GRC+ SERVICE SHEET · NOVEMBER 2026

ISO 42001 Internal Audit

Clause 9.2 of ISO/IEC 42001 requires internal audits of your AI management system at planned intervals, by auditors who are objective and impartial. We audit clauses 4 to 10 and the Annex A controls you apply, and give you findings in time to close them before your certification or surveillance audit.

SERVICE
Advisory service

What It Is

The internal audit clause 9.2 of ISO/IEC 42001 requires for your AI management system, by an auditor independent of it, timed so your findings are closed before the certification body arrives.

WHY IT MATTERS

Auditing your own work is not impartial

Clause 9.2 asks for objective and impartial auditors; the people who run the AI management system cannot audit it.
- A missing or weak internal audit is a nonconformity
- Findings found late leave no time to close them
- Annex A coverage gaps across the certification cycle

THE OUTCOME

A certification audit without surprises

You close findings before the certification body arrives and show a working audit programme.
- Corrective actions in place on time
- Evidence of impartial internal audit
- A stronger management review

What We Audit

The management system	Context, scope, leadership, AI risk assessment and treatment, AI system impact assessment, objectives, competence and management review.
Annex A controls	The controls in your Statement of Applicability, from AI policy and data for AI systems to the AI system life cycle, tested on evidence rather than policy text.
Earlier findings	Corrective actions from previous internal and external audits, and whether they worked.
Each finding with a recommendation	Nonconformities and observations graded as a certification body would, each with a practical recommendation.

What You Receive

The internal audit report PDF	Scope, criteria, method and a conclusion for each clause and control sampled.
Nonconformities and observations Excel finding list	Graded as a certification body would, each with a practical recommendation.
An audit programme Three-year plan	Which clauses and controls to cover in each year of your certification cycle.
Input for management review Presentation and a closing call	The results in the form clause 9.3 asks management to consider.

From Audit Plan to Report

1	**Audit plan** Scope, criteria, sampling and dates, agreed with your management system owner.
2	**Documents** Your scope, risk assessment, Statement of Applicability, policies and records.
3	**Interviews and testing** Sessions with control owners and tests of the controls on evidence.
4	**Closing meeting** Nonconformities and observations discussed before the report is final.
5	**Audit report** The report for your management review and the certification body.

A guide, not a fixed promise: the length of each phase depends on your scope and on how quickly evidence and people are available.

Regulations That Ask for It

ISO/IEC 42001	The internal audit clause 9.2 of ISO/IEC 42001 requires for your AI management system, by an auditor independent of it, timed so your findings are closed before the certification body arrives.
QCB AI Guideline (Qatar)	

Why Work with GRC+ on ISO 42001 Audits

An independent lead auditor	Audits are led by an experienced lead auditor who is independent of your AI management system.
Findings graded like the certification body	You see which findings would be major or minor nonconformities, so you fix the right things first.
Impartial by design	We do not implement your AI management system when we audit it, so the audit meets clause 9.2.
One audit, more frameworks	Our mappings link ISO 42001 to the EU AI Act and ISO 27001, so the evidence serves those reviews too.

Questions Buyers Ask

Can our own staff do the internal audit?

Only if they are independent of the work they audit. Many organisations use an external auditor so the audit is clearly independent and the certification body can rely on it.

How long before the external audit should we do it?

Leave enough time to correct nonconformities, usually a few weeks to a few months before your certification or surveillance audit.

Do we have to audit every Annex A control each year?

No. Clause 9.2 asks for an audit programme at planned intervals. Most organisations cover the management system every year and the Annex A controls across the three-year certification cycle; we plan it with you.

Can you also help us set up ISO 42001?

Yes, as a separate engagement, for example through our AI Governance Officer service. To keep the internal audit impartial, we do not audit the parts of the management system we helped build.

Talk to Us

Tell us your certification status, scope and the date of your next external audit. We send a written proposal with scope, dates and a fixed fee.
Book a 30-Minute Call · sales@grc.plus · grc.plus/service/iso-42001-internal-audit

