ISO/IEC 27001 Information Security Associate™

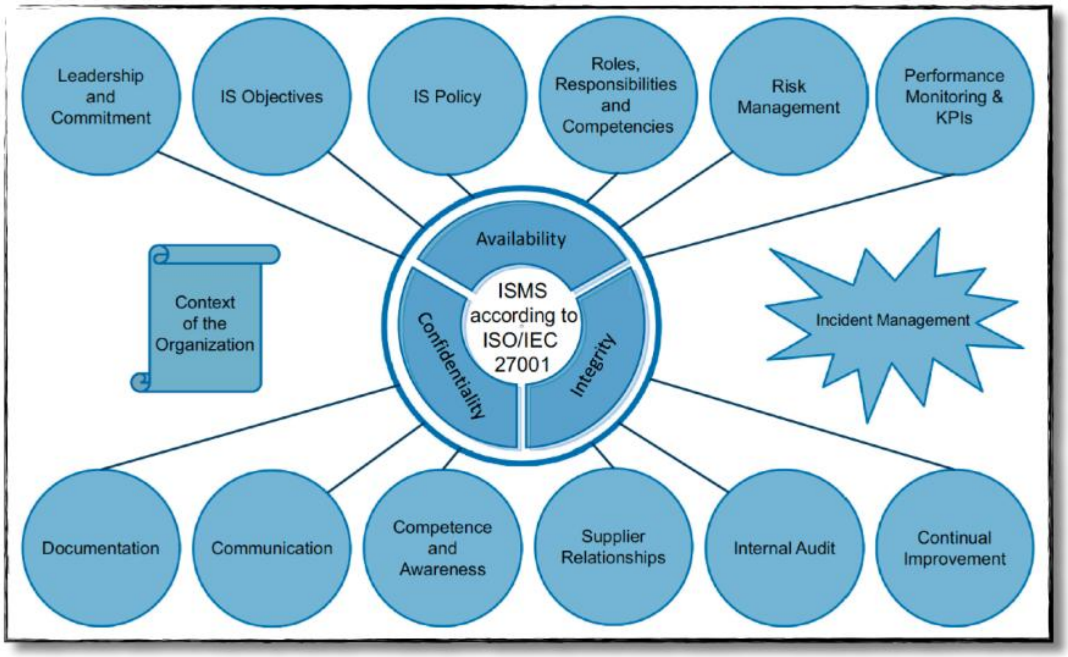
Table of Contents

  - Step 11. Implement Training And Awareness Programs
  - Step 12. Operate The ISMS
  - Step 13. Monitor The ISMS
  - Step 14. Internal Audit
  - Step 15. Management Review
  - Step 16. Corrective And Preventive Actions
- ISO 27001 - Roles And Responsibility In Organizations
  - Why Understanding Roles is Critical to the Security Program?
  - Five Typical Roles and Responsibilities
    - Security Leadership
    - Security Risk Management
    - Internal Audit
    - Control Owners
    - All Employees

ISO/IEC 27001 in Simple Terms

- **What it is:**
  ISO/IEC 27001 is an international standard that tells organizations how to manage information security in a structured way.
- **How it works:**
  - It sets up an **Information Security Management System (ISMS)** – a framework or governance system.
  - Through the ISMS, management identifies risks, decides how serious they are, and applies solutions (called controls).
  - It's not just a one-time setup – it keeps adapting as new threats and weaknesses appear.
- **Who can use it:**
  - Any type of organization: companies, government, NGOs.
  - Any size: from very small startups to very large multinationals.
  - Any sector: banking, defense, healthcare, retail, education, etc.
- **What it does not do:**
  - It **does not force every organization to use the exact same security controls**.
  - Because every business faces different risks, each organization chooses the controls that fit its own situation.
- **Controls (security measures):**
  - The standard points to **ISO/IEC 27002**, which is like a **menu of controls** (e.g., access control, backup, physical security).
  - Organizations pick from this menu based on their risks.
  - They can also add their own extra controls if needed (called extended control sets).

In short:
ISO/IEC 27001 gives you a **flexible framework** to manage information security risks. It doesn't say "do this exact thing," but instead says "look at your risks, then choose the right controls from the menu (27002) or others."



Components of an ISMS in accordance with ISO/IEC 27001

1. Selecting Controls (based on ISO/IEC 27002 "menu")

- Before choosing any security controls, the organization must first do a **comprehensive risk assessment** (find out what threats exist, what vulnerabilities they have, and what damage could occur).
- After that, management decides how to treat each risk. Options include:
  - **Avoid**: Stop doing the risky activity (e.g., not storing sensitive data at all).
  - **Share/Transfer**: Pass the risk to someone else (e.g., buy cyber insurance, outsource services).
  - **Accept**: Agree to live with the risk (if the impact is small or unlikely).
  - **Mitigate (control)**: Reduce the risk by applying security measures (like firewalls, encryption, backups).

This means not every risk requires a control — sometimes avoiding, sharing, or accepting is smarter.

2. A Brief History of ISO/IEC 27001

- **1999** → It started as **BS 7799 Part 2**, created by the British Standards Institute.
- **2002** → Revised to include the **Plan-Do-Check-Act (PDCA) cycle** (a quality management approach by Deming).
- **2005** → Adopted internationally by ISO as **ISO/IEC 27001 (1st edition)**.
- **2013** → Published **2nd edition** of ISO/IEC 27001. Major updates:

- Brought in line with other ISO management standards (like ISO 9001).
- PDCA cycle was no longer explicitly mentioned, but the idea of **continuous improvement** is still there.

- **2022** → (not in your text, but latest update) → Standard was revised again to simplify Annex A controls and align them with ISO/IEC 27002:2022.

In short:

- ISO/IEC 27001 is not static — it has evolved over time, from a UK standard to a global one.
- The heart of it is still **risk management + continuous improvement**.

Structure of ISO/IEC 27001

1. **Introduction**
   - Explains that the standard gives a process for managing information risks in a systematic way.
2. **Scope**
   - States that the ISMS applies to **any type, size, or nature of organization**.
3. **Normative References**
   - The only must-have reference is **ISO/IEC 27000** (which explains terms and concepts). Other ISO27k standards are optional.
4. **Terms and Definitions**
   - Provides key terms used in the standard.
5. **Context of the Organization (Section 4)**
   - Understand the environment (internal & external).
   - Identify stakeholders and their expectations.
   - Define the **scope** of the ISMS.
   - Requirement: the organization must **establish, implement, maintain, and continually improve** the ISMS.
6. **Leadership (Section 5)**
   - Top management must show commitment.
   - Approve and mandate security policy.
   - Assign roles, responsibilities, and authorities.
7. **Planning (Section 6)**
   - Identify and analyze risks.
   - Decide how to treat them.
   - Set **information security objectives**.
8. **Support (Section 7)**
   - Provide enough resources.
   - Ensure competence and awareness of staff.
   - Maintain and control documentation.
9. **Operation (Section 8)**
   - Carry out risk assessment and risk treatment.
   - Manage changes.
   - Keep proper documentation for audits.

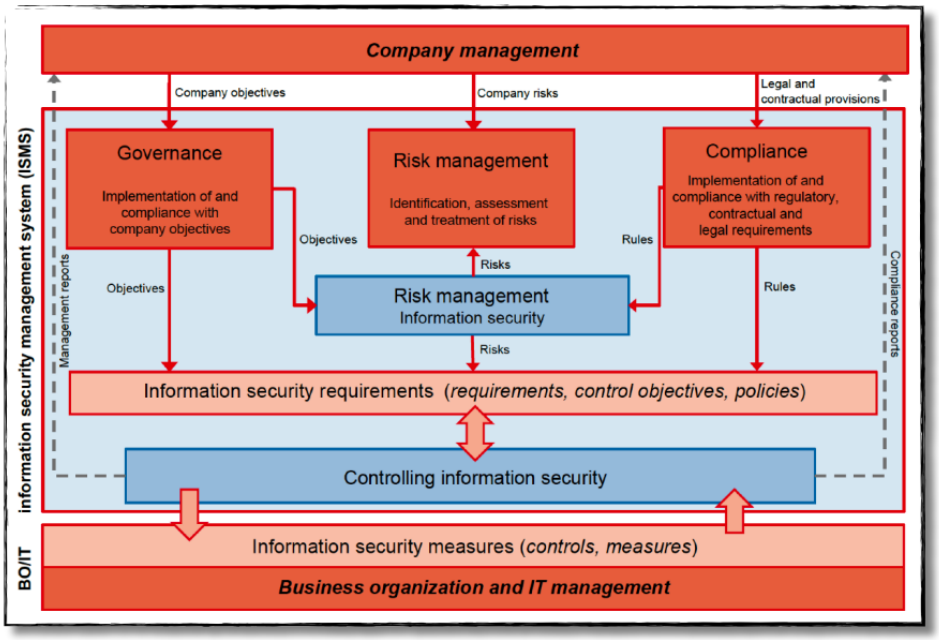
10. **Performance Evaluation (Section 9)**
    - Monitor and measure ISMS effectiveness.
    - Conduct internal audits and management reviews.
    - Evaluate and improve controls.
11. **Improvement (Section 10)**
    - Fix problems (non-conformities).
    - Take corrective actions.
    - Continually refine the ISMS.
12. **Annex A**
    - Provides a **list of security controls** (referencing ISO/IEC 27002 for details).
    - It's "normative" (expected to be used), but organizations can add or skip controls if justified.
13. **Bibliography**
    - References related standards like ISO/IEC 27000 (essential), ISO 31000 (risk management), and others for extra guidance.

☞ **In short:**

ISO/IEC 27001 is structured like a management system:

- **Plan** (Context, Leadership, Planning, Support)
- **Do** (Operation)
- **Check** (Performance evaluation)
- **Act** (Improvement)

And **Annex A** gives the "menu" of possible controls.


Company management
Company objectives
Company risks
Legal and contractual provisions
Governance
Implementation of and compliance with company objectives
Risk management
Identification, assessment and treatment of risks
Compliance
Implementation of and compliance with regulatory, contractual and legal requirements
Objectives
Rules
Risks
Risk management
Information security
Objectives
Rules
Management reports
Compliance reports
Risks
Information security requirements (requirements, control objectives, policies)
Controlling information security
Information security measures (controls, measures)
Business organization and IT management
information security management system (ISMS)
BO/IT

Incorporating the ISMS into corporate control processes

ISMS Scope and Statement of Applicability (SoA)

1. ISMS Scope

- **What it means:**
  The **scope** defines which parts of the organization are covered by the ISMS.
- **Key points:**
  - It can be **broad** (covering the entire company) or **narrow** (covering just one department, location, or function).
  - This decision is **very important** and must be formally documented.
  - The scope ensures that certification clearly states what areas are included (and what areas are excluded).

⚠ Example:
If **Acme Ltd.** certifies only **Department X**, then the ISO/IEC 27001 certificate says nothing about **Department Y** or the whole company.

2. Statement of Applicability (SoA)

- **What it means:**
  The SoA is a document that records the results of the **risk assessment** and shows which security controls were chosen (or not chosen) to treat risks.
- **Key points:**
  - It is **mandatory**, even though the standard doesn't give a fixed format.
  - It usually looks like a **matrix/table**, with:
    - Risks (from the risk assessment) on one side.
    - Risk treatment options (avoid, share, accept, mitigate) on the other.
    - Details on what controls are applied, and who is responsible.
- **Purpose:**
  - To **justify** why certain controls were included or excluded.
  - To provide clarity to auditors and third parties about how risks are managed.

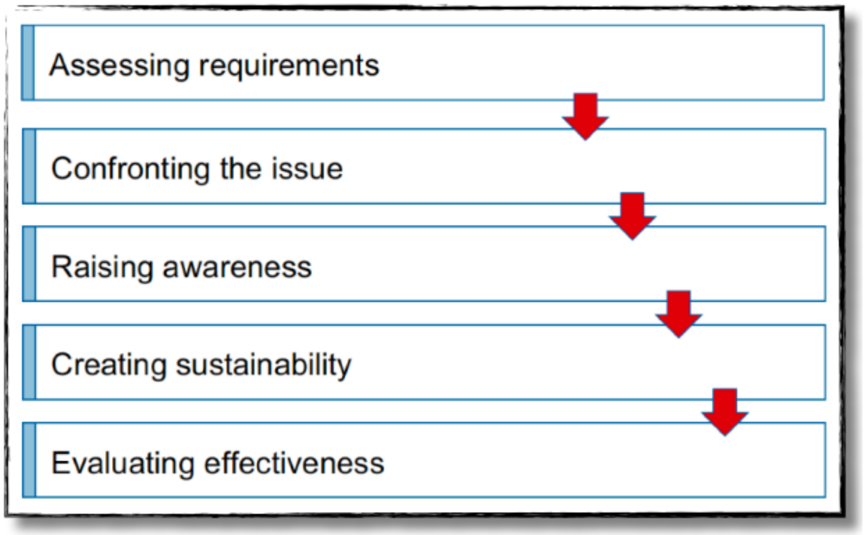
Example:
If management decides not to use **antivirus software** because they've done analysis and chosen another method (say, application whitelisting or strict access controls), that decision must be written in the SoA. The auditor may question it, but if the reasoning is valid, certification cannot be denied.

Why Scope + SoA Are Crucial

- The **Scope** tells us **"Where the ISMS applies."**
- The **SoA** tells us **"Which controls are used (or not used) and why."**
- Together, they give outsiders (like certification bodies, customers, partners) confidence in the organization's ISO/IEC 27001 compliance.

In short:

- **ISO** provides the *standards*.
- **ISMS** is the *system* an organization builds to follow ISO/IEC 27001, often using **forms and templates** like scope, risk assessment, SoA, and audit checklists.



Phase Model For ISMS Scope Definition and SoA Awareness Campaigns

Mandatory Requirements for Organizational ISO 27001 Certification

ISO/IEC 27001 is both:

1. A **blueprint** for designing an Information Security Management System (ISMS).
2. A **formal certification standard** that external auditors can use to certify an organization.

To get certified, organizations must **document and implement** certain mandatory elements.

1. ISMS Scope (Clause 4.3)

- **What it is:** Defines the boundaries of the ISMS — what parts of the organization are covered.
- **Requirements:**
  - Consider **internal issues** (e.g., culture, processes, IT systems).
  - Consider **external issues** (e.g., laws, regulations, customer expectations).
  - Define **interfaces and dependencies** (e.g., outsourcing IT to another company).

  - Scope must be **formally documented**.

Example: “This ISMS applies to the IT Department of XYZ Ltd., covering data centers in Karachi and Lahore.”

2. Information Security Policy (Clause 5.2)

- **What it is:** A high-level document set by **top management**.
- **Must include:**
  - Relevance to the organization’s purpose.
  - A framework for setting **security objectives**.
  - A **commitment** to meet legal/regulatory/customer requirements.
  - A **commitment to continual improvement** of ISMS.
- **Other requirements:**
  - Policy must be **documented**.
  - Shared with relevant stakeholders (employees, partners, auditors).

Example statement: “We commit to protecting customer data, meeting GDPR, and continuously improving our ISMS.”

3. Information Risk Assessment Process (Clause 6.1.2)

- **What it is:** A structured process to **identify, analyze, and evaluate risks**.
- **Requirements:**
  - Define **risk criteria** (acceptance rules, evaluation method).
  - Use a **consistent method** each time.
  - Identify **risks to confidentiality, integrity, and availability**.
  - Assign **risk owners**.
  - Analyze risks: consequences + likelihood → risk level.
  - Evaluate risks against criteria → prioritize them.
- **Must be documented** and repeatable.

Example risk: “Customer data may be stolen due to weak password policies → High likelihood, High impact → High risk.”

4. Information Risk Treatment Process (Clause 6.1.3)

- **What it is:** Deciding how to handle identified risks.
- **Requirements:**
  - Choose treatment options (Avoid, Accept, Share, Mitigate).
  - Decide **which controls** are needed.
  - Compare chosen controls with Annex A of ISO 27001.
  - Create a **Statement of Applicability (SoA)** → list of controls with reasons for inclusion/exclusion.
  - Create a **Risk Treatment Plan** (how risks will be handled, deadlines, responsibilities).

  - Obtain **risk owners' approval** and acceptance of residual risks.
- **Must be documented.**

☞ Example: Weak passwords risk → Mitigation → Control: Enforce multi-factor authentication.

5. Information Security Objectives (Clause 6.2)

- **What they are:** Specific measurable goals for security.
- **Requirements:**
  - Must align with security policy.
  - Must be measurable where possible.
  - Must consider risk assessment results and requirements.
  - Must be **communicated** and **kept up-to-date**.
- **Planning objectives must cover:**
  - What will be done.
  - Resources required.
  - Responsibilities (who does what).
  - Timeline.
  - How results will be evaluated.
- **Must be documented.**

☞ Example objectives:

- "Reduce phishing incidents by 30% in the next 12 months through awareness training."
- "Ensure 100% of servers have latest security patches within 2 weeks of release."

Summary Table of Mandatory Requirements

Clause	Requirement	Key Output (Documented)
4.3	ISMS Scope	Scope Statement
5.2	Information Security Policy	Security Policy
6.1.2	Risk Assessment	Risk Assessment Method & Records
6.1.3	Risk Treatment	SoA + Risk Treatment Plan
6.2	Security Objectives	Security Objectives + Plans

Key Takeaway

To get **ISO/IEC 27001 certification**, an organization **must document**:

1. **ISMS Scope**
2. **Security Policy**
3. **Risk Assessment process and results**
4. **Risk Treatment process + SoA + Risk Treatment Plan**
5. **Security Objectives and Plans**

These are **non-negotiable mandatory requirements** — without them, certification is impossible.

6. Evidence Of The Competence Of The People Working In Information Security (Clause 7.2)

The organization must:

- decide what skills are needed for people doing work that affects information security;
- make sure those people are skilled through education, training, or experience;
- if skills are missing, take steps (like training) to build them and check if those steps worked;
- keep records as proof that people are competent.

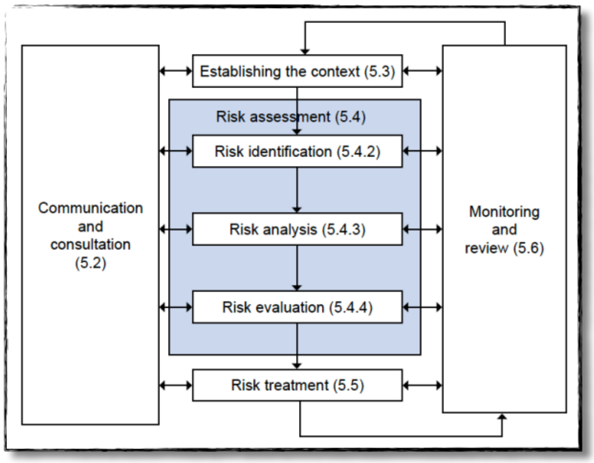
7. Other ISMS-related Documents Deemed Necessary By The Organization (Clause 7.5.1b)

The ISMS must include all documents the organization thinks are needed for the system to work well.

8. Operational Planning And Control Documents (Clause 8.1)

The organization must plan, implement, and control processes to meet information security needs.

- Plans should also include how to achieve security goals.
- Records should show that processes are followed as planned.
- Any changes must be reviewed, and risks managed if problems happen.
- Outsourced processes must also be checked and controlled.


Establishing the context (5.3)
Risk assessment (5.4)
Risk identification (5.4.2)
Risk analysis (5.4.3)
Risk evaluation (5.4.4)
Risk treatment (5.5)
Communication and consultation (5.2)
Monitoring and review (5.6)

Risk Management Process Based On ISO 31000

The Results Of The [Information] Risk Assessments (Clause 8.2)

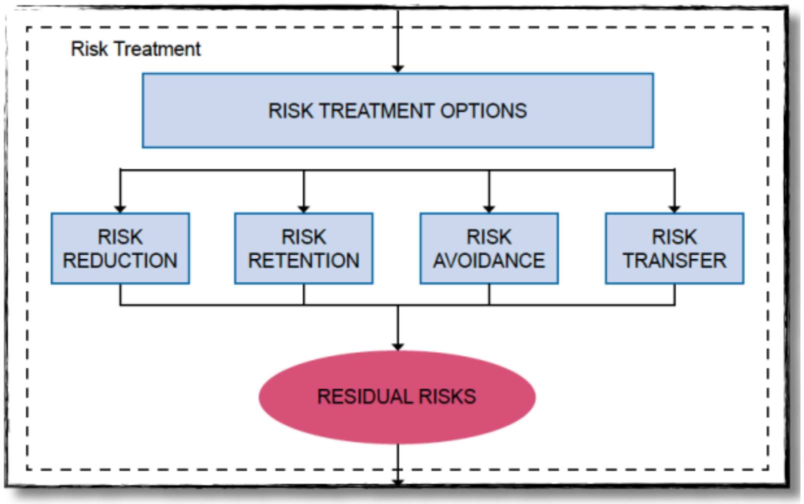
The organization must do risk assessments regularly or when big changes happen.

- Records of the results must be kept.

The Decisions Regarding [Information] Risk Treatment (Clause 8.3)

The organization must carry out the risk treatment plan.

- Records of treatment results must be kept.



Risk Treatment Options Based On ISO/IEC 27005

Evidence Of The Monitoring And Measurement Of Information Security (Clause 9.1)

The organization must check how well its ISMS is working.
It must decide:

- what to measure (e.g., processes, controls);
- how to measure and analyze results;
- when and by whom measurements are done;
- who will review the results.
- Records of the monitoring and results must be kept.

The ISMS Internal Audit Program And The Results Of Audits Conducted (Clause 9.2)

The organization must do audits at planned times to see if:

- the ISMS meets company and ISO requirements;
- the ISMS is working effectively.

The organization must:

- plan and maintain an audit program (frequency, methods, responsibilities, reporting);
- consider importance of processes and past results;
- set scope and criteria for each audit;
- choose independent and objective auditors;
- share results with management;
- keep records of the audit program and results.

Evidence Of Top Management Reviews Of The ISMS (Clause 9.3)

Top management must review the ISMS regularly to check if it is suitable and effective.
Reviews must consider:

- past actions;
- changes in internal/external issues;
- feedback on ISMS performance (trends in problems, monitoring, audits, and goals);
- feedback from stakeholders;
- results of risk assessment and treatment status;
- improvement opportunities.

The output of reviews should include decisions for improvements or changes.
Records of reviews must be kept.

Evidence Of Nonconformities Identified And Corrective Actions Arising (Clause 10.1)

If a problem (nonconformity) happens, the organization must:

- react quickly to control and fix it;
- check if action is needed to stop it from happening again;
- find the root cause;
- check if similar issues exist elsewhere;
- implement and review corrective actions;
- update ISMS if needed.

Records must show:

- what problems happened and actions taken;
- results of corrective actions.

Various Others

Annex A lists other documents such as:

- acceptable use of assets,
- access control policy,
- operating procedures,
- confidentiality agreements,
- secure system design principles,
- supplier relationship policies,
- incident response procedures,
- laws, contracts, and compliance procedures,
- continuity procedures.

These are not mandatory, but auditors usually expect to see them.

Documents should have clear titles, authors, formats, reviews, and approvals. They must also be controlled (like in ISO 9000).
Electronic documents (like intranet pages) are preferred since they are easier to update and control.

Certification

Getting ISO/IEC 27001 certification from an independent body is optional, but many partners and customers now demand it.

Benefits of certification:

- proves the organization takes security seriously;
- improves security through a structured process;
- gets management attention and support;
- has marketing and brand value.

ISO/IEC 27001 Mandatory Documentation Summary

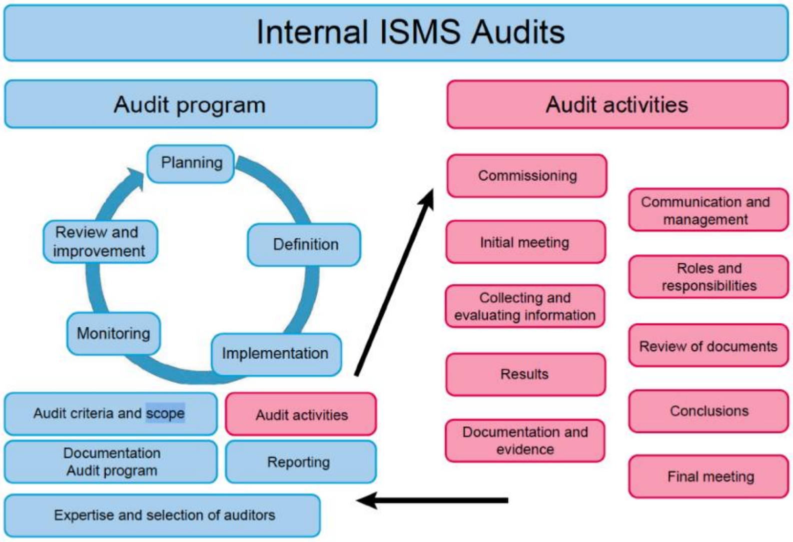
Clause	Requirement	Key Output (Documented Evidence)
4.3	Define ISMS scope (boundaries, parts covered, dependencies).	Scope Statement
5.2	Set an Information Security Policy (high-level, commitments, improvement).	Security Policy
6.1.2	Do structured risk assessment (identify, analyze, evaluate risks).	Risk Assessment Method & Records
6.1.3	Risk treatment (choose options, select controls, create SoA, treatment plan).	Statement of Applicability (SoA) + Risk Treatment Plan
6.2	Define measurable security objectives aligned with policy.	Security Objectives + Plans
7.2	Ensure staff competence (education, training, experience).	Competence Records
7.5.1(b)	Include other ISMS documents needed for effectiveness.	Supporting ISMS Documents
8.1	Plan and control operations, manage changes, control outsourcing.	Operational Control Records
8.2	Perform risk assessments regularly or after major changes.	Risk Assessment Results
8.3	Implement and record results of risk treatment plan.	Risk Treatment Records
9.1	Monitor and measure ISMS performance and controls.	Monitoring & Measurement Records
9.2	Conduct internal audits to check ISMS compliance and effectiveness.	Audit Program + Audit Results
9.3	Top management reviews ISMS at planned intervals.	Management Review Records
10.1	Handle nonconformities and corrective actions.	Nonconformity & Corrective Action Records
Annex A (supporting)	Policies & procedures like access control, asset use, incident response, supplier security, etc. (expected but not all mandatory).	Annex A Policies/Procedures (as needed)

Key takeaway:
To pass **ISO 27001 certification**, an organization must **document at least these 13 mandatory items** (Clauses 4–10). Annex A docs are strongly expected but flexible depending on the organization.

ISO 27001 Audit Programs

ISO 27001 Audit Programs

- Purpose: check two things — (1) the ISMS meets the organization's and ISO requirements (conformity); (2) the controls and actions are actually working (implementation & effectiveness).
- You must plan and run an **audit program** that sets frequency, procedures, roles, planning rules, traceability and reporting.
- The program must also define how corrective/preventive actions from audits will be handled and who will follow up.
- All business processes inside the ISMS scope should be audited at least once every **three years**.
- Evidence (audit reports, records) must be kept.
- The ISMS officer / CISO usually runs this program, using an internal audit team or outside help as needed.



Structure For Internal ISMS Audits (Audit Program vs. Audit Activities)

Structure For Internal ISMS Audits (Audit Program vs. Audit Activities)

- Two parts:
  1. **Audit program / framework** — the overall plan and control for all audit work (governance layer).
  2. **Audit activities** — the actual planning and running of each internal audit.
- Coordination with the internal audit department is recommended.
- In larger orgs: separate program management (audit team leader) from the audit team who do the audits.
- Design the program so it supports ISMS goals and gives good value for the audit effort.

Success Factors For Practical Implementation

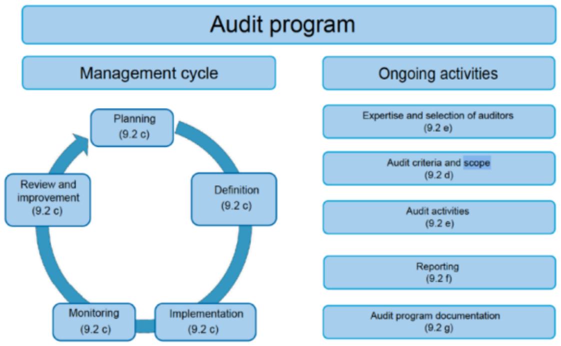
- Treat the audit program as a cycle: **plan → define → implement → monitor → review & improve**.
- Use **risk-based planning**: prioritize audits by process importance, business criticality and past audit results.
- Define general audit criteria in the program; you can also set specific scopes for each audit.
- Document finished audits and keep audit reports as proof.
- Produce regular management reports about the audit program and results.

The audit program

- Consider process importance, critical IT systems and previous audit findings when scheduling audits.
- Define audit criteria and, if needed, the exact scope for each audit.
- Ensure completed audits are recorded and available as evidence.
- Generate management reports on program performance and audit results.
- The program must be continually reviewed and improved.

Audit Program Requirements

- The program should state: frequency of audits, methods to be used, roles & responsibilities, planning requirements, reporting format, and traceability of evidence.
- Ensure objectivity and impartiality when selecting auditors.
- Ensure follow-up on corrective actions and track their closure.



Audit Program Requirements

ISO 27001 Step-ByStep Implementation Guide

If you are starting, these are the main steps from getting management buy-in to running and improving the ISMS.

Step 1. Obtain Management Support

- Get top managers to agree, provide budget and people, and sponsor the project.
- Without their support the project usually fails.

Step 2. Treat It As A Project

- Run implementation like a normal project: define tasks, owners, timeline, and resources.
- Use project management so work finishes and doesn't drag on.

Step 3. Define The Scope

- Decide which parts of the organization the ISMS will cover (one department or the whole company).
- Smaller companies can usually include the whole company; larger ones may scope a single area.

Step 4. Write An Information Security Policy

- Create a short, high-level policy from management that says what you want to protect and why.
- It sets the direction and framework for objectives and controls.

Step 5. Define The Risk Assessment Methodology

- Decide the rules: how to find risks, how to score likelihood and impact, and what level of risk is acceptable.
- If the rules are unclear, results will be unusable.

Step 6. Perform The Risk Assessment & Risk Treatment

- Identify assets, threats, vulnerabilities; assess impact and likelihood.
- Plan how to treat unacceptable risks (use controls, accept, transfer, avoid).
- Write a Risk Assessment Report and get approval for any residual risks.

Step 7. Write The Statement Of Applicability

- List all Annex A controls and mark which ones apply or not, with reasons.
- Describe how chosen controls meet objectives.
- Use the SoA to get management approval for the ISMS.

Step 8. Write The Risk Treatment Plan

- Make a concrete plan to implement chosen controls: who, when, cost, and priorities.
- This is your implementation schedule for controls.

Step 9. Define How To Measure The Effectiveness Of Controls

- Decide how you will measure if controls and objectives work (metrics, methods, frequency).
- If you can’t measure it, you can’t prove it works.

Step 10. Implement The Controls & Mandatory Procedures

- Put policies, procedures, and technical controls in place (those required by clauses 4–10 and your SoA).
- This often needs behavioural change — plan for that.

Step 11. Implement Training And Awareness Programs

- Teach staff why the changes matter and train them to follow new procedures.
- Lack of training is a common cause of failure.

Step 12. Operate The ISMS

- Make the ISMS part of daily work.
- Keep records of activities — auditors look for evidence that things were done.

Step 13. Monitor The ISMS

- Track incidents, measurements, control results, and whether objectives are met.
- If results are off, plan corrective or preventive actions.

Step 14. Internal Audit

- Run internal audits to find problems or gaps (not to punish people).
- Use audits to trigger corrective and preventive actions.

Step 15. Management Review

- Top management reviews ISMS results, audits, risks, and objectives and decides on actions.
- Management must be informed and make decisions based on reviews.

Step 16. Corrective And Preventive Actions

- When problems occur, find the root cause, fix it, and verify the fix works.

- Keep this process systematic and recorded.

Final note:

- Plan each step carefully. ISO 27001 is manageable if you follow these steps in order and keep records.

ISO 27001 - Roles And Responsibility In Organizations

ISO 27001 - Roles And Responsibility In Organizations

Understanding roles and responsibilities in security is critical for making your security program successful. In ISO 27001, every person involved must know what they are supposed to do.

Why Understanding Roles is Critical to the Security Program?

- An information security program affects the whole organization, not just the IT/security team.
- Leadership and departments must support, adopt, and spread the security culture.
- If only one team handles security (siloed), it will fail and only meet "basic compliance."
- To succeed, everyone must know **why** security matters and **what** they need to do.
- ISO 27001 certification also requires that roles and responsibilities are clear and communicated.

Five Typical Roles and Responsibilities

1. Security Leadership

- The leader can be a **CISO, Director, Manager, or even someone from IT/Legal** in smaller firms.
- This person has full responsibility and authority for the security program.

Typical duties:

- Align security program with business goals.
- Set strategy, budget, and resources.
- Build a roadmap and report progress (KPIs) to leadership/board.

2. Security Risk Management

- Often handled by a **Risk Committee or Council** (with members from finance, HR, legal, IT, sales, etc.).
- Ensures risk and policy management is done across the organization.

Typical duties:

- Attend quarterly meetings.
- Define and maintain the risk management process.
- Oversee annual risk assessments and update the risk register.
- Approve and enforce policies.
- Review results of assessments and manage incidents/response.

3. Internal Audit

- Internal audit ensures **continuous improvement** of the ISMS.
- Must be **qualified** and **independent** (cannot audit their own work).

Typical duties:

- Develop annual audit plan.
- Audit ISMS and Annex A controls.
- Report results to management.
- Sometimes third-party auditors are used for independence.

4. Control Owners

- People responsible for running and maintaining specific controls from Annex A (114 controls).
- These tasks differ by organization, but roles must be clearly assigned.

Typical duties:

- Secure software development and operations.
- Vulnerability management, intrusion detection, and monitoring.
- Network engineering and perimeter defense.
- System availability, backup, and disaster recovery.

5. All Employees

- Every employee is part of information security.
- Many incidents start with end users (phishing, weak passwords, careless mistakes).

Typical duties:

- Basic awareness training (phishing, safe browsing).
- Role-based training (finance staff, HR staff, etc.).
- Compliance training (GDPR, SOX, contractual requirements).

✅ In summary: ISO 27001 requires **everyone** (from leadership to employees) to have **clearly defined roles** in information security. Leadership drives, committees manage risk, auditors check compliance, control owners run operations, and employees practice secure behavior.