



DPC: 23/30470941 DC

BSI Group Headquarters

389 Chiswick High Road London W4 4AL

Tel: +44 (0)20 8996 9000

Fax: +44 (0)20 8996 7400

www.bsigroup.com

Date: 25 October 2023

Origin: International

Latest date for receipt of comments: 18 December 2023

Project No. 2023/00484

Responsible committee: ART/1 Artificial Intelligence

Interested committees:

Title: Draft BS EN ISO/IEC 42006 Information technology — Artificial intelligence — Requirements for bodies providing audit and certification of artificial intelligence management systems.

Please notify admin.start@bsigroup.com if you are aware of any keywords that might assist in clarifying or identifying the standard or of the content of this standard:

- i) has any issues related to 3rd party IPR, patent or copyright
- ii) affects other national standard(s)
- iii) requires additional national guidance or information

WARNING: THIS IS A DRAFT AND MUST NOT BE REGARDED OR USED AS A BRITISH STANDARD. THIS DRAFT IS NOT CURRENT BEYOND 18 December 2023

This draft is issued to allow comments from interested parties; all comments will be given consideration prior to publication. No acknowledgement will normally be sent. **See overleaf for information on the submission of comments.**

No copying is allowed, in any form, without prior written permission from BSI except as permitted under the Copyright, Designs and Patent Act 1988 or for circulation within a nominating organization for briefing purposes. Electronic circulation is limited to dissemination by e-mail within such an organization by committee members.

Further copies of this draft may be purchased from BSI Shop <http://shop.bsigroup.com> or from BSI Customer Services, Tel: +44(0) 20 8996 9001 or email cservices@bsigroup.com. British, International and foreign standards are also available from BSI Customer Services.

Information on the co-operating organizations represented on the committees referenced above may be obtained from <https://standardsdevelopment.bsigroup.com/>.

Introduction

This draft standard is based on national and international discussions. Your comments on this draft are invited and will assist in the preparation of the consequent standard.

For international standards, comments will be reviewed by the relevant UK national committee before sending the consensus UK vote and comments to the international committee, which will then decide appropriate action. If the international standard is approved, it is usual for the text to be published as a British Standard.

For national standards, comments will be reviewed by the relevant UK national committee and the resulting standards published as a British Standard.

UK Vote

Please indicate whether you consider the UK should submit a negative (with supporting technical reasons) or positive vote on this draft. Please indicate if you are aware of any reason why this draft standard should not be published as a British Standard.

Submission of Comments

- **Annotated drafts are not acceptable and will be rejected.**
- All comments should be submitted online at <https://standardsdevelopment.bsigroup.com/>. You will need to register in order to comment.

Template for comments and secretariat observations

Date: xx/xx/20xx	Document: ISO/DIS xxxx
------------------	------------------------

1	2	(3)	4	5	(6)	7
MB	Clause No./ Subclause No./Annex (e.g. 3.1)	Paragraph/ Figure/Table/Note	Type of comment	Comment (justification for change) by the MB	Proposed change by the MB	Secretariat observations on each comment submitted
	3.1	Definition 1	ed	Definition is ambiguous and needs clarifying.	Amend to read '...so that the mains connector to which no connection...'	
	6.4	Paragraph 2	te	The use of the UV photometer as an alternative cannot be supported as serious problems have been encountered in its use in the UK.	Delete reference to UV photometer.	

DRAFT INTERNATIONAL STANDARD

ISO/IEC DIS 42006

ISO/IEC JTC 1/SC 42

Secretariat: ANSI

Voting begins on:
2023-10-25

Voting terminates on:
2024-01-17

Information technology — Artificial intelligence — Requirements for bodies providing audit and certification of artificial intelligence management systems

ICS: 03.120.20; 35.020

THIS DOCUMENT IS A DRAFT CIRCULATED FOR COMMENT AND APPROVAL. IT IS THEREFORE SUBJECT TO CHANGE AND MAY NOT BE REFERRED TO AS AN INTERNATIONAL STANDARD UNTIL PUBLISHED AS SUCH.

IN ADDITION TO THEIR EVALUATION AS BEING ACCEPTABLE FOR INDUSTRIAL, TECHNOLOGICAL, COMMERCIAL AND USER PURPOSES, DRAFT INTERNATIONAL STANDARDS MAY ON OCCASION HAVE TO BE CONSIDERED IN THE LIGHT OF THEIR POTENTIAL TO BECOME STANDARDS TO WHICH REFERENCE MAY BE MADE IN NATIONAL REGULATIONS.

RECIPIENTS OF THIS DRAFT ARE INVITED TO SUBMIT, WITH THEIR COMMENTS, NOTIFICATION OF ANY RELEVANT PATENT RIGHTS OF WHICH THEY ARE AWARE AND TO PROVIDE SUPPORTING DOCUMENTATION.

This document is circulated as received from the committee secretariat.



Reference number
ISO/IEC DIS 42006:2023(E)
Documents
AVA Document Sharing Hub
© ISO/IEC 2023



COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2023

All rights reserved. Unless otherwise specified, or required in the context of its implementation, 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
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.....	v
Introduction.....	vi
1 Scope.....	1
2 Normative references.....	1
3 Terms, definitions, symbols and abbreviated terms.....	2
4 Principles.....	3
5 General requirements.....	3
5.1 Legal and contractual matters.....	3
5.2 Management of impartiality.....	3
5.2.1 General.....	3
5.2.2 Conflicts of interest.....	3
5.3 Liability and financing.....	4
5.3.1 General.....	4
5.3.2 Liability.....	4
6 Structural requirements.....	4
7 Resource Requirements.....	4
7.1 Competence of personnel.....	4
7.1.1 General.....	4
7.1.2 Generic competence requirements.....	4
7.1.3 Determination of competence criteria.....	4
7.2 Personnel involved in the certification activities.....	8
7.2.1 General.....	8
7.2.2 Selecting auditors and personnel reviewing the audit reports.....	8
7.2.3 Selecting an individual auditor for leading the personnel fulfilling the function of “auditor”.....	9
7.3 Use of individual external technical experts.....	9
7.3.1 General.....	9
7.3.2 Use of individual external technical within the certification process.....	9
7.4 Personnel records.....	9
7.5 Outsourcing.....	9
8 Information requirements.....	10
8.1 Public information.....	10
8.2 Certification documents.....	10
8.2.1 General.....	10
8.2.2 AIMS certification documents.....	10
8.3 Reference to certification and use of marks.....	10
8.4 Confidentiality.....	10
8.4.1 General.....	10
8.4.2 Access to the documentation of the organization.....	10
8.5 Information exchange between a certification body and its clients.....	10
9 Process requirements.....	11
9.1 Pre-certification activities.....	11
9.1.1 Application.....	11
9.1.2 Application review.....	11
9.1.3 Audit programme.....	11
9.1.4 Audit methodology.....	11
9.1.5 Determining audit time.....	12
9.1.6 Multi-site sampling.....	12
9.1.7 Multiple management systems.....	13
9.2 Planning audits.....	13
9.2.1 Determining audit objectives, scope and criteria.....	13

9.2.2	Selection and assignment of personnel conducting the AIMS audit.....	14
9.2.3	Audit plan.....	14
9.3	Initial certification.....	14
9.3.1	Initial certification audit.....	14
9.4	Conducting audits.....	15
9.4.1	General.....	15
9.4.2	General requirements.....	15
9.4.3	Specific elements of the AIMS audit.....	16
9.4.4	Audit report.....	16
9.5	Certification decision.....	17
9.6	Maintaining certification.....	17
9.6.1	General.....	17
9.6.2	Surveillance activities.....	17
9.6.3	Re-certification.....	18
9.6.4	Special audits.....	18
9.6.5	Suspending, withdrawing or reducing the scope of certification.....	18
9.7	Appeals.....	18
9.8	Complaints.....	18
9.9	Client records.....	18
10	Management system requirements for certification bodies.....	18
10.1	Options.....	18
10.2	Option A: General management system requirements.....	18
10.3	Option B: Management system requirements in accordance with ISO 9001.....	19
Annex A (normative) Audit time.....		20
Annex B (normative) Template for certification document.....		26
Annex C (informative) Examples for audit time calculations.....		28
Bibliography.....		29

Foreword

ISO (the International Organization for Standardization) is a worldwide federation of national standards bodies (ISO member bodies). The work of preparing International Standards is normally carried out through ISO technical committees. Each member body interested in a subject for which a technical committee has been established has the right to be represented on that committee. International organizations, governmental and non-governmental, in liaison with ISO, also take part in the work. ISO collaborates closely with the International Electrotechnical Commission (IEC) on all matters of electrotechnical standardization.

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 ISO documents 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).

ISO draws attention to the possibility that the implementation of this document may involve the use of (a) patent(s). ISO takes no position concerning the evidence, validity or applicability of any claimed patent rights in respect thereof. As of the date of publication of this document, ISO had not received notice of (a) patent(s) which may be required to implement this document. However, implementers are cautioned that this may not represent the latest information, which may be obtained from the patent database available at www.iso.org/patents. ISO shall not be held responsible for identifying any or all such patent rights.

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 42, *Artificial Intelligence*.

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.

Introduction

A management system for organizations providing, developing or using AI systems or place them on the market as suppliers is set up according to ISO/IEC 42001:—¹⁾. It entails, but is not limited to, various special aspects regarding the management of risks, data protection, data quality, information and cyber security, ethics as well as the validation and verification of algorithms. Also, the life cycle processes for traditional software systems need to include AI-specific life cycle characteristics defined in ISO/IEC 5338: —²⁾^[1] which needs to be considered.

The object of assessment in ISO/IEC 42001:— and the necessary combination and complex interface functions in a management system according to ISO/IEC 42001:— result in specific requirements for the certification bodies and their processes when they certify such management systems. This document intends to help certification bodies responsibly perform their role with respect to auditing and certifying organizations with AI management systems.

The certification of a management system according to ISO/IEC 42001:— can be embedded in a conformity assessment system for products, processes and services according to ISO/IEC 17065 in support of ISO/IEC 17067.^[2] ISO/IEC 17030^[3] applies if it is intended to mark the conformity of the AI systems with conformity marks. The certificate for the confirmation of the conformity of the manufacturer's, supplier's or distributor's AI management system according to ISO/IEC 42001:— should be able to be taken over according to ISO/IEC 17065:2012, 7.4.5 as far as possible to avoid double tests.

This standard is also intended to assist accreditation bodies and peer assessors in being able to assess the minimum requirements for personnel competence in certification bodies and the processes of certification in these certification bodies in an efficient and harmonized way.

NOTE This document can be used as a criteria document for accreditation and peer assessment.

1) Under preparation. Stage at the time of publication: ISO/IEC FDIS 42001:2023.

2) Under preparation. Stage at the time of publication: ISO/IEC FDIS 5338:2023.

Information technology — Artificial intelligence — Requirements for bodies providing audit and certification of artificial intelligence management systems

1 Scope

This document specifies additional requirements to ISO/IEC 17021-1. The requirements contained in this document, when implemented, support the demonstration of competence, consistency and reliability by the bodies performing auditing and certification of an artificial intelligence management system (AIMS) according to ISO/IEC 42001 for organizations that provide, develop or use AI systems.

Certification of AIMS is a third-party conformity assessment activity (as described in ISO/IEC 17000:2020, 4.5), and bodies performing this activity are third-party conformity assessment bodies.

This document also provides the necessary information and confidence to customers about the way certification has been granted.

NOTE This document can be used as a criteria document for accreditation or peer assessment.

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 17000, *Conformity assessment — Vocabulary and general principles*

ISO/IEC 17011, *Conformity assessment — Requirements for accreditation bodies accrediting conformity assessment bodies*

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

ISO/IEC 17029, *Conformity assessment — General principles and requirements for validation and verification bodies*

ISO/IEC 17065, *Conformity assessment — Requirements for bodies certifying products, processes and services*

ISO/IEC 42001:—, *Information technology — Artificial intelligence — Management system*

ISO/IEC 22989, *Information technology — Artificial intelligence — Artificial intelligence concepts and terminology*

ISO/IEC 5259-3:—³⁾, *Information technology — Artificial Intelligence — Data quality for analytics and machine learning (ML) – Part 3: Data quality management requirements and guidelines*

ISO/IEC 27001, *Information technology — Security techniques — Information security management 196 systems — Requirements*

ISO/IEC 27701, *Security techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — Requirements and guidelines framework*

3) Under preparation. Stage at the time of publication: ISO/IEC DIS 5259-3:2023.

3 Terms, definitions, symbols and abbreviated terms

For the purposes of this document, the terms and definitions given in ISO/IEC 17000, ISO/IEC 17021-1, ISO/IEC 42001:—, ISO/IEC 17065, ISO/IEC 22989 and the following apply.

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

- ISO Online browsing platform: available at <https://www.iso.org/obp>
- IEC Electropedia: available at <https://www.electropedia.org/>

3.1 artificial intelligence management system

AIMS

set of interrelated or interacting elements of an organization to establish policies and objectives, as well as processes to achieve those objectives, in the provision, development or use of an AI system

Note 1 to entry: An AIMS can be applied to mitigate risks related to the provision, development or use of an AI system.

3.2 statement of applicability

SOA

documentation of all necessary controls and providing justification for inclusion or exclusion of controls

Note 1 to entry: Organizations may not require all controls listed in Annex A of ISO/IEC 42001 or may even exceed the list in [Annex A](#) with additional controls established by the organization itself.

Note 2 to entry: All identified risks shall be documented by the organization according to the requirements of ISO/IEC 42001. All identified risks and the risk management measures (controls) established to address them shall be reflected in the SOA.

Note 3 to entry: In the context of ISO/IEC 42001, performance refers both to results achieved by using AI systems and results related to the AI management system. The correct interpretation of the term is clear from the context of its use.

[SOURCE: ISO/IEC 42001:—, 3.11, modified Note 1 to entry, Note 2 to entry and Note 3 to entry by replacing “this document” with “ISO/IEC 42001”.]

3.3 certification document

document indicating that an organization’s AIMS conforms to ISO/IEC 42001:—

3.4 site

physical location where the organization to be certified operates with its own resources

Note 1 to entry: A site can also be the location of another legal entity that is part of a network of legal entities of the client that are linked by ownership or control of the management and control body (unified management). The organization to be certified controls the legal entities in the network and exercises ultimate direction as defined in ISO 9000:2015, 3.1.1^[4] for the AI management system

3.5 sector-specific standard

international standard that extends Annex A of ISO/IEC 42001:— to support a specific sector

Note 1 to entry: A sector-specific standard can provide additions to the controls in ISO/IEC 42001:—, provide guidance on control implementation, or provide guidance on elements to consider based on organizational context and the expectations of interested parties.

Note 2 to entry: A sector-specific extension of ISO/IEC 42001:—doesn't change the requirements of ISO/IEC 42001:—, including any addition and modification.

4 Principles

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

5 General requirements

5.1 Legal and contractual matters

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

5.2 Management of impartiality

5.2.1 General

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

5.2.2 Conflicts of interest

In addition to the requirements of ISO/IEC 17021-1:2015, 5.2.5, certification bodies shall not provide consulting for management systems related to artificial intelligence, information security, data protection (e.g. in the form of an external data protection officer or data protection check) or risk management.

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

- a) when arranging and participating as a lecturer in training courses, that relate to artificial intelligence management systems, to management systems or auditing, only generic and publicly available information is provided by certification bodies;
- b) activities preceding the audit to identify the object of certification, the sole purpose of which is to determine the scope and capability for a certification audit;;
- c) adding value during certification and surveillance audits, e.g. by identifying opportunities for improvement, as they become evident during the audit.

In order to prevent potential conflict of interest when addressing the duties listed above, the certification body shall not

- a) provide company-specific advice;
- b) conduct activities which themselves take the form of an audit or lead to recommendations or advice that would be contrary to [5.2.2](#) of this document, or justify a reduction of the ultimate time of the certification audit;
- c) recommend specific solutions.

The certification body shall not carry out any internal audits for the client to be certified. The ban on conducting internal audits shall not be circumvented by renaming the activity as inspection, assessment or similar. Any prior involvement of the certification body with the client related to ISO/IEC 42001 leads to a violation of the ban on self-assessment and shall be avoided.

5.3 Liability and financing

5.3.1 General

The requirements of ISO/IEC 17021-1:2015, 5.3 apply. In addition, the following requirements and guidance apply.

5.3.2 Liability

In addition to the requirements of ISO/IEC 17021-1:2015, 5.3.1, certification bodies shall be able to demonstrate a contract with an insurance company or an alternative mechanism that is fully protected against insolvency. Either option shall cover an appropriate amount of cover for personal injury, property damage and financial loss in relation to the turnover of the clients with AI systems.

6 Structural requirements

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

7 Resource Requirements

7.1 Competence of personnel

7.1.1 General

The requirements of ISO/IEC 17021-1:2015, 7.1 apply. In addition, the following requirements and guidance apply.

7.1.2 Generic competence requirements

The certification body shall ensure that it has competent personnel with knowledge of the technical, legal and regulatory developments relevant to the AIMS of the client that is assessed.

The certification body shall describe the competence requirements for each certification function according to the functional approach as defined in ISO/IEC 17000:2020, Annex A, and shall comply with them using competence management. This competence management ensures that the required criteria for education as well as for knowledge and experience of the personnel involved in the certification process are verified.

Certification of an AIMS is based on multiple, diverse competencies unlikely to be present in one natural person. The certification body shall therefore appoint and deploy competent people that fulfil all the required competence criteria as a competent group, if applicable, and throughout all functions of the certification process. With regard to the criteria definition of the certification body, the criteria for each function of the certification process shall be defined in such a way that the personnel fulfilling the tasks of the function have sufficient knowledge and understanding imparted by training and education, as well as experience, to cover the AIMS scope of the organization to be audited. In this respect, for the certification of an organization running an AIMS, the use of technical experts in accordance with ISO/IEC 17021-1:2015, 9.2.2.1.3 can be necessary and is permissible within the scope of the audit, but also in other functions of the certification process.

7.1.3 Determination of competence criteria

7.1.3.1 Competence requirements for personnel conducting the application review

Personnel conducting the application review to determine the auditor competences required, to select the personnel for the auditor function and to determine the audit time shall have specific knowledge.