

ISO/IEC 27001 Readiness vs Independent Internal Audit: The Enterprise Evidence & Impartiality Guide



IG-Smart Ltd · Practical Guide Collection · 25 October 2026

General information and original working aids; not legal advice, certification, clinical authorisation or regulatory approval. NHS identity appearing in retained illustrative artwork does not imply NHS approval or endorsement.

Use this guide to make a better-evidenced decision. This is general information and an original working aid, not a client-specific legal opinion, certification, clinical safety authorisation or regulatory approval. Apply the relevant jurisdiction, current requirements and competent professional review to your circumstances. Examples are illustrative unless expressly attributed.

Your first three steps

1. Identify whether you need preparation, an internal audit or certification.
2. Document who implemented or operates the work to be audited.
3. Use the evidence checklist and independence decision tree to define the assignment.

How to distinguish implementation preparation from a Clause 9.2 audit, protect auditor objectivity, assemble defensible evidence and navigate accredited certification.

Executive answer: readiness is not the internal audit

ISO/IEC 27001 readiness assesses whether an organisation has established, implemented and evidenced an information security management system (ISMS) capable of meeting its chosen objectives and applicable ISO/IEC 27001 requirements. It may include gap assessment, risk-treatment planning, documentation, control design, testing and management support. Its purpose is to identify and close gaps before formal assurance. [S1]

The ISO/IEC 27001 Clause 9.2 internal audit is a distinct, planned and impartial assessment. It tests whether the ISMS conforms both to ISO/IEC 27001 and to the organisation's own ISMS requirements, and whether the system has actually been implemented and maintained effectively. The organisation must plan an audit programme, define criteria and scope for individual audits, select auditors so the audit process is objective and impartial, report findings to relevant management and retain evidence of the programme and results. [S1][S2]

Third-party certification is a further, different activity undertaken by a certification body, with its own impartiality, competence, accreditation and certification decision arrangements. ISO and UKAS do not themselves certify an organisation's ISMS. [S5][S6][S7]

Buyer decision: Purchase readiness when you need to prepare or remediate the ISMS; appoint a suitably objective internal-audit function when you need Clause 9.2 assurance; engage an appropriate certification body when you require third-party certification. Do not treat the three as interchangeable, or ask an adviser to independently certify the effectiveness of its own work.

Inside this guide: A service comparison, Clause 9.2 programme guide, IG-Smart Audit Independence Gate (original decision framework), conflict and responsibility matrices, 20-domain evidence crosswalk, 32-point practical checklist, findings and remediation model, certification-body selection controls, executive decision briefing and procurement questions. A separately editable worksheet includes the decision tree, conflict assessment and audit evidence register.

1. Three activities, three different claims

Dimension	Readiness / gap assessment	Clause 9.2 internal audit	External certification audit
Question	What is missing or ineffective, and how do we prepare?	Does the ISMS conform and operate effectively under defined criteria?	Does the ISMS meet the certification requirements?
Sponsor	ISMS owner, executive sponsor, programme lead	Organisation's audit programme and relevant management	Organisation commissions an independent certification body
Typical timing	Before or during implementation; whenever scope or risks change	At planned intervals under the audit programme, including before initial certification where required for readiness	Initial Stage 1 / Stage 2 and subsequent ongoing certification activities under the body's scheme
People	Internal team or adviser who may help design/remediate	Competent internal or external auditors acting on the organisation's behalf, selected to support objectivity and impartiality	Audit team and impartial certification decision personnel of a certification body
Permitted work	Advising, identifying gaps, helping implement controls where contracted	Examining evidence, sampling operation, reporting findings, evaluating conformance	Independently assessing for certification and making certification decisions
Conflict boundary	May implement the very controls under review	Must avoid self-review and manage bias; do not assign authors to audit their own implementation	Certification body must protect impartiality and observe relevant restrictions on consultancy and internal auditing
Expected output	Gap register, prioritised action plan, governance/evidence map	Audit plan, sampling record, evidence, findings, report, follow-up	Certification body reports, nonconformities and, if successful, a certificate covering a defined scope
What it does not establish	Clause 9.2 completion or certification	Third-party certification or an independent certification decision	Permanent security, guaranteed contractual acceptance or the absence of risk

Important nuance: An internal audit need not always be carried out by an external company. Clause 9.2 requires objectivity and impartiality, not a blanket external-auditor mandate. An external consultant may conduct the organisation's internal audit, but the same risk of self-review arises where the consultant designed, operated or materially controlled what is being audited. ISO 19011:2026 provides guidance on independence and evidence-based, risk-based auditing. [S1][S3]

Buyer-trigger situations

What the buyer says	What to commission or check first	Why
"A prospect wants our ISO 27001 certification before contracting."	Confirm the precise procurement requirement, intended certification scope, timescale and accredited-body expectation; assess readiness	A client requirement is not the same as a certificate already issued
"We have the policies but almost no operating evidence."	Readiness and operating-evidence remediation	A document set does not demonstrate the controls work
"We need our annual ISO audit."	Verify the documented audit programme and actual scope; arrange a competent objective audit if due	The standard specifies planned intervals, not a universal fixed annual interval

What the buyer says	What to commission or check first	Why
"Our implementation consultant offers to certify our programme."	Clarify what is offered and by whom; reject conflation	Consultants cannot substitute their opinion for a certification-body decision
"The CISO who designed the controls can check their own programme."	Independent assignment or conflict mitigation and a separate objective audit	Self-review creates an impartiality risk
"Our certification audit starts next month."	Validate internal-audit completion, management review, evidence, issues and certification body's readiness conditions	A rushed audit does not cure missing operational evidence
"We already passed Stage 1; is that our internal audit?"	Check Clause 9.2 evidence separately	Certification-body Stage 1 is not the organisation's internal audit programme
"We changed our cloud platform and scope."	Reassess material risks, controls, SoA, evidence and audit programme	Significant change may alter the necessary audit coverage and evidence

2. What ISO/IEC 27001 readiness actually involves

An ISMS is a management system for information security risks, not merely an IT hardening checklist. ISO/IEC 27001:2022 establishes ISMS requirements; its 2024 climate-action amendment adds context-related considerations. Organisations should assess whether climate change is relevant to their ISMS context and interested-party requirements, without assuming it creates a prescribed cybersecurity control for every company. [S1][S9]

A robust readiness engagement typically works through six practical activities, selected according to scope rather than sold as a fixed bundle:

- 1. Define the intended ISMS boundary.** Confirm entities, services, locations, people, suppliers, cloud environments, data, contractual commitments and exclusions. A neat scope statement that omits a critical outsourced process will not survive meaningful review.
- 2. Understand requirements and information security risks.** Review context, interested parties, security objectives, applicable legal/contractual obligations, risk assessment methodology, risk ownership and treatment decisions.
- 3. Evaluate control selection and rationale.** Confirm the Statement of Applicability (SoA), control-treatment decisions, relevant Annex A references and evidence that selections and exclusions are justified. The 2022 Annex A contains 93 reference controls across organisational, people, physical and technological themes; it is not a rule that all 93 are mandatory in every ISMS. [S1][S8]
- 4. Test evidence of implementation.** Follow representative processes: joiner/mover/leaver, asset changes, supplier onboarding, incidents, backup/restore, access review, logging, vulnerability management and secure development where applicable. Distinguish control descriptions from proof of control operation.
- 5. Prepare leadership and assurance mechanisms.** Check monitoring and measurement, management review, corrective action and a suitably impartial internal audit programme. Readiness work can prepare the materials but must not be labelled an independent audit merely because it reviewed records.
- 6. Agree a decision-based remediation plan.** Record finding, risk, owner, action, due date, dependency and acceptance evidence. The client retains management accountability for risk treatment and the decision to proceed.

The difference between a gap and a nonconformity

During readiness, advisers may call issues "gaps", "observations" or "potential nonconformities". Their labels should not imply that a Clause 9.2 audit took place. An actual internal-audit nonconformity must be grounded in defined audit criteria and objective evidence. Severity classifications should use a disclosed methodology; neither ISO/IEC 27001 nor this guide imposes a universal major/minor grading scheme on every internal audit. Certification bodies may use scheme-specific grading and closure requirements.

Readiness outputs a buyer can defend

Output	Buyer acceptance test
ISMS scope and applicability note	Can leadership explain what the system covers and why?
Requirements/obligations register	Can requirements be traced to owners, processes and evidence?
Risk assessment and treatment record	Is the methodology applied consistently, with residual risk ownership?
SoA review	Can each selection/exclusion be explained and reconciled with risk decisions?
Evidence sufficiency register	Does it distinguish current operational proof from a policy statement?
Readiness gap register	Are gaps linked to a requirement, accountable owner and remediation plan?
Internal-audit handoff record	Are the reviewer's implemented activities separated from the later independent audit assignment?
Executive readiness briefing	Are unresolved high-consequence exceptions presented plainly, without a false assurance of certification?

Readiness creates informed decisions and improved evidence. It cannot guarantee that another auditor will accept every interpretation or that a certification body will issue a certificate.

3. Clause 9.2: the assurance obligation in practical language

The 2022 edition separates internal-audit requirements into **9.2.1 (general purpose)** and **9.2.2 (audit programme)**. The following is an original practical summary, not a reproduction of the copyrighted standard. Buyers and auditors must check the licensed, current normative text. [S1][S2]

Clause 9.2 theme	Meaning for an ISMS	Evidence an enterprise should retain
Planned intervals	Audit on a defined, appropriate schedule informed by ISMS risks and changes	Approved programme and rationale for frequency
Conformance to ISO requirements	Test relevant applicable requirements	Criteria-to-evidence mapping and results
Conformance to own ISMS requirements	Test whether documented procedures, policies and self-imposed commitments are followed	Process testing, interviews and evidence samples
Effective implementation and maintenance	Examine actual operation, not just documents	Sampling records and observed outcomes over meaningful periods
Programme governance	Define frequency, methods, responsibility, planning and reporting	Documented audit programme and roles

Clause 9.2 theme	Meaning for an ISMS	Evidence an enterprise should retain
Prioritisation	Consider critical processes and previous audit results	Risk-based programme rationale and prior findings
Audit-by-audit criteria and scope	Specify applicable requirements, period, processes, entity and exclusions	Audit plan, scope and criteria
Objectivity and impartiality	Choose auditors and arrangements that mitigate conflicts and bias	Independence declarations and assignment approvals
Reporting	Report results to relevant management	Dated report, distribution, actions and management receipt
Retained documented information	Preserve evidence of both programme implementation and results	Controlled reports, evidence index, follow-up records

Do not confuse an audit programme with an audit event. One concentrated audit may cover much of an initial scope, but ongoing assurance requires a documented programme with appropriate coverage. Equally, an organisation should not assert that every Annex A control must be audited on every occasion; coverage, materiality, risk and scope should be justified, and the whole programme must provide meaningful assurance.

Can a company audit itself?

Yes, in the sense that internal audits are first-party audits undertaken by or on behalf of the organisation. An organisation may assign competent employees who are independent of the activity examined, or external auditors operating on the organisation's behalf. The key test is not whether the auditor's business card says "external"; it is whether the audit is competent, evidence-based, objective and impartial. [S3][S4]

For a small organisation, complete structural separation may not be feasible. That does **not** legitimise having someone sign off the effectiveness of work they own without controls. Document the constraint and consider independent peer review, a separate external auditor or a carefully defined alternative arrangement. Where material self-review cannot be mitigated, the proposed work should not be represented as an impartial Clause 9.2 audit.

Do not postpone necessary internal audit merely to conceal immaturity. An audit can identify missing evidence, nonconformities and limitations. The question is whether the assignment has appropriate scope, access and competence, not whether the organisation can already demonstrate perfection. Management should address findings through its corrective-action process rather than relabel a readiness review as an audit.

What an independent audit should produce

An appropriately scoped engagement should normally deliver a clear audit plan and criteria; a defensible sampling methodology; referenced objective evidence; findings or an explicit explanation where no nonconformities were identified in tested samples; a conclusion with scope and limitations; communication to relevant management; and documented follow-up responsibility. The buyer should be able to trace a finding through **criterion -> evidence -> judgement -> responsible owner -> correction/corrective action -> effectiveness review**.

4. The IG-Smart Audit Independence Gate (original practitioner framework)

Purpose: Determine whether a proposed person or provider can credibly conduct a Clause 9.2 internal audit of a given ISMS scope, and whether the engagement is being confused with readiness or accredited certification.

Status: An illustrative IG-Smart decision-support model, not a standard, accreditation decision, legal opinion or substitute for an organisation's formal auditor selection controls.

The seven decision gates

Gate	Question	Green: proceed	Amber/red: action required
G1 - Assignment	Is the buyer requesting readiness, first-party audit or third-party certification?	Service and contractual label match actual purpose	Re-scope; do not sell an implementation review as independent audit
G2 - Authority	Who appoints the auditor and receives conclusions?	Organisation retains audit programme and management accountability	Clarify authority and reporting independence
G3 - Self-review	Did this auditor/team design, implement, own or manage activities it must judge?	No material self-review in assigned scope	Separate people/scope or appoint a genuinely independent reviewer
G4 - Commercial influence	Could fees, incentives, prior advice or relationships distort findings?	Conflicts disclosed and credibly mitigated	Reassign or decline the relevant audit work
G5 - Competence	Does the auditor understand the standard, ISMS risks, audit methods and sector context?	Demonstrable competence and adequate capacity	Appoint a suitably qualified auditor/team
G6 - Evidence authority	Can the auditor access records, interview owners and report unfiltered findings?	Agreed unrestricted access, protected confidentiality and reporting rights	Correct engagement terms or do not issue assurance
G7 - Certification boundary	Is an accredited certificate being represented or promised?	Certification decision remains exclusively with the selected certification body	Stop misleading claims and verify body/accreditation/scope

Hard stop: A high score on commercial convenience or cost cannot compensate for a material, unmitigated self-review or certification-body conflict.

Accessible decision tree

- 1. Is the need a certification decision?** If yes, obtain proposals directly from suitable certification bodies; verify recognition and scope. No consultant internal-audit report is a certificate.
- 2. Is the need to design, strengthen or remediate the ISMS?** If yes, scope readiness/implementation support. Do not market the resulting gap report as a Clause 9.2 audit.
- 3. Is the need a Clause 9.2 internal audit?** Check the documented programme and define audit scope, criteria, period and reporting authority.
- 4. Has the proposed auditor, or the same delivery team, designed, implemented, operated or owned the controls being audited?** If yes, document the activities and risk of self-review. Separate the auditable activities or appoint an independent party for the affected scope. If a material risk remains, do not assign the audit.

5. **Is there another financial, employment, managerial, certification or personal conflict?** If yes, assess whether credible safeguards remove the risk. If not, reassign.
6. **Is the auditor competent, able to obtain evidence and free to report unwelcome conclusions?** If not, remedy or select another auditor.
7. **Can the organisation retain sufficient programme, execution, reporting and follow-up evidence?** If yes, conduct the audit. If not, agree controls before relying on the result.

Decision examples

Proposed arrangement	Independence assessment	Defensible next action
Developer of the ISMS policies offers to audit those same policies	Material self-review risk	Use a distinct, impartial auditor for that work
Separate internal auditor has not owned or operated examined controls	Potentially acceptable	Check competence, reporting independence and actual conflicts
External auditor with no prior role in implementation	Potentially acceptable	Verify competence, scope, conflicts and objective reporting
Consultant conducted a high-level readiness review only, without implementing controls	Case-specific, not automatically forbidden	Assess whether prior advice compromises the planned audit judgement; document separation and any remaining risk
Same consulting firm sends a different team after extensive hands-on implementation	Separation of personnel alone may be insufficient	Assess organisational and commercial conflicts; external independent audit may be safer
Certification body proposes the client's internal audit as part of a consulting bundle	Certification impartiality red flag	Request written clarification from the accredited body; avoid the arrangement
The buyer pressures the auditor to remove an evidence-supported finding	Reporting-integrity failure	Escalate to audit sponsor and retain objective record

IG-Smart service boundary: IG-Smart does not independently audit an ISMS it helped implement in the same cycle. Merely assigning a different colleague does not override this firm policy. Auditor competence, objectivity and conflicts are checked before acceptance. Readiness support, management review and independently commissioned internal audit remain distinct engagements.

5. Who owns what? A defensible responsibility map

Activity	Management / ISMS owner	Readiness adviser	Clause 9.2 internal auditor	Certification body
Define business and ISMS scope	Accountable	May advise	Tests the scope and evidence	Independently assesses certification scope
Accept risks / resource decisions	Accountable	May recommend	Reports on decision processes	Assesses relevant requirements
Design and implement controls	Accountable	May support where contracted	Must avoid auditing own work	Must protect certification impartiality
Maintain evidence	Accountable	May organise/prepare	Samples and verifies	Samples and verifies for certification
Establish internal-audit programme	Accountable	May advise without compromising independence	May assist in programme governance within appropriate role	Does not replace the buyer's first-party programme

Activity	Management / ISMS owner	Readiness adviser	Clause 9.2 internal auditor	Certification body
Conduct objective Clause 9.2 audit	Selects/authorises competent auditor	Not automatically part of readiness	Responsible within assigned scope	Must not be treated as the client's internal auditor
Correct findings	Accountable	May provide separately scoped remediation	Tests follow-up as appropriate, protecting objectivity	Reviews closure under the certification scheme
Certification decision	No	No	No	Only the certification body

Risk ownership does not transfer: An audit finding does not instruct the organisation to accept a particular risk, spend a fixed amount or select a particular product. Management owns decisions and demonstrable follow-up. Independent audit adds challenge; it does not replace leadership accountability.

6. The evidence crosswalk: 20 high-value domains

The crosswalk below is an **illustrative request and sampling framework**, not a claim that every organisation must keep the same document title or all Annex A controls. Audit criteria must derive from the licensed standard, the organisation's own ISMS arrangements and relevant obligations. The relevance of an evidence item depends on scope and risk. [S1][S3][S4]

Evidence domain	Representative evidence / sampling approach	Readiness challenge	Internal-audit assurance question
1. Organisational context	Context assessment; interested parties; climate relevance where appropriate	Are relevant external/internal issues understood?	Does context genuinely influence ISMS decisions?
2. ISMS scope	Approved boundaries; entity, system and outsourced-service inventory	Does scope omit critical dependencies?	Is scope reasonable and consistently applied?
3. Leadership and governance	Policy approval; roles; executive minutes	Is accountability allocated and resourced?	Is leadership engagement evidenced in practice?
4. Information security objectives	Measurable objectives and progress reviews	Are aims meaningful and monitored?	Do reported results support effectiveness claims?
5. Risk assessment methodology	Risk criteria, assessments, change events	Is method documented and consistently applied?	Do sampled risks follow criteria and actual treatment?
6. Risk treatment and SoA	Treatment plan, decisions, SoA, control rationale	Are justifications current and traceable?	Do selections/exclusions match risks and operation?
7. Legal/contractual requirements	Applicable obligations and control mapping	Are requirements identified with owners?	Are selected obligations demonstrably addressed?
8. Competence and awareness	Roles, training, outcomes, interviews	Are training activities appropriate?	Can sampled people fulfil assigned ISMS duties?
9. Documented-information control	Version, approval, access and retention practices	Can the team find reliable current records?	Are required ISMS records controlled and available?
10. Asset inventory and classification	Hardware, SaaS, data and ownership samples	Are assets and owners known?	Are changes captured and classifications applied?
11. Identity and access	Joiner/mover/leaver events; privilege reviews; MFA	Are procedures actually run?	Do transaction samples match approved access rules?

Evidence domain	Representative evidence / sampling approach	Readiness challenge	Internal-audit assurance question
12. Supplier and cloud security	Supplier due diligence, responsibilities, periodic review	Are outsourced dependencies under control?	Is review proportionate and evidenced over time?
13. Secure development/change	Change requests; reviews; testing; deployment samples	Are critical controls integrated into delivery?	Do changes meet declared gates in actual samples?
14. Vulnerability/patch management	Scans, triage, exceptions, patch verification	Are backlogs and exceptions managed?	Are remediation priorities justified and followed?
15. Incident management	Incidents, drills, notifications, lessons	Are roles and escalation mechanisms workable?	Do records show execution, learning and correction?
16. Backup and resilience	Restore tests, backups, recovery assumptions	Has recovery actually been exercised?	Does evidence support recovery commitments?
17. Physical/environmental security	Site or provider assurance appropriate to scope	Are dependencies and responsibility boundaries clear?	Does sampled evidence address actual applicable risks?
18. Monitoring and measurement	Control measures, trends, security reviews	Are effectiveness measures meaningful?	Does management act on adverse results?
19. Internal audit and management review	Programme, report, minutes, decisions	Is the required assurance cycle ready and independent?	Are programme, reporting, review and follow-up functioning?
20. Nonconformity and improvement	Actions, root-cause analysis, effectiveness checks	Are unresolved issues transparently owned?	Were appropriate corrections made and checked?

Sampling note: Audits use selected evidence within defined periods. A clean sample is not a guarantee that every transaction or control is flawless. The report should disclose tested processes, sampling boundaries, unavailable records and uncertainty material to the conclusion.

What a strong evidence record looks like

A useful record has a stable identifier, relevant criterion, owner, system/process, period, source link, version, review date, confidentiality handling, sample selection, auditor evaluation and an outcome. Screenshots without timestamps, undocumented exported spreadsheets and policy PDFs with no operational linkage are generally weaker than traceable transaction records.

Four evidence traps

- **Paper-only compliance:** a policy says privileges are reviewed quarterly, but no review record exists.
- **Sample distortion:** a single recent test is presented as proof of ongoing performance without noting the period examined.
- **Scope mismatch:** supplier evidence relates to another legal entity, system, hosting environment or product release.
- **Unclosed audit trail:** findings are marked complete without evidence of correction, root-cause action or effectiveness verification where appropriate.

7. An evidence-based internal audit, from commission to follow-up

ISO 19011:2026 is published audit guidance; it is not itself a certifiable management-system standard. Select the current applicable audit guidance and licensed standards for the engagement. This guide's own readiness/internal-audit distinction is not a reproduction of ISO normative text. [S3][S4]

Stage A - Commission and independence declaration. Identify sponsor, recipient, ISMS boundary, criteria and reporting protocol. Examine the proposed auditor's previous consulting, control ownership, incentives and access to management. Record any mitigation before appointment.

Stage B - Risk-based programme and plan. Use prior findings, major changes, critical processes, contractual commitments and risk concentration to set frequency and coverage. Define exact scope and sampling rationale for each audit. "Audit all 93 controls tomorrow" is rarely a defensible plan by itself.

Stage C - Objective evidence collection. Interview owners, inspect controlled records, trace selected activities end to end and corroborate claims against actual outputs. Protect client secrets and sensitive information; minimise collection and restrict access.

Stage D - Fair assessment and reporting. Record criteria, objective evidence, findings, opportunities where permitted, and boundaries of assurance. Allow factual clarification without negotiating away evidence-supported conclusions. Report to relevant management.

Stage E - Correction and corrective action. Management decides containment, cause analysis, proportionate action, owner and completion date. The auditor or another appropriately independent reviewer verifies closure where required. A new procedure is not proof it works; examine later operation when feasible.

Stage F - Feed the continuing programme. Update risk, objectives, management review and future audit coverage. Independent audit should be a recurring decision process, not a ceremonial document obtained just before a certification visit.

How to write a defensible finding

Criterion: The organisation's approved access-review procedure requires periodic review of privileged accounts. **Sample:** Three of seven selected systems had no review record for the tested period. **Finding:** A documented process requirement was not consistently followed in the defined sample. **Impact:** Privileged access may remain unchallenged. **Owner:** Identity and Access Management lead. **Required management action:** Assess scope, risk, cause and corrective action, then retain verifiable follow-up evidence.

This is a fictional teaching illustration only; it is not an IG-Smart client finding, a real audit, or a mandated nonconformity grade.

Findings should distinguish five things

1. **Criterion** - the ISO/contractual/organisation-specific requirement actually assessed.
2. **Evidence** - what was observed, how, when and in which sample.
3. **Judgement** - conformity, nonconformity or an appropriately labelled observation.
4. **Decision** - accountable management's containment, risk and remediation response.
5. **Verification** - what shows implementation and effectiveness, not merely that a ticket was closed.

8. Certification-body boundaries: accredited certification is a separate decision

A buyer seeking certification must distinguish its own readiness adviser, its internal auditor and the independent body that can issue a certificate. ISO publishes the standard but does not certify organisations. In the UK, UKAS accredits qualifying certification bodies; UKAS does not perform IG-Smart's client certification. Accreditation applies to the certification body's specified competence and scopes, so the body's own accreditation schedule and the exact certificate should be checked. [S5][S6][S7]

ISO/IEC 17021-1 defines general management-system certification-body requirements, supplemented for ISMS by ISO/IEC 27006-1:2024. These include significant competence and impartiality safeguards. Do not assume that a readiness consultant can also act as the independent certifier; do not assume a certification body can provide the client's management-system consultancy or conduct its first-party audit and still certify the same client under accreditation requirements. Seek written advice from the chosen body about any complex relationships. [S5][S6][S10]

The common three-stage assurance journey

Internal preparation / readiness: The organisation develops and operates the ISMS and resolves gaps with internal resources or contracted support. It maintains its own risk, management-review and Clause 9.2 obligations.

Stage 1 certification audit: The independent certification body typically reviews preparedness, documented scope and relevant system information, and plans Stage 2. The precise process is governed by the body's scheme and applicable requirements. Stage 1 is **not** a replacement for the organisation's Clause 9.2 internal audit.

Stage 2 and certification decision: The body assesses implementation and effectiveness and makes an independent decision through its authorised process. Findings, remediation and follow-up depend on the scheme and evidence. Ongoing surveillance and recertification maintain the certification cycle. No adviser can promise a pass or issue a UKAS-accredited certificate by completing a gap checklist.

Seven certification-body procurement checks

Check	Procurement evidence
1. Is the body itself accredited for the relevant activity?	Current accreditation-body schedule / register
2. Is ISO/IEC 27001 certification within that scope?	Standard and scope in accreditation schedule
3. Will the intended legal entity and ISMS boundaries appear accurately?	Draft scope statement, legal-entity names
4. Are Stage 1, Stage 2, findings and surveillance arrangements transparent?	Proposal and scheme terms
5. Are impartiality and consultant relationships addressed?	Conflict disclosures and impartiality controls
6. Are sector, cloud and outsourced-process risks reflected?	Competence and audit programme planning
7. Is the resultant certificate verifiable?	Issuer, accreditation source, certificate identifier and current status

For certificates claiming UKAS accreditation, use the UKAS directory or CertCheck, as applicable; for recognised international accreditation, verify the relevant accredited body and current scope. A certificate that is out of scope, expired or issued without the required accreditation may not satisfy an enterprise tender. [S6][S7]

What about ISO/IEC 27001 certification claims by a consultant?

A consultancy may legitimately hold its own ISMS certificate. That is evidence about the consultancy's certified activities within the certificate's scope, **not** accreditation to certify clients and not proof that every client engagement meets ISO/IEC 27001. Claims must identify the holder, issuer and approved scope correctly and should not describe the consultancy as an "ISO-accredited certification body" unless that separate accreditation is verified.

9. Procurement and assurance: an original 10-point decision matrix

For a proposed supplier, answer each item with **Pass / Clarify / Fail**. This is an IG-Smart buyer tool, not a formal standard scoring method. Any material unresolved independence or misrepresentation issue is a **hard stop**, not something offset by a low fee.

Question	Pass evidence	Escalation trigger
1. What are we actually buying?	Contract identifies readiness, internal audit or certification	Interchangeable terms or misleading "certificate"
2. Is the requested scope defined?	Legal entities, locations, systems, period and exclusions documented	Vague or misleading boundaries
3. Who is accountable for risk decisions?	Named management owner	Adviser purportedly accepts business risk
4. Are audit criteria current?	Licensed 27001:2022 + amendment where applicable; own requirements	Outdated or invented obligations
5. Is auditor competence evidenced?	Relevant training, experience, ISMS and sector understanding	Credentials asserted without verification
6. Are conflicts disclosed?	Role/implementation history and safeguards	Self-review or commercial interference
7. Is sampling proportionate?	Documented coverage and rationale	"100% compliant" assertion from superficial review
8. Is operational evidence available?	Current, attributable records from actual processes	Policies only or missing evidence
9. Is reporting independent?	Direct reporting to appropriate management	Findings filtered by implementers
10. Is certification distinct?	Correct body, status, scope and decision route	Consultant or auditor claims accredited certification

10. The board and procurement decision briefing

Decision sought: [Commission readiness / commission impartial internal audit / shortlist accredited certification bodies / defer pending evidence]

Entity, ISMS scope and business requirement: [Reader to complete: organisation, products, contractual deadline and systems]

Reason for action: [RFP requirement, internal risk, first certification, surveillance, material scope change or observed control failure]

Current assurance position: [Policies/evidence in place; planned programme; last internal audit; available certification status]

Independence decision: [Who designed/operates controls; proposed auditor; material conflicts; safeguards; residual concern]

Evidence sufficiency: [Highest consequence missing records; known untested processes; current SoA and treatment plan]

Options:

- **Readiness first:** use when controls/evidence or ISMS governance are not sufficiently established.
- **Independent internal audit:** use when programme, operating evidence and impartial auditor assignment are ready.
- **Certification procurement:** use when the business requires a third-party certificate and the organisation can evidence readiness, subject to certification body's assessment.
- **Delay / targeted remediation:** use if evidence or independence defects make immediate audit unreliable.

Residual risks: [Owner, impact, due date, accepted exception and management sign-off]

Management decision and conditions: [Approved action, scope, budget owner, evidence acceptance conditions and next review]

Executive principle: "We have appointed independent audit" is a claim about the **quality and objectivity of the assessment process**, not a promise that the ISMS has no weaknesses.

11. Common mistakes that damage assurance credibility

Mistake 1 - Using an implementation gap report as the completed internal audit. A gap assessment may be valuable but does not become an impartial, scoped Clause 9.2 audit through relabelling.

Mistake 2 - Misstating independence. A different employee at the same vendor is not automatically independent where the firm materially designed and owns the subject being judged.

Mistake 3 - Treating "annual" as a universal ISO clause. The required frequency should be planned and justified against risk, process importance and previous audit results, as well as relevant certification requirements.

Mistake 4 - Treating all Annex A reference controls as universally mandatory. Examine the SoA, risks, control selection and actual obligations; do not audit against an invented 93-control mandate.

Mistake 5 - Mistaking penetration testing for a full ISMS audit. Security testing can inform evidence but does not evaluate all management-system governance requirements.

Mistake 6 - Claiming the client is "ISO certified" after Stage 1 or a pre-certification assessment. Certification arises only from the appropriate certification decision and covers the specified scope.

Mistake 7 - Closing an issue on paper. Confirm operational effectiveness where appropriate and report remaining uncertainty rather than treating new policy wording as proof.

Mistake 8 - Copying 2013 control numbering into a 2022 SoA. Verify edition, mapping and current scope; Annex A categories changed in 2022.

Mistake 9 - Using old ISO 19011 references without checking status. The current general guideline is ISO 19011:2026; published ISMS-specific guidance remains ISO/IEC 27007:2020 pending its revision. [S3][S4]

Mistake 10 - Publishing confidential security evidence. Audit workpapers and supplier records can contain exploitable details and personal data. Public guides should use illustrative, sanitised examples, not copies of client evidence.

12. Practical preparation checklist (32 checks)

This is a buyer's working list, not a claim that ISO mandates 32 specific records in identical formats. The companion worksheet expands each item into Owner / Status / Evidence / Next action.

Context and governance

- [] 01. Confirm the current legal-entity and ISMS scope boundaries.
- [] 02. Identify important business, regulatory and contractual obligations.
- [] 03. Review interested-party needs and climate relevance where applicable.
- [] 04. Identify accountable ISMS and executive owners.
- [] 05. Confirm policy, objectives and evidence of leadership oversight.

Risk and control framework

- [] 06. Approve and apply a consistent security risk assessment method.
- [] 07. Document material risks, owners and residual-risk decisions.
- [] 08. Maintain a current risk treatment plan and Statement of Applicability.
- [] 09. Validate control applicability, justification and mapped risks.
- [] 10. Identify outsourced-process and critical supplier dependencies.

Operation and records

- [] 11. Demonstrate access lifecycle control through sampled transactions.
- [] 12. Evidence privileged access and periodic review where required.
- [] 13. Confirm asset, data and cloud ownership records.
- [] 14. Evidence applicable supplier assurance and contractual controls.
- [] 15. Provide change/security development samples if in scope.
- [] 16. Provide vulnerability treatment and exception samples where applicable.
- [] 17. Provide actual incident handling and lessons evidence where available.
- [] 18. Confirm backup and recovery claims with proportionate evidence.
- [] 19. Retain competence, awareness and training evidence.
- [] 20. Control document versions and evidence access.

Audit objectivity and execution

- [] 21. Approve the Clause 9.2 audit programme and its risk-based coverage.
- [] 22. Define criteria, scope and tested period for the planned audit.
- [] 23. Record who designed, implemented and operates each audited process.
- [] 24. Obtain auditor conflict declaration and independent assignment approval.
- [] 25. Check audit team competence, authority and evidence access.

- [] 26. Define defensible sampling and confidential-evidence handling.
- [] 27. Retain finding-to-evidence traces and balanced audit conclusions.
- [] 28. Deliver the report to relevant management without suppression.

Decisions, correction and certification

- [] 29. Record management review, decisions and accepted risks.
- [] 30. Assign and track corrective actions with appropriate effectiveness checks.
- [] 31. Verify the selected certification body's accreditation, scope and independence if certification is sought.
- [] 32. Document management's proceed / remediate / defer decision and next review.

13. Questions enterprise procurement teams should ask

1. Are you engaged for readiness, a Clause 9.2 internal audit, or another clearly described assurance service?
2. What is the exact legal-entity, system and date range in scope?
3. Which edition and amendment of the standard will be used?
4. Who will lead and sign the audit; what relevant competence can be demonstrated?
5. Have you, your colleagues or affiliated businesses designed or operated the processes you will audit?
6. How will you document and manage self-review, fee, referral, certification or personal conflicts?
7. Can you report findings directly to the relevant governing owner without edit or suppression by the implementing team?
8. Which processes and risk themes will be sampled, and how is coverage justified?
9. How do you test operation, not simply review policies?
10. Which evidence will you collect, and what retention, security and confidentiality protections apply?
11. What exactly is delivered: plan, workpapers/index, findings report, management presentation and follow-up?
12. How are disagreements, factual corrections and nonconformity classifications handled?
13. How will outstanding actions and follow-up reviews be scoped and priced, if required?
14. What activities remain the client's responsibility?
15. If certification is sought, which accredited certification body will independently assess it?
16. Can any certification claims be independently verified and matched to the intended scope?

14. Buyer FAQs

Can our ISO 27001 consultant perform our internal audit?

Not automatically. Clause 9.2 requires objectivity and impartiality. A consultant who designed, implemented or operates the processes under review presents a self-review risk. Assess the actual work and relationships, document safeguards, and use an appropriately independent auditor for any scope where impartiality cannot credibly be maintained. [S1][S3]

Must we appoint an external internal auditor?

No blanket external-appointment rule appears in Clause 9.2. Competent internal personnel can perform audits where conflicts and bias are adequately controlled. External auditors may be useful when internal independence, competence or capacity is insufficient.

Is a readiness assessment the same as a Clause 9.2 audit?

No. Readiness helps establish gaps and plan remediation. A Clause 9.2 audit is a planned, objective and impartial evaluation against specified criteria, supported by audit-programme and results evidence.

Does ISO require us to conduct a full audit every 12 months?

The standard requires audits at planned intervals and an appropriate programme; it does not impose a universal 12-month interval in the Clause 9.2 wording. Actual coverage and frequency should reflect risk, important processes, previous audit results, significant changes and relevant certification arrangements. [S1]

Do we have to implement all 93 Annex A controls?

Not automatically. The SoA documents the rationale for needed controls and exclusions in light of risks and requirements. Control selection and implementation must be defensible, not a mechanical all-controls checklist.

Is penetration testing sufficient for an ISO 27001 audit?

No. Penetration testing can supply technical security evidence, but it cannot substitute for management-system auditing of governance, risk treatment, monitoring, management review, competence and other relevant requirements.

Can the internal auditor issue an ISO 27001 certificate?

No. The internal auditor reports to the organisation. Certification decisions are taken by a separate certification body. ISO itself does not issue certificates; UKAS accredits certification bodies rather than certifying your ISMS. [S5][S6]

Does a Stage 1 certification audit replace the internal audit?

No. Stage 1 is part of the external certification process; it does not discharge the organisation's Clause 9.2 responsibility.

Is a firm automatically independent if it sends a different consultant?

No. Different personnel may help, but organisational incentives, knowledge of previous implementation, ownership and contractual arrangements may leave material self-review risk. Evaluate and document the entire arrangement.

Is the certification body required to be UKAS accredited?

Not in every situation. Buyers must determine their contractual, regulatory and market-recognition requirements. Where UKAS-accredited certification is specified, verify the body and its current scope. Other internationally recognised accreditation arrangements may be accepted depending on procurement requirements. [S6][S7]

Does an ISO 27001 certificate guarantee there will be no breach?

No. Certification concerns a management system and defined scope assessed at a point and over a cycle. It cannot eliminate all cybersecurity threats, incidents or failures.

What if our audit identifies serious gaps just before an RFP deadline?

Disclose the actual assurance position, assess contractual requirements, prioritise risk-based remediation and seek a decision from the relevant owner. Do not present an incomplete internal audit, an unissued certificate or unsupported "pass" as completed assurance.

15. How IG-Smart supports distinct buyer needs

IG-Smart's governance-led services should be selected according to the client's actual assurance problem:

- [ISO/IEC 27001 Readiness](#) - assess the ISMS, identify gaps and support appropriate preparation or remediation within a separately agreed scope.
- [ISO/IEC 27001 Internal Audit](#) - provide a defined-scope, impartial Clause 9.2 audit where an acceptable independent assignment can be established. Any conflicting readiness implementation must be separated, independently audited or excluded from IG-Smart's independent audit remit.
- [Managed Cyber Governance & vCISO](#) - support ongoing governance capacity and board reporting, without mislabelling management support as an independent audit of the same work.
- [Managed Supplier Assurance](#) - help evaluate third-party evidence and risk within agreed commercial scope.
- [Jigsaw Create readiness case study](#) - read permission-approved evidence of an ISO/IEC 27001 readiness and cyber assurance engagement. This case must not be used to imply that IG-Smart performed an independent Clause 9.2 audit or achieved certification unless separately evidenced.

Recommended next action: Talk to a Senior Practitioner if you need to establish the appropriate service, independence boundary and evidence requirements. If you already have an RFP or defined scope, **Submit a Requirement** through the existing approved enquiry route. Do not submit confidential audit records through an unapproved form or assume an engagement has begun before a statement of work is agreed.

IG-Smart's working model: Assess -> Build -> Manage -> Assure -> Improve. The separation between advisory and assurance activities remains an explicit governance control, not a guaranteed package of services.

16. Sources, scope and currency

Date researched: 24 October 2026. **Review trigger:** ISO/IEC 27001 or 27007 revision, UKAS/IAF certification rule changes, material interpretation updates, IG-Smart service changes or materially misleading published examples. **Review cadence:** At least annually, sooner for significant changes.

Authoritative primary-source references

Independence and scope note: ISO/IEC 27001 requires an objective, impartial internal audit process; whether a particular practitioner can audit a particular scope depends on the actual work performed, influence over controls, reporting arrangements and safeguards. Do not infer that different individuals from the same supplier automatically eliminate a self-review threat; equally, the standard does not impose a universal requirement to hire an external auditor.

Copyright and accuracy note: ISO standards are copyrighted. This guide contains original explanatory summaries and IG-Smart illustrative frameworks, not full standard clauses, control catalogue or reproduction of the normative text. Authoritative interpretations require consultation of the licensed current standards and the relevant certification/accreditation arrangements.

Sources

- [S1] ISO — ISO/IEC 27001:2022, Information security management systems — Requirements. <https://www.iso.org/standard/27001>
- [S2] ISO/IEC 27001:2022 Clause 9.2.1 and 9.2.2. <https://www.iso.org/standard/27001>
- [S3] ISO — ISO 19011:2026, Guidelines for auditing management systems. <https://www.iso.org/standard/19011>
- [S4] ISO — ISO/IEC 27007:2020, Guidelines for ISMS auditing. <https://www.iso.org/standard/77802.html>
- [S5] ISO — ISO/IEC 27006-1:2024. <https://committee.iso.org/cms/live/live/en/sites/isoorg/contents/data/standard/08/29/82908.html>
- [S6] UKAS — Certification Body Accreditation. <https://www.ukas.com/accreditation/standards/certification-body-accreditation/>
- [S7] UKAS — Validating management system certificates; UKAS CertCheck. <https://www.ukas.com/accreditation/about/validating-ms-certificates/>
- [S8] ISO — ISO/IEC 27000 family / ISO/IEC 27002:2022 context. <https://www.iso.org/standard/iso-iec-27000-family/>
- [S9] ISO — ISO/IEC 27001:2022/Amd 1:2024, Climate action changes. <https://www.iso.org/standard/88435.html>
- [S10] ISO — Certification and conformity assessment; ISO does not issue certificates. <https://committee.iso.org/certification.html>