bodies providing audit and certification of IT asset management systems

1 Scope

This document specifies requirements and provides guidance for certification bodies providing audit and certification of an ITAMS in accordance with ISO/IEC 19770-1. It does not change the requirements specified in ISO/IEC 19770-1.

This document can also be used by accreditation bodies for the accreditation of certification bodies. However, this document does not specify requirements or provides guidance for accreditation bodies to audit certification bodies.

A certification body providing ITAMS certification is expected to be able to demonstrate fulfilment of the requirements specified in this document, in addition to the requirements in ISO/IEC 17021-1.

2 Normative references

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

ISO/IEC 17021-1:2015, *Conformity assessment — Requirements for bodies providing audit and certification of management systems — Part 1: Requirements*

ISO/IEC 19770-1, *Information technology — IT asset management — Part 1: IT asset management systems — Requirements*

ISO/IEC 19770-5, *Information technology — IT asset management — Part 5: Overview and vocabulary*

ISO/IEC 20000-1, *Information technology — Service management — Part 1: Service management system requirements*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 17021-1 and ISO/IEC 19770-5 apply.

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

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

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

4 Principles

The principles in ISO/IEC 17021-1:2015, Clause 4 apply.

5 General requirements

5.1 Legal and contractual matters

The requirements in ISO/IEC 17021-1:2015, 5.1 apply.

5.2 Management of impartiality

5.2.1 General

The requirements in ISO/IEC 17021-1:2015, 5.2 apply. In addition, the following requirements and guidance apply.

5.2.2 SM5.2.2 Conflicts of interest

Certification bodies may carry out the following duties without them being considered as consultancy or having a potential conflict of interest:

a) arranging and participating as a lecturer in training courses; where these courses relate to ITAM, related management systems or auditing, certification bodies shall confine themselves to the provision of generic information and advice which is publicly available, i.e. they shall not provide company-specific advice;

b) making available or publishing on request information describing the certification body's interpretation of the requirements of the certification audit standards;

c) activities prior to audit, solely aimed at determining readiness for certification audit; these activities shall not result in the provision of recommendations or advice that would contravene this subclause; certification bodies shall be able to confirm that such activities do not contravene these requirements and that they are not used to justify a reduction in the eventual certification audit duration;

d) performing second and third-party audits according to other standards or regulations not directly related to the ITAMS;

e) adding value during certification audits, e.g. by identifying opportunities for improvement, as they become evident during the audit, without recommending specific solutions.

Certification bodies shall not provide internal ITAM reviews of the client's ITAMS subject to certification. Certification bodies shall be independent of the body or bodies (including any individuals) which provide the internal ITAMS audit.

5.3 Liability and financing

The requirements in ISO/IEC 17021-1:2015, 5.3 apply.

6 Structural requirements

The requirements in ISO/IEC 17021-1:2015, Clause 6 apply.

7 Resource requirements

7.1 Competence of personnel

7.1.1 General considerations

7.1.1.1 General

The requirements in ISO/IEC 17021-1:2015, 7.1.1 apply. In addition, the following requirements and guidance apply.

7.1.1.2 SM7.1.1.2 Generic competence requirements

The certification body shall ensure that it has knowledge of the technological, legal and regulatory developments relevant to the ITAMS of the client which it assesses.

The certification body shall define the competence requirements for each certification function as referenced in ISO/IEC 17021-1:2015, Table A.1. The certification body shall take into account all the requirements specified in ISO/IEC 17021-1, 7.1.2 and 7.2.2 that are relevant for the ITAMS technical areas as determined by the certification body.

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

7.1.2 Determination of competence criteria

7.1.2.1 General

The requirements in ISO/IEC 17021-1:2015, 7.1.2 apply. In addition, the following requirements and guidance apply.

7.1.2.2 SM7.1.2.2 Competence requirements for ITAMS auditing

7.1.2.2.1 The term “technical area”

ISO/IEC 19770-1 states that all requirements are generic and intended to be applicable to IT assets of organizations regardless of their types and sizes. IT assets encompass asset types such as executable software (e.g. application programs, operating systems), non-executable software (e.g. fonts, configuration information), and IT hardware (e.g. PC, server, printer). In addition, the requirements of ISO/IEC 19770-1 can be applied to all technological environments and computing platforms (e.g. virtualized software applications, cloud-based software-as-a-service). For ISO/IEC 19770-1 audits, the term “technical area” relates to the ITAMS, including all ITAM-related processes and governance within the scope of the ITAMS. “Technical area” does not relate to any underlying technology used to enable ITAM.

7.1.2.2.2 General requirements

The audit team members shall at least have knowledge of:

a) management systems in general;

b) ITAMS maturity assessments;

c) service management system (SMS) or information security management systems (ISMS) as ITAMS related management systems;

d) principles of auditing.

NOTE Further information on the principles of auditing can be found in ISO 19011.

Criteria a), b) and d) apply to all auditors being part of the audit team. Criteria c) is only relevant for audit team members involved in a combined management system audit as addressed in 9.1.6.

7.1.2.2.3 ITAMS standards and normative documents

Collectively, all members of the audit team shall have knowledge of all requirements specified in ISO/IEC 19770-1 as well as the terminology specified in ISO/IEC 19770-5.

7.1.2.2.4 ITAM principles, practices and techniques

All members of the audit team shall have knowledge of:

a) ITAM roles and responsibilities;

b) processes applicable to ITAM;

c) organizational interfaces of ITAMS;

d) ITAM related tools, methods, techniques and their application;

The audit team shall also have team members with knowledge of IT compliance and software license compliance in particular. This competency can be shared among the auditors in the audit team.

7.1.2.2.5 Business management practices

Auditors involved in ITAMS auditing shall have knowledge of:

a) business requirements for ITAM;

b) ITAM stakeholders;

c) general business management concepts, practices and the inter-relationship between ITAM policies, objectives and results;

d) management processes and related terminology.

NOTE These processes also include human resources management, internal and external communication and other relevant support processes.

7.1.2.2.6 Client business sector

Auditors involved in ITAMS auditing shall have knowledge of:

a) legal and regulatory requirements relating to ITAM, depending on geography and jurisdiction(s), e.g. country-specific laws on internal control systems for IT assets, intellectual property, copyright, data privacy and environmental regulations;

   NOTE Knowledge of legal and regulatory requirements does not imply a profound legal background.

b) ITAM risks related to business sector, e.g. software license compliance as part of the overall IT compliance following regulatory requirements for financial institutions;

c) generic terminology, processes and technologies related to the client business sector;

d) relevant business sector practices.

The criteria a) and b) may be shared amongst the audit team.

7.1.2.2.7 Client products, processes and organization

Collectively, auditors involved in ITAMS auditing shall have knowledge of the impact of organization type, size, governance, structure, functions and relationships on development and implementation of the ITAMS and certification activities, including outsourcing.

7.1.2.3 SM7.1.2.3 Competence requirements for leading the ITAMS audit team

In addition to the requirements in 7.1.2.2, audit team leaders shall fulfil the following requirements, which shall be demonstrated in audits under guidance and supervision:

a) knowledge and skills to manage the certification audit process and the audit team;

b) demonstration of the capability to communicate effectively, both orally and in writing.

The certification body shall ensure auditors keep knowledge and skills in ITAM and auditing up to date through continual professional development.

7.1.2.4 SM7.1.2.4 Competence requirements for reviewing audit reports and making certification decisions

7.1.2.4.1 General requirements

The personnel reviewing audit reports and making certification decisions shall have knowledge that enables them to verify the appropriateness of the scope of certification as well as changes to the scope and their impact on the effectiveness of the audit. Additionally, the personnel reviewing audit reports and making the certification decisions shall have knowledge of:

a) management systems in general;

b) audit processes and procedures;

c) audit principles, practices and techniques.

7.1.2.4.2 ITAMS standards and normative documents

The personnel reviewing audit reports and making certification decisions shall have knowledge of relevant ITAMS standards and other normative documents used in the certification process.

7.1.2.4.3 ITAM principles, practices and techniques

The personnel reviewing audit reports and making the certification decisions shall have knowledge of the items listed in 7.1.2.2.4 a), b) and c).

7.1.2.4.4 Client business sector

The personnel reviewing audit reports and making certification decisions shall have knowledge of the generic terminology and risks related to the relevant business sector practices.

7.1.3 Evaluation processes

7.1.3.1 General

The requirements in ISO/IEC 17021-1:2015, 7.1.3 apply. In addition, the following requirements and guidance apply.