IAF Mandatory Document

Application of ISO/IEC 17021:2011 in the Service Management Sector (ISO/IEC 20000-1)

Issue 1

(IAF MD 18:2015)

The International Accreditation Forum, Inc. (IAF) facilitates trade and supports regulators by operating a worldwide mutual recognition arrangement among Accreditation Bodies (ABs) in order that the results issued by Conformity Assessment Bodies (CABs) accredited by IAF members are accepted globally.

Accreditation reduces risk for business and its customers by assuring that accredited Conformity Assessment Bodies (CABs) are competent to carry out the work they undertake within their scope of accreditation. Accreditation Bodies (ABs) that are members of IAF and the CABs they accredit are required to comply with appropriate international standards and the applicable IAF application documents for the consistent application of those standards.

ABs that are signatories to the IAF Multilateral Recognition Arrangement (MLA) are evaluated regularly by an appointed team of peers to provide confidence in the operation of their accreditation programs. The structure and scope of the IAF MLA is detailed in IAF PR 4 - Structure of IAF MLA and Endorsed Normative Documents.

The IAF MLA is structured in five levels: Level 1 specifies mandatory criteria that apply to all ABs, ISO/IEC 17011. The combination of a Level 2 activity(ies) and the corresponding Level 3 normative document(s) is called the main scope of the MLA, and the combination of Level 4 (if applicable) and Level 5 relevant normative documents is called a sub-scope of the MLA.

- The main scope of the MLA includes activities e.g. product certification and associated mandatory documents e.g. ISO/IEC 17065. The attestations made by CABs at the main scope level are considered to be equally reliable.

- The sub scope of the MLA includes conformity assessment requirements e.g. ISO 9001 and scheme specific requirements, where applicable, e.g. ISO TS 22003. The attestations made by CABs at the sub scope level are considered to be equivalent.

The IAF MLA delivers the confidence needed for market acceptance of conformity assessment outcomes. An attestation issued, within the scope of the IAF MLA, by a body that is accredited by an IAF MLA signatory AB can be recognized worldwide, thereby facilitating international trade.

TABLE OF CONTENTS

Introduction to IAF Mandatory Documents

The term "should" is used in this document to indicate recognised means of meeting the requirements of the standards. A Conformity Assessment Body (CAB) can meet these in an equivalent way provided this can be demonstrated to an Accreditation Body (AB). The term "shall" is used in this document to indicate those provisions which, reflecting the requirements of the relevant standard, are mandatory.

Application of ISO/IEC 17021:2011 in the Service Management Sector (ISO/IEC 20000-1)

This document is mandatory for the consistent application of ISO/IEC 17021. All clauses of ISO/IEC 17021 continue to apply and this document does not supersede any of the requirements in that standard.

1.   SCOPE

This mandatory document specifies requirements and provides guidance for bodies providing audit and certification of an information technology service management system (ITSMS, ISO/IEC 20000-1), in addition to the requirements contained within ISO/IEC 17021. It is primarily intended to support the accreditation of bodies providing ITSMS certification.

2.   NORMATIVE REFERENCES

ISO/IEC 20000-1:2011 Information Technology – Service Management – Part 1: Service management systems requirements

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

3.   TERMS AND DEFINITIONS

The terms and definitions from ISO/IEC 17021, Clause 3 and ISO/IEC 20000-1 apply.

4.   PRINCIPLES

The principles from ISO/IEC 17021, Clause 4 apply.

5.   GENERAL REQUIREMENTS

The requirements from ISO/IEC 17021, Clause 5 apply.

6.   STRUCTURAL REQUIREMENTS

The requirements from ISO/IEC 17021, Clause 6 apply.

7.   RESOURCE REQUIREMENTS

The requirements from ISO/IEC 17021, Clauses 7.1 to 7.2.7 apply.

NOTE ISO/IEC 17021 Annex A: The following ITSMS-specific requirements and guidance apply.

The requirements from ISO/IEC 17021, Clause 7.2.8 apply. In addition, the following ITSMS-specific requirements and guidance apply.

The CB shall provide the opportunity of continuing professional development to its certification personnel in order to maintain and improve their competence in ISO/IEC 20000 certification. In particular, the CB shall ensure the auditor's knowledge in IT service management practices and relevant regulatory requirements are maintained up to date. Continual professional development may include, but is not limited to:

  i.   additional work experience;
  ii.   participating in training courses;
  iii.   coaching;
  iv.   private study; and
  v.   participating in meetings, seminars or other relevant activities.

The requirements from ISO/IEC 17021, Clauses 7.2.9 to 7.5 apply.

8.   INFORMATION REQUIREMENTS

The requirements from ISO/IEC 17021, Clauses 8.1 to 8.4 apply.

8.5   Confidentiality

The requirements from ISO/IEC 17021, Clause 8.5 apply. In addition, the following ITSMS-specific requirements and guidance apply.

Before the certification audit, the Certification Body shall ask the client organization to report if any ITSMS records cannot be made available for review by the audit team because they contain confidential or sensitive information and to provide the corresponding justification. The Certification Body shall determine and record whether the ITSMS can be adequately audited in the absence of this confidential information and detail the corresponding rationale. If the Certification Body concludes that it is not possible to adequately audit the ITSMS without reviewing the identified confidential or sensitive records, it shall advise the client organization that the certification audit cannot take place until appropriate access arrangements are granted.

Note: Alternatively an intermediary who has adequate competence and the required level of clearance to view the confidential or sensitive information may be used to view the records and confirm, or otherwise, the information requested. This intermediary shall be accepted by both the CB and its client. However, such an intermediary should be independent of the client organization.

The requirements from ISO/IEC 17021, Clause 8.6 apply.

9.   PROCESS REQUIREMENTS

9.1   General requirements

The requirements from ISO/IEC 17021, Clauses 9.1.1 and 9.1.3 apply

9.1.2 The requirements from ISO/IEC 17021, Clause 9.1.2 apply. In addition, the following ITSMS-specific requirements and guidance apply.

The audit team shall audit the ITSMS of the client organization covered by the defined scope against all applicable certification requirements. The Certification Body shall ensure that the scope and boundaries of the ITSMS of the client organization are clearly defined in terms of the characteristics of the business, the organization, its location, assets and technology and considering ISO/IEC 20000-3. The Certification Body shall confirm that the client organizations address the requirements stated in the scope of their ITSMS.

9.1.4 The requirements from ISO/IEC 17021, Clause 9.1.4 apply. In addition, the following ITSMS-specific requirements and guidance apply.

The time allocated shall consider the following ITSMS specific factors:

    i.   the size of the ITSMS scope;

ii.   complexity of the ITSMS and complexity of the service(s) delivered by the client organization;

iii.   the type(s) of business performed within scope of the ITSMS;

iv.   extent and diversity of technology utilized in the implementation of the various components of the ITSMS;

v.   number of sites;

vi.   previously demonstrated performance of the ITSMS;

vii.   extent of SLAs and third party arrangements used within the scope of the ITSMS;

viii. the standards and regulations which apply to the certification; and

ix.   the number of other parties, such as suppliers, internal groups or customers acting as suppliers, involved in the provision of services.

9.1.5 The requirements from ISO/IEC 17021, Clause 9.1.5 apply. In addition, the following ITSMS-specific requirements and guidance apply.

The requirements from IAF Mandatory document MD1 (certification of Multiple Sites Based on Sampling), Clauses 0 to 5.2 apply. Where a multi-site organization operates some dissimilar processes or activities at the different sites, or a combination of sites, the Certification Body needs to justify and document the rationale for any sampling it decides to implement during the certification of the management system. This shall demonstrate how the same level of confidence in the conformity of the management system across all the sites listed can be obtained. Attention also has to be paid to the auditing of "virtual locations", e.g. non-permanent sites, online sites, etc. where sampling may or may not be appropriate.

The requirements from ISO/IEC 17021, Clauses 9.1.6 to 9.1.9 apply.

9.1.10   The requirements from ISO/IEC 17021, Clause 9.1.10 apply. In addition, the following ITSMS-specific requirements and guidance apply.

The certification audit report shall provide the information on the client IT organization's identification, assessment and management of risks to the services.

The requirements from ISO/IEC 17021, Clauses 9.1.11 to 9.1.15 apply.

9.2   Initial audit and certification

The requirements from ISO/IEC 17021, Clauses 9.2.1 to 9.2.2 apply.

9.2.3 Initial certification audit

IAD MD 18:2015

International Accreditation Forum, Inc.

Issue 1

**Application of ISO/IEC 17021:2011 in the
Service Management Sector (ISO/IEC 20000-1)**

Page 9 of 11

9.2.3.1 Stage 1 audit

9.2.3.1.1 The requirements from ISO/IEC 17021, Clause 9.2.3.1.1 apply. In addition, the following ITSMS-specific requirements and guidance apply.

In this stage of the audit, the Certification Body shall obtain documentation on the design of the ITSMS covering the documentation required in Clause 4.3.1 of ISO/IEC 20000-1.

The objective of the stage 1 audit is to provide a focus for planning the stage 2 audit by gaining an understanding of the ITSMS in the context of the client organization's ITSMS policy and objectives, and, in particular, of the client organization's state of preparedness for the audit.

The stage 1 audit includes, but should not be restricted to, the document review. The Certification Body shall agree with the client organization when and where the document review is conducted. In every case, the document review shall be completed prior to the commencement of stage 2 audit.

The results of the stage 1 audit shall be documented in a written report. The Certification Body shall review the stage 1 audit report for deciding on proceeding with the stage 2 audit and for selecting stage 2 audit team members with the necessary competence.

The Certification Body shall make the client organization aware of the further types of information and records that may be required for detailed examination during the stage 2 audit.

The requirements from ISO/IEC 17021, Clauses 9.2.3.1.2 and 9.2.3.1.3 apply.

9.2.3.2 Stage 2 audit

The requirements from ISO/IEC 17021, Clause 9.2.3.2 apply. In addition, the following ITSMS-specific requirements and guidance apply.

The audit shall focus on the client organization's:

i. documentation requirements listed in Clause 4.3.1 of ISO/IEC 20000-1;
ii. effectiveness of the controls implementing, monitoring, measuring and reviewing service management objectives plans and processes;
iii. internal ITSMS audits and management reviews; and
iv. management responsibility for the policy.

The requirements from ISO/IEC 17021, Clauses 9.2.4 and 9.2.5 apply.

The requirements from ISO/IEC 17021, Clauses 9.3 to 9.9 apply.

10. MANAGEMENT SYSTEM REQUIREMENTS FOR CERTIFICATION BODIES

The requirements from ISO/IEC 17021, Clause 10 apply.

End of IAF Mandatory Document on the Application of ISO/IEC 17021:2011 in the Service Management Sector (ISO/IEC 20000-1).

Annex A

(normative)

Required knowledge and skills

The requirements from ISO/IEC 17021, Annex A apply. The terms in ISO/IEC 17021 Annex A shall be read as follows.

"Knowledge of client business sector" shall include generic knowledge of information technology and relevant regulatory requirements.

"Client products" means the services provided by client organization. "Client processes" means the service management processes implemented by client organization.

"Specific management system standards" mean the ISO/IEC 20000 series. Auditors shall have the understanding in interactions of service management processes prescribed in ISO/IEC 20000 Part 1.

Further Information

For further Information on this document or other IAF documents, contact any member of IAF or the IAF Secretariat.

For contact details of members of IAF see the IAF website: http://www.iaf.nu

Secretariat:

Elva Nilsen

IAF Corporate Secretary

Telephone: +1 (613) 454-8159

Email: secretary@iaf.nu