iGUIDE

ISMS

Information Security External Audits

iNFOSECBASE

Contents

A Guide to External Audits

Introduction

ISO 27001 external audits are conducted by independent UKAS accredited certification bodies to assess whether an organisation's ISMS complies with the requirements of the ISO 27001 standard. These audits are a mandatory step for organisations seeking ISO 27001 certification, establishing their commitment to information security to clients, partners and stakeholders.

The process typically involves two key stages: Stage 1 focuses on reviewing documentation to confirm the ISMS design aligns with ISO 27001 requirements, while Stage 2 involves a more detailed, on-site or remote evaluation of the ISMS's implementation and operational effectiveness, where the auditor examines policies, procedures and evidence of compliance. Successful completion results in ISO 27001 certification, demonstrating the organisation's commitment to information security best practices.

Choosing a Certification Body

Engage with your chosen certification body early in your implementation process and ensure that are UKAS accredited.

When choosing your certification body, consider recommendations from other business, online reviews, their location, their reputation etc.

It’s a good idea to retain the same provider for your external audit programme as they will become familiar with your ISMS and, hopefully, build a rapport with the ISMS manager and team. Shortlist your preferred certification bodies and request at least 2 or 3 quotes before making a decision; the quotes will generally include a 3-year programme: Stage 1, Stage 2, Year 1 and 2 Surveillance and Year 3 Re-certification audits.

Stage 1 Audit

Aim

The aim of the Stage 1 Audit is to achieve the auditor's recommendation to proceed to the Stage 2 Audit.

Format

- Conduct an initial review of your ISMS documentation to assess its readiness for certification.
- Assess the documentation in your Requirement clauses (clauses 4 to 10) and confirm that they are supported by relevant policies, processes and procedures.
- Confirm that your controls (policies, processes and procedures) are accurate and relevant to your organisation.
- Confirm that relevant risks have been identified and that controls are in place to mitigate them.
- Verify that you have established and documented the necessary policies, procedures and controls required by ISO 27001.
- Identify any gaps or areas for improvement that need to be addressed before proceeding to the next stage.

Outcomes

There are two potential outcomes subsequent to the Stage 1 Audit:

- **Not recommended to progress to Stage 2 Audit**: this outcome is uncommon if the ISMS implementation is well managed; if not recommended, it will generally be the result of a systematic failure of the ISMS due to significant lack of leadership commitment and support.

  In this case the certification body will outline the issues that require addressing and the actions necessary to rectify the issues; it may be necessary to repeat the Stage 1 audit.
- **Recommended to progress to Stage 2 Audit**: once the Stage 1 Audit has been successful there's a strong probability that some Nonconformities (NCs) and/or Opportunities for Improvement (OFIs) will be identified (this is usual).

  Any nonconformities will need to be addressed, actioned and evidenced prior to the Stage 2 Audit and OFIs should be logged, considered and addressed if practicable or, if not actioned, the reason should be justified.

Store a copy of your Stage 1 Audit Report in the External Audit Reports folder.

Before the Stage 2 Audit it is best practice to complete a minimum of 2 internal audits; these should be planned in your ISMS Internal Audit Programme.

Stage 2 Audit

Aim

The aim of the Stage 2 Audit is to prove to the certification body that your ISMS is compliant with, and operating within, the parameters of the ISO27001:2022 Standard and that your organisation is operating in accordance with the policies, processes and procedures defined in your ISMS. The auditor will want to see that your organisation is delivering a sufficient level of information security adequate and proportionate to the identified risks to your organisation's information.

Format

Having conducted the Stage 1 Audit, the auditor will be familiar with your organisation, ISMS and approach to information security management.

During the course of the Stage 2 Audit, they will want to see evidence that you are operating in accordance with your ISMS and will want to see evidence that the details defined within your policies, processes and procedures are actually in practice. The auditor will also want to see evidence that you are testing the effectiveness of your ISMS (e.g. monitoring, evaluating, MRT meetings, auditing) and are managing and logging continual improvement.

The Stage 2 Audit is much more thorough than the Stage 1 Audit and is generally completed over three to five days, depending on the certification body and the size and scope of the organisation (some large businesses may require a significantly longer audit).

this will be either an on-site audit (wholly or partially) or a fully remote audit where the auditor will:

- Conduct an assessment to verify the implementation and effectiveness of the ISMS.
- Ensure that any findings from the Stage 1 Audit have been logged, managed and tracked and that all nonconformities have been actioned and closed.
- Ensure that the senior management team are providing sufficient leadership and support by ensuring that all necessary resources are available to ensure the effective management of the ISMS. They will want to interview (see 'Certification Body External Auditor Potential Questions' below):
    - Departmental personnel
    - Representative(s) from the Senior Management Team (SMT)
    - ISMS Team members (to discuss the policies, processes and procedures for which they're responsible)
    - Organisational personnel (to confirm awareness of the ISMS and Information Security in general)
- Review documentation and examine evidence to ensure that the ISMS is being followed as documented.
- Conduct a physical inspection either in person or virtually.

- Assess your organisation's compliance with ISO 27001:2022 requirements and identify any nonconformities and opportunities for improvement.
- Provide feedback on areas of strength and areas requiring improvement.

The auditor will also want to verify that:

- The Information Security Objectives are being achieved.
- The Risk register is being maintained and updated as scheduled.
- The Information Security Awareness programme is being maintained and operated.
- Any competence gaps have, or are being, addressed.
- Performance monitoring is being maintained.
- The internal audit programme is adequate and adhered to with all corrective actions logged, tracked and managed.
- The ISMS Management Review Team (MRT) meetings programme is adequate and adhered to with all actions logged, tracked and managed.
- Where Security Incidents have been identified that they have been logged, tracked and managed.

Non-Conformity Resolution

If any non-conformities are identified during the audit, you must:

- Develop and implement a corrective action plan to address them.
- Provide evidence of corrective actions taken to the certification body (usually within 10 days) for review and verification.

Certification Decision

- Based on the findings of the audit, the certification body makes a decision regarding ISO 27001 certification.
- If the organisation has successfully demonstrated compliance with ISO 27001:2022 requirements and has addressed any identified nonconformities, the certification body issues an ISO 27001:2022 certificate.
- The certificate is typically valid for a specific period (generally 3 years), subject to the successful completion of annual surveillance audits to maintain certification.

Outcomes

There are two potential outcomes subsequent to the Stage 2 Audit:

- **Not recommended for certification**: this means that the organisation has not met the necessary requirements to achieve certification for its ISMS. This outcome indicates that significant nonconformities were found during the audit, which prevent the organisation from demonstrating adequate implementation of the standard's requirements.

  The organisation will need to address all major nonconformities and potentially some minor ones. They must implement corrective actions and may need to undergo a partial or full re-assessment, depending on the certifying body’s guidelines.

After addressing the issues, the organisation can schedule a follow-up audit to verify compliance with ISO 27001. If the corrective actions are effective, certification may be recommended.

Receiving a "Not Recommended for Certification" outcome isn't a failure but an opportunity to close gaps; it's part of the certification process for identifying and resolving weaknesses to strengthen the ISMS before certification is granted.

- **Recommended for certification**: this means that the organisation has successfully demonstrated that its ISMS meets the requirements of the ISO 27001 standard. This is a positive outcome indicating that the audit found no major non-conformities and that any minor non-conformities identified do not prevent the organisation from achieving certification.

  Store a copy of your Stage 2 Audit Report in the External Audit Reports folder.

Surveillance Audits (AKA Continuing Assessment Visits [CAV])

After initial certification, the organisation undergoes periodic surveillance audits, typically at the end of years 1 and 2 following certification, conducted by the certification body to ensure ongoing compliance with ISO 27001.

The organisation must continue to demonstrate the effectiveness of its ISMS and address any non-conformities identified during surveillance audits.

Recertification Audits

Once achieved, the certification certificate is valid for three years, subject to the outcome of your annual surveillance audits.

At the end of the 3-year surveillance period, a recertification audit is undertaken; this will be similar in detail and intensity to the stage two audit.

The recertification audit explores the same areas as surveillance audits but looks more deeply into the holistic and global implications of your implementation strategy. It reviews the whole of the ISMS processes and systems from beginning to end, as well as investigating the organisation's sustained commitment to continual improvement.

External Audit Preparation

External Audit Document Requirements

Below is a list of typical documents/evidence that an external auditor may want to see prior or during an ISO 27001 audit:

Examples

- ICO Registration Certificate (ensure you're in the correct tier)
- Copy of the ISO/IEC 27001:2022 Standard
- Employers' Liability Insurance (with whom and when does it expire)
- Scope Statement
- Interested Parties
- Information Security Policy (signed & dated)
- Organisation Chart
- Main Internal & External Issues that could affect the organisation
- Risk Register/Matrix
- Risk Management Methodology
- Planning of Changes
- Statement of Applicability
- Access Control Policy
- Business Continuity Plan
- Business Continuity Test details (within the last 12 months)
- Penetration Testing details (within the last 12 months)
- Information Security Objectives, how they are measured and results
- Staff Handbook (if applicable)
- Training Matrix (or details of training, qualifications, competence, certificates achieved by individuals)
- Security Awareness Training Program and attendance record/results
- Controlled Document Register
- Asset Inventory
- Details of Office Security (if relevant)
- Details of Equipment Maintenance
- Details of the most recent recruit
- Supplier/Customer Agreements and NDAs
- Two or three internal audits.
- Minutes of the most recent management review
- Corrective and Preventive Action Log (CAPA)
- Evidence of Non-conformities and Remediation Action
- Legal Register plus details of how you ensure you stay legally compliant
- Fire Equipment (inspected by whom and when, if applicable)
- Date of last fire evacuation drill (if relevant)

Certification Body External Auditor Potential Questions

Below are a few questions that the ISO 27001 certification body auditor may ask interviewees during the audit process; it is not exhaustive but covers some of the most commonly asked questions.

Senior Management Team (SMT)

The external auditor often requests that a member of the SMT be present during the opening meeting and will generally ask for some background information about the company and the SMT responsibilities, for example:

- Provide an overview of the organisation and its history.
- What you do to lead information security and awareness?
- What are your responsibilities, e.g.
    - Participating in and providing active support of information security
    - Providing strategic direction and support to security initiatives
    - Participation in MRT meetings and risk analysis sessions
    - Development and design of information security controls
    - Reviewing of security policies and practices
    - Ensuring that adequate resources to maintain the ISMS are in place

General

The auditor may ask any of the below questions to any interviewee during the audit.

- What aspects of information security are relevant to your role?
- Have you seen a version of your organisation's Information Security Policy; do you know where to find it?
- Are you able to show me where the ISMS policies relevant to your role are and are you able to access them?
- If there was a cybersecurity incident, what would you do and who would you contact?
- Have you had any cyber security training; how often do you have it?

HR (A.6: People Controls)

The auditor will ask general questions during the audit and will also ask to see specific documentation; these will generally include examples of the below.

- Details of how recruitment is managed including screening/background checks
- Competency matrix for personnel involved in the ISMS
- Training records
- Staff DSE (Display Screen Equipment) assessments
- Staff Appraisal records (to ensure information security competence)
- Employee handbook

- Details of the most recent recruit:
  - Background checks
  - Contract
  - Start date
  - Job title
  - Job description
  - Induction date and Induction process/checklist

Facilities Management Department (A.7: Physical Controls)

In addition to the physical security controls, the auditor will ask in advance for specific documentation to be available and will, as a minimum, generally include the below.

Evidence of:

- PAT testing (if applicable)
- HVAC certificates (if applicable)
- Fire Equipment (inspected by whom & when, if applicable)
- Date of last fire evacuation drill (if relevant) and/or the last fire alarm test

IT Department (A.8: Technological Controls)

When covering the technical controls, the auditor will, where applicable, often ask to see the below evidence.

Technical evidence:

- Software Licence Agreements
- Cookie Reports
- Virus reports
- Patch Records
- Firewall Rules (screenshots or configurations showing firewall rules and changes)
- Restore Test Evidence (records or logs showing periodic restoration tests)
- Configuration Settings (screenshots or setup details of backup systems and configurations for critical systems)
- Encryption Evidence (proof of data encryption e.g. screenshots or configuration files)
- SIEM Logs (logs from Security Information and Event Management (SIEM) systems)
- Monitoring Alerts (alerts generated by monitoring systems and their resolutions)
- User Access Lists (evidence of access rights for systems and applications)
- Vulnerability Assessments/Scan Reports
- Penetration Test Report(s)
- IDS/IPS Logs

- System Access Files/Logs (system and application access logs showing who accessed what and when)
- Role-Based Access Controls (RBAC) (screenshots or system configurations showing access restrictions)
- Backup Policy/Logs (evidence of regular backup activities and successful completions)
- Network Diagrams (up-to-date network architecture diagrams)
- Change Logs (documentation of changes made to systems, networks and applications)
- Data Destruction Certificates (if applicable)

Summary

ISO 27001 external audits are independent evaluations performed by accredited certification bodies to assess an organisation's adherence to the ISO 27001 standard, which outlines best practices for information security management systems (ISMS). These audits are crucial for verifying that the organisation has implemented effective security controls, risk management processes and policies to protect sensitive information.

The purpose of these audits is not only to achieve ISO 27001 certification but also to provide an objective assessment of the organisation's information security posture. Certification demonstrates to customers, partners and regulators that the organisation is committed to safeguarding information assets and continuously improving its security measures. Regular surveillance audits are conducted after certification to ensure ongoing compliance and effectiveness, helping the organisation stay resilient against evolving security threats.