

Auditing and Certification of AI Management Systems (ISO/IEC 42001)

Guidance for Accredited Conformity Assessment Bodies

Purpose and scope

This guidance sets out ASCB's expectations for certification bodies auditing and certifying an organization's AI management system (AIMS) against ISO/IEC 42001. It walks through how an AIMS certification differs from a conventional management system certification and points to where ISO/IEC 42006 sets specific requirements, across impartiality, audit team competence, the scope and statement of applicability, the audit criteria and objectives, audit time, access to documentation, remote auditing, surveillance and re-certification, records, and certificate content.

It is intended for certification bodies accredited by, or seeking accreditation from, ASCB for ISO/IEC 42001.

The guidance is deliberately high-level. A certification body intending to apply for ISO/IEC 42001 accreditation must recognize that ISO/IEC 42006 applies, and it must obtain the standard and work from it directly. ASCB's purpose here is to orient that work and to flag where the AIMS scheme departs from ordinary management system practice, not to restate the standard.

The applicable standards

For an ISO/IEC 42001 client, the governing certification-body standard is ISO/IEC 42006, the scheme-specific standard for bodies providing audit and certification of AI management systems. ISO/IEC 42006 does not replace ISO/IEC 17021-1; it sits on top of it, adding AIMS-specific requirements in a number of areas, and its normative Annex A governs the determination of audit time. ISO/IEC 42006 in turn relies on ISO/IEC 22989 for the AI life-cycle role definitions, namely AI user, AI provider and AI producer.

In setting these expectations, ASCB applies the ISO standards above and does not require certification bodies to apply additional mandatory documents on top of them.

Impartiality and conflicts of interest

The general impartiality requirements apply through ISO/IEC 17021-1 clause 5.2, which already bars management system consultancy (5.2.5) and the provision of internal audits to certified

clients (5.2.6). ISO/IEC 42006 clause 5.2.2.1 adds to this for ISO/IEC 42001 clients by extending the consultancy bar to consulting on artificial intelligence, information security, data protection and risk management, including acting as an external data protection officer or performing a data protection check. ISO/IEC 42006 also sets out worked examples of activities that do and do not amount to a conflict (clauses 5.2.2.2 and 5.2.2.3), and makes clear that the internal-audit restriction cannot be circumvented by renaming the activity. Certification bodies should map their own activities against both standards before taking on AIMS work.

Audit team competence and auditor selection

Competence is where ISO/IEC 42006 adds the most. Clause 7.1, with its Table 1, sets out the knowledge and skills the audit team needs, covering artificial intelligence itself, the AI and AIMS related legal obligations, AIMS terminology and practice, the client's business sector, and the client's products, processes and organization, on top of the baseline in ISO/IEC 17021-1 Annex A. Clause 7.2.2 sets minimum auditor selection criteria, including relevant education, practical experience in information technology or data protection with experience related to AI systems, AIMS-specific training, and supervised AIMS auditing experience. Outsourcing of the audit is not permitted within the ISO/IEC 42001 scope (clause 7.5). Certification bodies should confirm their competence scheme and auditor records demonstrate these requirements before auditing.

Scope of certification and the statement of applicability

For an AIMS the statement of applicability (SoA) defines the scope of certification. ISO/IEC 42006 clause 9.1.3 requires the client's definition of scope to capture all significant processes and risks relevant to the AI system, reflected in the SoA, and clause 9.2.1.3 expects at least one SoA per certification scope. The certification body should confirm that the client's risk assessment and risk treatment genuinely reflect its activities and extend to the boundaries of the scope, including interfaces to services or systems that sit outside it.

Audit criteria and objectives

The audit criterion is ISO/IEC 42001 itself, together with any other documents required for the certification (clause 9.2.1.4). The audit objectives (clause 9.2.1.2) are to determine the effectiveness of the AIMS, to confirm the client has identified the controls its risk assessment requires, and to confirm the established AIMS objectives have been achieved.

Audit duration

Audit-time procedures built for other schemes commonly start from effective personnel numbers, sometimes with turnover as a secondary factor. For an AIMS, the determination is governed by Annex A of ISO/IEC 42006. ISO/IEC 17021-1 clause 9.1.4.2 itself requires that where scheme-specific audit-time criteria exist they are applied, and ISO/IEC 42006 Annex A is those criteria; it is normative.

The Table A.1 figures are a documented starting point, not a fixed schedule of days. ISO/IEC 42006 states that the figures cannot be used on their own; they must be adjusted case by case through the Annex A (A.3.2) factors, with the reasoning recorded, and the calculated time is treated as a minimum.

In substance, the Annex A starting point is the number of persons involved in the AI life cycle (Table A.1), not total personnel or turnover, adjusted by the A.3.2 factors: the number of AI systems, the number of high-risk or sensitive-purpose AI systems, the number of regulatory frameworks and third-party agreements in scope, and the number of controls in the statement of applicability. The starting point is also role-dependent, so the certification body should establish whether the client is an AI user, provider or producer (per ISO/IEC 22989), as this sets the applicable Table A.1 column. Turnover does not feature as an audit-time factor in ISO/IEC 42006.

Access to documentation and confidential information

AI systems often involve confidential or sensitive material, including source code and raw data. ISO/IEC 42006 clause 8.4.2 requires the certification body, before the audit, to ask the client to report any AIMS related information that cannot be made available for review, and to determine whether the AIMS can still be adequately audited. If it concludes that the AIMS cannot be adequately audited without that information, the audit does not take place until appropriate access arrangements are granted. The certification body and client should establish safeguards for protected and sensitive information in the certification agreement.

Remote auditing

Audits frequently make some use of remote auditing, and ISO/IEC 42006 sets specific conditions on it. Clause 9.2.4 requires the certification body to define procedures for the level of remote auditing, supported by a documented risk analysis carried out before any remote audit, taking into account factors such as the available infrastructure, the sector, the type of audit in the cycle, the competence of those involved, prior remote-audit performance, and the certification scope. The audit plan and report must indicate clearly where remote methods have been used, the risk assessment must be reviewed across the certification cycle, and

remote methods must not be used where the assessment identifies unacceptable risks to audit effectiveness.

Surveillance and re-certification

Surveillance procedures follow the same approach as the certification audit, with the programme adapted to the AI system risks and effects on the client, and surveillance reviews the records of appeals and complaints (clause 9.6.2). Surveillance time should be proportional to the initial audit, with the total spent annually being around one third of the initial certification time, reviewed for changes that affect audit time (Annex A.4). Re-certification audit time depends on the results of prior audits and is at least two thirds of the initial certification audit time for the same organization (Annex A.5). Where the AIMS manages high-risk or sensitive-purpose AI systems, ISO/IEC 42006 also envisages additional monitoring arrangements agreed with the client.

Certificate content

ISO/IEC 42006 clause 8.2.2 requires two items on the certificate over and above the ISO/IEC 17021-1 clause 8.2.2 content: the version of the statement of applicability on which certification is based, and a statement that the certificate does not authorize the labeling of products, processes or services. Certification bodies should ensure their AIMS certificate template accommodates both.

Documentation and records

ASCB will look for an auditable record of how the audit program was determined and justified. This includes the sampling rationale (clause 9.1.5), the justification for the audit-time determination (clause 9.1.4 and ISO/IEC 42006 Annex A), the assessment of same and different activities and the resulting site selection, and, for the certification decision, a clear evidential thread linking what was audited, what was found, and the conformity conclusions reached. ISO/IEC 17021-1 clause 9.9.2 specifically requires records of the methodology used for sampling of sites and the justification for the audit-time determination. Where the same and different activities assessment is well recorded, much of the remaining documentation follows from it.

Multi-site certification

The remainder of this guidance addresses the additional considerations that arise when a multi-site organization seeks certification of its AIMS, in particular multi-site sampling, the

assessment of whether sites conduct the same AI activity, the information to gather for audit determination, and the treatment of the central function.

Is a sample acceptable, or must every site be audited?

A multi-site organization does not necessarily require every site to be audited at initial certification, but a sample is not automatic. Sampling is permitted in principle: neither ISO/IEC 17021-1 nor ISO/IEC 42006 prescribes a fixed sampling formula or requires every site to be visited, and ISO/IEC 42006 Annex A.7 confirms that ISO/IEC 17021-1 clause 9.1.5 governs multi-site sampling for an AIMS. The qualification that matters is that clause 9.1.5 only permits sampling where the sites cover the same activity, and for an AIMS whether they genuinely do is the central question, addressed in the next section.

Where sampling is used, the certification body must develop a sampling program and document the rationale for each client (clause 9.1.5). ASCB does not mandate a particular sampling formula; it will expect the sample, and the basis on which it was selected, to be justified and recorded, and to support a sound certification decision (clause 9.5).

What counts as the same activity for an AI system

The multi-site sampling concept rests on activities being substantially the same across sites under a centrally controlled management system. For an AIMS, what counts as the same activity warrants closer thought than it might for a conventional standard, and the nature of the AI systems is central to it. In ISO/IEC 42006 terms, the relevant considerations are the AI systems themselves: how many are in use, and in particular whether any are high-risk or sensitive-purpose systems. These are among the Annex A factors that bear on audit time, and they also shape the risk picture for sampling.

The question for a multi-site program is whether the systems, and the way they are used and governed, are genuinely consistent across the sites. Where the same systems are deployed and controlled centrally and behave the same way everywhere, the sites are conducting the same activity and lend themselves to sampling. Where systems are configured, retrained or tuned locally, or where some sites operate higher-risk or additional systems that others do not, the activity is no longer uniform and the basis for sampling weakens. A system fixed centrally behaves consistently wherever it runs, whereas one that adapts to local data can reach different outcomes from site to site even when it is nominally the same system.

Where that consistency is not present, the multi-site provisions distinguish same-activity from different-activity sites: sampling may be applied to the same-activity sites, while sites conducting materially different or higher-risk AI activities are audited individually. ASCB expects the certification body's audit-determination records to show how it assessed whether sites are conducting the same or different AI-related activities, and to justify the resulting split. Getting

this assessment right at the outset is the single most effective way to make the program defensible.

Information to gather for audit determination

In addition to the baseline information ordinarily collected for multi-site audit determination, that is the number and addresses of sites, personnel numbers at each site, the activities at each site, and confirmation of whether the same processes and procedures are followed at each site, ASCB recommends gathering enough information to characterize the AI activities and their risk, for example:

- The client's role in the AI life cycle, that is whether it is an AI user, provider or producer; ISO/IEC 22989 defines these roles, and the role sets the audit-time basis under ISO/IEC 42006 (see Audit duration above).
- The nature of the AI systems deployed or developed at each site, and whether they are fixed centrally or adapt to local data.
- Whether AI-related governance, policy, risk management and monitoring are centralized or exercised locally.
- Whether any site undertakes higher-risk AI activities.

The central function

The central function, or head office, should be included in the audit program in effectively all cases. It typically holds responsibility for governance, policy, risk management, objectives, competence management, monitoring, internal audit and management review, and for an AIMS these central functions are usually where the management system is genuinely operated. The depth of the central-function audit should reflect the actual distribution of responsibility between the center and the sites, informed by the client's AI risk assessment.

ASCB's focus at assessment

At assessment and surveillance, ASCB's focus is on confirming that the certification body's documented approach holds together in practice: that the sampling and site-selection decisions are justified, that the audit time follows the ISO/IEC 42006 Annex A method, and that the evidence gathered supports the certification decisions. The sampling and site-selection judgments remain the certification body's, consistent with ISO/IEC 17021-1, while the audit-time basis for an AIMS is the one set by ISO/IEC 42006. Certification bodies are encouraged to engage with ASCB early where an AIMS program raises novel questions.

Quick reference

Does ISO/IEC 42006 replace ISO/IEC 17021-1?

No. It adds AIMS-specific requirements on top of ISO/IEC 17021-1, and its Annex A method for determining audit time is normative.

May a certification body advise its ISO/IEC 42001 clients?

No. ISO/IEC 17021-1 clause 5.2 already bars management system consultancy and the provision of internal audits to certified clients. For ISO/IEC 42001 clients, ISO/IEC 42006 clause 5.2.2.1 extends the consultancy bar to AI, information security, data protection and risk management.

What competence must the audit team have?

Knowledge across artificial intelligence, the AI and AIMS related legal obligations, AIMS terminology and practice, and the client's business sector, products and processes, in addition to the ISO/IEC 17021-1 Annex A baseline (clause 7.1 and Table 1). Auditor selection criteria are in clause 7.2.2.

What defines the scope of certification?

The statement of applicability (SoA), which should capture the significant processes and risks relevant to the AI system, with at least one SoA per scope (clauses 9.1.3 and 9.2.1.3).

Must all sites be audited at initial certification?

No. Sampling is permitted where the sites cover the same activity (ISO/IEC 17021-1 clause 9.1.5). Sites conducting materially different or higher-risk AI activities are audited individually.

Does ISO/IEC 42006 introduce its own multi-site sampling rules?

No. Annex A.7 applies ISO/IEC 17021-1 clause 9.1.5.

What is the basis for audit time?

ISO/IEC 42006 Annex A, which is normative: the number of persons involved in the AI life cycle (Table A.1), role-dependent, adjusted by the A.3.2 factors, with the calculated time treated as a minimum and a documented rationale.

Must the central function be audited?

In effectively all cases, since it is usually where the management system is operated.

What appears on an AIMS certificate beyond a standard certificate?

The version of the statement of applicability, and a statement that the certificate does not authorize labeling of products, processes or services (ISO/IEC 42006 clause 8.2.2).