ClausePass27001

ISO 27001 Implementation: Start to Success

A practical 12-stage journey from the first implementation decision to a functioning, evidence-backed ISMS.

Edition	Standard	Publisher	Online	Page
First edition	ISO/IEC 27001:2022	ClausePass27001	clausepass27001.com	1

Contents

Publication note

This guide explains how to use the ClausePass27001 toolkit during an ISO/IEC 27001 implementation. It is written for the person who must turn a management-system requirement into an implementation activity with a named owner. Each activity must leave a current record, produce a result that can be reviewed, and reach management when a decision is needed.

Terms this guide uses from the start

Term	Meaning in this guide
Information security management system (ISMS)	An information security management system (ISMS) is the management system used to establish, implement, maintain, and continually improve information security.
Information security	Information security is the preservation of confidentiality, integrity, and availability of information. Confidentiality means that information is not made available or disclosed to unauthorized people, entities, or processes. Integrity means that information remains accurate and complete. Availability means that authorized users can access information and related assets when required.
Management system	A management system is the set of interrelated organizational elements used to establish policies and objectives and to achieve those objectives. An ISMS applies that structure to information security.
Control	A control is a measure that maintains or modifies information security risk. A control may involve people, process, technology, physical measures, or a combination of them.
Documented information	Documented information is information the organization must control and maintain, together with the medium on which it is contained. The term covers both directions that must remain current and records retained as evidence.
Effectiveness	Effectiveness describes whether the organization carried out the activities it intended and obtained the intended results. Finishing a task does not, by itself, demonstrate effectiveness.
Requirements standard	In this guide, the requirements standard is ISO/IEC 27001:2022 together with any amendment that applies to the implementation. It states requirements against which conformity may be assessed.
Control guidance	Control guidance explains information security controls and implementation considerations without replacing the requirements standard. ISO/IEC 27002 is the principal control-guidance source used here.
Third-party certification	Third-party certification is an independent conformity-assessment process conducted by a certification body; it is not approval or certification by ISO.

The following terms govern decisions made later in the journey. Their short definitions are placed here so that the journey map and the modules can use them consistently. Each module returns to the relevant distinction in its working context.

Term	Meaning in this guide
Interested party	An interested party is an individual or organization that can influence an ISMS decision or activity, experience its consequences, or consider itself affected by it.
Implementation project time	Implementation project time is the elapsed time used to establish or materially repair the ISMS.
Operating time	Operating time begins when an approved process or control is used in normal conditions.
Implementation trace	An implementation trace is a linked sequence from an initiating source or decision through implementation activity, operating records, evaluation, and follow-up that another reviewer can reconstruct.
ISMS scope	The ISMS scope is the documented boundary and applicability of the information security management system.
Information security risk assessment	An information security risk assessment is the systematic process of identifying, analysing, and evaluating information security risk under approved risk criteria.
Information security risk treatment	Information security risk treatment is the process of selecting and implementing measures that modify, retain, avoid, or share information security risk under the approved method.
Statement of Applicability (SoA)	The Statement of Applicability (SoA) is the maintained statement of necessary controls, the justification for including them, their implementation status, and the justification for excluding Annex A controls that the organization has determined are not necessary.
Internal audit	An internal audit is a systematic, independent, and documented process conducted by or on behalf of the organization to obtain and evaluate audit evidence against audit criteria for its own management-system purposes.
Nonconformity	A nonconformity is non-fulfilment of a requirement.
Correction	A correction is action to eliminate a detected nonconformity.
Corrective action	Corrective action is action to eliminate the cause of a nonconformity and prevent recurrence.
Management review	A management review is top management's formal evaluation of whether the ISMS remains suitable, adequate, and effective and what changes or decisions are required.

ClausePass27001 provides editable working material, from implementation guidance and registers to workshop exercises. Its fictional examples are clearly marked. Your organization supplies the facts and sets the boundary of the ISMS. It interprets the obligations that apply, makes the risk decisions, and chooses how necessary controls will operate. It also approves its documented information and remains responsible for every public claim.

Keep a licensed copy of ISO/IEC 27001:2022 and its applicable amendment available. This guide does not reproduce the standard and cannot determine conformity for an organization. ISO/IEC 27002 supplies control guidance; it is not a substitute for the requirements standard. Questions of law or contractual duty require the

current source and a competent interpretation. Technical questions need the same care. Accreditation and certification questions must be decided through the applicable scheme and an authoritative party.

Certification is optional unless an applicable obligation makes it necessary for the organization. ISO develops standards; it does not audit organizations or issue ISO/IEC 27001 certificates. An external certification body conducts the certification process and makes the certification decision. If accredited certification matters, verify the body's current accreditation and scope through an appropriate authoritative route.

The standard and related guidance continue to develop. At the date of this edition, ISO/IEC 27000:2026 explains the main ISMS concepts and shows how the standards relate. ISO 19011:2026 is the current general guideline for auditing management systems. ISO/IEC 27006-1:2024 contains the ISMS-specific requirements for certification bodies. Check current editions before relying on any version-sensitive statement in a later project.

What this book expects from you

You do not need a finished ISMS before starting. You do need access to the people who know how the in-scope service operates and where its information moves. Use current sources to establish the obligations and the actual working practices. If a necessary fact is missing, name the gap and give it an owner. Record when the dependent decision will be reconsidered. A blank field with an assigned follow-up is safer than an invented answer that later travels into scope, risk, or audit work.

The modules assume that you will use current organizational records wherever they already exist. Do not recreate an operational system inside the toolkit. Asset details belong in the approved asset inventory; service cases belong in the ticketing system. Keep supplier and personnel facts in their established sources as well. A toolkit workbook can become authoritative when the organization deliberately assigns it that job. Otherwise, use it to govern the links and decisions needed by the ISMS while detailed facts remain in the operational source.

How the journey is organized

The main route contains twelve modules:

1. use the toolkit under controlled conditions
2. establish the implementation mandate and plan against implementation project time and operating time
3. determine context, interested parties, scope, interfaces, and governance
4. define and run the information security risk-assessment method
5. treat risk and build the Statement of Applicability
6. adapt the policy, standard, and procedure system
7. establish authoritative registers, plans, and logs
8. run the first ordinary operating cycle
9. set objectives, evaluate performance, and conduct internal audit
10. correct nonconformities, take corrective action, and conduct management review
11. prepare for the certification lifecycle where certification is approved
12. govern sector sources, changes, examples, handover, and the next cycle.

Four laboratories appear at natural transfer points. Each one uses a current organizational case or a clearly marked toolkit example. The laboratories are part of the course, not decorative questions. Complete the

requested record, exchange it with a reviewer where possible, and repair any point at which the reviewer has to guess.

The records you will keep returning to

Several records recur throughout the implementation:

- `05 ISO IEC 27001 Implementation Planning Record.docx` preserves the starting basis, checkpoint decisions, certification objective, major return decisions, and handover.
- `ISMS Implementation Plan and Action Tracker.xlsx` holds accepted actions, owners, dependencies, dates, status, and links to completed results.
- `Context, Interested Parties and Scope Register.xlsx` holds changing context, requirement, boundary, interface, and scope decisions.
- `Risk Register and Risk Treatment Plan.xlsx` holds the assessed risk population and the actions used to deliver approved treatment.
- `Statement of Applicability.xlsx` records necessary controls, applicability reasoning, Annex A comparison, exclusions, and implementation status.
- `Master Document Register.xlsx` governs the current policy, standard, procedure, and other controlled-document population.
- `Evidence Register.xlsx` governs recurring evidence requests, sources, periods, limitations, review status, and retention decisions.
- `Internal Audit Plan and Checklist.xlsx` governs the audit programme and individual audit work.
- `Findings, Nonconformity and Corrective Action Register.xlsx` governs findings, immediate correction, cause analysis, corrective action, effectiveness review, and closure.
- `Management Review Actions and Performance Register.xlsx` preserves performance information, management-review decisions, actions, and follow-up.

These records are connected, but they do not have the same job. Preserve the stable identifier when a matter moves between them. Do not duplicate a changing conclusion merely to make every file look complete.

A note about examples

Hearthline Data Services and Asterline are fictional examples supplied with the toolkit. Hearthline is used across several subjects; Asterline is a separate planning chronology. Never blend the two example organizations or transfer their facts into a live organization. An example is useful because it exposes a relationship. A scope choice changes the risk population, for instance, and a risk decision should be visible in the Statement of Applicability. Elsewhere, an operating record may support an audit conclusion. A finding should lead back to the process condition that caused it.

The stopping rule

Pause a dependent decision when the missing item could change the scope or the interpretation of an applicable obligation. Do the same when it could alter the risk evaluation, the proposed treatment, or the authority needed to proceed. A public claim or audit conclusion must also wait when the missing fact bears on it. Record the established facts and the remaining uncertainty. Give the follow-up to the person who can obtain or decide the missing point, and state when work may resume. Continue with unaffected work. This is ordinary management-system discipline, not a failed implementation.

Module 1: Use the toolkit without borrowing its authority

Treat the delivered folder as release media. Before entering any organizational detail, make one unchanged preservation copy and one controlled working copy. Record the repository and its administrator. Link the working copy to the delivered release, then define who may approve a later change. This small piece of housekeeping matters because a filled template may soon contain sensitive operational information and become documented information within the ISMS.

Open `00 Welcome to ClausePass 27001.docx`, then `00 Start Here.docx`. The welcome file explains the package and points to the commercial terms. The start file routes by the implementation task you are trying to complete. That is more useful than browsing by file type. The same implementation question may call for a document, a workbook or a workshop, but each produces a different record.

Four kinds of authority in one project

The implementation will use several source types. Keep their authority separate.

Source	What it can supply	What it cannot settle by itself
ISO/IEC 27001 requirements standard	The requirements against which conformity is assessed	Your scope, facts, risk decisions, control design, evidence, or readiness
ISO/IEC 27002 and related guidance	Control guidance and useful implementation considerations	A universal list of controls that every organization must implement unchanged
Applicable law, regulation, contract, sector rule, and organizational commitment	Requirements and constraints within their actual jurisdiction and scope	An interpretation outside the source or beyond the interpreter's authority
ClausePass27001 toolkit	Editable structures, questions, procedures, registers, workshops, and teaching examples	A live organizational decision, proof that a control operates, a legal opinion, or a certification decision

The organization's maintained records sit across these sources. A risk owner can accept residual risk only within assigned authority. A document approver can release a policy but cannot use that approval to settle a contractual interpretation reserved for legal counsel. An internal auditor can report an audit finding but should not take ownership of the process change needed to close it. A certification body controls its audit and certification decisions; the implementation team controls the accuracy and accessibility of the information it supplies.

The distinction becomes useful whenever somebody says that a template is "ISO compliant." Ask which proposition is actually meant. The template may cover fields commonly needed for a subject, and its wording may be aligned to a toolkit design. That says nothing about whether the organization chose an appropriate method or supplied accurate content. It also does not prove operation or conformity with a requirement.

Choose a file by the required deliverable

Start with the current question and the record that should hold the answer.

Current question	First place to work	Maintained result

Current question	First place to work	Maintained result
Why are we implementing an ISMS, and who can approve the starting assumptions?	01 Implementation Planning	Implementation planning record and action tracker
What service and information are inside the ISMS?	02 Scope and Governance	Context, interested-party, interface, and scope records
How will people be directed and how will a process run?	03 Policies, Standards and Procedures	Approved policy, standard, procedure, or exception record
What are the information security risks, and what will be done about them?	04 Risk and Statement of Applicability	Approved method, risk register, treatment plan, residual-risk decisions, and SoA
Where will changing facts and operating results be kept?	05 ISMS Registers, Plans and Logs	The selected authoritative workbook or an approved referenced system
What does the available evidence support, and what needs audit or correction?	06 Evidence, Internal Audit and Improvement	Evidence record, audit work, finding, corrective action, or management-review input
Should the organization seek certification, and how will the external process be coordinated?	07 Certification Preparation	Certification plan, readiness decision, coordination record, and finding response
Does a sector or discipline source apply?	08 Sector Guidance	Source-applicability and conflict decision
How does an end-to-end example connect the records?	09 Worked Examples	A critique or learning note, never a copied live record

If no supplied file fits, do not force the answer into the nearest spreadsheet. Use the organization's approved system and place an identifier or stable reference in the toolkit record where a connection is needed.

Establish the working controls

Set up the working copy before distributing it.

1. Record the delivered release identity and location of the preserved copy.
2. Create the implementation copy in an approved repository. Apply access restrictions appropriate to the information that will be entered.
3. Identify the document-control owner and the authority that will approve adapted policies, standards, procedures, and management-system records.
4. Decide how versions, approvals, effective dates, review triggers, superseded files, and retained records will be handled.
5. Decide which workbooks will become authoritative records and which will only point to another approved system.
6. Remove sample or prompt content only after its purpose is understood. Do not leave a prompt in a released document, and do not replace it with invented certainty.
7. Keep the fictional-example folder visibly separate from live material. Preserve the fictional label in every exported or copied example.
8. Confirm where commercial terms and license questions are handled. Use `10 License and Release/01 ClausePass 27001 Commercial Terms.docx` for the actual terms; this guide does not reinterpret them.

The source check for every populated field

Before accepting an entry, ask four practical questions.

Where did it come from? A role name might come from an approved responsibility model, a system owner, or an old policy. Those sources do not carry equal weight.

What is its state? Separate an established fact from an assumption. Keep a proposal visibly different from a decision, and mark an unknown instead of filling it with a guess. A proposed audit date should not appear as an approved certification commitment.

Who may decide it? The person entering data may be coordinating a decision rather than making it. Preserve that distinction in the owner and approval fields.

What would make it change? A service or platform change may reopen the entry. So may a change in the supplier or contractual position. New legal analysis, an incident, or an audit finding can have the same effect. Record the trigger where it matters.

This check is especially important when an existing ISMS is being repaired. Approved documents may describe a former service boundary, former role structure, or discontinued system. Test a small sample of current operating records before accepting the old design as the starting point. One normal case and one late, failed, or disputed case usually reveal more than a folder review.

First-day setup

Complete the following before planning a long document-production effort:

- preserve the delivered package and establish the controlled working copy
- open the start and welcome files
- locate the source that initiated the implementation request
- name the provisional sponsor and implementation lead
- identify the scoped service or organizational result that appears to be involved
- record any external statement already made about scope, timing, certification, or readiness
- choose one current operating record that can help test the starting picture
- create the initial entry in `05 ISO IEC 27001 Implementation Planning Record.docx`
- place accepted actions in `ISMS Implementation Plan and Action Tracker.xlsx` rather than maintaining a private task list.

The module is complete when a second person can locate both the preserved release and the controlled working copy. That person must also find the current planning record and its action tracker. A licensing question should have an obvious route. Finally, the reviewer should be able to explain why a populated toolkit file becomes an organizational record only after the organization has adopted and controlled it.

Fieldwork

Inspect five files you expect to use in the next month. For each file, write a short use note that answers three questions. What work will the file perform, and who will eventually own it? Where will its authoritative result live, and what approval or review will apply? What sensitivity and opening event govern its use? If two files

appear to govern the same changing fact, choose one authoritative record or define the synchronization method before either is populated.

The next decision is whether the implementation has a usable mandate. Carry forward the initiation source, a provisional service description, the people who can settle priority and scope assumptions, and the first sample of current operation. Module 2 uses those four inputs to separate project promises from supportable operating dates.

Turn the Guide Into a Working ISMS

Get your clausepass27001 toolkit

EXPLANATION

Module 2: Establish the mandate and separate project time from operating time

An ISO/IEC 27001 request often arrives already compressed. A tender may ask for a certificate, or a customer questionnaire may suddenly become urgent. Elsewhere, a group function may set a target date while management asks for “the policies.” Recover the source before expanding that request into a programme. Read the actual contract or tender question when either initiated the implementation project. For an internal request, find the document that authorized it. That may be a board paper or group instruction; sometimes the source is a risk decision. An incident record or customer communication may reveal a different purpose again.

Record the request in `05 ISO IEC 27001 Implementation Planning Record.docx`. At this stage, leave most of the record empty. Identify the initiating source and the business reason. Describe the provisional service boundary, then name the sponsor and the authority available to proceed. Record any external statement that already constrains the implementation project. Put actions in `ISMS Implementation Plan and Action Tracker.xlsx`.

Write a purpose that survives a moving audit date

“Achieve ISO compliance” gives no help when resources compete or evidence is late. A useful purpose identifies the organizational result that the ISMS is expected to support. One organization may need consistent governance of a customer-facing service and better protection of entrusted information. Another may be trying to improve material-risk decisions or customer assurance. A third may need to integrate practices that developed separately. Use only the reason leadership has actually accepted.

Test the draft purpose by moving the proposed audit date. If the purpose disappears, the programme is being defined by a calendar event rather than the management need. Certification may still be an important objective. Record it separately so that a change to the external timetable does not erase the reason for operating the ISMS.

Dates also need to be separated. A single statement such as “we need the certificate in October” may contain:

- the date a tender response is due
- the date a customer will make a procurement decision
- the last acceptable date for an audit visit
- the certification body’s provisional availability
- the hoped-for date of a certification decision
- the date on which a public or contractual statement has already been made.

For each date, record its source and whether it is fixed or preferred. Show the dependency it controls and the consequence of moving it. The sponsor handles any inaccurate or premature external statement. The implementation lead should not quietly reshape scope or evidence to make the statement look true.

Establish the starting condition

Use `01 Initial Implementation Decisions.docx` to organize the first inquiry. Begin with a current description of the scoped service and the way it is governed. Add the applicable commitments already identified and the

known risk information. Bring a sample of operating records so the discussion can be checked against actual process operation.

For a new ISMS, identify existing practices before designing replacements. Access administration and supplier review may already work under local names. The same may be true of incident response, change control or recovery testing. Training and legal review can also form part of the current system. For each practice, identify the owner and the inputs that start the process. Follow its decisions into the retained record, including the route for exceptions and later review. A process that works well should be connected to the ISMS rather than rewritten to resemble a template.

For an existing ISMS, compare the documented design with current operation. Select at least one ordinary case and one case that took a difficult route. A late or rejected case is useful; an escalated or disputed one can reveal a different weakness. Follow each from its initiating source to the final record. Note where the written procedure differs from the actual route. Also record a mismatch in responsibility or retained evidence. These differences belong in the starting assessment; they should not be hidden until internal audit.

Keep observations in proportion. Two weak cases do not prove that every case failed. They do justify a wider look when the governing source or population appears unreliable. A broken interface or authority model calls for the same response.

Give leadership a decision, not a progress display

The kickoff should produce an approved mandate. Use `09 Leadership Kickoff Workshop.pptx` and `10 Leadership and Implementation Discussion Cards.docx` to prepare the discussion. Adapt the material to the organization and remove questions that do not apply.

The decision pack should state:

Matter	What leadership needs to see
Business purpose	The organizational result sought and the initiating source
Provisional boundary	The scoped service, information, organizational elements, locations, technology, and external dependencies currently thought to be involved
Known commitments	Customer, group, legal, regulatory, contractual, or public statements already made
Certification objective	Whether certification is currently intended, why, and for what proposed boundary
Starting condition	Existing practices worth retaining, material gaps, and uncertainties that could change the programme
Authority	Sponsor, implementation lead, process and control decision rights, escalation route, and deputies
Resources	Available people, competence, time, systems, funding, and external support
First operating trace	One material process that will be followed end to end
Immediate choices	Proceed, proceed with conditions, hold for a missing fact, replan, or stop

Leadership does not need a completed policy set to make this decision. It needs enough reliable information to authorize the next stage and make the limits visible.

Project time and operating time

The roadmap must distinguish implementation project time from operating time.

Implementation project time is the elapsed time used to establish or materially repair the ISMS. Inquiry and management decisions come first because they determine the design. Document adaptation and technical implementation follow, with configuration and any needed pilot completed before normal use. More people or a narrower deliverable may shorten some project stages.

Operating time begins when an approved process or control is used in normal conditions. An event starts the process, and an operator applies its criteria. Exceptions reveal how the route behaves under pressure. Owner review gives meaning to the resulting records over time. Some conclusions require this elapsed experience. Adding staff cannot create a past quarter or a second recovery test that has not occurred.

Build the schedule around dependency and observation rather than document count. For each material process, record:

1. the source decision or design that must exist first
2. the implementation activity needed to release the process or control
3. the first normal operating opportunity
4. the expected population and source records
5. the owner review
6. the earliest evaluation that can support the intended claim
7. any internal audit, management review, risk, certification, or public decision that depends on the result.

This sequence produces an earliest supportable decision date. It is more useful than a percentage-complete chart because it shows why a later decision cannot yet be made.

Select one end-to-end trace

Choose a process that is material enough to receive serious attention and narrow enough to observe. User access or supplier assurance often gives a clear population. Vulnerability handling and secure change expose technical dependencies, while incident response or backup recovery can test a rarer event. Choose according to the scoped service. Use a current organizational process, not a convenient invented case.

Trace the process in its operating order:

1. locate the initiating event and its authoritative source
2. establish the complete population for the period
3. identify the operator and approving authority
4. apply the criteria that change the route
5. follow the process through systems and external providers
6. locate the normal result and maintained record
7. test the exception, failure, and escalation route
8. obtain the owner’s review; and
9. state the evidence needed for a bounded conclusion.

The first trace will show which policy or procedure is needed. It will also reveal the authoritative register and any technical change required to make the route work. Access rights and competence needs become visible at the hand-offs. The implementation can then test its operating model before scaling it to every subject.

Build the roadmap by dependency

Use the planning sources according to the decision they support:

- `02 Implementation Planning and Governance.docx` establishes the main governance choices.
- `06 Implementation Planning and Coordination.docx` connects those choices to owners and dependencies.
- `07 ISMS Implementation Lifecycle.docx` shows the wider lifecycle.
- `08 ISO IEC 27001 Implementation Sequence.pptx` supports discussion of the proposed order.

Keep the accepted roadmap in `ISMS Implementation Plan and Action Tracker.xlsx`.

A practical order is:

1. approve the mandate and working authority
2. determine context, interested parties, obligations, scope, interfaces, and governance
3. approve the risk method and assess the in-scope risk population
4. decide treatment, necessary controls, and the Statement of Applicability
5. adapt only the policies, standards, procedures, and technical arrangements needed to operate those decisions
6. establish the authoritative records and release processes into ordinary ownership
7. gather normal operating results, including exceptions and failed cases
8. monitor, measure, review, test, and internally audit the system
9. correct nonconformities, take corrective action, and verify effectiveness
10. conduct management review and decide what changes
11. prepare for certification only if that objective remains approved and supportable
12. continue the operating and improvement cycle.

The order is not a waterfall. A supplier fact discovered during treatment may reopen scope. A failed operating case may expose an unrealistic policy. An audit finding may require the risk method to be reconsidered. Record the return to the owning source and propagate the approved change to its consumers.

Assign work at the right level

Use `11 Control Ownership and Evidence.docx` to distinguish governance and evidence responsibilities. Use `12 Technology Responsibilities and Evidence.docx` where the route depends on technical operation. Together they separate roles that are often compressed into “information technology (IT)” or “security.” Resolve each material control or process through this matrix.

Role	Decision or work held	Evidence responsibility	Continuity check
Accountable control owner	Accepts the intended result and material control changes	Reviews whether the control result remains supportable	Names a deputy with matching authority where timing matters

Role	Decision or work held	Evidence responsibility	Continuity check
Process owner and operators	Run the defined route and respond to exceptions	Create and maintain the operating record	Demonstrate that another authorized operator can enter the route
System or technology owner	Maintains the technical capability and approved configuration	Provides configuration, change, and service records	Provides an escalation route for unavailable capability
Risk owner	Decides whether treatment and residual conditions remain acceptable	Maintains the risk decision and its conditions	Delegation does not silently transfer risk acceptance
Performance or evidence reviewer	Tests source, population, period, and limitations	Records the review and bounded conclusion	Is independent enough to challenge the operator's account
Escalation and exception authority	Decides cases outside the ordinary route	Records reason, scope, safeguards, and expiry	Has a named route when the primary authority is unavailable
External provider	Performs only the responsibilities assigned by agreement	Supplies the evidence required by the organization's review	Organization-side ownership and escalation remain explicit

The same person may hold several roles in a small organization. The record should still distinguish the decisions. Someone who performs an access review may not be authorized to approve their own exception or accept the resulting risk.

Define evidence before the process runs

Use `03 Evidence and Readiness Decisions.docx` to write a short evidence specification for the first trace. Organize it by the question the evidence must answer:

- **Proposition:** the claim, its boundary, the period and the population.
- **Production:** the source, operator and expected exceptions.
- **Control:** the reviewer, storage safeguards and planned test.

The specification prevents a folder of screenshots from becoming the evidence strategy.

Separate three states:

- **design**: the control or process has an approved description
- **implementation and operation**: the arrangement exists and has been used for the stated boundary and period
- **effectiveness**: evaluation supports the conclusion that the intended result was achieved within the stated limits.

An approved procedure supports design. A configuration record may support implementation. An operating conclusion needs a complete population and the treatment of exceptions. Review and an appropriate evaluation may then support a bounded effectiveness conclusion. Do not use one state as shorthand for the others.

Procure help for a defined gap

External support can fill a competence or capacity gap. It may also provide technical testing or a qualified legal interpretation. Audit and certification services occupy a different assurance role and must preserve the applicable independence. Define the gap and the required output before selecting a provider. Record conflict constraints where the provider may later audit work it helped design.

Ask what the organization must still decide and retain. A consultant can facilitate a risk workshop; the organization's risk owner remains responsible for the live decision. A tool can store evidence; it does not decide whether the evidence supports a claim. A certification body can explain its process; it must preserve the impartiality required for its role.

Recover a stalled implementation

When the action tracker is full but no process has reached normal ownership, return to one end-to-end trace. Identify the earliest missing dependency. Common causes include:

- the business purpose or sponsor authority was never approved
- scope and external interfaces remain provisional
- the risk method cannot be applied consistently
- control owners were assigned names without decision rights or capacity
- documents were approved before operators tested the process
- the population or authoritative record cannot be established
- operating time was omitted from the schedule
- evidence was requested without a defined claim
- certification dates were treated as internal readiness decisions.

Repair the earliest cause and replan its dependents. Avoid producing more documents while the blocked decision remains unchanged.

Before scope work begins

Give the scope team the approved mandate and a current account of the scoped service. Include the initiating source and the first operating trace. Keep unresolved conditions visible rather than folding them into the proposed boundary. The sponsor should already have settled the purpose and provisional boundary. The team also needs clear authority, committed resources and any immediate condition on proceeding. Certification, if requested, must appear as a separate objective rather than an assumed outcome. Check the roadmap for both implementation project time and genuine operating time. Assign an owner and return point to any assumption that could change the scope or an applicable obligation. Do the same when it could alter a risk decision or the authority to proceed.

Turn the Guide Into a Working ISMS

Get your clausepass27001 toolkit

Module 3: Determine context, scope, interfaces, and governance

The **ISMS scope** records where the information security management system applies and where its boundary ends. It identifies the included organizational activities and scoped-service delivery. The boundary also records the information and locations involved. Relevant technology and each external interface must be visible as well. An **interested party** is a person or organization whose position may change an ISMS decision, or who may experience or perceive its effects.

The context, interested-party, and scope analysis is recorded in `Context, Interested Parties and Scope Register.xlsx`. Use the supporting resources according to the implementation function they perform:

- `01 Context and Governance.docx` develops the reasoning.
- `02 ISMS Scope and External Interfaces.docx` supplies the boundary method.
- `03 Context, Scope and Governance Approval Workshop.pptx` supports leadership challenge.
- `04 ISMS Operating Model.docx` can preserve one explanation of the system's relationships when that explanation is needed.

`05 First ISMS Operating Cycle and Issue Recovery.docx` will later test whether the foundation survives ordinary ownership.

Start with the organization and the scoped service

Establish the internal and external issues that can affect the ISMS purpose or intended results. Draw the context from sources that describe real decisions and operation:

- strategy and service material for the result the organization is trying to provide
- organization and governance records for authority
- architecture and supplier arrangements for technical and external dependency
- customer commitments and competent legal or regulatory analysis for applicable obligations
- incident, risk and performance information for observed conditions; and
- workforce information and approved change plans for the capacity and future state.

An issue deserves a place in the context record when it changes a decision. Record the affected part of the ISMS and the trigger for reconsideration. The analysis should reach the scope or risk work when the issue changes the boundary or exposure. It should reach resources and objectives when it alters what can be delivered. Where authority or operation is affected, connect it to governance or control design. A long environmental scan with no such destination will not help the operator who later needs to respond.

At the research date for this edition, ISO/IEC 27001:2022/Amd 1:2024 applies to the requirements standard. Consult the licensed standard and amendment when evaluating the relevance of climate change within the organization's context and interested-party requirements. Do not copy a generic climate statement into the register. Record the organization's supported determination and its source.

Identify interested parties and applicable requirements

Begin with the parties whose needs or expectations matter to the ISMS. Identify the specific requirement behind each entry, then decide whether the organization will address it through the ISMS. A category such as

“customers” is too broad to operate. Name the source that gives the entry force. It may be a contract class or service commitment. In other cases, procurement sets the useful boundary. A reporting duty or assurance need can do the same.

For each entry, retain:

- the interested party or defined class
- the source and current edition or version
- the requirement in decision-safe language
- the owner of interpretation
- the affected service, information, process, control, record, or claim
- how fulfilment is incorporated into the ISMS
- the review or change trigger
- unresolved conflicts or conditions.

Legal, regulatory, and contractual interpretation must come from a competent and authorized source. The register preserves the result and its lineage; it does not create the interpretation. Detailed obligations can remain in `Legal, Regulatory and Contractual Requirements Register.xlsx`, linked by stable identifier.

Trace at least one important requirement into normal operation. Make the hand-offs explicit:

1. identify the source and record the authorized interpretation
2. show how that interpretation affects scope and risk
3. locate the policy position or necessary control
4. follow it into the operating procedure and record; and
5. show how monitoring and review return the result to governance.

If the trace stops at an approved policy, the requirement has not yet reached the activity expected to fulfil it.

Trace the boundary through the scoped service

A usable ISMS scope lets another practitioner begin with the scoped-service result and follow how it is produced. The trace should reveal the operating activities and information involved, then show the technology and authority on which they depend. Location matters where it changes responsibility or applicable conditions. The scope boundary appears wherever applicability or responsibility changes. It may fall between teams or systems. A legal-entity or location boundary can matter as well, and an external provider creates another crossing that must remain visible.

Write a short scoped-service proposition in operating language. State the result supplied and who relies on it. Explain what information the scoped service handles and the main operating activities needed to deliver it. Name the authority accountable for the scoped service. Keep current operation separate from planned expansion. Otherwise, a proposed platform or future location may be described as though it already exists while a current dependency remains obscure.

Trace representative paths from current evidence. Process descriptions and architecture material show the intended route; contracts show external commitments. Use operating records to test that design and knowledgeable owners to resolve what the sources do not explain. Include several of the following paths where they are material:

- ordinary delivery of the scoped-service result

- creation, alteration, review, and removal of access
- support work requiring privileged action or access to information
- release or configuration change
- supplier onboarding, change, or termination
- incident response and customer notification
- disruption, recovery, and return to normal operation.

At each handoff, identify the activity and the information transferred. Record where the transfer occurs and who performs it. Then capture the required authorization, the next dependency and the response to failure. This trace often exposes reliance on identity administration and the worker lifecycle. Procurement and facilities may support the scoped service from outside the apparent process. Shared platforms and subscription management introduce technical dependencies, while specialist support or an external provider introduces another responsibility boundary.

Classify activities rather than whole departments

A central function may perform one activity inside the ISMS and several outside it. An out-of-scope function may still be indispensable to an in-scope service. Classify each material activity and record:

- the basis for treating it as in scope or out of scope
- the authority that can approve or change the treatment
- responsibilities that continue across the boundary
- the condition that will cause reconsideration.

If an out-of-scope payroll or human-resources process supplies worker status used to administer access, govern the organization side of that interface. Define the expected input and its timing. Name the owner, then state what happens when the input fails and where that response is recorded. The whole upstream function need not be absorbed into the ISMS merely because the dependency matters.

Apply the same discipline to an external provider. Record the choices the organization retains, including selection and configuration. State who grants authority for use. Monitoring and review should lead to a defined response when the provider-operated service fails. Record what the provider is expected to perform and where that expectation is established. Avoid wording that implies control over the provider's entire environment. When a contract conflicts with the architecture or observed practice, preserve the disagreement. A conflicting responsibility statement remains open until an authorized interpretation or decision resolves it.

Test exclusions by removing the activity from the scoped-service map. The activity is a material dependency if the scoped service could no longer be delivered or protected. Loss of support or recovery may establish the same conclusion. The activity may remain outside the boundary, but its interface must enter the risk assessment and receive an owner. Necessary controls and normal operating procedures must then reflect it.

Draft the scope statement

Write the formal scope after the trace. Keep it short enough to maintain and precise enough to prevent silent widening or narrowing. Test it against each decision below.

Scope test	What the statement must make decidable
Service	Which delivered services the ISMS governs

Scope test	What the statement must make decidable
Organization and activity	Which organizational elements and operating activities participate
Place	Which physical and virtual locations are included
Technology	Which environments support the governed service
Exclusions	What is outside, why it is outside, and whether the exclusion is supportable
Interfaces and dependencies	Where responsibility, information, or operation crosses the boundary
Authority	Which version is approved and which events require review

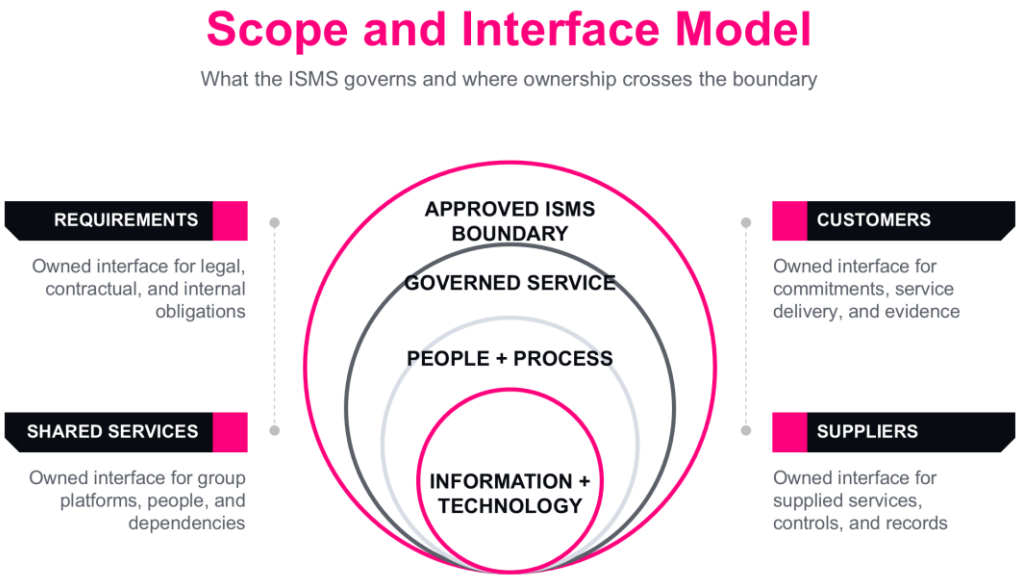

Figure 1. Scope is a governed service boundary, not a list of assets. Every material crossing remains visible as an owned interface.

Detailed handoffs, rationales, and unresolved conditions belong in the working register. The scope statement expresses the approved boundary; the register shows how it was derived. Mark the statement provisional when a disputed responsibility, supplier assumption, or service definition could materially change it.

Give the draft to people who operate, support, and authorize the scoped service. Ask them to follow the selected paths using the wording and supporting map. They should be able to identify in-scope and out-of-scope activities, responsibility at each material crossing, and the organization-side duties that remain for an external provider. Repair any point that only the original author can explain.

Design the governance model

List the decisions the ISMS needs before assigning names. Typical decisions concern:

- approving purpose, scope, policy, objectives, and resources
- approving the risk method and risk criteria
- owning and accepting information security risk
- selecting and changing controls

- approving policies, standards, procedures, exceptions, and waivers
- interpreting obligations
- accepting an operating result or evidence conclusion
- approving audit programmes and responding to findings
- conducting management review and directing change
- deciding whether and when to pursue certification
- approving public or contractual claims.

For each decision, name the accountable authority and define what that role may approve. Separate preparation from operation so responsibility does not disappear into one label. Record any required advice or conflict. Finally, name the deputy and escalation route. A responsible, accountable, consulted, and informed (RACI) chart may help, but it should not replace the decision description. “Accountable” is not useful if nobody knows what the role may approve or what happens during absence.

Test one consequential decision under inconvenient conditions. Absence or disagreement can test the internal authority route. An external-provider delay or urgent change can test the timing, while incomplete evidence tests whether the decision stops when it should. Establish whether the deputy can act and whether escalation works. Locate the decision record, then follow its result into the downstream records that depend on it.

Decide whether an operating-model narrative is needed

`04 ISMS Operating Model.docx` is optional. Use it when the relationships among maintained records remain difficult to explain, particularly during handover or across a complex operating structure. Its value lies in showing the return paths:

- context informs the approved scope
- policy and delegated authority reach the operating processes
- risk treatment and the Statement of Applicability explain why controls are necessary; and
- performance and audit results return through management review to the decisions that must change.

Keep changing facts in their authoritative records. The operating-model narrative should point to the scope and risk sources rather than copying their values. Do the same for objectives and controlled documents. Audit results should remain in the audit source, while management-review and corrective-action records retain their own changing state. Remove every prompt and fictional example before release.

Leadership approval workshop

Prepare the approval workshop around unresolved decisions, not around a tour of completed files. Give participants the source record before the meeting and show where evidence disagrees.

The workshop should determine:

1. whether the context and interested-party analysis is sufficient for the stated decision
2. which requirements will be addressed through the ISMS and who owns their interpretation
3. whether the scoped-service analysis and exclusions are accurate
4. whether material interfaces and external providers are represented
5. whether decision rights, deputies, and escalation are workable

6. which conditions remain open and whether work may proceed around them
7. what must be transferred to risk assessment and ordinary ownership.

Record the decision and its limits in the context and scope register. Put resulting tasks in the action tracker. A discussion without a maintained decision is not approval.

Change and return paths

Define scope-review triggers by the part of the boundary they can disturb:

- **Service boundary:** a material change to a scoped service, its location or legal entity, including acquisition or disposal.
- **Delivery model:** a change in supplier, technology, data handling or organizational structure.
- **Obligation:** a new or changed contract, law or other applicable requirement.
- **Observed failure:** a serious incident, repeated interface failure, or evidence that the maintained scope no longer matches operation.

When a trigger occurs, trace the change before editing the scope statement. Identify the changed condition and the activities or interfaces it affects. Decide whether the formal boundary should move. Then locate the dependent risk assessments and controls. Correct any public or contractual claim that no longer matches the approved scope. Update the authoritative scope source, then propagate the approved result.

Module completion

The foundation is ready to transfer when:

- current context sources and material issues are recorded
- interested-party requirements have interpretation owners and ISMS destinations
- scoped-service and information flows can be traced
- each material activity has an applicability decision
- important exclusions remain visible as interfaces where necessary
- external-provider and retained organization responsibilities are separated
- the scope statement is approved or explicitly conditional
- decision rights, deputies, conflicts, and escalation have been tested
- review triggers and unresolved conditions are owned
- risk assessment receives the approved scope, service paths, interfaces, obligations, and open assumptions.

Do not wait for the wording to become elegant. Wait until affected owners can use it without private explanation.

Turn the Guide Into a Working ISMS

Get your clausepass27001 toolkit

Laboratory A: Approve a boundary that can survive contact with operations

This is the guided laboratory. Follow the supplied sequence, then compare the result with CP-SRC-122 only after drafting. Use a current service from the organization. If live information is unavailable for training, use the toolkit's clearly marked Hearthline example. Its context material establishes the case, while the related scope and governance records carry the exercise. Keep the fictional label on every working page. Reviewer feedback should identify the boundary decision that failed and the source or interface needed to repair it.

Inputs

- the initiating request and approved implementation purpose
- current service, process, architecture, location, and organization information
- relevant customer, supplier, legal, regulatory, contractual, and group sources
- two current operating cases, including one exception, delay, or disagreement
- `Context, Interested Parties and Scope Register.xlsx`
- the scope and governance guides and approval workshop.

Work

1. Write the scoped-service proposition and identify the information needed to deliver the result.
2. Trace at least three paths through the scoped service, marking every material handoff.
3. Classify the activities on each path as in scope or out of scope and retain the reasoning.
4. Record organization-side responsibility at every external-provider or shared-service interface.
5. Trace one interested-party requirement into an operating process and record.
6. Draft the scope statement and list the open conditions outside the formal wording.
7. Build the decision inventory and assign authority, responsibility, advice, deputies, conflicts, and escalation.
8. Ask an affected owner who did not draft the material to walk the paths and challenge the boundary.
9. Repair each point at which the reviewer had to guess.
10. Prepare the approval workshop and record its actual decision.

Deliverables

- approved or conditionally approved scope statement
- service and interface map
- completed context, interested-party, requirement, and scope entries
- role and decision-authority map
- open-condition list with owners and return triggers
- risk-assessment transfer note.

Review criteria

The reviewer should be able to perform five checks without asking the author to interpret the submission:

- locate every material activity
- distinguish applicability from dependency
- identify the organization-side owner at each boundary crossing
- find the source behind an interested-party requirement; and
- explain which condition would reopen the scope.

A polished diagram does not compensate for an unowned interface.

Feedback route

Return an incorrect service or boundary decision to the scope record. Return a disputed obligation to its interpretation owner. Return an unworkable authority assignment to the governance model. Put tasks in the action tracker, then regenerate the risk-assessment transfer only after the governing source is corrected.

EXPLANATION

Module 4: Build and run the risk method

An **information security risk assessment** is the systematic process of identifying, analysing, and evaluating information security risk under approved risk criteria. It produces a decision basis; it does not itself select or approve treatment.

Begin this module only when the ISMS scope is approved or its remaining conditions are explicit. Bring the scoped-service and interface map together with the applicable requirement records. Current asset, system and supplier information will help establish the assessment population. Use incident and vulnerability records to test the current exposure, and involve the people who understand normal operation. The risk method belongs in `02 Information Security Risk Method.docx`; assessed risks and treatment planning belong in `Risk Register and Risk Treatment Plan.xlsx`.

`01 Risk Management and the Statement of Applicability.docx` explains the full risk-decision sequence. `03 Risk and Statement of Applicability Decisions Workshop.pptx` supports facilitated decisions. `04 Risk Decisions and Reassessment.docx` is the recovery guide when a rating no longer agrees with the evidence. Use it as well when treatment state or an inherited record has become unreliable.

Decide what the assessment must support

“Perform the annual risk assessment” describes an activity, not a decision. State the purpose in terms that determine depth and participation. An assessment for a service launch differs from one supporting supplier renewal. Treatment prioritization calls for another level of coverage. A serious vulnerability or delayed change may require a tightly bounded decision, while a periodic assessment may examine the wider risk position of the scoped services.

Record:

- the decision to be made
- the approved scope and any relevant interface
- the assessment population and exclusions
- the time horizon
- the method version
- the decision and escalation authorities
- participants and their role in the assessment
- current sources and known limitations
- the point at which missing information will stop or qualify the decision.

This boundary keeps the analysis proportionate. A missing data point matters when it can change the consequence or likelihood reasoning. It also matters when the evaluation or proposed treatment would move. Stop when the missing information changes who has authority to decide. Additional precision is not automatically useful if it cannot change the choice.

Configure the method before rating live risks

The supplied method template contains decision prompts and draft scales. Replace each prompt with an organizational decision and remove options that do not apply. Test the configured model against representative cases. Reconcile the results with the workbook before obtaining approval. Only the approved method may govern live ratings. Its draft five-level model is an adaptable starting point, not an ISO requirement.

The approved method should specify at least:

Method element	Decision to record
Purpose and scope	Which information security decisions and ISMS boundary the method covers
Risk frame	Whether assessments are organized around services, processes, information, systems, suppliers, locations, changes, events, or an approved combination
Time horizon	The period considered and how urgent or long-lived exposures are handled
Scenario form	The minimum description needed to identify source, event or condition, and consequence
Current-control treatment	How current controls and uncertainty about their operation affect analysis
Consequence criteria	Dimensions, anchors, aggregation rule, and treatment of multiple serious consequences
Likelihood criteria	Meaning, anchors, period, population, and relationship to current controls
Risk level	How consequence and likelihood are combined, and what the result can and cannot decide
Evaluation criteria	Priority and escalation bands, additional constraints, and the authority needed for acceptance
Uncertainty	How missing, conflicting, or weak source information remains visible
Treatment and acceptance	Permitted options, required approvals, and relationships to necessary controls and residual risk
Review and change	planned reviews, event-driven triggers, method-change handling, and migration of open risks

Keep the information security risk assessment distinct unless the organization has deliberately integrated it with another method. Enterprise and financial risk may operate at a different decision level. Privacy and safety methods may apply different consequence criteria. Continuity, product and project risk can also have their own population and authority. Use shared identifiers or approved links where the same condition belongs in more than one system.

Establish the assessment population

An asset list can contribute to coverage, but it should not silently define the whole population. Build the assessment population from the way the scoped service operates:

- the processes and information needed to provide the scoped service
- the technology and people involved
- the relevant locations and suppliers
- shared capabilities on which several activities depend; and
- commitments, approved changes and other operating dependencies that can alter the scenario.

Record how coverage was tested. Use sources that expose different omissions.

Comparison source	Coverage question
Approved scope and interface map	Does every included service and material boundary crossing appear?
Service and process catalogues	Are delivery and support activities represented?
Information and asset inventories	Are material information and technical dependencies present without letting the inventory define the whole assessment?
Supplier and cloud-service records	Are externally operated and shared capabilities visible?
Applicable obligations	Do binding duties introduce a population, consequence, or decision condition?
Incident, problem, vulnerability, and change information	Do current conditions add scenarios the static inventories miss?
Business impact and recovery requirements	Are time-sensitive dependencies and consequences represented?
Material projects and planned changes	Is future state visible without being reported as current operation?
Earlier risk, audit, and management-review outputs	Have unresolved findings and decisions returned to the population?

Keep a proposed service or acquisition identifiable as a future state. Apply the same label to a planned location or platform change. Such plans may influence current treatment, but their assumptions should not be reported as present operation.

Write a risk scenario that can be assessed

A risk title such as “cyber attack,” “data breach,” or “supplier risk” leaves too much interpretation to the reader. Describe the scenario with enough structure to analyse it:

- the information, service, decision, or dependency affected
- a source of risk and the relevant event or condition
- a weakness, exposure, or dependency that permits the event to matter
- the consequence for confidentiality, integrity, availability, or another applicable information-security outcome
- the affected parties and operational extent
- the relevant period or circumstances
- current controls assumed in the assessment
- significant uncertainty and source references.

Avoid scenarios containing several independent events and consequences. Split a broad record when two causes would lead to different decisions. A different consequence or risk owner may also justify a separate scenario. Treatment that follows a separate route is another reason to divide the record. Conversely, do not create dozens of near-identical entries where one common dependency and treatment decision is the real subject.

Use sources for defined purposes

Assign each source a job. Architecture can establish a dependency, while a contract may establish an obligation. Incident records show what occurred in the past. Vulnerability information describes a technical condition at a stated time. The operator can explain how exceptions are handled. A control owner can describe the design and current implementation. None of these sources should be stretched to support a proposition it does not contain.

Distinguish an observation from an assumption. If current-control operation is inferred from a successful sample, preserve the sample boundary. If an external provider supplies a broad assurance statement, identify the provider-operated service and period it covers. Then establish its scope and the provider responsibility being assured. Where sources disagree, record the disagreement before attempting to resolve it.

Assess consequence before choosing a cell

Use the organization’s approved consequence dimensions and anchors. Consider the complete scenario rather than selecting the easiest visible effect. Depending on the method and scope, the analysis may include:

- interruption or degradation of the scoped service
- unauthorized access, use, change, disclosure, or destruction of information
- incorrect or unavailable decisions based on affected information
- breach of an applicable legal, regulatory, contractual, or customer requirement
- impact on people, customers, partners, or other interested parties
- financial, operational, strategic, or reputational effects where the method includes them
- concentration and common-dependency effects
- recovery difficulty, irreversibility, and delayed discovery.

Record the reasoning and source, not only the selected level. If several consequence dimensions are serious, apply the method’s aggregation rule; do not average them informally.

Assess likelihood for the complete scenario

Likelihood needs a declared meaning. It may represent frequency within a defined period, probability under stated conditions, or another approved interpretation. Everyone in the workshop should use the same one.

Consider the full path from source and condition to consequence. Evidence that scanning is frequent does not by itself establish the likelihood of a material compromise. Evidence that one control exists does not establish coverage across the population or period. Threat and exposure information describe different parts of the scenario. Control-operation records and incident history show observed conditions. Change and dependency information may alter the basis again. Use each source only at the strength it supports.

Record disagreement. Two assessors may be using different time horizons, control assumptions, or definitions of “likely.” Resolve the underlying assumption or present the decision owner with the materially different views. Voting and averaging should not erase a real ambiguity in the method or source base.

Understand what the matrix does

A matrix applies the approved combination rule. It helps produce consistent categorization, but it does not write the scenario or supply its sources. It cannot assign ownership or resolve uncertainty. Nor does a cell set the priority, choose treatment, or grant acceptance authority.

Check boundary behavior before adopting it. Use cases just above and below each threshold. Add a high-consequence, low-frequency scenario and one built around a common dependency. A case with weak source information should reveal how uncertainty affects the result. Confirm that the resulting bands drive actions the organization can actually govern. A label such as “medium” is useful only when the method defines the resulting priority and escalation. It should also set the review expectation and the authority required.

Use quantitative or semi-quantitative analysis when suitable data and a decision need justify it. Do not manufacture numeric precision from unsupported frequencies or costs. Preserve ranges and sensitivity where they affect the result.

Evaluate and prioritize

Risk evaluation compares the analysed result with the approved risk criteria. Keep priority and acceptance separate. A contract or applicable law may require treatment even when the result lies within a general acceptance band. Concentration and uncertainty can have the same effect. Leadership may also set a lower threshold for the particular decision. A risk outside an acceptance band may require treatment or escalation; the score itself does not grant someone authority to accept it.

Record:

- evaluated status and priority
- the criteria used
- constraints that override or qualify the calculated level
- the risk owner
- required escalation or additional authorization
- the next decision date or event
- any source gap that keeps the result conditional.

Facilitate the workshop

Send the method and assessment population early enough for review. Include the proposed scenarios and their sources. Invite people because they contribute knowledge or authority, not because a standard workshop list says so. Explain the rating anchors using the organization’s own approved examples where available.

During the session:

1. confirm the decision, scope, population, method version, and roles
2. review each scenario before displaying the proposed rating

3. examine current controls and the evidence supporting their assumed state
4. assess consequence and likelihood separately
5. record sources, uncertainty, dissent, and missing information
6. apply the calculation and evaluation criteria
7. assign the risk owner and next decision
8. leave materially unsupported results open.

After the workshop, the risk owner reviews the record and any required authority acts. Attendance is not approval.

Maintain and reassess

Plan periodic review and event-driven reassessment. Group event triggers by the basis they can change:

- **Boundary:** a material change to a scoped service, the ISMS scope, location or ownership.
- **Dependency:** a supplier or technology change.
- **Exposure:** a new obligation, threat, vulnerability or incident.
- **Method and control:** a change to the assessment method, control design or assumed operation.
- **Decision state:** treatment delay, expiry of acceptance, a failed effectiveness evaluation, or an audit finding that changes the assessment basis.

When a trigger arrives, preserve chronology. Retain what was known when the earlier decision was made. Add the new source and link the affected risk and control records. State why the result is being reconsidered. Do not overwrite the earlier basis as though it never existed.

When inheriting an old register, accept custody without silently endorsing every rating. Establish what each legacy field meant and where its value came from. Identify the authority behind a decision and the workflow behind its status. Words such as “implemented” or “residual” may have been used differently. The same is true of “accepted” and “closed.” Keep the old value and its uncertainty until it can be re-established under the approved method.

Transfer to treatment

Treatment can begin when three foundations are sound:

1. the method is approved and versioned
2. the population has been tested against the scope and its material interfaces; and
3. each scenario retains its source, causal event or condition, consequence, current-control basis and material uncertainty.

Before transfer, confirm that the approved criteria governed both analysis and evaluation. The risk owners must hold the necessary authority, and material disagreement must remain visible. Every open risk also needs a next decision or reassessment trigger.

Treatment can start only from this evaluated population. Give Module 5 the approved method version and the scenarios and sources used for the assessment. Include the recorded uncertainty, named risk owners, evaluation results, and reassessment triggers. Module 5 must return any control that cannot be traced to one

of those decisions or to another approved requirement; reconstructing a convenient risk afterward would break the trace.

Turn the Guide Into a Working ISMS

Get your clausepass27001 toolkit

Module 5: Treat risk and build the Statement of Applicability

Information security risk treatment turns an evaluated risk into an authorized response under the approved method. The response may change the risk, retain it, avoid the activity that creates it, or share part of it with another party. The **Statement of Applicability (SoA)** then preserves the organization's necessary-control decisions and its comparison with Annex A. Each entry states the reasoning and current implementation status. An Annex A control that is not necessary also needs a recorded justification.

Risk treatment begins with the result to be achieved. Buying a product or revising a policy may contribute to that result. A configuration task or training session can contribute as well. None of them, by itself, states how the assessed risk will change. Write the intended treatment outcome in relation to the scenario and risk criteria.

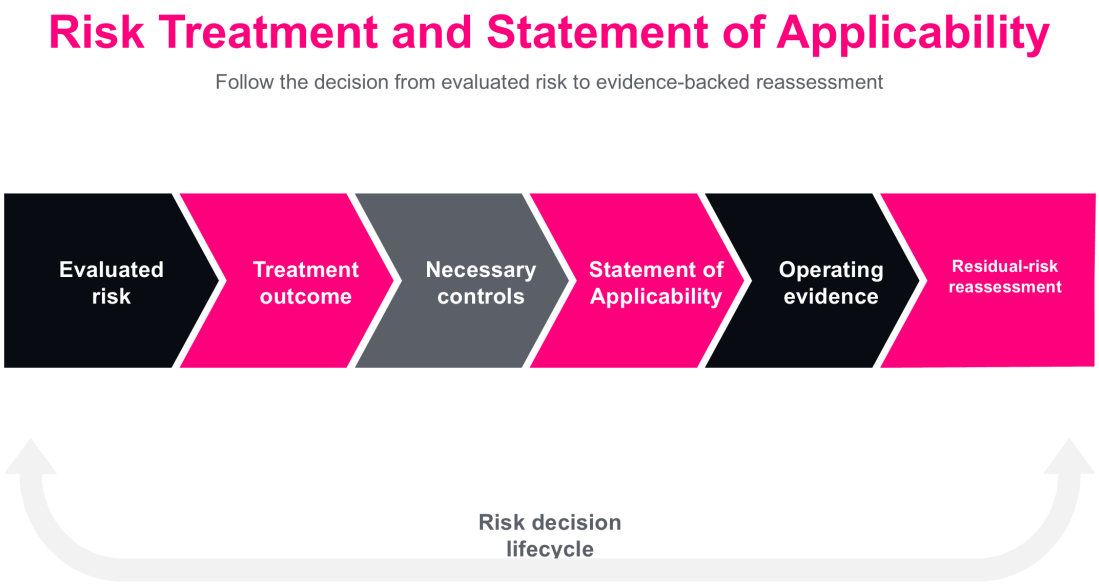

Figure 2. The SoA preserves a decision trace. It does not replace the risk assessment, treatment plan, implementation sources, or operating evidence.

Use the treatment portion of `Risk Register and Risk Treatment Plan.xlsx` for the decision and delivery plan. Use `Statement of Applicability.xlsx` to record the necessary-control decision and its comparison with Annex A. The same workbook preserves the applicability rationale, any exclusion, and the stated implementation status. Keep detailed operating evidence in its source system or the evidence register.

Select and govern treatment options

Apply only the treatment options allowed by the approved method. Record the selected route explicitly:

- **Modify:** introduce or change controls so the scenario changes.
- **Avoid:** stop the activity that creates the risk.
- **Share:** allocate part of the consequence or delivery through an arrangement without erasing retained responsibility.
- **Retain:** accept the evaluated risk through the authorized route.

A scenario may require more than one option, but each part still needs its own rationale.

For each selected option, record:

- the intended change to the scenario or consequence
- why the option is suitable under the evaluation criteria
- assumptions and dependencies
- parties responsible for delivery
- decision and acceptance authority
- conditions or time limits
- affected obligations and interfaces
- the point at which the option will be reconsidered.

Sharing service delivery or financial loss does not necessarily transfer the organization's responsibilities or remove the underlying risk. Record what the external provider or insurer does, what the organization retains, and how failure of that arrangement is handled.

Turn the outcome into an executable plan

Break the treatment into actions. Give each action an owner and the authority needed to complete it. State the resources and timing, then identify any dependency. Define the completion condition and the record in which completion will be shown. Identify how control implementation and operation will be observed and how effectiveness will later be evaluated.

Keep the following states separate:

State	Question answered
Treatment selected	What option and intended outcome have been approved?
Action assigned	Who must do what, by when, with which dependency?
Action completed	Was the specified task delivered?
Control implemented	Does the designed measure exist for the stated boundary?
Control operated	Was it used for the stated population and period?
Evidence reviewed	What source and sample were examined, and what limitations remain?
Effectiveness evaluated	Did the control achieve its intended result within the stated conditions?
Risk reassessed	What risk remains under the approved method?
Residual risk accepted	Did the authorized risk owner accept the current residual risk and conditions?

One progress field should not stand for all nine propositions. A project action can be complete while a quarterly control has not yet reached its first operating opportunity.

Determine necessary controls

Derive controls from the treatment outcome and other applicable requirements. Let the need determine the form. Some controls govern organization or people; others are physical or technological. A contractual control may support either route, and combined controls are common. For each control, define its purpose and boundary. Name its owner and set the operating criteria. Then identify the expected record, the response to failure and the evaluation method.

Use the Annex A reference set as a completeness comparison after the organization has determined the controls it needs. The comparison may reveal an omitted control or a weakly defined part of treatment. Return to the treatment reasoning when that happens. Annex A does not prevent the organization from using controls from another appropriate source or designing a control for a need not represented by a convenient one-to-one reference.

ISO/IEC 27002 contains guidance for the Annex A control set. Its 2022 edition organizes 93 controls into four themes. Organizational and people controls form two of them; physical and technological controls form the other two. Attributes support alternative views of the same set. Those themes and attributes can help navigation and analysis. They do not decide whether a control is necessary for the organization.

Build the Statement of Applicability

The Statement of Applicability (SoA) records the controls the organization has found necessary and the reason for including each one. Implementation status is a separate proposition. For an Annex A control that is not necessary, the SoA preserves the exclusion rationale. Keep enough linkage for another owner to follow each decision.

For each entry, establish:

- the control identifier and controlled title or reference
- whether the control is necessary
- the basis for inclusion, linked to risks or other applicable requirements
- the implementation status at the stated date
- the control owner and any shared or external-provider responsibility
- the implementing policies, standards, procedures, systems, or other sources
- the destination for operating evidence and evaluation
- the justification for excluding an Annex A control where it is not necessary
- open actions or conditions that limit the entry
- approval and review history.

Applicability and implementation status answer different questions. A control can be necessary and not yet implemented. A control can exist operationally for business reasons and still require a recorded applicability decision within the SoA. Do not mark a control “not applicable” merely because work has not begun.

Write rationales that can be traced

An inclusion rationale should point to the reason the control is necessary. Usually that source is a risk-treatment decision or an applicable obligation. A business requirement or another approved basis may also establish the need. The rationale need not repeat the whole risk record. Use stable identifiers and a concise explanation of the relationship.

An exclusion justification should show what was considered against the approved scope. It should also address the relevant risks and obligations, then remain consistent with the treatment decisions. “Not relevant” is rarely enough for an incoming owner. Avoid claiming that an excluded system or function has no relationship to the ISMS when it remains a material external dependency.

Where an Annex A control is broad, document the coverage the organization has actually determined. A provider may operate part of a technical service, but the organization still selects and configures that provider-operated service. It may retain access administration and monitoring. Incident response and contractual oversight can remain with the organization as well. The SoA should not assign the entire control to the provider and erase those duties.

Review coherence across the records

Use the following reconciliation:

Compare	Question
Risk register to treatment plan	Does every approved treatment address the current scenario and evaluation?
Treatment plan to necessary controls	Can each control be traced to an intended treatment outcome or other approved requirement?
Necessary controls to Annex A	Was the reference set used to check that no necessary control was omitted?
SoA to implementation sources	Does the implementation status agree with current policies, procedures, systems, and actions?
SoA to evidence sources	Are operating and effectiveness references scoped to the same service, population, and period?
SoA exclusions to scope and obligations	Does the justification remain supportable after boundary or requirement changes?
Residual risk to control state	Is the reassessment based on current operation rather than planned benefit?

Repair the governing source first. If an SoA rationale is wrong because the treatment decision changed, correct treatment and then propagate the result. Editing the SoA alone leaves the risk record inconsistent.

Reassess residual risk

After treatment actions reach their completion conditions, return to the original scenario. Confirm the scope and population, then set the period being assessed. Use the approved method version. Establish the current-control state from the available evidence. Reperform the relevant risk analysis and evaluation. Do not reduce the earlier rating by a guessed control percentage.

The risk remaining after treatment is residual risk. Where controls have not operated sufficiently, record a forecast or target state rather than presenting an established residual result. Explain the uncertainty and any material dependency. Set the conditions for continued operation and identify further treatment where it is required.

Residual risk acceptance is a separate decision. Give the risk owner the current scenario and the assessment basis. Show what treatment was actually delivered and where the evidence remains limited. The decision

should state the remaining exposure and any dependency. It also needs an expiry or reassessment trigger. Obtain any additional governance approval required by the organization.

Approval of the treatment plan, acknowledgement that project actions closed, and residual risk acceptance are separate records. Do not let a signature on one page stand for all three.

Handle delay, expiry, and change

When a treatment action is late, reassess the effect of the delay. Interim protection or restricted operation may be necessary. The owner may instead need to change the priority, escalate the delay, or revise the treatment. Keep the target benefit out of the current-control assessment until the measure is in place.

When an acceptance or exception expires, review the current scenario and authority. Avoid renewing it solely because the reminder arrived. Establish whether the control design, business activity, or treatment should change.

When the risk method or scope changes, identify the affected risk and SoA entries. A supplier or obligation change can trigger the same review, as can a change in control design. Preserve the old basis before updating the authoritative records. Then notify the owners of dependent policy and procedure sources. Evidence, audit and external-claim records may also need correction.

Practical exercise: build one live risk-treatment trace

Select a current risk with a named owner and adequate source material. Open the maintained risk record, treatment plan, and SoA. Locate the authoritative action record and the source that shows control operation. Then identify the evidence review and any acceptance decision.

Recover the assessment

Recover the assessment in the order in which another practitioner must test it:

1. confirm the scenario, scope, population and time horizon
2. identify the approved method version and the sources used
3. reconstruct the consequence and likelihood reasoning
4. establish the current-control state and material uncertainty; and
5. locate the evaluation and the risk owner’s authority.

List every place where you would have to guess. Stop the dependent decision when a gap could change assessment, treatment, or authority.

State the outcome and plan

Describe the intended risk change before listing actions. State the treatment option and its dependencies. Assign the owners and resources, then set the timing and completion conditions. Name the record that will show implementation. Finish the plan with its evaluation method and the response to delay.

Determine and compare controls

Derive the necessary controls from the treatment. Define their purpose and boundary. Compare them with Annex A and return to treatment if the comparison reveals an omission. Complete the relevant SoA entries, preserving inclusion or exclusion reasoning and implementation status as separate propositions.

Reassess and obtain acceptance

Use actual implementation and operation information. Label an unobserved post-treatment state as forecast. Reassess under the approved method, record remaining uncertainty, and route residual risk to the authorized owner.

Set a reopening condition

Define at least one observable reassessment trigger. Name the source that reveals it, the person who initiates review, and the records that reopen.

Give the risk-treatment trace to another authorized practitioner. The reviewer should be able to locate the current risk decision and its treatment outcome. The necessary controls must lead into the SoA rationale and the stated implementation condition. The residual-risk decision should then be obvious. Any open condition must point to the next reassessment trigger without oral explanation.

Hand the control design to its operators

Before drafting instructions, inspect the transfer as an operator would. Each treatment needs an intended outcome, executable actions, and an owner. Necessary controls should be derived and compared with Annex A. The SoA must keep reasoning separate from implementation status, show shared responsibility, and lead back to current risk evidence. Residual-risk acceptance needs the right authority and any applicable conditions.

If that trace is intact, Module 6 can turn the selected controls and other requirements into directions and operating methods. If it is not, repair treatment or the SoA before asking a policy author to hide the gap in prose.

Turn the Guide Into a Working ISMS

Get your clausepass27001 toolkit

Module 6: Build the policy and procedure system people will actually use

Risk treatment tells you what must be controlled. Module 6 turns those decisions into directions, operating criteria, and repeatable methods. Begin with the process as it is performed. Interview the approver and the people who carry out the process. Include whoever supports the tools and whoever receives the resulting record. Observe at least one ordinary case. Then choose a difficult case for a reason: a delay or rejection can test decision timing, while a failure or emergency tests recovery. A disputed case can expose unclear authority. The second case usually reveals the missing hand-off or escalation that a clean process description overlooks.

Open `03 Policies, Standards and Procedures/00 Start Here.docx` (CP-SRC-022) before selecting a template. The governing sources have distinct jobs:

- `04 Managing Policies and Procedures.docx` (CP-SRC-069) establishes document governance.
- The decisions workshop (CP-SRC-070) supports choices that need several authorities.
- The operating model (CP-SRC-071) connects those choices to the rest of the ISMS.
- `07 Policy Adoption, Exceptions and Change.docx` (CP-SRC-072) governs release, departure and later revision.

Together they explain the document lifecycle without imposing one architecture on every organization.

Decide what kind of instruction is needed

Do not create one document for every Annex A control. Controls often share a policy position, depend on the same standard, or operate through several procedures. Start with the audience and the action that must become consistent.

Instrument	Use it for	Typical content	Do not use it as
Policy	A governing position, required behaviour, authority, and broad accountability	Purpose, scope, principles, mandatory requirements, roles, exceptions, enforcement, review	A detailed click-by-click operating script
Standard	Mandatory, testable criteria that several teams or systems must meet	Baseline values, approved methods, technical conditions, minimum settings, verification criteria	General aspiration with no measurable condition
Procedure	A repeatable activity with a trigger, sequence, responsibility, record, and failure route	Inputs, steps, decisions, hand-offs, outputs, records, exceptions, escalation	A summary of what a policy already says
Work instruction or runbook	Detailed execution for a particular tool, platform, or local task	Commands, screens, checks, rollback, local contacts	The organization-wide source of policy authority
Register or log	Changing facts, decisions, cases, status, and retained operating results	Stable identifiers, dates, owners, source references, review status	A substitute for the rule governing how entries are created and reviewed

A policy may require strong authentication for specified access. A standard can define the approved factors and required authentication strength. It can also govern secret handling and controlled exceptions. The privileged-access procedure then follows the lifecycle from request and approval into provisioning. Verification and periodic review precede eventual revocation. Platform runbooks hold the product-specific steps. The authorized systems of record retain each access request and approval. Later changes and reviews belong there as well.

That document hierarchy is more useful than repeating the same requirement in five documents. When a value or rule appears in more than one place, name the authoritative source and use references elsewhere. Otherwise, the first routine change creates conflicting instructions.

Establish the document hierarchy

Record the hierarchy used by the organization. Begin with externally imposed requirements and the board or executive policies that carry internal authority. Place ISMS policies beneath that governing layer. Standards and procedures then translate policy into testable criteria and repeatable work. Local instructions guide execution, while operating records show what happened. Define how conflicts are escalated. A local procedure must not quietly weaken a mandatory standard; a security policy must not purport to resolve a legal interpretation that belongs to qualified counsel.

Assign a controlled identifier only when the document enters the organization's control system. The toolkit identifier tells you which source template you opened. It does not automatically become the organization's identifier. If an existing numbering system is already maintained, use it.

For every controlled document, establish:

- title, identifier, version, status, owner, and approver
- purpose, audience, scope, exclusions, and relationship to the ISMS boundary
- source requirements and related internal documents
- effective date, communication route, competence or acknowledgement needs
- review interval and event-driven review triggers
- exception route and delegated authority
- change history, superseded version, retention, and disposal treatment
- the register or repository that proves current release and adoption.

The document owner maintains the content and coordinates review. A control owner is accountable for the design and performance of a control. A process owner is accountable for the process through which work is carried out. A risk owner owns the relevant risk decision. One person may hold several roles, but the roles should remain distinguishable because their decisions are not interchangeable.

Adapt a template from operational facts

Read the complete template rather than only its main paragraphs. Guidance text and prompts can carry assumptions; tables and appendices may do the same. Give each part one controlled editing decision:

- **Retain** when it already fits the approved need.
- **Adapt** when the structure fits but organizational facts or criteria differ.
- **Replace** when a different organization-controlled source must govern the subject.
- **Remove** when the content does not apply.

- **Escalate** when the author lacks the authority or evidence to decide.

These are working annotations, not final-document labels.

Use the following sequence:

1. **Confirm the governing need.** Link the proposed document to treatment decisions, applicable requirements, current operations, or an identified coordination problem.
2. **Define the affected population.** Name the services, information, technologies, locations, workers, suppliers, and events to which it applies. Avoid “all systems” unless the inventory and governance genuinely support that statement.
3. **Locate existing authority.** Identify current corporate policies, technical baselines, contracts, service procedures, and platform rules. Decide which source remains authoritative.
4. **Map the real workflow.** Record the trigger, inputs, decision points, roles, tools, hand-offs, output, retained record, and end condition. Include the non-routine route.
5. **Set workable criteria.** Use thresholds, time limits, classifications, approval levels, or baseline values that an owner can apply and an evaluator can test.
6. **Resolve responsibility.** Confirm who requests, approves, performs, verifies, records, reviews, and escalates the selected process. For a supplier-operated activity, preserve the organization’s retained responsibility.
7. **Specify records.** Name the authoritative destination, minimum fields, sensitivity, access, retention, and relationship to another register or source system.
8. **Design failure handling.** State what happens when a required step cannot be completed, a target is missed, a tool is unavailable, evidence is incomplete, or urgent action is necessary.
9. **Review with practitioners.** Walk one ordinary case and one difficult case through the draft. Correct the document when the actual work contradicts it; do not coach the interviewee into confirming the wording.
10. **Approve and adopt.** Remove prompts and sample text, complete document control, obtain the right approval, publish the current version, communicate it, supply any required training, and retain adoption records.

Wording becomes dangerous when it exceeds operational authority. “Backups are tested quarterly” is a factual claim about a defined population and period. Establish which backups the claim covers and how the test is performed. Name the responsible owner, define the response to failure and identify the retained result before approving the statement. If the operating design has not been decided, record an action rather than placing an unsupported promise in policy.

Policy template navigator

The 23 policy templates offer subject coverage, not a mandatory document architecture. Combine subjects where a smaller controlled set will be clearer. Separate them when the approval authority or audience differs materially. A separate review cycle or operational owner can also justify a separate document.

ID and template	Use when the organization needs to settle	Adaptation questions to resolve
CP-SRC-023: CP-POL-001 AI and Emerging Technology Security	Conditions for evaluating, acquiring, developing, or using emerging technology	Approved use, prohibited data or decisions, assessment authority, human oversight, supplier and model change, testing, monitoring, incident handling

ID and template	Use when the organization needs to settle	Adaptation questions to resolve
CP-SRC-024: CP-POL-002 Governance Roles and Responsibilities	ISMS authority and accountability	Leadership body, delegated approvals, role conflicts, deputies, reporting line, escalation and acceptance limits
CP-SRC-025: CP-POL-003 Information Security	The organization's overall information security direction	Business purpose, commitments, scope relationship, objectives, responsibility, consequences and review
CP-SRC-026: CP-POL-004 Intellectual Property and Confidentiality	Protection and permitted use of confidential or proprietary material	Ownership, licences, confidentiality duties, disclosure authority, marking, external material and departure obligations
CP-SRC-027: CP-POL-005 Asset Management	Accountability for information and other associated assets	Inventory boundary, ownership, acceptable use, return, authoritative inventory, discovery and reconciliation
CP-SRC-028: CP-POL-006 Data Masking and Data Loss Prevention	Conditions for masking and controls intended to prevent unauthorized disclosure	Data classes, channels, rules, tuning, alert handling, authorized override, false positives and monitoring responsibility
CP-SRC-029: CP-POL-007 Information Classification	Classification and handling decisions	Classification scheme, default, marking, handling by state and channel, reclassification, inherited labels and exceptions
CP-SRC-030: CP-POL-008 Information Transfer	Authorized movement and exchange of information	Transfer methods, recipient verification, agreements, encryption, physical transfer, failed delivery and evidence
CP-SRC-031: CP-POL-009 Privacy and PII Protection	Security-related treatment of personally identifiable information (PII)	Applicable obligations, roles, purpose and access boundaries, retention, incident route, processor or supplier duties; obtain specialist interpretation where required
CP-SRC-032: CP-POL-010 Records Retention and Disposal	Retention and defensible disposal	Record classes, owners, periods, holds, approved disposal, evidence of disposal and conflicts among obligations
CP-SRC-033: CP-POL-011 Acceptable Use and Remote Working	Permitted use of information-processing facilities and remote arrangements	Users, devices, locations, monitoring notice, prohibited activity, travel, household or public settings, reporting and return
CP-SRC-034: CP-POL-012 Endpoint and Removable Media	Security expectations for managed endpoints and portable media	Device classes, build ownership, encryption, patching, local privilege, media authorization, loss, quarantine and disposal
CP-SRC-035: CP-POL-013 Human Resources Security	Security duties across the working relationship	Screening where lawful, terms, onboarding, awareness, role change, disciplinary route, departure, contractor differences

ID and template	Use when the organization needs to settle	Adaptation questions to resolve
CP-SRC-036: CP-POL-014 Cloud Services Security	Governance of cloud selection, use, configuration and exit	Shared responsibility, approved services, data and region restrictions, identities, logging, resilience, supplier evidence, change and exit
CP-SRC-037: CP-POL-015 Supplier Security	Information security through supplier relationships	Population and tiering, due diligence, requirements, agreements, monitoring, material change, incident coordination, termination and concentration risk
CP-SRC-038: CP-POL-016 Backup and Recovery	Protection and restoration of information and systems	Population, frequency, isolation, retention, recovery objectives, restore testing, failures, ownership and dependency on providers
CP-SRC-039: CP-POL-017 Malware Protection and Endpoint Detection	Prevention, detection and response for malicious software and endpoint events	Coverage, exclusions, agent health, alert ownership, containment authority, evidence, tuning and unsupported systems
CP-SRC-040: CP-POL-018 Web Filtering and Internet Access	Web access and protective filtering	Populations and network routes, categories, inspection constraints, bypass authority, blocked-event review and privacy considerations
CP-SRC-041: CP-POL-019 Access Control and Identity Management	Identity lifecycle and access decisions	Identity sources, joiner/mover/leaver triggers, authentication, authorization, segregation, review, emergency access and shared-account restrictions
CP-SRC-042: CP-POL-020 Cryptography and Key Management	Approved cryptographic use and key lifecycle	Use cases, approved algorithms or services, key custody, generation, storage, rotation, recovery, revocation, destruction and regulatory constraints
CP-SRC-043: CP-POL-021 Network and Communications Security	Protection and administration of networks and communications	Network boundaries, segmentation, administration, remote access, service security, diagrams, monitoring, change and external connections
CP-SRC-044: CP-POL-022 Secure Development Lifecycle	Security through software and system development	Covered development, requirements, design review, code control, testing, dependencies, environments, release approval and urgent change
CP-SRC-045: CP-POL-023 Physical and Environmental Security	Protection of premises, secure areas and equipment	Site and zone model, entry, visitors, monitoring, environmental threats, equipment siting, maintenance, off-site assets and emergencies

An organization may need another policy or may decide that an existing enterprise policy adequately governs a subject. Record that choice in the SoA and document map. Do not reproduce an enterprise policy merely to make the toolkit folder look complete.

Standard template navigator

The supplied standards contain criteria that should be testable against a defined population.

ID and template	Establish before release	Operating connection
CP-SRC-046: CP-STD-001 Secure Configuration Baseline	In-scope technology classes, baseline authority, required settings, approved source benchmarks, deviation route, update and verification method	Configuration management, vulnerability management, change records, technical compliance review and exceptions
CP-SRC-047: CP-STD-002 Authentication, MFA and Secrets	Identity populations, multi-factor authentication (MFA) requirements, authenticator lifecycle, secret types, storage and transmission rules, recovery, emergency access and machine identities	Identity administration, privileged access, application development, supplier access, monitoring and periodic review

Avoid placing product-specific settings in the organization-wide standard when they change on a different cycle. The standard can state the mandatory outcome and controlled baseline source. Platform baselines or runbooks can then carry exact settings and retain the technical approval history.

Procedure template navigator

Each procedure should state its operating structure:

1. the event that starts the process
2. the maintained input on which the operator relies
3. the decisions that require authority
4. the output record; and
5. the route used when the expected sequence cannot be followed.

ID and template	Trigger and principal output	Failure or exception that must be rehearsed
CP-SRC-048: CP-PRC-001 Control Assurance and Security Testing	Approved assurance plan produces test results and remediation or acceptance decisions	Unsafe test, unavailable environment, inconclusive result, uncontrolled finding disclosure
CP-SRC-049: CP-PRC-002 Document and Record Control	New or changed documented information produces an approved current version and controlled history	Urgent release, conflicting copy, inaccessible authoritative version, retention hold
CP-SRC-050: CP-PRC-003 Evidence Collection and Preservation	Evidence need produces an identified, protected, reviewable record	Volatile source, restricted access, failed export, unclear provenance, integrity concern
CP-SRC-051: CP-PRC-004 Legal and Regulatory Compliance	New, changed, or scheduled requirement review updates the obligations record and affected controls	Conflicting interpretation, missed change, unclear jurisdiction, overdue owner response
CP-SRC-052: CP-PRC-005 Objectives and Compliance Review	Planned review produces measure results, analysis, action and reporting	Bad denominator, missing data, target missed, measure no longer informs a decision
CP-SRC-053: CP-PRC-006 Risk Assessment and Treatment	Trigger or planned review updates approved risk and treatment records	Incomplete population, method inconsistency, unavailable owner, overdue treatment or acceptance

ID and template	Trigger and principal output	Failure or exception that must be rehearsed
CP-SRC-054: CP-PRC-007 Supplier Assurance	New, changed, renewed, monitored, or terminated supplier relationship updates assessment and action records	Supplier refuses evidence, service changes unexpectedly, issue is overdue, exit route fails
CP-SRC-055: CP-PRC-008 Capacity and Performance Management	Forecast, threshold, degradation, or review produces capacity decisions and action	Monitoring gap, sudden demand, third-party constraint, breached threshold
CP-SRC-056: CP-PRC-009 Change and Configuration Management	Proposed or emergency change produces approval, implementation result and current configuration record	Failed change, unauthorized change, rollback failure, emergency approval, incomplete configuration update
CP-SRC-057: CP-PRC-010 Clock Synchronization	Build, review, drift, or source failure produces synchronized time settings and exception handling	Untrusted time source, excessive drift, isolated asset, timestamp inconsistency during investigation
CP-SRC-058: CP-PRC-011 Logging, Monitoring and Detection	Defined events and detection use cases produce collected logs, alerts, triage and retained cases	Source silence, time error, excessive noise, missed alert, storage limit, restricted log content
CP-SRC-059: CP-PRC-012 Threat Intelligence	Scheduled or event-driven collection produces assessed relevance and an assigned response	Unverified report, duplicate noise, urgent credible threat, intelligence that cannot be shared broadly
CP-SRC-060: CP-PRC-013 Vulnerability and Patch Management	Discovery or advisory produces validated findings, prioritization, remediation and closure evidence	No patch, failed deployment, unsupported asset, disputed severity, expired exception
CP-SRC-061: CP-PRC-014 Privileged Access Management	Privileged need or lifecycle event produces approved, time-bound access and review evidence	Emergency access, orphaned account, failed vault, unreviewed activity, overdue revocation
CP-SRC-062: CP-PRC-015 Application Security Testing	Development or release gate produces scoped test results and disposition	Environment unavailable, finding accepted without authority, release urgency, test limitation
CP-SRC-063: CP-PRC-016 Security in Project Management	Project initiation or change produces security requirements, risk decisions and gate records	Security engaged late, project bypass, unresolved requirement at release, ownership after handover
CP-SRC-064: CP-PRC-017 Source Code Repository and Secrets	Repository or contributor lifecycle produces controlled access, protected secrets and monitoring records	Exposed secret, branch protection bypass, external contributor, unavailable scanning
CP-SRC-065: CP-PRC-018 Test Data and Environment Management	Test need or environment change produces approved data, segregation and disposal records	Production data appears in test, shared credential, unmanaged environment, delayed disposal
CP-SRC-066: CP-PRC-019 Business Continuity and ICT Readiness	Analysis, plan review, exercise, or disruption produces maintained information and communication technology (ICT) recovery arrangements and lessons	Recovery dependency unavailable, test objective missed, unsafe workaround, unplanned invocation
CP-SRC-067: CP-PRC-020 Incident Response	Report or detection produces triage, containment, investigation, recovery, communication and lessons	Severity dispute, unavailable lead, evidence risk, external notification question, prolonged incident

ID and template	Trigger and principal output	Failure or exception that must be rehearsed
CP-SRC-068: CP-PRC-021 Secure Disposal and Reuse of Equipment	Reuse, return, transfer, or disposal produces authorization and verified treatment records	Device cannot be sanitized, custody gap, failed destruction evidence, retained component

Several procedures may act on the same case. A threat-intelligence assessment can open a vulnerability case for an exposed service. That case may require an emergency change and a security test. If the change cannot be completed normally, an exception or incident investigation may follow. Supplier action and risk reassessment can then address dependencies outside the immediate technical fix. Use stable references. Do not paste the whole case into every workbook and expect the copies to stay synchronized.

Adoption is part of implementation

Approval establishes authority; it does not establish use. Identify affected roles and decide what each group must understand or demonstrate. Communication may be sufficient for a simple change. A technical standard may require instruction and a practical check. Emergency work or a new incident role usually needs rehearsal and observation.

Record who received the release and which version was communicated. State the method and date, then retain completion or acknowledgement where it is meaningful. Give unresolved questions an owner and follow-up. If the rule changes an existing workflow, update the forms and access needed to carry it out. Automation and service targets must agree with the released rule. Check supplier instructions and local runbooks as well. Publishing a policy while the old workflow remains in place creates two operating systems.

Adoption review should use current cases. Select a small sample after the effective date. Check whether people found the current instruction and applied its criteria. Then locate the required record and, where the case departed from the normal route, test the escalation. Interpret a failure from its facts. An unclear document or unavailable tool points to design and enablement. Insufficient competence or a local workaround points to adoption. Weak supervision and deliberate noncompliance require a different management response.

Control exceptions and policy waivers

Use the organization’s approved terms consistently. An exception usually permits a defined departure from a control or standard under stated conditions. A waiver may refer to an authorized release from a particular requirement. The label matters less than a controlled process that prevents indefinite, invisible departures.

An exception record should identify:

- the exact requirement and affected asset, process, service, population, or location
- the business reason and requested duration
- related risks and obligations
- compensating or interim controls
- requester, technical reviewer, control owner, risk owner, and approval authority
- start, expiry, review, and revocation conditions
- monitoring and evidence requirements
- actions needed to restore conformity with the normal rule or adopt a different approved treatment
- linked risk, change, incident, supplier, action, and SoA records.

Emergency action may sometimes precede the usual approval. Name the role that can invoke it and set the maximum duration. Require immediate safeguards and a defined retrospective review. State the condition that turns the case into an incident or requires management escalation. Do not convert repeated emergency approvals into an unofficial permanent standard.

Govern document change

Document review is not satisfied by changing the next-review date. Reopen the content when its governing basis changes:

- a changed requirement, scope or risk decision
- a change to the control design or supporting technology
- a changed supplier, workflow or responsible role; or
- a different evidence destination or approved technical term.

Review a sample of records and ask practitioners where the document no longer matches actual process operation.

Classify the proposed change. A correction to spelling has a different review need from a changed access criterion or incident authority. Trace the effect through the system:

- revise dependent documents and tools
- update training and contractual instructions where the operating rule changed
- review active exceptions plus the underlying risk-treatment and SoA decisions
- correct affected measures and audit criteria; and
- withdraw or amend any external claim that no longer matches the approved position.

Approve the change at the correct level and release it. Withdraw superseded copies, communicate the new rule, and verify adoption where the effect is material.

Keep superseded information according to the approved retention and disposal rules. It may be needed to explain which instruction applied when an earlier record was created. Prevent normal users from mistaking it for the current release.

Test one instruction set in operation

Choose one necessary control from Module 5 that already has operating activity. Build its complete linked instruction set.

1. State the control purpose, affected population, owner, operating criteria, evidence source, and failure route.
2. Identify the existing policy, standard, procedure, runbook, form, system rule, and register that touch it.
3. Mark duplicate or conflicting statements and choose the authoritative source for each changing rule.
4. Observe one ordinary case and one difficult case. Record where the draft process diverges from practice.
5. Adapt only the documents needed to close the identified gaps.
6. Walk through the revised instruction set with the people who request, approve, perform, verify, and review the process.

7. Route the documents through approval and adoption. Define the first sample that will test use after the effective date.

Give the released instruction set to an operator who did not draft it. The operator should be able to explain each document’s purpose and distinguish a governing policy from a testable standard. The procedure must lead into the local runbook and retained record without blurring their authority. Ask the operator to apply the criteria to the right population and handle one non-routine case. During the same exercise, check who owns and approves the instruction. Test its exception and change routes, then confirm that a superseded version cannot be mistaken for the current one. Any private explanation the author still has to supply belongs in the repair log.

The tested instruction set now creates a record contract for Module 7. It identifies the authoritative destination and required fields, then defines stable identifiers and access. It also fixes the retention period, review point, and correction route. If any of those remain implicit, the record design must expose the gap rather than make the operator compensate with a private spreadsheet.

Turn the Guide Into a Working ISMS

Get your clausepass27001 toolkit

Laboratory B: Adapt and rehearse one control implementation trace

This laboratory removes part of the scaffold. Begin with a necessary control, not with a favourite template, and explain why each link is sufficient before using the acceptance clauses. Use a real control within the approved ISMS scope. If live information cannot be used in the learning setting, select one existing fictional Hearthline teaching case from CP-SRC-123 or CP-SRC-128 through CP-SRC-130 and keep its fictional label visible throughout. Reviewer feedback must identify the failed link and the governing source to repair.

Materials

Assemble the material in governing and execution order:

1. the current scope and risk record
2. the treatment decision and its SoA entry
3. any instruction that already governs the selected process
4. the selected policy, standard or procedure template; and
5. one operating case that can be walked through.

Also bring the document register and the approved exception mechanism. Those two sources show how the result will be controlled after release.

Part 1: Establish the source-to-operation links

Build the page as a trace rather than an inventory. Begin with the applicable requirement or risk and show the treatment outcome it produced. Link that outcome to the necessary control, then to the policy position that authorizes it. From there, follow the operating criteria into the procedure and its evidence source. End with the method that will evaluate the result. Mark every broken link. If two sources claim authority for the same setting or approval, resolve that conflict before drafting.

Part 2: Test the population

Define the population across three dimensions:

- **Operational boundary:** the services, systems and information involved.
- **Place and participation:** the relevant locations, workers and suppliers.
- **Trigger boundary:** the event types that put the instruction into use.

Now choose one easily missed case. A service account may expose a people-and-access gap; a temporary worker can do the same. An unmanaged device tests the technical boundary, while an emergency change tests the route around normal timing. An inherited supplier or archived record can show whether the boundary survives time and external dependency. Establish whether the proposed instruction handles the selected case and whether an omission changes the treatment or scope assumptions.

Part 3: Run two cases

Walk an ordinary case from trigger to retained record. Then choose a difficult case that tests the control at one particular pressure point:

- a missing prerequisite
- a missed target time
- an unavailable approver
- a supplier that refuses necessary information; or
- a need for urgent action.

Participants must use only the documented authority and sources available to an operator. Note every point where they have to ask the document author what was meant.

Part 4: Repair and release

Revise the smallest appropriate set of documents. First confirm what the operator must decide and who holds each responsibility. Trace every hand-off to its destination record. Then test the exception route and its escalation authority. Complete the organization's document-control fields and obtain approval. Communicate the released instruction, addressing any competence gap found in the walkthrough. Finally, set the first post-release sample and name its reviewer.

Deliverables

The submission is complete only when every deliverable meets its acceptance clause.

Deliverable	Acceptance clause
One-page control implementation trace	A reviewer can move from requirement or risk through treatment, control, instruction, record, and evaluation without oral explanation
Population and boundary note	Included and excluded cases are explicit, and the difficult case falls inside a reasoned boundary decision
Two walkthrough records	One ordinary and one difficult case preserve their trigger, route, decision, timestamps, exception handling, and resulting record
Adapted controlled documents	The smallest sufficient document set contains executable criteria, authority, hand-offs, evidence destination, and failure route
Approval and adoption record	The approved version, authority, effective date, communication, and competence response are identifiable
First-operation sampling plan	The proposition, population, sample method, reviewer, timing, and adverse-result route are fixed before review
Repair actions	Each discovered risk, SoA, supplier, system, or register defect has an owner, destination record, and completion condition

Review

The reviewer traces the released documents back to the treatment decision and forward to a real record. Reject the submitted document set when any of these conditions is present:

- the operator needs undocumented knowledge
- an exception lacks authority or expiry
- a supplier duty has erased responsibility that the organization retains; or
- the policy claims operation that has not yet occurred.

Module 7: Make the registers carry the system

The toolkit includes 23 operational workbooks. They cover a useful range of ISMS work, but they should not become 23 competing databases. Decide which changing facts each workbook will govern, which facts remain in an existing business system, and how references will connect them. The aim is a maintained record topology in which an authorized person can locate the current state and its history without reconciling private copies.

Read `05 ISMS Registers, Plans and Logs/00 Start Here.docx` (CP-SRC-078) and `01 Maintaining ISMS Registers, Plans and Logs.docx` (CP-SRC-079) first. Before entering live data, inspect the workbook as a working instrument. Check its worksheets and named tables. Trace the validation rules and formulas, then read the instructions and sample rows. Make structural changes in a controlled master, test them in a copy, and record the reason. A convenient spreadsheet must not weaken record identity or approval. It must also preserve history and the relationships between records.

Choose the authoritative record

An authoritative record is the approved source used for a defined fact or case. A supplied workbook may serve that purpose, but so may a specialist business platform. Identity and access facts often belong in the identity system; asset facts may belong in an asset repository. Learning or contract records may already have their own controlled applications. Choose the source by asking who owns the data and who can gain access. Then test whether it preserves usable history and supports the real workflow. Finally, confirm that it can retain and reproduce the information the ISMS needs for reporting.

For each workbook, decide among three uses:

Authoritative. The workbook holds the maintained record. Name its administrator and define the access model. Set the backup and recovery arrangements. Document how entries are validated and reviewed, then control structural change and archival.

Referential. Another approved system governs the detailed data. The workbook identifies the governed record and carries only what the ISMS needs to interpret it. That may include a scope field or review result. Define how broken links and mismatches are detected.

Temporary migration or analysis. The workbook supports bounded import, reconciliation, or review work. Give the temporary copy an owner and an end date. State how it will be disposed of. Make clear that it cannot become an unnoticed parallel source.

Do not make a workbook authoritative merely because it arrived with the toolkit. Conversely, do not dismiss it because a larger platform exists. Confirm that the platform carries the fields the ISMS needs and preserves their history. Its access model and review process must also fit the intended use.

Design identifiers before links

Assign a stable identifier whenever a record must be cited outside its own row. Use one scheme across each record family, not one improvised convention per worksheet.

Record family	Records that need a durable identity
Scope and obligation	Assets, suppliers and requirements
Risk and control	Risks, treatments, controls and SoA entries
Operational case	Exceptions, incidents and vulnerabilities
Assurance	Evidence items, audits, findings and corrective actions
Governance	Documents, objectives, changes and management actions

People and roles should normally be referenced through the organization's authoritative directory or role model. Avoid identifiers based only on row number. Sorting or deletion can change the row while the case remains the same; copying can duplicate it.

Document how identifiers are issued. Specify the prefix and sequence, then name the issuing source. Add a uniqueness check. For imported records, preserve the former identifier and define how it maps to the new one. State whether an identifier may ever be reused. If a new record supersedes another, link them; do not silently overwrite the history.

Relationships should support a trace such as:

```
service or asset → requirement or risk → treatment → control → SoA entry → instruction → operating record → evidence → measure or audit finding → corrective action → management decision
```

Not every link belongs in every workbook. Store it where the relationship is governed and use a stable reference elsewhere. Document the minimum links required for the organization's reporting and review work.

Set field rules and states

Create a short data dictionary for each authoritative workbook. It should answer the following questions.

Field rule	Question the dictionary must answer
Meaning	What fact does this field represent?
Authority	Who may set or change it?
Input	Which values and format are permitted?
Provenance	Which source supports the value?
History	How is a change recorded?

Pay particular attention to status fields. A label such as "open" says little without a defined starting event. "Implemented" does not necessarily mean effective, and "accepted" is not the same as "closed."

A case normally needs more than one state dimension. For a vulnerability, validation establishes that the condition is real. Assignment and scheduling govern the response. Remediation does not finish the record because technical retest and any residual-risk decision may occur later. A finding can have an immediate correction while its corrective action remains open. A treatment action can be completed before the control has operated long enough to evaluate effectiveness.

Give every date a defined event meaning. The following groups cover the common distinctions.

Date group	Event represented

Date group	Event represented
Discovery	Identified or reported
Authority	Approved or made effective
Commitment	Due or scheduled
Performance	Completed or reviewed
Decision	Accepted or closed
Time limit	Expired

Avoid a single “date” column. Store the time zone where event order matters. Keep the source period with imported metrics and audit evidence.

Workbook navigator

The table below routes each supplied workbook. The named business system may replace it only after the organization confirms that the same purpose and necessary history are controlled there.

ID and workbook	Maintained subject	Minimum connections and review
CP-SRC-080: Asset Register	Information and other associated assets within the adopted inventory boundary	Owner, service, classification, location or custodian, lifecycle state, supplier, risk and return/disposal; reconcile with discovery and business ownership
CP-SRC-081: Backup and Restore Test Log	Backup jobs or arrangements and restore-test results	Protected population, method, frequency, retention, result, failure, recovery objective, action and evidence; review gaps and failed restores
CP-SRC-082: Business Continuity and Recovery Test Register	Exercises and tests of continuity and ICT readiness arrangements	Plan, scenario, objective, participants, dependencies, result, observed gap, action and retest
CP-SRC-083: Business Impact and Continuity Requirements Register	Prioritized activities and their continuity requirements	Service owner, impact over time, dependencies, recovery objectives, minimum resources, approval and change trigger
CP-SRC-084: Change Register	Security-relevant normal, standard, urgent, or emergency change	Request, affected assets/services, assessment, approval, implementation, test, rollback, result, incident/problem and configuration update
CP-SRC-085: Context, Interested Parties and Scope Register	Context issues, interested parties, requirements, scope components, exclusions, interfaces and dependencies	Source, owner, relevance decision, scope effect, external provider, review trigger and scope-statement version
CP-SRC-086: Evidence Register	Evidence specifications, locations, collections, custody, access and review status	Control/process, population, period, source owner, collector, integrity or provenance, retention, restriction, audit use and gap

ID and workbook	Maintained subject	Minimum connections and review
CP-SRC-087: Exceptions and Waivers Register	Authorized departures from requirements or baselines	Exact requirement, affected population, reason, risk, compensating control, approval, expiry, monitoring, action and closure
CP-SRC-088: Findings, Nonconformity and Corrective Action Register	Evaluation results, nonconformities, corrections, causes, corrective actions and effectiveness reviews	Source, criteria, evidence, scope, owner, due dates, related cases, verification and closure authority
CP-SRC-089: Internal Audit Plan and Checklist	Audit programme, engagement plans, criteria, sampling prompts and results	Objectives, scope, criteria, auditor competence/independence, timing, process status, previous results, evidence, findings and report
CP-SRC-090: ISMS Implementation Plan and Action Tracker	Approved implementation and improvement actions	Outcome, owner, authority, dependency, resources, due date, completion condition, evidence, blocker and escalation
CP-SRC-091: ISO 27001 Gap Assessment	Baseline assessment of arrangements against identified criteria	Requirement reference, current state, source, evidence, gap, consequence, action and verification; do not use as a certification verdict
CP-SRC-092: Legal, Regulatory and Contractual Requirements Register	Identified information-security obligations and interpretations	Source, jurisdiction, applicability, qualified owner, requirement, affected process/control, review date, change and evidence
CP-SRC-093: Management Review Actions and Performance Register	Management-review inputs, measures, decisions, actions and follow-up	Review date, participants/authority, input source and period, decision, owner, due date, resources, completion and next review
CP-SRC-094: Master Document Register	Controlled documented information and its release state	Identifier, title, type, owner, approver, version, status, effective date, location, review trigger, retention and superseded version
CP-SRC-095: Risk Register and Risk Treatment Plan	Information security risk scenarios, assessments, treatment and residual-risk decisions	Scope, owner, method version, sources, controls, evaluation, treatment, actions, SoA, evidence, reassessment, acceptance and trigger
CP-SRC-096: Security Incident Register	Reported events and incidents through triage, response, recovery and lessons	Reporter/source, affected service/assets/data, severity, chronology, actions, evidence, communication decision, root or contributing cause and follow-up
CP-SRC-097: Security Objectives and KPI Register	Information security objectives and associated key performance indicator (KPI) monitoring and measurement	Objective, owner, baseline, indicator, method, population, source, frequency, target, result, analysis, limitation and action
CP-SRC-098: Statement of Applicability	Necessary controls, Annex A comparison, inclusion/exclusion reasoning and implementation status	Risk/requirement basis, owner, implementation sources, evidence, status date, open action, exclusion justification, approval and version

ID and workbook	Maintained subject	Minimum connections and review
CP-SRC-099: Supplier Register and Assessment	In-scope suppliers, services, information access, dependencies, assurance and issues	Business owner, service, tier, data/access, locations, subcontractors, requirements, assessment source, findings, monitoring, change, renewal and exit
CP-SRC-100: Training and Awareness Register	Role-based competence, awareness activities and completion or evaluation	Population, learning need, content/version, delivery, completion, assessment, overdue case, exception, role change and follow-up
CP-SRC-101: User Access Register and Access Review	Access assignment and review where another identity system is not authoritative	Identity, role, system, entitlement, approver, provision date, authentication condition, review, discrepancy, action and revocation
CP-SRC-102: Vulnerability and Patch Register	Validated vulnerabilities, exposure, prioritization, remediation and exceptions	Asset/service, source, identifier, exploit context, severity basis, owner, due date, patch/change, test, exception, retest and closure

Protect sensitive records

The workbooks do not all carry the same sensitivity. Technical records may expose weaknesses or system architecture. Incident and access records can reveal personal information. Supplier files may contain commercial concerns, while continuity records disclose recovery arrangements. Apply access by job need and separate administration from ordinary contribution where the platform permits it. Prevent uncontrolled sharing links and local downloads. Put the records within the approved backup and recovery arrangements. Their retention must also account for legal holds and secure disposal.

Do not turn a register into a secret store because a nearby cell appears convenient. Passwords and recovery codes belong in the approved authentication system. Private keys belong in managed key storage. Keep exploit material and unnecessary personal data out of the workbook. The register should retain only the identifier or restricted reference needed for the case.

Some evidence may need to remain hidden from the general ISMS team or from an auditor without the required clearance. The register can still prove that it exists. Record its identifier and owner, then state the covered period and approved access route. Keep the review result without reproducing the restricted content. Access can then be arranged under the appropriate conditions.

Maintain data quality

Data quality needs an owner and a routine. Use validation lists for controlled values, but keep the list under change control. Protect formulas and identifiers. Test filters and pivots after structural change. Record imports and transformations. Run a uniqueness check on identifiers and an integrity check on dates. Find records without an owner or with overdue work. Look separately for expired exceptions and broken references. Finally, test whether linked status values contradict one another.

Review frequency should follow the subject. An incident log may change during the day; a scope review may be scheduled annually and triggered by material change. “Quarterly review” is not automatically suitable for both. Name the event trigger and any calendar trigger. Identify the reviewer and the check that person performs. The procedure must say how the resulting decision becomes an owned action.

Use a population total before interpreting percentages. A report that says 95 per cent of access was reviewed is incomplete if the population source and excluded accounts are unknown. Preserve the denominator and extraction time. Document exclusions, then account for duplicate or failed records. Associate the result with its reporting period. Reconcile critical totals to their source systems.

Control workbook changes

Treat structural changes differently from record updates. Adding a risk entry is ordinary operation. Renaming a field or changing a risk formula can alter the meaning of many records. So can a revised validation value or a deleted worksheet. Assess the structural change and obtain approval before release. Test it on representative data and preserve the earlier version. During migration, document how the conversion affected existing records.

If a workbook becomes too large or workflow-dependent, plan migration before it becomes unreliable. Organize the migration plan around four controls.

Migration control	Required decision
Meaning	Target data model and mapping from each source field
Transfer boundary	Source cut-off, duplicate resolution and treatment of rejected rows
Acceptance	Reconciliation totals and tests that authorize use
Transition	Access, rollback and archival, including the date the new system becomes authoritative

During transition, label both sources clearly. Do not allow silent dual entry.

Reconcile the system

Run a relationship review on a manageable sample. Start with one service and a supplier that supports it. Follow a related risk into its necessary control, then find the relevant exception or open operational case. Continue through an audit finding to the management action, where those records exist. Follow the identifiers across the authoritative sources.

Resolve these common breaks:

- an asset has no service or accountable owner
- a requirement has no applicability decision or affected control
- a risk treatment names a control absent from the current SoA
- the SoA states implemented while the action remains planned
- an exception is expired but still used as authority
- an evidence entry points to a moved or inaccessible file
- an audit finding and its corrective action use unrelated identifiers
- a supplier’s service changed without scope or risk review
- a management-review action was copied into a separate tracker and closed in only one place.

Correct the authoritative source. Then update references and derived reports. Preserve enough history to explain the correction. If the break shows a failure to meet a requirement, use the nonconformity and

corrective-action process. If it changes exposure, reassess the risk. If the repair alters the system itself, place that alteration under change control. Do not merely edit the appearance of the records.

Prove the record topology

Build a register topology for the organization. Use one row per supplied workbook and organize the decision fields as follows.

Decision area	What to record
Adoption	Authoritative, referential, temporary or not adopted
Accountability	Business owner and administrator
Custody	Approved location and sensitivity class
Record identity	Key identifier and any governing source system
Use	Downstream consumer and review trigger
Lifecycle	Retention rule and known migration issue

Then test one end-to-end record trace. Give the test to a reviewer who did not build the registers. That person should locate the source facts and distinguish current state from planned activity. The reviewer should also reproduce the relevant report total, find its approval, and follow an open condition to its owner. Record every manual reconciliation the reviewer needed. A private explanation usually points to a missing field rule or relationship; it may instead reveal that the procedure itself is unclear.

Move into the first operating cycles only after the authoritative sources are named and the important relationships can be traced. Identifiers must survive sorting and migration. Status fields need controlled meanings, and sensitive records need suitable restrictions. A structural workbook change requires more control than an ordinary case update. Owner reviews should already have a route for corrections and actions.

The topology is ready for operating pressure when another practitioner can reconstruct a case without its author. Module 8 uses that condition to test ordinary, difficult, and event-driven work; any missing relationship returns to the authoritative register or instruction that owns it.

Turn the Guide Into a Working ISMS

Get your clausepass27001 toolkit

Module 8: Run the first operating cycles

An approved document and a configured tool establish only part of implementation. A selected process must reach its intended users and produce real records. Its exceptions need an authorized route, and its owner must review the result. The first operating cycles are planned opportunities to find where the design meets or misses real work.

Use the implementation plan (CP-SRC-090) to schedule these cycles. Use the operating model and adoption sources (CP-SRC-020, CP-SRC-021, CP-SRC-071, and CP-SRC-072) to confirm governance. Place results in the appropriate records described in Module 7. The implementation lead coordinates the first operating cycle; process and control owners remain responsible for operation.

Define the operating unit

For each process, identify what counts as one case or one cycle. Choose the unit according to the process being observed.

Operating family	Suitable unit of observation
Identity	One access request or one leaver
Technical operation	One production change, vulnerability or restore test
External dependency	One supplier assessment or information transfer
Event response	One reported security event or policy exception
Governance	One audit engagement or scheduled review

State the population and observation period. “Access review completed” means little until the reviewer can identify the people and systems within scope. The population boundary should also explain which entitlements were tested. Account classes need explicit treatment, especially privileged or externally held access. Record the dates covered by the review. For continuous processes, choose a period long enough to include ordinary variation. For infrequent controls, use a planned exercise or inspect an earlier comparable event, while labelling the limits of that evidence.

An operating-cycle card should contain:

Field	What to establish
Process and purpose	What result the process is meant to achieve and which control or requirement it supports
Population	The complete set of cases, assets, users, suppliers, systems, or events from which work arises
Trigger and frequency	Event, threshold, schedule, request, alert, or change that starts the process
Entry criteria	Required input, authority, information, and system availability
Roles	Requester, approver, performer, verifier, record owner, reviewer, and escalation authority

Field	What to establish
Ordinary route	Expected sequence, decisions, hand-offs, output, and completion condition
Non-routine route	Rejection, delay, emergency, exception, tool failure, dispute, or missing information
Records	Authoritative source, required fields, evidence, sensitivity, and retention
Service criteria	Time, quality, coverage, approval, or other operating limits
Review	Owner review, sampling method, issue route, and next cycle

Sequence by dependency

Some processes create prerequisites for others. Identity lifecycle work depends on a usable population of people, roles, and systems. Vulnerability management depends on asset and service identification. Supplier assurance depends on a supplier population and owned contracts. Monitoring first needs defined sources and synchronized time. It also needs a detection owner and controlled storage. Internal audit depends on criteria and an operating period that can be sampled.

Schedule the first cycles in that order. When a prerequisite is weak, record and repair it; do not compensate by declaring the dependent process complete. The implementation plan should show the next operating opportunity as well as the document or technology delivery date.

Use a small number of representative processes first. Select those that cross organizational boundaries, carry material risk, or create evidence needed by several later activities. Follow one access lifecycle and one production change from beginning to end. Add a vulnerability or supplier case to test ownership across boundaries. A restore test or reported security event can expose the recovery route. Together, these cases reveal more about the operating model than a mass release of policies.

Prepare without rehearsing the answer

Brief participants on the approved process, their authority, and the location of current instructions. Supply access to the required systems and forms. Confirm who will observe, how sensitive information will be handled, and how a real operational issue will be escalated during the exercise.

Do not give participants a pre-filled ideal record or privately guide them past unclear steps. The first cycle should test whether the adopted system is usable. An observer may stop an unsafe action or protect confidential information. The observer may also clarify the boundary between an exercise and live operation. Record the point of every intervention.

Where a simulation is necessary, label it. Describe the assumed facts and simulated timing. Identify any system that was represented rather than used. Then distinguish simulated decisions or communications from what observers saw in the live environment. Simulation can demonstrate understanding and uncover design gaps; it does not establish that an event-driven control has operated over a real population and period.

Observe the ordinary case

Start at the actual trigger. Check whether the case enters the process without the implementation lead noticing it first. Follow the approved path and preserve its natural timestamps. Record each decision and hand-off as it occurs. The case output should lead to its authoritative record. Ask the performer to use the released instruction rather than a draft or a private checklist.

The observer should note:

- whether the case belongs to the defined population
- whether required inputs were available and trustworthy
- whether the assigned role had the authority and access needed
- where a decision criterion was interpreted differently by participants
- whether hand-offs preserved ownership and target time
- whether the authoritative record was updated at the point of work
- whether required evidence can be located by its identifier
- whether completion was checked rather than assumed
- whether the process produced an unexpected risk, change, or obligation question.

Avoid correcting the workbook after the case so that it resembles the expected route. Keep the original operating record, record the defect, and make any authorized correction with its date and reason.

Run the non-routine case

Choose a credible variation that stresses a known failure mode.

Failure mode	Example variation
Authority	Rejected access request or unavailable approver
Urgency	Urgent production change or alert during staff absence
Technical recovery	Failed restore or vulnerability without a vendor patch
External dependency	Supplier that will not provide the expected assurance
Record integrity	Incomplete evidence export or expired exception
Confidentiality	Case record containing restricted information

First confirm that the operator recognizes the departure and keeps an owner on the case. Where an interim safeguard is necessary, the operator should know who may authorize it. Any affected party must receive the required communication. The case record should show how and when work returned to the normal route. Measure how long the case remains without an owner or decision.

If participants invent an approval or workaround because the documented route fails, stop and capture the exact gap. A design defect may require a procedure or tooling change. An authority gap may call for role delegation, while a knowledge gap may justify competence work. Problems across an external boundary may require a revised service agreement. Material exposure belongs in risk reassessment or before management for decision. It is not automatically a training problem.

Use the toolkit records during operation

The workbooks support different points in the cycle:

- the Asset Register supplies owned population and lifecycle information
- the Change Register carries implementation, test, rollback, and result records
- the User Access Register or authoritative identity source carries entitlement decisions and reviews
- the Vulnerability and Patch Register carries exposure, priority, remediation, exception, and retest
- the Supplier Register carries service tiering, assessment, findings, monitoring, and change
- the Backup and Restore Test Log and continuity test register carry planned tests, results, failures, actions, and retests
- the Security Incident Register carries chronology, classification, response, evidence, communication decisions, recovery, and lessons
- the Exceptions and Waivers Register carries authorized departures and expiry
- the Training and Awareness Register carries the defined audience, content version, completion, assessment, and follow-up
- the Evidence Register locates protected sources and records their review state
- the Implementation Plan carries design or rollout actions that arise
- the Findings, Nonconformity and Corrective Action Register carries qualifying evaluation results and their resolution.

Do not open every workbook for every case. Define the primary case record and use references when a linked process becomes necessary. An incident may lead to a vulnerability record and emergency change, but the chronology should still have one authoritative home.

Review the result with the owner

The process owner reviews the complete population or a justified sample. Establish how the sample was selected and what was excluded. Compare the record with the approved criteria. Record observed conformity as well as departures; otherwise later readers cannot tell whether only problems were examined.

Classify what happened without rushing to a label:

Observation	Likely route
Individual entry contains a correctable data error and the process design remains sound	Controlled correction and owner review
Required step was missed in one case	Assess consequence; correct the case; determine whether broader action is needed
Procedure does not cover a recurring real condition	Document/process change and assessment of affected completed cases
Tool or access prevents the assigned role from acting	Operational repair, action tracking, possible risk reassessment or interim control
Approved requirement was not fulfilled	Evaluate as a potential nonconformity using the applicable criteria and evidence
Control operated but did not achieve its intended result	Control and risk review; treatment may require redesign

Observation	Likely route
Evidence is too weak to determine performance	Record the limitation; improve collection; do not infer success or failure

Separate correction of the sampled case from action intended to prevent recurrence. Module 10 develops that distinction. During early operation, record what appears to have caused the departure. Identify the affected population and note whether the condition has recurred. That information supports the later decision.

Avoid manufactured maturity

Do not backdate evidence. A review or approval must carry the date on which it actually occurred. The same rule applies to competence records and operational tests. Access removal and supplier assessment records must preserve their real timing, as must management decisions. Do not populate several months of fictional metrics to make a dashboard look established. If a control has reached only one operating opportunity, report one result and its limits.

Where historical business records exist, they may be assessed against the current purpose. Identify their source and the population they cover. State the criteria used for the new assessment, along with the evidence limits. A restore performed before formal ISMS adoption might supply useful technical evidence. It does not become an ISMS review performed under a procedure that did not yet exist.

Use the implementation status that the evidence supports:

- **designed**: the control and operating criteria are defined
- **enabled**: required tools, access, roles, and instructions are available
- **adopted**: the intended population has received the applicable direction or competence support
- **operated**: cases or cycles have occurred and records exist
- **reviewed**: an authorized owner has evaluated the results
- **effectiveness evaluated**: suitable evidence has been compared with the intended control result
- **changed or accepted**: an authorized response has been recorded.

The organization may use different labels, but each label needs a controlled definition. Never let “implemented” silently cover all of them.

Assemble the first-cycle plan

Plan enough operation to test the management system, not merely the easiest controls. Include:

1. the process and owner
2. complete population or expected volume
3. first natural operating opportunity
4. any safe simulation needed for a rare event
5. ordinary and non-routine cases
6. participating roles and observers
7. released instruction and system access
8. authoritative record and evidence destination
9. owner review date and sampling method
10. route for defects, risks, findings, changes, and lessons
11. dependency on another process

12. the next cycle needed to establish repeatability.

Stagger the operating cycles. Owners need time to respond to what the first cases reveal. Running every procedure in the same week tends to produce staged records and a corrective-action backlog that nobody can analyse.

Run and review three operating cases

Select three processes that stress different parts of the system. Begin with a frequent administrative process. Add a technical or supplier process, then choose an event-driven or recovery process. For each, define the operating unit and population. Run or observe one ordinary case and one difficult case. Have the owner review the resulting records without assistance from the implementation lead.

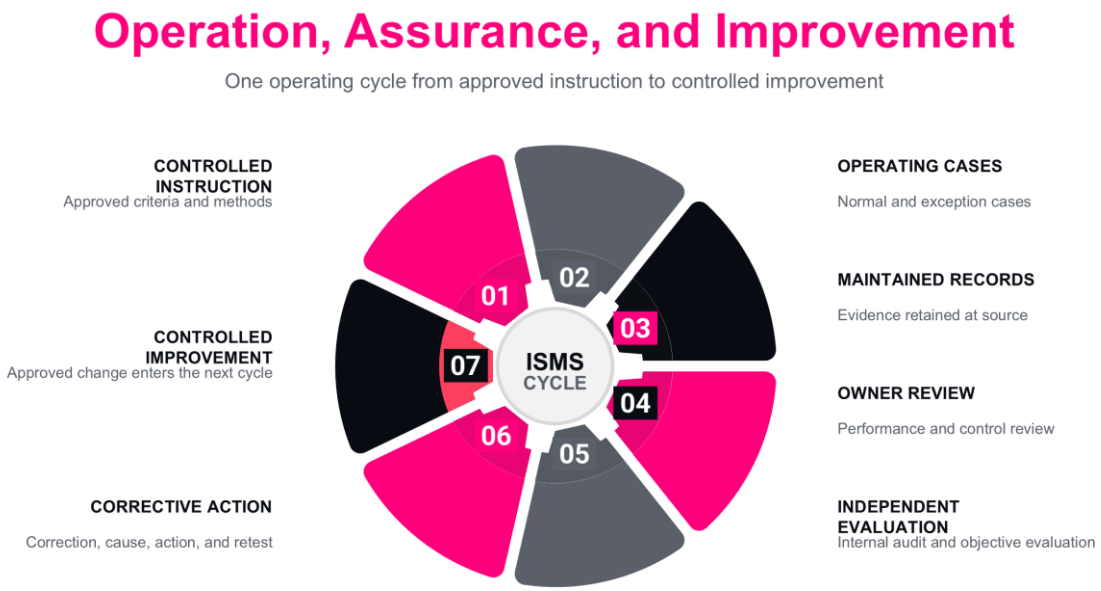

Figure 3. Operation, assurance, and improvement are separate decision stages. An adverse result returns through controlled repair; it does not disappear into revised prose.

At the review, ask the owner to begin with the current instruction and its input source. Follow the record to the applicable approval and natural timestamps. The evidence should establish the completion condition. If the case departed from the ordinary route, locate its response and any resulting risk or action. Record every point where a private message, memory, or undocumented spreadsheet was required. Assign repairs and repeat the affected portion.

At this point the priority processes should have genuine operating records, including failed or exceptional cases where they occurred or were safely exercised. Owners should have reviewed a complete population or a justified sample. Check every status claim against the implementation-state sequence above. Do not report a later state until the evidence for its earlier dependencies exists. Route the gaps and put the next operating opportunity on the calendar.

Assurance begins with these observed populations, not a new evidence folder. Transfer the maintained records, owner reviews, exceptions, limitations, and next operating opportunities. Module 9 uses them to define reproducible measures and independent audit work without confusing operation, review, and assurance.

Turn the Guide Into a Working ISMS

Get your clausepass27001 toolkit

Module 9: Measure performance and conduct internal audit

Operation produces many records. Performance evaluation begins when the organization decides what question a record can answer, how it will be examined, and what action follows. An **internal audit** gives the organization its own independent, documented evaluation against audit criteria. It follows a systematic method and relies on audit evidence.

Use the Evidence Register (CP-SRC-086) with the Security Objectives and KPI Register (CP-SRC-097). Plan the audit in CP-SRC-089 and consult the guidance in CP-SRC-103 through CP-SRC-105. Operational monitoring and control testing may examine the same source, but they answer different questions. Management reporting and internal audit must remain distinguishable from both.

Start with the management question

Select information because somebody needs to decide, intervene, or learn. A large dashboard assembled from easily counted events can hide the condition that matters. For each objective or measure, name the decision it supports. Do the same for a scheduled review, then identify who receives the result.

Examples of useful questions include:

- Are leaver accounts being disabled for the complete in-scope population within the approved time?
- Are restore tests demonstrating recovery of the selected service components under the stated conditions?
- Are critical supplier findings resolved within their treatment or acceptance terms?
- Is the vulnerability process finding and treating exposed assets before the approved deadlines?
- Are repeated policy exceptions concentrated in one technology, team, or requirement?
- Has the risk treatment changed the scenario as intended, or only completed project tasks?
- Are internal audit findings recurring in processes that were previously reported as corrected?

The question comes before the chart. It defines the population and its source. It also determines how often analysis occurs and when the result must be escalated.

Set information security objectives

An objective must fit the information security policy and matter to the organization. Write it so that the result can be evaluated. Communicate it to the people who affect the outcome, then monitor it and revise it when circumstances require. The implementation record should name the planned action and its owner. It should also state the resources and completion date. Define how the eventual result will be evaluated.

Write the intended result precisely. “Improve security awareness” leaves the owner to invent the meaning later. A usable objective names the affected population and the behaviour or capability expected to change. Anchor that change to a supported baseline. Set a time horizon and an evaluation method, then state the practical limits. Completion of training may be one implementation measure; it is not automatically evidence that behaviour or incident exposure changed.

For each objective, enter in CP-SRC-097:

Element	Working question
Intended result	What condition should change, for whom or what, and why?
Population and boundary	Which services, roles, systems, suppliers, sites, or cases are included?
Baseline	What current result is supported, over which period, by which source?
Indicator	What value will show progress or deterioration?
Method	How will data be collected, validated, calculated, analysed, and reported?
Target or criterion	What value, range, trend, deadline, or condition requires a response?
Owner and participants	Who owns the result, supplies data, checks quality, and acts?
Resources and timing	What capacity, system, budget, or dependency is required, and when?
Limitations	What exclusions, latency, uncertainty, or data-quality issue affects interpretation?
Action route	What happens when the result misses the criterion or the measure becomes misleading?

Distinguish monitoring and measurement

Monitoring determines status through observation or critical review. The subject may be a system, process or activity. Measurement determines a value. One review may contain both. A security operations team can monitor alert-source health and measure the percentage of required sources reporting during a period.

Define the method before collecting the value.

Method element	Definition to retain
Calculation	Numerator, denominator and unit
Period	Time window and extraction time
Provenance	Source query and authoritative system
Boundary	Exclusions and treatment of missing records
Data quality	Duplicate handling, validation checks and rounding rule
Accountability	Analyst responsible for producing the value

Preserve the underlying result or reproducible query where appropriate.

Percentages are particularly easy to misuse. If 98 per cent of critical vulnerabilities were treated within target, the reader needs the total population. The method must say how it treated cases still open at period end and any disputed finding. Assets outside scan coverage cannot disappear silently from the denominator. Accepted exceptions also need an explicit treatment. A small denominator or incomplete asset population can make a strong-looking percentage unreliable.

Set a review cadence that matches the decision. Fast-changing exposure may require frequent operational monitoring. An annual objective may still need monthly or quarterly indicators so that the owner can act before the end date. Event-driven review should sit alongside the calendar. A major incident or supplier change may invalidate the measure; so may a significant technology or regulatory change.

Specify evidence before requesting it

An evidence request should tell the source owner what proposition is being examined. “Send proof of access control” is not workable. Name the control or process, then define its population and period. Identify the expected source and only the fields needed for review. State whether the reviewer needs a sample or the complete population. Give handling restrictions their own instruction.

Use the Evidence Register to record:

- evidence identifier and requested proposition
- related requirement, control, process, risk, objective, or audit engagement
- source system and source owner
- population and period
- collection or extraction method, date, and collector
- original format, protected location, and stable reference
- authenticity, integrity, provenance, or custody information appropriate to the use
- access restriction, classification, retention, and disposal
- review performed, result, limitation, and reviewer
- related finding, action, or follow-up request.

Evidence strength depends on the claim. A screenshot may show a setting at one moment. It rarely establishes that the setting covered the complete population or remained active for a period. A procedure shows designed work. It does not prove operation. A ticket can show one case. A system export may show a population, but only when the query and returned fields are understood. Its exclusions must be known and its source must be reliable.

Prefer the least intrusive source that supports the question. Controlled read-only access may remove the need to copy sensitive data. A supervised inspection can do the same. Where a copy is necessary, consider a redacted export or retain a stable source-system reference. Record any restriction and how the evaluator addressed it.

Review evidence quality

Before relying on evidence, inspect:

1. **Relevance:** does it address the stated criterion, control, population, and period?
2. **Source:** who or what produced it, and is that source authoritative for the fact?
3. **Completeness:** is the population complete, or is the sample and exclusion basis known?
4. **Timing:** was it created during the activity, reconstructed later, or extracted for review?
5. **Integrity:** can unauthorized alteration be detected or reasonably controlled for the use?
6. **Consistency:** does it agree with linked systems and records?
7. **Accessibility:** can an authorized reviewer retrieve it without relying on a private account or expired link?

8. **Interpretability:** are fields, status values, calculations, time zones, and limitations understood?

If quality is insufficient, record the limitation. Seek corroboration or inspect the source. A different sample may answer the question; otherwise narrow the conclusion. Never strengthen the wording of the conclusion to compensate for weak evidence.

Build the internal audit programme

The audit programme coordinates one or more audits over a defined period. Set programme objectives that reflect the importance of processes, changes affecting the organization, and results of previous audits. Across the programme, cover the full ISMS scope and its applicable audit criteria. This does not require equal time for every clause or control. Nor does every department need the same audit frequency.

The programme should record:

- programme objectives and period
- organizational and ISMS scope to be covered
- audit methods, including any remote activity or virtual location
- process importance, risk, change, prior results, complaints, incidents, and management concerns used for prioritization
- engagements, timing, responsible audit lead, and resource needs
- competence requirements and auditor selection
- independence, objectivity, confidentiality, and conflict controls
- reporting, escalation, record retention, and programme review
- follow-up of findings and evaluation of programme performance.

The 2026 edition of ISO 19011 is the current general guideline for auditing management systems. It addresses audit programmes and conducting audits, including remote auditing and auditing of virtual locations. ISO/IEC 27007 provides information-security-specific guidance for auditing an ISMS; its 2020 edition remains published while revision work is underway. Use the editions adopted by the organization and record the source status. These guidance standards do not replace the internal-audit requirements in ISO/IEC 27001.

Plan an audit engagement

Define the audit objectives, scope, and criteria before preparing the checklist.

Objectives state what the audit is intended to accomplish. Examples include determining whether a process conforms to specified requirements, evaluating implementation and maintenance, or following up prior findings.

Scope sets the boundaries and extent of the audit. State those boundaries by dimension.

Scope dimension	Boundary to state
Organization	Functions and organizational units
Work	Activities and processes
Technology	Systems and services

Scope dimension	Boundary to state
Place	Physical or virtual locations
Time	Period covered by the engagement

Criteria are the requirements used as the reference against which audit evidence is compared.

Criterion source	Example
Management-system requirement	Applicable ISO/IEC 27001 requirement
Internal direction	Adopted policy, standard or procedure
External obligation	Contractual term or appropriately interpreted legal requirement
Control specification	Approved design or operating criterion for the control

Do not list the entire standard as criteria for a two-hour supplier-onboarding audit. Identify the requirements and internal rules relevant to the assigned scope. Confirm that the current controlled versions are available.

Prepare a process route rather than a questionnaire of clause headings. Begin with the transaction or event that starts the audited process. Follow its input into authorization and operation. Inspect the resulting record, then see how the owner reviews it. Include the route used when normal handling fails. The checklist is a memory aid; it should not prevent the auditor from following evidence into an unanticipated issue within scope.

Select competent and objective auditors

Determine competence for the assigned audit by area.

Competence area	Capability required
Audit practice	Management-system audit methods and tools
Subject matter	Information-security discipline relevant to the scope
Context	Organization and applicable criteria
Evaluation	Collection and evaluation of audit evidence
Communication	Interviewing, discussion and reporting
Specialist knowledge	Sector or legal knowledge where the assignment requires it

Maintain evidence of competence and evaluation.

Internal auditors need objectivity and impartiality. They should not audit their own work or make management decisions for the process under review. In a small organization, structural independence may be difficult. A cross-functional auditor or external specialist can reduce a direct conflict. Careful scope assignment may separate the auditor from prior work. Where that is insufficient, add independent review. Record the conflict and safeguard rather than claiming perfect independence that the structure cannot provide.

An auditor may identify a gap and explain the evidence. Process management owns correction and corrective action. If the auditor designs and implements the response, later verification should be assigned to somebody who can evaluate it objectively.

Sample with a stated rationale

Sampling is a practical response to populations that cannot all be examined. Document the design before selecting records.

Sampling decision	What the audit plan must state
Frame	Population and sampling unit
Method	Selection method and rationale
Extent	Sample size and period
Interpretation	Known limitations

Build relevant variation into the sample.

Variation axis	Contrasts worth considering
Organization	Location, role or supplier
Technology	System or privilege level
Information	Classification
Route	Normal versus emergency handling
Outcome	Successful versus failed case
Time	Different points in the audit period

Random selection can reduce selection bias in a stable population. Judgmental selection can target higher-risk or unusual cases. A combined sample is often useful. Do not invite the process owner to supply only their best examples. Preserve the population source and the auditor's selection.

Expand the sample when results indicate a possible systemic issue, but record why and how. A single record can establish a factual failure for that case. A broader conclusion must fit the criterion and population. Consider how consistently the process is designed, then weigh corroborating evidence against the sampling limits.

Conduct the audit

Use the opening meeting to settle the engagement conditions.

Opening subject	Confirmation required
Assignment	Objectives, scope and criteria
Conduct	Methods and timing
Coordination	Communication and availability of people
Information	Availability and confidentiality of records
Protection	Safety requirements
Change	Route for emerging issues or necessary plan adjustments

Adjustments should be authorized and recorded.

Use an evidence method suited to the proposition. Interviews explain how people understand the audited process; observation shows how they perform it. Documents and records establish approved direction and retained history. Data analysis can test a population, while system inspection can establish a technical condition. A remote method is suitable only when it preserves the needed access and reliability. Corroborate material statements. Record enough source detail for the audit evidence to be reviewed without collecting unnecessary sensitive content.

Compare audit evidence with the criteria. An audit finding is the result of that evaluation. Use the organization's controlled finding categories. Where a nonconformity is reported, state the unmet requirement and the objective evidence. Then describe the factual gap between them. Avoid blame, speculation, and prescribed solutions.

A clear finding can be read in this order:

1. the criterion that applies
2. the population, case, location, or period examined
3. the objective evidence obtained
4. the observed condition
5. the conclusion under the audit method and any relevant limitation.

Discuss factual accuracy with the responsible owner. Do not negotiate away a supported finding because correction is inconvenient. Equally, do not retain a finding when the evidence or criterion is wrong. Record disagreements and follow the approved resolution route in CP-SRC-105.

Report conclusions and follow up

The audit conclusion addresses the audit objectives within the scope and evidence obtained. Structure the report so that a reader can reconstruct that boundary.

Report section	Content
Basis	Audit methods and criteria
Extent	Population sampled and resulting limitations
Results	Findings and useful positive observations
Resolution	Unresolved factual differences and follow-up route

Do not convert a limited internal audit into a declaration that the whole ISMS is conformant or certification-ready.

Issue the report to the authorized recipients. Protect restricted details. Transfer accepted findings to CP-SRC-088 with stable references. The process owner first records any correction and investigates cause. Where corrective action is necessary, name its owner and due date. Attach evidence that permits later verification. The audit function verifies follow-up according to the programme; it does not close actions from status emails alone.

Review the audit programme itself.

Review question	Evidence to consider
Was the programme delivered?	Completion against plan and achieved coverage

Review question	Evidence to consider
Could the audit team perform it?	Auditor competence and availability
Were results dependable?	Quality and consistency of findings
Did the process respond?	Timeliness of reporting and follow-up
What should change?	Stakeholder feedback, recurring issues and changes to the ISMS

Adjust future priorities on that basis.

Design one measure and one audit

Choose one process that has completed at least one genuine operating cycle. Define one management question, one measure, and one internal-audit engagement without making them duplicates.

For the measure, complete a reproducibility record.

Measure record	Required content
Boundary	Population and exclusions
Method	Calculation and source query
Reliability	Quality checks and known limitation
Result	Reported value and recipient
Decision	Criterion that requires a response

Recalculate the value from the retained source.

For the audit, complete the engagement plan.

Plan area	Required content
Assignment	Objectives, scope and criteria
Audit team	Competence evidence and objectivity safeguards
Examination	Population, sample rationale and evidence plan
Output	Authorized reporting route

Conduct the audit. Write each finding from criterion and evidence before assigning a category. Give the report to a reviewer who was not on the audit team and ask them to reproduce the evidence trail.

Assurance is usable when objective owners know how results will be evaluated. Every measure must retain its population and calculation basis. An evidence request should state the proposition and source, then set the period and access restrictions. Plan programme coverage according to process importance and risk. Organizational change and previous audit results should alter that priority. Confirm auditor competence and objectivity. Findings must remain criterion-based, with a follow-up trail that another auditor can verify.

Adverse findings and unresolved management questions now need owned response routes. Transfer the exact criterion, population, evidence, limitation, and due decision. Module 10 uses that basis to distinguish immediate correction, causal corrective action, effectiveness review, and matters reserved for management.

Turn the Guide Into a Working ISMS

Get your clausepass27001 toolkit

Laboratory C: Audit one process through its records

This is the first independent attempt. The auditor selects the criterion, population, sample, and evidence route from current organizational records before consulting CP-SRC-125. Use a process that has operated during a defined period. Choose one with a population that can be reconstructed. Access lifecycle and vulnerability treatment are suitable, as are production change and supplier assurance. A restore test, incident-response case or control exception can support a narrower engagement. The process owner supplies access and explains the workflow but does not select the audit sample. Feedback must reason from criterion and evidence; a category or model answer alone is insufficient.

Audit assignment

Structure the assignment so that its boundaries can be reviewed before fieldwork:

- **Purpose:** the audit objectives and criteria.
- **Extent:** the scope, relevant physical or virtual locations, and period.
- **Execution:** the methods and competence needed for the assignment.
- **Handling:** confidentiality conditions and the intended report recipients.

Record any conflict of interest and the safeguard used. If suitable objectivity cannot be established, change the auditor or scope.

Population and sample

Obtain the complete population from an identified source. Reconcile its total. The sample needs ordinary work plus at least one case that could reveal a different route. Choose that variation deliberately. Late or failed work tests whether the process recovers. An emergency route, high-risk item or exception tests whether its authority holds under pressure. Record the selection method and limitation.

Evidence route

Trace each sampled case from trigger to completion. Compare it with current audit criteria. Use interviews to understand the process, then corroborate important statements through observation or records. Record the evidence identifier rather than keeping a loose copy. Collect a copy only when it is necessary and authorized.

Finding conference

Build each potential finding in a fixed evidential order. State the criterion first, then identify the evidence examined. Describe the observed condition before drawing the audit conclusion. Ask the process owner to check factual accuracy and identify relevant evidence that was not available during sampling. Resolve disputes through the approved route. The auditor does not choose the corrective action.

Deliverables

- approved audit plan

- population and sample record
- evidence trail and working notes
- audit findings with criteria and objective evidence
- audit report and distribution record
- transferred follow-up entries
- a short review of the audit method, limitations, and future programme implications.

The laboratory is complete only when another competent auditor can reconstruct it. That auditor must be able to identify what was examined and reproduce the important evidence trail. Each finding must show how the conclusion was reached and where its limits lie.

Module 10: Correct, improve, and obtain management decisions

Four terms govern the response. A **nonconformity** is non-fulfilment of a requirement. A **correction** is action to eliminate a detected nonconformity. **Corrective action** is action to eliminate the cause of a nonconformity and prevent recurrence. A **management review** is top management's formal evaluation of whether the ISMS remains suitable, adequate, and effective and what changes or decisions are required.

Evaluation matters only when the organization responds at the proper level. Some cases need an immediate correction. Some show a nonconformity whose cause and possible recurrence require corrective action. Other cases alter risk or call for a changed objective. Management may need to provide resources or redesign part of the system. Module 10 establishes those routes and brings the unresolved management questions into review.

Use the Findings, Nonconformity and Corrective Action Register (CP-SRC-088) for the maintained case. Use CP-SRC-103 through CP-SRC-105 for evidence and issue handling. The Management Review Decisions Workshop (CP-SRC-106) helps prepare and conduct the review. CP-SRC-093 carries the performance information and management decisions. It also retains resulting actions through follow-up.

Classify the issue from facts

Record the origin of every issue. Use a source family so that later analysis can show where weaknesses are being found.

Source family	Typical origin
Internal evaluation	Internal audit, control test or monitoring result
Operational experience	Incident, complaint or ordinary operation
External dependency	Supplier review or certification audit
Obligation	Legal or contractual review
Governance	Management review or risk review

Preserve the original wording and source reference. Confirm the applicable criterion and the affected population before deciding its route.

An operational problem is not automatically a nonconformity. A nonconformity is non-fulfilment of a requirement. State the requirement that was not fulfilled and the evidence showing the gap. The requirement may come from the management-system standard or an adopted internal rule. It may instead come from an applicable contract or another controlled source within the assessment remit.

Several records may arise from one event. A delayed critical patch may show that a procedure was missed while an exception expired. If the asset record is inaccurate, correct that source as a separate case. Reassess the risk and take any concern requiring authority to management. Link the records without forcing every issue into one category.

Control the immediate condition

Act first where the condition creates ongoing harm or exposure. Unreliable information and loss of control can also require immediate action. Containment limits the immediate extent. Correction addresses the detected nonconformity or error. Revoke access that should not exist, or restore a required configuration. Isolate an affected device where necessary. A record error needs a traceable correction; an incomplete decision may need to be issued again. Perform an omitted review rather than marking it complete.

Record the action and the person who performed it. Identify the authority used and the time of intervention, then record the result. Preserve the original evidence. Assess consequences and similar cases. If one leaver account remained active, establish whether the population or process permits the same failure elsewhere. Do not wait for a root-cause workshop before controlling a material exposure.

Correction does not by itself prevent recurrence. Reperforming a missed backup test closes the immediate omission. It does not explain why the schedule or assigned ownership failed. Nor does it explain why monitoring and escalation allowed the omission to persist.

Determine the extent

Define the affected period and population. Look first across services and locations that use the same process. Then examine other teams or technologies exposed to the same condition. Include supplier-held or related records when they fall within the plausible extent. Use a reproducible query or documented sample. Record what was excluded and why.

The extent review may change the issue. An apparent one-off data error can reveal that an import rule corrupted every record. A repeated failure may still have different causes. Avoid declaring an issue systemic merely because it occurred more than once; establish the common process or condition that connects the cases.

Update risk information when the issue changes the scenario or its consequence. Revise the likelihood when the new evidence warrants it. Record any effect on current controls, uncertainty or a treatment assumption. Notify the affected owners. Link the finding to its risk and treatment. Keep separate links to any related exception or operational case, including a supplier issue or controlled change.

Analyse causes without choosing a favourite technique

Cause analysis should explain why the requirement was not fulfilled and why the management system did not prevent or detect the condition earlier. Go deeper when the consequence is significant or recurrence is plausible. Uncertain or complex conditions also justify more investigation.

Build the analysis from evidence suited to the case.

Evidence perspective	Sources to examine
People and work	Interviews, workload information and competence records
Process	Process map, timeline and operating records
Technology	Configuration and technical analysis
Change	Release or change history

Evidence perspective	Sources to examine
External dependency	Supplier information

Repeated “why” questions or a causal tree may help organize the evidence. Barrier analysis is useful when a safeguard failed; fault analysis may suit a technical failure sequence. The name of the technique is less important than the quality of the evidence and reasoning.

Look beyond the last person who touched the case. Relevant causes can include:

- population was incomplete or not owned
- trigger did not enter the process
- criterion was ambiguous or conflicted with another rule
- responsibility existed on paper but lacked authority, time, access, or competence
- system design made the required route impractical
- supplier responsibility or hand-off was misunderstood
- monitoring did not cover the failure mode
- change was released without updating dependent instructions or controls
- exception handling became the ordinary route
- previous action corrected a symptom and left the enabling condition in place.

Do not write “human error” as the endpoint. Establish what the person was trying to achieve and what information was available. Examine the tools and competing demands present at the time. Then ask which safeguard should have detected the error and why recovery failed. Deliberate misconduct may require a different route, but it still does not excuse examination of control design.

Where evidence does not support a single root cause, record contributing conditions and uncertainty. Test competing explanations. A forced, tidy cause statement leads to weak action.

Select corrective action

Corrective action eliminates the cause of a nonconformity and is intended to prevent recurrence. Choose action that addresses the supported cause and the affected extent. Name an owner who has the authority to deliver it. Record the resources and unresolved dependencies. Set a due date with a defined completion condition. State what will prove implementation and how effectiveness will later be checked.

Compare the proposed action with the cause:

Cause condition	Weak response	Better-directed response
Process population is not generated reliably	Remind the reviewer to be careful	Establish an authoritative population source, reconciliation, ownership, and missing-record alert
Approval authority is unavailable during urgent work	Retrain staff on the normal process	Define delegation, emergency authority, time limit, retrospective review, and monitoring
Two documents contain conflicting criteria	Ask teams to follow both	Choose the authoritative criterion, change dependent sources, withdraw superseded text, and test adoption

Cause condition	Weak response	Better-directed response
Supplier evidence is accepted without defined review	Request another certificate	Set tiered evidence criteria, reviewer competence, limitation handling, issue route, and change triggers
Alert volume hides material cases	Tell analysts to work faster	Tune use cases, repair source coverage, set prioritization and escalation, review staffing and automation
Prior action was closed on delivery	Add another action date	Define an effectiveness proposition, population, observation period, method, result criterion, and independent reviewer

Consider unintended effects. A stricter control may delay critical recovery or provoke an unsafe workaround. It may also drive activity into an unmonitored channel. If the response changes a contractual commitment, obtain the required authority. Assess new risks and required changes before release.

Verify implementation and effectiveness separately

Implementation verification establishes that the approved action was delivered as specified. Inspect the changed artifact or system configuration. Where the action changes work, follow the revised workflow and role assignment. Check that required competence support took place. For an external action, inspect the supplier term or delivered capability. Confirm the affected population and effective date.

Effectiveness review determines whether the action addressed the cause and prevented recurrence under stated conditions. Define the proposition while planning the action.

Review element	Decision to make in advance
Boundary	Observation period and affected population
Evidence	Authoritative source and any sampling method
Criterion	Result that will support effectiveness
Authority	Reviewer able to challenge implementation
Failure route	Response to an inconclusive or adverse result

Allow enough operating opportunity. A revised quarterly review cannot be judged from a screenshot produced the next day. Use leading information where helpful, but label it. For a rare event, a simulation can test understanding and design inspection can test the revised control. Monitoring may show whether prerequisites remain ready. The next real occurrence is still needed to test operation; state the limit of each source.

The person who implemented the action can supply evidence. Assign effectiveness review to somebody able to challenge it. A significant management-system issue may need internal audit. A technical claim may instead need independent testing, while a high-risk governance decision may require management oversight.

Close the case only when the defined closure conditions are met. The closure record should permit this reconstruction.

Closure stage	Evidence required
Immediate response	Correction and affected extent

Closure stage	Evidence required
Analysis	Supported cause assessment
Prevention	Corrective action where necessary
Delivery	Implementation verification
Outcome	Effectiveness result
Consequential change	Updated risk or controlled document
Authority	Recorded closure review

If effectiveness fails, reopen or create a linked case; do not change the criterion after seeing the result.

Prepare management review from current records

Management review is performed by top management at planned intervals to establish whether the ISMS remains suitable, adequate, and effective. It is a decision process, not a presentation ceremony. Plan it early enough for complete inputs to be assembled, checked, and circulated to participants with the necessary authority.

Use CP-SRC-106 to work through the decisions. In CP-SRC-093, retain the period covered by each input and the resulting conclusion. Record each decision with its resulting action. The action needs an owner and committed resource, followed by its due date and follow-up status. An existing executive or governance meeting can perform the review. Its agenda must cover the adopted inputs, and participants must hold the necessary authority. The meeting record must preserve both the information considered and the decisions made.

Prepare the following areas from authoritative sources:

- status of actions from previous management reviews
- relevant changes in external and internal issues
- changes in interested-party needs and applicable requirements
- information about ISMS performance, including trends in nonconformities and corrective actions, monitoring and measurement, audit results, and fulfilment of information security objectives
- feedback from interested parties where relevant
- results of risk assessment and status of the risk treatment plan
- opportunities for continual improvement
- material resource, competence, supplier, scope, policy, technology, or operating concerns requiring management authority.

Do not copy every register onto slides. State the current condition and any meaningful trend. Explain the consequence, then make uncertainty visible. End the item with the decision required. Preserve stable references so that a participant can examine the underlying source. State the period and population behind each metric. Highlight missing or unreliable data rather than filling the gap with a green indicator.

Put decisions on the agenda

Frame agenda items in a form management can decide. For example:

- approve, reject, or change an ISMS scope proposal

- accept, further treat, avoid, or escalate a residual risk within authority
- assign resources for an overdue or ineffective treatment
- change an objective or target because the business context changed
- resolve a conflict among policy, service delivery, and contractual commitments
- approve a control redesign or exception boundary
- direct corrective action for a recurring management-system weakness
- authorize certification planning or postpone an external claim
- commission a sector or legal interpretation
- change the review frequency or reporting route.

Avoid “management noted the report” when a decision is required. Use a decision record with defined fields.

Decision field	Required entry
Conclusion	What management decided and any necessary rationale
Accountability	Owner of the resulting work
Commitment	Resource and due date
Condition	Assumption, limit or prerequisite attached to approval
Follow-up	How and when completion will return to governance

If the group lacks authority, record the escalation destination and interim control.

Conduct and record the review

Confirm attendance and delegated authority. Declare material conflicts. Work through previous actions before adding new ones. Ask owners to explain adverse trends and unreliable data. Examine overdue treatment together with any expired risk acceptance. Bring gaps in audit coverage or recurring incidents to the responsible owner. Supplier concerns should be discussed with the consequences for the scoped service visible. Give uncertain evidence the weight it deserves.

The output should include decisions related to continual-improvement opportunities and any need for changes to the ISMS. Classify the decision so that its downstream effects are visible.

Decision area	Possible effect
Direction	Scope, policy or objectives
Risk	Risk criteria, treatment or controls
Capability	Resources, responsibilities or competence
Dependency	Supplier arrangement
Assurance	Evaluation approach or controlled document
Delivery	Timing and implementation priority

Record each decision at the level approved; do not convert discussion notes into approval.

Issue the record to authorized recipients. Transfer actions into CP-SRC-093 or the adopted authoritative action system. Link them to the review, preserve status, and bring overdue or ineffective actions to the next

suitable governance point. Keep legal and personnel material within its approved access boundary. Apply the same care to vulnerability and incident details.

Continual improvement as ordinary work

Improvement can start with evaluation, including monitoring or audit. Operational experience contributes incidents and practitioner observations. Feedback or an exercise may expose a usability problem. Change and risk review reveal a different class of need, while supplier performance can expose an external dependency. Maintain a backlog only when its entry and priority rules are defined. Every item also needs an owner and a decision route. Otherwise the backlog becomes a place where important weaknesses wait without authority.

Assess proposed improvement against the ISMS purpose and risk. Route it according to the reason for the proposed change.

Reason	Work route
Prevent recurrence of a nonconformity	Corrective action
Change exposure	Risk treatment
Pursue a measurable management result	Information security objective
Improve how work is performed	Process improvement
Repair a deferred technical weakness	Technical-debt route

Select the right owner and funding route. Define the expected result and evaluation before delivery.

Small changes can proceed through ordinary process ownership. Material changes may need management review. Preserve the reason for rejecting or deferring a proposal when the underlying risk or obligation remains.

Close one adverse case

Select one current finding or operational issue. Complete the case in a causal order.

Case stage	Required record
Basis	Criterion and objective evidence
Boundary	Affected population and immediate condition
Response	Correction and extent review
Analysis	Supported causes and recurrence risk
Prevention	Necessary corrective action

Define implementation and effectiveness checks separately. Have an independent reviewer challenge whether the planned action addresses the cause.

Then prepare one management-review decision pack. Use current records and state their periods and limitations. For each subject, explain the condition and consequence. Present feasible options, followed by a recommendation and the authority required. Conduct the review or rehearse it with the actual decision owners. Capture the decision precisely and transfer actions to the maintained register.

A completed case should connect the nonconformity to its requirement and evidence. It should show the immediate control and correction, then explain the affected extent. Supported causes must lead to corrective action that addresses them. Effectiveness review needs a suitable population and period. Management-review records should contain decisions and owned actions, not presentation summaries. Improvement work then returns to ordinary governance.

An external certification decision is supportable only after management has resolved or explicitly bounded the adverse state. Give Module 11 the approved scope and current SoA, together with the audit and management-review results. Identify open findings, the evidence of effectiveness, and the authority for any claim. Module 11 tests whether that record supports proceeding, rescheduling, or withdrawing.

Turn the Guide Into a Working ISMS

Get your clausepass27001 toolkit

Module 11: Decide on certification and manage the audit lifecycle

Certification is an organizational choice unless a customer or contract makes it necessary. A regulatory or tender commitment may create the same need. The decision should state the business purpose and intended scope. Set acceptable timing and budget in relation to that purpose. Identify the market or contractual recognition required and who may authorize public claims. Certification is then maintained through an audit programme; it is not a one-day inspection or a substitute for operating the ISMS.

Begin with `07 Certification Preparation/00 Start Here.docx` (CP-SRC-107) and `01 Certification Planning and Lifecycle.docx` (CP-SRC-108). Use `02 Certification Audit Coordination and Findings.docx` (CP-SRC-109) with the readiness-decision workshop (CP-SRC-110). Keep certification coordination separate from internal audit. The implementation team can organize access and records; it cannot decide what the certification body will find or whether certification will be granted.

Establish the certification objective

Record the source of the request and the exact result expected. A sales team may need a certificate recognized by a named customer. A regulated entity may face scheme-specific conditions. Leadership may want an independently audited management system without a fixed tender date. Those situations affect which certification body can conduct the certification audit and what scope is appropriate. They also change the schedule and the claims the organization may need to make.

Confirm:

- the intended certificate scope and its relationship to the approved ISMS scope
- products, services, legal entities, functions, locations, remote work, virtual locations, and outsourced processes involved
- customer, contractual, market, regulatory, or procurement conditions
- target dates and the event driving them
- required language, geography, sector competence, and audit access
- budget and internal availability across Stage 1, Stage 2, finding response, surveillance, and recertification
- who may negotiate the application, contract, and scope wording
- who may approve external certification claims
- what happens if timing or certification outcome changes.

Do not narrow the management-system boundary simply to exclude a difficult dependency when a scoped service still relies on it. The certificate wording may be more concise than the maintained scope analysis, but it should remain accurate and not mislead customers about covered services or organizations.

Understand the parties

ISO develops and publishes standards; it does not certify organizations. A certification body performs the conformity-assessment and certification work. Accreditation is an independent attestation of a certification body’s competence for specified activities. Accreditation is not universally compulsory. A customer or

regulator may nevertheless require an accredited certificate. Procurement and recognition arrangements can impose the same condition, sometimes within a specified accreditation scope.

ISO/IEC 17021-1 sets requirements for bodies that audit and certify management systems. ISO/IEC 27006-1:2024 adds requirements for bodies that audit and certify an information security management system. The organization is not being certified directly by ISO or by the accreditation body.

Verify the proposed certification body rather than relying on a logo.

Verification subject	Detail to confirm
Provider identity	Exact legal entity
Accreditation	Accreditation body, current status and directory entry
Authority	Standard and edition within the accredited scope
Technical fit	Sector or technical scope where relevant
Recognition	Geographic or scheme recognition needed for the intended use

Check any customer-specific requirement directly. Date the check and cite its source. Record the result and the person who performed it because status and arrangements can change.

Advisers may help the organization design or improve its system. Preserve management ownership. Discuss impartiality and prior consultancy with the certification body; do not assume that a preferred adviser can also make the certification decision.

Select a certification body

Obtain enough information to compare providers on the conditions that matter. Price is only one element.

Ask about:

- accreditation and recognition relevant to the intended certificate
- experience and auditor competence for the organization’s sector, technology, geography, and working language
- treatment of multiple locations, remote work, virtual locations, outsourced processes, and integrated management systems
- application information, audit-time determination, and assumptions that can change the quotation
- Stage 1 and Stage 2 approach, location, timing, and expected interval between stages
- finding categories, response times, verification, and circumstances requiring additional audit activity
- certification decision, certificate issue, directory listing, use of marks, and public claims
- surveillance cycle, recertification planning, scope change, significant-change notification, suspension, withdrawal, transfer, and complaints or appeals
- confidentiality, audit records, remote-audit technology, information security, and handling of restricted evidence
- travel, cancellation, rescheduling, interpreter, and additional-day terms.

Give each provider the same accurate boundary information. A quotation that omits sites or workforce size is not comparable. The provider also needs the operating pattern and material complexity, including outsourced

work. Record assumptions and obtain clarification in writing through the organization's approved procurement and legal routes.

Complete the application accurately

The certification body uses application information to review the request and determine the competence it needs. The same information informs resources, the audit programme and audit time. Supply current facts through a controlled application record.

Application area	Information normally required
Organization	Legal organization and relevant locations
Boundary	Intended certification scope
Operation	Activities, services and material processes
Workforce	Headcount and shift pattern relevant to audit planning
Technology	Significant technologies within scope
External work	Outsourced functions
Obligations	Applicable requirements and existing certifications
Impartiality context	Use of consultants
Schedule	Readiness position and desired timing

Coordinate the boundary response with the scope and service owners. Workforce facts belong with HR, while technology or supplier facts need their respective owners. Legal and leadership owners should review commitments within their authority. Keep the submitted version. When a material fact changes, tell the certification body through the agreed route. Do not allow a commercial deadline to turn an estimate into a false statement.

Review the proposed scope and audit plan carefully.

Plan dimension	Fact to confirm
Boundary	Sites, virtual locations and included processes
Organization	Functions participating in the audit
Delivery	Audit times and methods
Team	Assigned auditors and any technical expert
Communication	Working language
Protection	Confidentiality and safety conditions
Access	Availability of people, systems and records

Raise competence or conflict concerns promptly. The certification body retains control of its audit plan and sampling; the organization can correct facts and identify legitimate access constraints.

Prepare for Stage 1

Initial certification audit is normally conducted in two stages. During Stage 1, the certification body examines relevant management-system information and develops its understanding of the organization and scope. It reviews preparedness for Stage 2. The result also informs planning for the later audit. The exact activity and deliverables follow the certification body's approved process.

Before Stage 1, confirm that the organization can present its own system coherently:

- approved ISMS scope and boundary analysis
- context, interested parties, and applicable requirements
- information security policy and objectives
- risk-assessment and risk-treatment method
- current risk results, treatment plan, and SoA
- governance, responsibilities, competence, and resources
- controlled policies, standards, procedures, and records relevant to operation
- monitoring and measurement arrangements and available results
- internal-audit programme, completed audit work, reports, and follow-up
- management-review inputs, decisions, and actions
- nonconformity and corrective-action records
- significant changes, incidents, exceptions, and unresolved limitations.

This is a retrieval and coherence check, not an invitation to assemble a display folder. Use the authoritative sources. Test links and access. Each owner should be able to explain the current process and locate its records. The same owner must state any known gap and the next action.

Treat concerns raised at Stage 1 according to their substance and the certification body's process. Record them in the coordination file and the appropriate organizational register. Test first for an effect on scope or risk. A concern may change treatment and its SoA representation, or reveal an operating failure. It may also affect internal audit or management review. If resolution needs new resources, take that decision to the proper authority. Reconsider the Stage 2 date whenever the remaining work changes readiness. Correct the management system, then supply the agreed response. Do not edit a presentation while leaving the underlying process unchanged.

Decide whether to proceed to Stage 2

Use CP-SRC-110 with the actual decision owners. The question is whether the organization supports proceeding under the agreed scope and schedule, given current evidence and unresolved conditions. Consider:

- whether Stage 1 issues are resolved to the extent required for progression
- whether the scope and application remain accurate
- whether the risk method, treatment, and SoA are coherent and approved
- whether priority controls have operated over sufficient opportunities and populations
- whether internal audit covered the ISMS according to the approved programme
- whether management review was conducted with usable inputs and real outputs
- whether significant nonconformities, ineffective corrective actions, expired exceptions, or unsupported claims remain

- whether process owners and records will be available
- whether material changes or incidents require notification or replanning
- whether the remaining time encourages retrospective or staged evidence.

Use an explicit decision. Proceed when the evidence supports the agreed event. If organizational conditions remain, state them and confirm that the certification body accepts the schedule. Otherwise reschedule or withdraw the planned event. Record who made the decision and why. Identify unresolved risk, then retain the resulting communication and actions. A postponement is sometimes the only accurate response; it should not be hidden by creating records that did not exist.

Coordinate Stage 2 without staging the system

Stage 2 evaluates implementation and effectiveness against the certification criteria within the audit scope. Auditors will use sampling. A selected record may cross a team boundary or several systems. It may also lead to a supplier or another location. The auditor can follow that evidence across the relevant period. Prepare the organization to retrieve and explain its normal work.

Create an audit coordination plan covering:

- official contact with the audit team
- schedule, locations, remote sessions, escorts, and safety
- participants and deputies for each process
- controlled document and record access
- secure display or transfer of restricted evidence
- requests, ownership, status, and response tracking
- daily factual review and escalation
- note-taking and preservation of supplied information
- handling of availability failure, technical failure, scope questions, and confidential material
- closing meeting attendance and finding receipt.

Brief participants to answer from current practice, demonstrate the source, and state when they do not know. They should not memorize a script. If a record is unavailable, identify its source and owner. Explain why it is unavailable and how authorized retrieval will occur. Never substitute a different record without telling the auditor what it is.

Keep one request log.

Log field	Purpose
Request and time	Preserve what the auditor asked for and when
Owner	Assign retrieval responsibility
Source	Identify the authoritative record
Response	Record what was supplied or demonstrated
Restriction	Preserve any access or handling condition
Completion	Show whether the request remains open

This prevents duplicate uncontrolled exports and makes unresolved requests visible. The log is coordination evidence; it does not limit the auditor’s sampling.

Respond to findings

Obtain the certification body's exact finding and category. Preserve the cited criterion and evidence. Record the required response format and due date. Confirm factual understanding promptly through the body's route. Do not argue from reputation, intent, or the number of controls that worked.

Transfer the finding into CP-SRC-088 while preserving the external reference. Apply Module 10:

1. control and correct the detected condition
2. determine consequence and affected extent
3. analyse supported causes
4. decide whether similar nonconformity exists or could occur elsewhere
5. select corrective action proportionate to the cause and extent
6. implement it and update related risk, control, document, and operating records
7. verify implementation and evaluate effectiveness
8. submit the required response and evidence through the authorized channel.

The certification body decides whether the response and verification are sufficient for its process. Internal action closure does not compel external closure. Preserve later requests and decisions.

Do not rewrite a record to make it look as if the nonconformity never occurred. Correct it with a traceable history. Do not fabricate earlier meeting minutes or approvals. The same prohibition applies to tests and audit samples. An operating record must retain its real creation date. A current correction is stronger than false history.

Understand the certification decision

The audit team gathers evidence and reports according to the certification body's process. The certification decision is made by the certification body using its required review and decision arrangements. The organization should not announce certification before receiving and verifying the formal result and certificate details.

When a certificate is issued, verify its contents before public use.

Certificate area	Detail to check
Holder	Exact legal entity
Basis	Certified standard and edition
Boundary	Scope wording and listed sites
Validity	Issue and expiry information
Identity	Certificate identifier and certification body
Recognition	Accreditation details where applicable
Limits	Any stated condition

Store the controlled certificate and verification reference. Correct discrepancies before public use.

Define an approval route for certificate and mark use. Public sales pages and individual email signatures can both overstate what is certified. Review proposals and tender responses before submission. Apply the same control to product statements and supplier questionnaires. The certificate covers the stated management

system within its scope. It does not separately certify each product or service. Nor does it certify every control, person or data item. Follow the certification body's rules and any accreditation conditions for marks and claims.

Operate through surveillance and recertification

After initial certification, maintain the ISMS and the relationship with the certification body. The audit programme normally includes surveillance activity between initial certification and recertification. The body determines its programme and sampling under the applicable certification rules and contract.

Maintain:

- planned audit dates, locations, scope, and contacts
- notification triggers for significant organizational, scope, service, technology, ownership, legal, incident, or control changes
- current internal-audit and management-review cycles
- open external findings and effectiveness evidence
- certificate and claim review
- audit request and supplied-evidence records
- surveillance results, actions, and changed programme information
- recertification preparation early enough to avoid a last-minute reconstruction exercise.

Certificate status may change in several ways.

Status event	Meaning to prepare for
Suspension or withdrawal	Existing certification claim may no longer be usable
Reduction or expansion	Certified scope changes
Transfer	Certification responsibility moves under an approved arrangement
Expiry	Certificate validity ends

Understand the certification body's terms and the effect on claims. The response plan should update the website and contractual material. It must also reach customer communications, tenders and other sales material.

Make the certification-readiness decision

Prepare the certification decision using current organizational facts. Verify two potential certification bodies through primary directory or accreditation sources and record the check. Draft the intended certificate scope and compare it with the maintained ISMS scope. Identify every word that could mislead a customer about the covered organization, location, or service.

Run the readiness workshop with leadership and the implementation lead. Bring in process owners and internal audit, along with the people who approve external claims. Select a sample that follows the way an external auditor may move through the system.

Sample layer	Records to retrieve

Sample layer	Records to retrieve
Service context	One in-scope service
Risk decision	Two risks with their treatment and SoA decisions
Operation	Three operating processes and one exception
Performance	One objective and one internal audit
Improvement	One corrective-action case
Governance	Latest management review

Measure retrieval time and record any inconsistency. Note missing ownership or evidence limits. Keep unresolved changes visible.

Make and record the proceed, reschedule, or withdraw decision. If proceeding, create the coordination plan and request log. If not, update the implementation plan with the conditions required before the decision is reconsidered.

Close the readiness decision only after leadership has authorized the certification objective and scope. Check provider recognition and competence for the intended use. The application facts must agree with current records. Stage 1 and Stage 2 remain certification-body activities. The organization must make an honest readiness decision and provide evidence from ordinary operation. It should address findings through controlled corrective action and keep public claims within the certified boundary. Planning must continue through surveillance and recertification.

Certification planning does not close source governance. Give Module 12 the exact scope and claim boundaries, along with the completed provider checks and programme dates. Preserve the requests and findings with their status-change routes. Module 12 places those sources beside sector obligations and operating ownership so later change does not depend on the implementation lead’s memory.

Turn the Guide Into a Working ISMS

Get your clausepass27001 toolkit

Module 12: Govern sector sources and hand over the living ISMS

An ISMS rarely operates from one standard alone. Law and sector regulation may govern the same service as a customer contract. Official guidance or a professional standard can shape how those duties are understood. Assurance schemes and technical benchmarks add another layer, while the organization may have made commitments of its own. The final implementation task is to govern those inputs without allowing a newly discovered source to rewrite the system through an informal spreadsheet or a hurried policy edit.

Use the five resources in `08 Sector Guidance` (CP-SRC-111 through CP-SRC-115) to make applicability and conflict decisions. Use the worked examples (CP-SRC-116 through CP-SRC-131) for study and rehearsal only. Consult CP-SRC-132 for toolkit release questions and CP-SRC-133 for the supplied commercial terms. This module also transfers implementation work into ordinary ownership and sets the next cycle.

Build the source population

Start with sources already visible in organizational records.

Discovery route	Records or owners to consult
External obligation	Contracts and regulatory inventories
Customer representation	Questionnaires and published security commitments
Management system	Risk records, policies and audit reports
Interpretation	Legal, compliance and privacy owners
Product delivery	Product, engineering and service owners
Supporting operations	Procurement, physical security and human resources (HR)
Resilience	Continuity owner

Record uncertain candidates rather than silently treating them as applicable.

Classify each source accurately:

Source type	Examples of what it may establish	Interpretation owner to identify
Law or regulation	Binding duties within jurisdiction, activity, entity, or data scope	Qualified legal or regulatory owner
Regulatory decision, rule, or official guidance	Mandatory or expected practice according to its legal status and remit	Compliance or legal owner with sector knowledge
Contract, tender commitment, or customer term	Agreed security, notification, evidence, audit, location, or service conditions	Contract owner and authorized legal/commercial reviewer
Certification or assurance scheme	Scheme criteria, audit rules, claims, or recognition conditions	Scheme owner and competent assurance lead
ISO or other consensus standard	Requirements or guidance within the published scope	Subject owner who understands its role and edition
Technical benchmark or vendor baseline	Configuration or testing criteria for a technology or product	Technical owner with control and risk authority

Source type	Examples of what it may establish	Interpretation owner to identify
Industry code or professional guidance	Practice expectations or useful methods	Sector or discipline owner; determine whether adoption is voluntary or committed
Internal policy, architecture principle, or public commitment	Requirements the organization has adopted or represented	Document owner and approving authority

Do not label every source “regulatory.” Give each source record enough identity and authority information to support later decisions.

Source field	Entry required
Identity	Issuer and exact title
Version	Edition or version
Time	Publication date and effective date where relevant
Reach	Jurisdiction or other boundary
Provenance	Official locator
Classification	Source type and legal or contractual status
Interpretation	Person competent to interpret it

Make an applicability decision

Use `01 Sector Context and Source Use.docx` (CP-SRC-112), `02 Sector Review Questions.docx` (CP-SRC-113), and the applicability workshop (CP-SRC-115). For each source, establish:

- which legal entity, service, product, processing activity, information, technology, location, customer, supplier, or role it addresses
- the event or condition that makes it applicable
- whether the complete source, a part, or no part applies
- whether its content is a requirement, interpretation, guidance, benchmark, or contractual commitment
- the qualified owner and approval authority
- affected scope, risks, controls, SoA entries, policies, standards, procedures, registers, evidence, audits, and claims
- implementation actions, dependencies, and timing
- monitoring source and next review trigger
- uncertainty or external advice still needed.

Record the reasoning even when the result is not applicable. “Not our sector” is too weak when the organization supplies that sector or processes its information. Operations in a covered jurisdiction require a separate test. So does a source adopted through contract. Conversely, customer interest does not automatically make an entire framework binding.

Separate applicability from conformity. A source may apply while implementation remains incomplete. A voluntary source may be adopted as internal criteria. Record the decision and state; do not use the applicability field to hide a gap.

Establish precedence and relationships

Create a source hierarchy that reflects actual legal and contractual authority. It will rarely be a single universal ranking. A contract cannot remove a statutory duty. A corporate standard may exceed a regulatory minimum. Two customer contracts may apply to different service instances. A technical benchmark may contain settings unsuitable for a particular architecture but still supply useful baseline input.

For related sources, classify the relationship:

Relationship	Meaning for the applicability record
Additive	One source adds a duty, control, evidence type, or population.
More specific	One source supplies detail for a defined sector, technology, or activity.
More stringent	Both apply and one sets the stronger condition for the same case.
Alternative	The source permits several methods or outcomes.
Interpretive	The source explains how another requirement is commonly understood within its remit.
Overlapping	The sources address the same subject with no material conflict.
Conflicting or apparently conflicting	Both cannot be followed as currently understood.
Out of scope	The source or provision does not apply under the approved analysis.

Use `03 Resolving Sector-Source Conflicts.docx` (CP-SRC-114) when conditions do not align. Quote or reference the exact provisions in the restricted legal or source record as permitted. Identify the affected case and applicable jurisdiction. Name the contract or service boundary, then state the time at which the conflict arises. Obtain qualified interpretation. Do not resolve the issue by selecting the wording that is easiest to implement.

Retain the conflict decision in a structured record.

Decision field	Required entry
Conclusion	Approved interpretation or chosen route
Authority	Person or body that may decide
Basis	Material assumptions
Response	Controls and any residual risk
Notice	Required communication
Reconsideration	Event that reopens the decision

Where the conflict cannot be resolved immediately, establish interim safeguards and escalation. Preserve the earlier interpretation so later owners can understand why the system changed.

Propagate an adopted source

Once applicability and interpretation are approved, update the governing records in dependency order:

1. context, interested-party, and obligations records
2. ISMS scope or interface analysis if affected
3. risk scenarios, criteria, assessments, and treatment
4. necessary controls and the SoA
5. policy positions and mandatory standards
6. procedures, runbooks, contracts, and system configurations
7. roles, competence, supplier duties, and communication
8. registers, evidence specifications, measures, and audit criteria
9. exceptions, open findings, management-review inputs, and external claims.

Use change control. Identify the effective date and transition period. Define how legacy cases will be handled and what will prove adoption. A changed encryption benchmark may govern future builds differently from existing systems. Supplier contracts and approved exceptions may need their own transition. Test methods must follow the adopted technical state, while disposal arrangements may change on another schedule. Define each population.

Do not insert a sector-source name into the SoA or policy and call the source-adoption decision complete. State the condition that actually applies. Put its implementation under change control and collect evidence from operation. Define how the result will be evaluated.

Maintain a source watch

Assign monitoring by subject and source. Standards belong with their official publisher, while legal change should be checked through the relevant regulator. Contract owners monitor agreed terms. Accreditation and scheme owners publish status within their respective remits. For a product baseline, use the vendor's authoritative channel. Search summaries and newsletters may alert the owner; verify the change at the authoritative source before changing the ISMS.

Keep the source watch as a maintained decision record.

Field	Purpose
Source and monitored locator	Identifies the authority to be checked
Current edition, amendment, correction, or effective status	Establishes the adopted reference point
Owner and deputy	Keeps the watch operable through absence or role change
Monitoring frequency and event subscription	States when a check becomes due
Last check, result, and evidence	Preserves what was examined and concluded
Announced draft or transition information	Separates possible future change from an effective source
Applicability-review deadline	Prevents a confirmed change from remaining an unowned alert
Affected records and change action	Defines where an approved decision must propagate
Completion and verification	Shows adoption rather than mere awareness

At this guide's source-check date, the published ISO/IEC 27001 requirements edition is ISO/IEC 27001:2022 with Amendment 1:2024. ISO/IEC 27000:2026 is the current overview edition. Its focus is the relationship between the family's concepts and principles. ISO 19011:2026 replaced the 2018 edition as the general management-system audit guideline. ISO/IEC 27004:2016 and ISO/IEC 27007:2020 remain published, with replacement work under development. Verify this status again before relying on it for a later implementation or publication.

The source watch should also cover the certification body's current programme rules and finding-response process. Monitor mark-use conditions with the certificate's current status. Verify the relevant accreditation listing separately. These can change without a new edition of ISO/IEC 27001.

Use the fictional examples as teaching material

Everything under `09 Worked Examples` is teaching material, not evidence from the reader's organization. Keep "FICTIONAL EXAMPLE" in the filename and heading. Preserve it in any extract or screenshot. An export or workshop pack needs the same label. Do not remove it when sharing one page.

Start with CP-SRC-116, the worked-examples start file. The Hearthline end-to-end set then provides four complementary views:

Resource	Teaching use
CP-SRC-117: Hearthline Example Overview	Establish what the fictional case covers and how the materials relate
CP-SRC-118: Hearthline End-to-End ISMS Example	Follow the fictional implementation narrative across the management-system journey
CP-SRC-119: Fictional Example Review Workshop	Critique decisions, evidence, omissions, and possible alternatives with a group
CP-SRC-120: Hearthline Worked ISMS Records	Trace identifiers and relationships across fictional register entries

The module examples let the reader isolate one part of the journey:

- CP-SRC-121: Hearthline Data Services Implementation Chronology
- CP-SRC-122: Hearthline Context, Scope and Governance
- CP-SRC-123: Hearthline Policy and Procedure Adaptation
- CP-SRC-124: Hearthline Risk Management and Statement of Applicability
- CP-SRC-125: Hearthline Evidence, Internal Audit and Improvement
- CP-SRC-126: Hearthline Certification Preparation
- CP-SRC-127: Hearthline Sector Context and Source Applicability.

Three controlled-instruction examples show different document types within the same fictional setting:

- CP-SRC-128: HDS-POL-041 Information Security and Decision Authority Policy
- CP-SRC-129: HDS-STD-041 Authentication and Service Credential Standard
- CP-SRC-130: HDS-PRC-041 Customer Incident Communication Procedure.

Compare the three instructions by purpose.

Comparison question	What to examine

Comparison question	What to examine
Who directs adoption and maintenance?	Authority and intended audience
How prescriptive is it?	Level of detail and decision criteria
How does it operate?	Workflow and retained record

Do not copy fictional names or thresholds into live documents. Role assignments must come from the actual organization. The same applies to service descriptions and approvals. Ask what organizational fact would justify each choice.

CP-SRC-131 supplies the fictional Asterline implementation chronology. Use it to compare sequencing and dependency choices with the Hearthline chronology and with the reader's current implementation plan. The purpose is not to select the more polished example. It is to identify which assumptions, constraints, and operating opportunities would make the sequence suitable or unsuitable in the reader's organization.

Use a consistent study method:

1. identify the question the example is answering
2. mark the fictional facts and assumptions on which its answer depends
3. trace the answer to related records and later consequences
4. find at least one plausible condition under which the answer would fail
5. compare that condition with the live organization
6. write a new decision from live sources and route it through approval.

An example is not an ideal answer merely because it is complete. Look for a missing decision or ambiguous language. Challenge weak evidence and claims that sound more certain than the facts. Then test whether another approach would better fit the live organization. This turns the example into practice rather than a source of borrowed organizational facts.

Hand implementation into operation

The implementation lead should not remain the private route through which every ISMS activity passes. Transfer each maintained process to its operating owner. Test readiness by area.

Readiness area	Handover condition
Mandate	Owner has authority and sufficient capacity
Enablement	Owner has required access and competence
Continuity	A deputy can perform the essential work
Method	Current instructions and records are available
Oversight	Review routine and escalation route are understood
Operation	Next genuine operating opportunity is scheduled

Prepare a handover index containing:

- current approved scope and unresolved boundary matters
- governance bodies, role holders, delegated authority, and deputies
- current risk method, risk population, treatment plan, SoA, and unaccepted residual risks
- authoritative document and record map

- process calendar and event triggers
- open exceptions, incidents, vulnerabilities, supplier issues, findings, corrective actions, changes, and implementation actions
- objectives, measures, reporting schedule, internal-audit programme, and management-review schedule
- certification programme and claim controls where applicable
- source-watch responsibilities and announced changes
- sensitive repositories, access administration, retention, backup, and recovery
- current limitations, manual reconciliations, and technical debt
- licence and release information for the toolkit.

Use role names as well as current people so that a personnel change does not break the index. Test deputy access. Walk one upcoming case with each owner and require them to locate the relevant source without the implementation lead's private folder.

Set the next cycle

The first implementation release is a baseline for further operation. Schedule each next event from its real cadence and trigger.

Operating cycle	Cadence or trigger	Owner to name
Risk assessment, treatment, and SoA	Planned review plus material scope, threat, control, or obligation change	Risk method and risk owners
Documents and sources	Planned review plus approved process, authority, technology, or source change	Document and process owners
Access, supplier, vulnerability, backup, continuity, incident, and exception processes	Their operating calendar plus service events and failed criteria	Assigned process owners
Objectives, measures, and control assurance	Reporting period and any result outside an approved response band	Objective and control owners
Internal audit and follow-up	Programme priority, engagement schedule, change, and finding due dates	Audit programme owner
Management review	Approved governance cadence and availability of usable inputs	Top-management governance owner
Certification activity	Surveillance or recertification programme and certificate-status event	Certification coordination owner
Cross-system change	Incident, complaint, contract, technology, or sector-source trigger	Owner of the affected governing record

Use due dates only where the process is calendar-driven. Preserve event triggers alongside them. Assign the next action and operating opportunity before closing the implementation action.

Conduct a 30-, 60-, or 90-day stabilization review at a timing suited to the process volume. Examine the system by theme.

Review theme	Condition to examine
Records	Quality and accessibility of evidence
Flow	Late or failed cases and approved exceptions
Ownership	Workload and repeated questions
Performance	Reliability of reported measures
Independence	Actions still dependent on the implementation team

Adjust the operating model and risk treatment where the results warrant it.

Control toolkit release and licence information

Open `10 License and Release/00 Start Here.docx` (CP-SRC-132) for release routing. Use `01 ClausePass 27001 Commercial Terms.docx` (CP-SRC-133) as the source for the supplied commercial terms. This guide does not interpret or replace those terms.

Keep the preserved delivery copy with its release identifier in the approved administrative location. Retain the receipt or entitlement record there, along with update correspondence. Separate the unmodified delivery package from adapted organizational documents. When a toolkit update is received, compare release information and affected source files before replacing anything. Treat the update as input to document change, not as automatic authority to overwrite approved records.

Do not distribute templates, examples, or this guide outside the permissions that apply to the organization. If use or sharing is uncertain, consult the actual terms. The authorized commercial or legal owner should decide questions about modification and publication.

Qualify and adopt one sector source

Complete one sector-source applicability decision in this order.

1. Obtain an official copy and identify the competent interpreter.
2. State the affected population and exact provisions.
3. Classify the source's relationship with current requirements.
4. Resolve any conflict through the authorized route.
5. Propagate the approved decision through one complete control implementation trace.

Have a reviewer trace the change from source to operating record and audit criterion.

Then conduct the handover. Select five upcoming operating events and ask their assigned owners or deputies to run the entry steps using only the controlled sources. Record any missing access or knowledge. Treat an authority gap separately from missing data. Repair the handover index and schedule the stabilization review.

The first implementation pass ends with named owners, not with a finished folder. Sector sources need applicability and change decisions, conflicts need competent resolution, and source editions need monitoring. Keep every fictional example labelled. Transfer operating knowledge and leave open conditions visible. Schedule the next assurance and management cycles. Route toolkit release or licence questions to their governing sources.

The handover decision belongs to Laboratory D. Its trace must survive five upcoming operating events, one sector-source change, and a reviewer who uses only controlled sources. Acceptance fails if authority, access, source status, or the next cycle still depends on the implementation lead’s private knowledge.

Laboratory D: Defend the complete implementation trace

This capstone tests independent transfer. Assemble and defend the trace without following a supplied solution order. Use the live organization where authority and confidentiality permit. Otherwise use CP-SRC-127 and the existing fictional chronologies CP-SRC-121 or CP-SRC-131 as visibly fictional counterexamples after the first trace is complete. Do not invent a third organization to fill gaps. Feedback must state which decision, source, interface, or operating result broke and why the proposed repair returns to the correct authority.

Assignment

Select one in-scope service and one material information security risk. Assemble the implementation trace from the mandate through the next planned operating cycle. Ground each statement in the kind of record that can support it. Use a controlled source for an established requirement, a decision record for an approved choice, and an operating record for activity that has occurred. Label anything else as unknown.

The implementation trace to assemble

1. business purpose, sponsor, authority, resources, and implementation action
2. context, interested parties, obligations, service boundary, interfaces, and scope approval
3. risk scenario, method, sources, analysis, evaluation, owner, and uncertainty
4. treatment outcome, actions, necessary controls, Annex A comparison, SoA reasoning, and residual-risk decision
5. policy, standard, procedure, runbook, exception route, adoption, and document control
6. authoritative registers and stable identifiers
7. one ordinary operating case and one difficult case
8. evidence specification, measure or control review, and internal-audit coverage
9. finding, correction, cause, corrective action, implementation verification, and effectiveness review where a case exists
10. management-review input, decision, owner, resource, and follow-up
11. certification implication and claim boundary where certification is an approved objective
12. sector-source applicability, source watch, handover owner, and next trigger.

Challenge round

Assign the challenge roles by the perspective each participant must defend:

- **Governance:** sponsor and risk owner.
- **Operation:** process owner, control owner and evidence owner.
- **Assurance:** internal auditor and the relevant sector-source or certification coordinator.

They challenge the implementation trace with source-based questions:

- Which service result and population does the scope include?
- Where is the external dependency represented after it leaves the organizational boundary?
- What evidence supports the current-control description?
- Why is the control necessary, and where is its SoA status qualified?

- What happened when the ordinary process failed?
- Which source is authoritative when two registers disagree?
- How was the audit sample selected?
- What cause does the corrective action address?
- Which management decision remains open?
- What statement may accurately be made outside the organization?
- Which change would require this implementation trace to be reassessed first?

The presenter may answer only from the assembled sources or by recording a gap. A fluent explanation without a maintained source does not close the question.

Deliverables

- one-page map of the complete implementation trace
- indexed evidence and decision pack
- list of broken, ambiguous, duplicate, or privately held links
- repairs assigned to authoritative owners
- claim-boundary statement
- handover confirmation and next operating trigger
- short reflection identifying where the toolkit helped, where organizational design was still required, and what the next audit should test.

Completion review

The capstone passes when a second practitioner can perform the following review without private explanation:

- reconstruct the current state
- follow each material decision to its authority
- distinguish planned work from operation and demonstrated effectiveness
- locate exceptions and failed cases
- state the limits of the evidence; and
- identify the next owned action.

Remove every unsupported conformity or readiness claim before release. Apply the same rule to statements about certification or authorship.

Appendix A: Implementation planner

This planner converts the twelve modules into a controlled sequence. It is not a promised certification timetable. Set the pace from the actual boundary and the size of the organization. Then account for how often its processes run and how much system change is under way. Contract dates and decision authority may constrain the plan, but the schedule still needs enough time to observe real operation. Preserve dependencies when compressing it.

Readiness gates

Gate	Minimum result before dependent work is treated as established	Return route when the gate fails
G1: Controlled start	Preserved toolkit release, controlled working copy, mandate source, sponsor, implementation lead, action tracker	Module 1 or 2
G2: Approved boundary	Current context, interested parties, obligations, service boundary, interfaces, scope statement, governance and role authority	Module 3 and Laboratory A
G3: Repeatable risk method	Approved criteria, defined risk population, current assessment sources, named risk owners	Module 4
G4: Governed treatment	Treatment outcomes and actions, necessary controls, Annex A comparison, current SoA, residual-risk route	Module 5
G5: Usable instructions	Adapted documents, testable criteria, normal and exception paths, document control, adoption and change arrangements	Module 6 and Laboratory B
G6: Maintained records	Authoritative-source map, stable identifiers, field definitions, access, retention, review and reconciliation	Module 7
G7: Observed operation	Priority processes have ordinary and difficult cases, owner review, retained evidence and scheduled next cycles	Module 8
G8: Independent evaluation	Objectives and measures operate; evidence is controlled; audit programme, engagements, findings and follow-up are current	Module 9 and Laboratory C
G9: Management response	Corrections and corrective actions are controlled; effectiveness is evaluated; management review makes owned decisions	Module 10

Gate	Minimum result before dependent work is treated as established	Return route when the gate fails
G10: External objective controlled	Certification purpose, scope, provider checks, readiness decision, coordination, findings and claims are governed	Module 11, where certification is approved
G11: Living-system handover	Sector sources, owners, source watch, open conditions, next cycles, release and licence routes are transferred	Module 12 and Laboratory D

A 26-week planning frame

The frame below assumes that an organization has functioning business processes but is establishing or materially repairing its ISMS. Workstreams can overlap after their inputs are stable. Allow more time when the organization itself is new or the scope crosses many sites. Major technology change and incomplete inventories also slow the implementation project. So do controls whose natural operating cycle occurs only occasionally.

Period	Primary work	Operating or assurance work that should begin
Weeks 1–2	Preserve source material; confirm mandate, sponsor, authority, resources, project records and provisional service boundary	Sample current records; record external claims and fixed commitments
Weeks 3–5	Analyse context, interested parties, obligations, interfaces, dependencies, scope and governance	Reconcile service, supplier, asset and responsibility sources; run Laboratory A
Weeks 5–8	Approve risk method; build population; identify, analyse and evaluate risks	Trial the method with multiple assessors; resolve owner and source gaps
Weeks 7–10	Select treatment, determine necessary controls, compare Annex A, build SoA and residual-risk route	Start high-priority treatment actions; preserve current versus target state
Weeks 9–14	Adapt policies, standards, procedures, exceptions and document controls	Walk ordinary and difficult cases; release in manageable groups; run Laboratory B
Weeks 10–15	Establish authoritative registers, identifiers, field rules, access and retention	Reconcile samples across source systems; migrate only after acceptance tests
Weeks 13–19	Run first operating cycles and owner reviews	Record ordinary, late, failed, emergency and exception cases; repair dependencies
Weeks 16–21	Operate objectives, monitoring, measurement, evidence and internal audit	Complete audit engagements across the approved programme; run Laboratory C
Weeks 19–23	Correct cases, analyse causes, implement corrective actions and evaluate suitable early results	Prepare management-review inputs from authoritative periods and populations

Period	Primary work	Operating or assurance work that should begin
Weeks 22–24	Conduct management review and transfer decisions	Verify action ownership, resources, risk updates and next review triggers
Weeks 23–26	Where approved, make the certification readiness decision and coordinate provider activity	Preserve ordinary operation; do not stage or backfill records
Week 26 onward	Complete source applicability, handover, capstone and stabilization review	Continue control cycles, audits, improvement, surveillance and source watch

Do not place an internal audit or management review in the calendar solely to meet a date. The audit needs suitable criteria and an operating period. Management review needs current performance and risk information. Its audit results must be usable, and management must also be able to see progress against objectives and material change. If those inputs are not ready, repair the earlier dependency and record the schedule decision.

Weekly implementation control

Use the implementation plan and action tracker as the authoritative action source. A weekly control meeting should examine decisions and impediments, not ask every owner for a percentage complete.

Use one row per active item so that the meeting can decide rather than reconstruct each item.

Weekly control field	Decision made from it
Intended result and completion condition	What “closed” means for this item
Owner, authority, participants, and deputy	Who performs, decides, contributes, and preserves continuity
Current state and supporting source	What is known now and where it can be verified
Dependency and next operating opportunity	What must happen first and when the result can next be observed
Due date and reason	Which real commitment or operating need controls timing
Blocked decision or resource	What must be escalated rather than reported as progress
Risk created by delay	What exposure the schedule creates
Interim control or restriction	How the organization operates before the final result is available
Destination record and reviewer	Where closure will be maintained and who will challenge it
Changed assumption	Which part of the plan must be reopened

Close work only at the state defined in the action. “Procedure approved” may be a valid document action. Approval does not show that people have adopted the procedure or that it has operated. Owner review and evidence of control effectiveness come later.

Minimum meeting set

Use existing governance where it has the right authority and records. Avoid building a second meeting structure around the toolkit.

Forum	Practical purpose	Maintained output
Sponsor or steering review	Scope, priority, resource, conflict, risk and external-commitment decisions	Approved decisions and implementation actions
Scope and risk working session	Source-based boundary, scenario, criteria, treatment and ownership work	Updated scope, risk, treatment and SoA records
Policy/process owner session	Adapt instructions and test normal and failed cases	Controlled drafts, walkthrough results, adoption actions
Operating owner review	Examine populations, cases, service criteria, exceptions and evidence	Register updates, corrections, risks and improvement actions
Audit programme review	Prioritize coverage, competence, engagements, reporting and follow-up	Updated programme, plans, reports and findings
Management review	Evaluate suitability, adequacy, effectiveness and required change	Decisions, resources, actions and follow-up
Certification coordination	Manage accurate application, audit access, requests, findings and claims	Coordination log and controlled external records

Existing or stalled ISMS route

Do not begin by rewriting every document. Establish a live baseline:

1. preserve the current approved scope, risk method, SoA, policies, procedures, audit reports and management-review record
2. sample one normal and one failed or late case from several material processes
3. compare documented population, roles, criteria and evidence with current operation
4. identify the weakest dependency that can change later conclusions
5. repair source and authority records before derived dashboards or presentation packs
6. run the affected process again and evaluate the repair
7. expand according to risk, change, recurring failure and audit coverage.

An old approval does not prove current suitability. A recent record does not prove that the complete population is covered. Use both design and operation when setting the baseline.

Pre-certification compression check

If a fixed external date requires a shorter programme, show exactly where the evidence will become thinner. Organize that disclosure by the part of the programme being compressed:

- **Observation:** shorter operating periods, fewer natural events, or a smaller sample.
- **Delivery and assurance:** incomplete treatment, narrower audit coverage, less time to evaluate corrective-action effectiveness, or weaker management-review inputs.
- **Capacity:** reduced provider availability or insufficient time from accountable owners.

Obtain an explicit decision on the resulting risk and on the accuracy of any external commitment.

Never compress by inventing history or backdating an approval. Fictional example rows do not become evidence when copied, and a planned control benefit is not current operation. Reschedule when the available evidence cannot support the intended external event.

Appendix B: Working glossary

These working descriptions support consistent use of terms in this manual. They are not governing definitions. A licensed standard or applicable legal source prevails within its scope. Contractual definitions and certification rules do as well. When a governing source defines a term, use that definition for the case it controls.

Term	Working use in this manual
Accreditation	Independent attestation concerning a conformity-assessment body's competence for specified activities. Verify the body, scope and current status needed for the intended certificate.
Annex A reference controls	The reference set used during treatment work to check necessary controls and support the SoA. It is not an automatic universal implementation checklist.
Applicable requirement	A requirement the organization has determined applies within a stated entity, service, activity, jurisdiction, contract or other boundary.
Applicability	The result of deciding whether and how a source, requirement or control relates to the defined case. It is separate from implementation or conformity status.
Asset	Information or another associated item of value or importance that is governed within the organization's adopted inventory and risk approach.
Audit	A systematic, independent and documented process for obtaining and objectively evaluating evidence against audit criteria.
Audit conclusion	The result of an audit after considering its objectives and findings within the assigned scope and evidence limits.
Audit criteria	Requirements used as the reference against which audit evidence is compared.
Audit evidence	Records, statements of fact or other information relevant to the audit criteria and capable of verification.
Audit finding	The result of evaluating audit evidence against audit criteria.
Audit objective	What an audit is intended to accomplish.
Audit programme	Arrangements for one or more audits planned over a period for a stated purpose.
Audit scope	Boundaries and extent of an audit, including relevant locations, functions, activities, processes, systems and period.
Authoritative record	The approved source used to maintain a defined changing fact, decision, case or result.

Term	Working use in this manual
Availability	Availability means that authorized users can access information and related assets when required. Apply the governing definition where one is adopted.
Third-party certification	Third-party certification is an independent conformity-assessment process conducted by a certification body; it is not approval or certification by ISO.
Certification body	The organization that conducts management-system audit and certification work and makes the certification decision under its arrangements.
Confidentiality	Confidentiality means that information is not made available or disclosed to unauthorized people, entities, or processes.
Continual improvement	Recurring activity intended to enhance performance. It includes ordinary process and management-system change, not only corrective action.
Control	A control is a measure that maintains or modifies information security risk. A control may involve people, process, technology, physical measures, or a combination of them.
Control guidance	Control guidance explains information security controls and implementation considerations without replacing the requirements standard. ISO/IEC 27002 is the principal control-guidance source used here.
Control owner	The role accountable for the design, operation or performance oversight assigned to a control under the organization’s model. Define the exact authority locally.
Correction	A correction is action to eliminate a detected nonconformity. It addresses the observed condition; it may not address recurrence.
Corrective action	Corrective action is action to eliminate the cause of a nonconformity and prevent recurrence.
Documented information	Documented information is information the organization must control and maintain, together with the medium on which it is contained. The term covers both directions that must remain current and records retained as evidence.
Effectiveness	Effectiveness describes whether the organization carried out the activities it intended and obtained the intended results. Finishing a task does not, by itself, demonstrate effectiveness.
Evidence specification	A maintained description of the proposition, population, period, source, fields, collection, protection, review and limitation expected from evidence.
Exception	An authorized, bounded departure from an approved requirement or baseline under stated conditions. The organization may use a different controlled label.
External provider	An organization or party outside the defined organizational boundary that performs a function or supplies a process, product or service on which the ISMS relies.

Term	Working use in this manual
Finding	A result from evaluation. State its source and criteria; not every finding is a nonconformity.
Information security	Information security is the preservation of confidentiality, integrity, and availability of information. Other properties may also be relevant in a defined context.
Information security objective	A result sought by the organization that is relevant to information security and has an owned evaluation method.
Interested party	An interested party is an individual or organization that can influence an ISMS decision or activity, experience its consequences, or consider itself affected by it. Record the specific need or expectation and the organization's applicability decision.
Internal audit	Internal audit is a systematic, independent, and documented process conducted by or on behalf of the organization to obtain and evaluate audit evidence against audit criteria for its own management-system purposes.
Integrity	Integrity means that information remains accurate and complete. Apply the governing definition and technical context where needed.
Information security management system (ISMS)	An information security management system (ISMS) is the management system used to establish, implement, maintain, and continually improve information security.
Implementation project time	Implementation project time is the elapsed time used to establish or materially repair the ISMS. It is distinct from operating time.
Implementation trace	An implementation trace is a linked sequence from an initiating source or decision through implementation activity, operating records, evaluation, and follow-up that another reviewer can reconstruct.
Likelihood	Possibility of an event or scenario occurring, expressed under the organization's approved risk method. Define scales and time horizon.
Management review	A management review is top management's formal evaluation of whether the ISMS remains suitable, adequate, and effective and what changes or decisions are required.
Management system	A management system is the set of interrelated organizational elements used to establish policies and objectives and to achieve those objectives.
Measurement	Process used to determine a value. Preserve the unit, population, method, period, source and limitations.
Monitoring	Determining the status of a system, process or activity through supervision, observation or critical review. Monitoring and measurement may be combined but are not synonyms.
Necessary control	A control the organization has determined is needed through risk treatment or another applicable basis. Necessary controls are recorded in the SoA.

Term	Working use in this manual
Nonconformity	A nonconformity is non-fulfilment of a requirement. Record the applicable criterion and objective evidence.
Objective evidence	Data supporting the existence or truth of something. Its sufficiency depends on the proposition, population, period, source and method.
Operating cycle	One defined case, event, transaction, review or period through which a process produces its intended record and result.
Operating time	Operating time begins when an approved process or control is used in normal conditions. It accumulates genuine operating cases, records, and owner review over an elapsed period.
Policy	Controlled statement of organizational intention and direction, formally expressed through appropriate authority.
Population	Complete set of items or cases relevant to a process, measure, test or audit sample.
Procedure	Specified way to carry out an activity or process, including its trigger, responsibilities, sequence, decisions, records and failure route.
Process owner	Role accountable for the maintained process and its result under the organization’s governance model.
Record	Documented information retained as evidence of results achieved or activities performed.
Requirements standard	In this manual, the requirements standard is ISO/IEC 27001:2022 together with any amendment that applies to the implementation. It states requirements against which conformity may be assessed.
Residual risk	Risk remaining after treatment. Distinguish a forecast residual state from one reassessed using observed operation.
Risk	Effect of uncertainty on objectives. Information security risk is expressed and managed under the organization’s approved context and method.
Risk acceptance	Authorized decision to retain a stated risk under recorded conditions. It is separate from approval of a treatment plan.
Risk analysis	Work used to comprehend the nature of risk and determine its level under the approved method.
Information security risk assessment	An information security risk assessment is the systematic process of identifying, analysing, and evaluating information security risk under approved risk criteria.
Risk criteria	Terms against which the significance of risk is evaluated, including scales, thresholds, time horizon and decision rules adopted by the organization.
Risk evaluation	Comparison of risk-analysis results with risk criteria to determine significance and support decisions.

Term	Working use in this manual
Risk identification	Finding, recognizing and describing risks, including sources, events, causes and consequences as defined by the method.
Risk owner	Person or entity with accountability and authority to manage a risk within assigned limits.
Information security risk treatment	Information security risk treatment is the process of selecting and implementing measures that modify, retain, avoid, or share information security risk under the approved method.
Risk treatment plan	Maintained plan that translates approved treatment into executable actions, controls, responsibilities, timing, evidence and acceptance routes.
ISMS scope	The ISMS scope is the documented boundary and applicability of the information security management system. It identifies the conditions to which the ISMS applies.
Statement of Applicability (SoA)	The Statement of Applicability (SoA) is the maintained statement of necessary controls, the justification for including them, their implementation status, and the justification for excluding Annex A controls that the organization has determined are not necessary.
Standard	In this manual, a controlled internal document containing mandatory and testable criteria that supports policy and consistent implementation.
Supplier	External organization that provides a product or service. The relevant population and responsibilities are defined by the organization’s supplier-governance approach.
Surveillance	Certification-body audit activity within the certification cycle after initial certification and before recertification, according to the body’s programme.
Threat	Potential cause of an unwanted incident that may result in harm to a system or organization. Apply the adopted risk vocabulary consistently.
Vulnerability	Weakness that can be exploited or contribute to an unwanted event. Validation, exposure and risk context matter alongside a severity score.
Waiver	A term some organizations use for an authorized release from a stated requirement. Define whether it differs from an exception and control it accordingly.

Controlled-term index

This index points back to the first full explanation and to the glossary entry above. It is limited to the terms needed across the complete implementation journey; topic-specific terms remain available through the glossary and the module contents.

- **Term index: information security management system (ISMS):** established in “Terms this manual uses from the start”; developed throughout Modules 1–12.
- **Term index: information security:** established in “Terms this manual uses from the start”; applied throughout the manual.
- **Term index: confidentiality:** established in “Terms this manual uses from the start”; used in risk and control analysis.
- **Term index: integrity:** established in “Terms this manual uses from the start”; used in risk and control analysis.
- **Term index: availability:** established in “Terms this manual uses from the start”; used in risk and control analysis.
- **Term index: management system:** established in “Terms this manual uses from the start”; developed in Modules 2, 3, 8, and 10.
- **Term index: interested party:** established in “Terms this manual uses from the start”; developed in Module 3.
- **Term index: documented information:** established in “Terms this manual uses from the start”; developed in Modules 1, 6, and 7.
- **Term index: control:** established in “Terms this manual uses from the start”; developed in Modules 5–9.
- **Term index: effectiveness:** established in “Terms this manual uses from the start”; developed in Modules 5, 8, 9, and 10.
- **Term index: requirements standard:** established in “Terms this manual uses from the start”; applied wherever ISO/IEC 27001 requirements are discussed.
- **Term index: control guidance:** established in “Terms this manual uses from the start”; developed in Module 5.
- **Term index: third-party certification:** established in “Terms this manual uses from the start”; developed in Module 11.
- **Term index: implementation project time:** established in “Terms this manual uses from the start”; developed in Module 2.
- **Term index: operating time:** established in “Terms this manual uses from the start”; developed in Module 2.
- **Term index: implementation trace:** established in “Terms this manual uses from the start”; developed through Modules 2–12 and Laboratories B–D.
- **Term index: ISMS scope:** established in “Terms this manual uses from the start”; developed in Module 3.
- **Term index: information security risk assessment:** established in “Terms this manual uses from the start”; developed in Module 4.
- **Term index: information security risk treatment:** established in “Terms this manual uses from the start”; developed in Module 5.
- **Term index: Statement of Applicability (SoA):** established in “Terms this manual uses from the start”; developed in Module 5.
- **Term index: internal audit:** established in “Terms this manual uses from the start”; developed in Module 9.
- **Term index: nonconformity:** established in “Terms this manual uses from the start”; developed in Module 10.

- **Term index: correction:** established in “Terms this manual uses from the start”; developed in Module 10.
- **Term index: corrective action:** established in “Terms this manual uses from the start”; developed in Module 10.
- **Term index: management review:** established in “Terms this manual uses from the start”; developed in Module 10.

Implementation-state vocabulary

The following labels are used in Module 8 to prevent a single status from carrying several unsupported meanings.

State	Evidence expected
Designed	Approved control purpose, population, owner, criteria, process, records, failure route and evaluation method
Enabled	Necessary systems, access, resources, instructions and roles are available
Adopted	The affected population received the applicable communication, instruction or competence support
Operated	One or more genuine cases or cycles produced maintained records
Reviewed	An authorized owner evaluated the population or a justified sample against operating criteria
Effectiveness evaluated	Suitable evidence was compared with the intended result over a stated population and period
Changed or accepted	Authorized response, further treatment, exception or risk-acceptance decision was recorded

Organizations may use their own status scheme. Map each local value to a defined proposition and prevent users from inferring a stronger state than the evidence supports.

Appendix C: Current-source note

The sources below were checked on 22 August 2026 for terminology and lifecycle accuracy. This list does not replace a licensed copy. The organization must determine the applicable edition and amendment. It must also establish which scheme rules and contractual conditions govern its case.

Source	Status at the source-check date	Role in this guide
ISO/IEC 27001:2022, including Amendment 1:2024	Published requirements edition and applicable amendment at the research date	ISMS requirements and Annex A reference controls
ISO/IEC 27000:2026	Published in July 2026	Overview, concepts, principles and relationships within the ISMS family; this guide does not describe it as primarily the current terminology standard
ISO/IEC 27002:2022	Published third edition	Guidance for information security controls; 93 controls arranged in organizational, people, physical and technological themes with attributes for alternative views
ISO/IEC 27005:2022	Published fourth edition	Guidance for managing information security risks
ISO/IEC 27004:2016	Published edition at the research date; replacement work was underway	Guidance for monitoring, measurement, analysis and evaluation; recheck before a later release
ISO 19011:2026	Published fourth edition, replacing ISO 19011:2018	General guidance for management-system audit programmes and audits, including current treatment of remote auditing and virtual locations
ISO/IEC 27007:2020	Published edition at the research date; revision work was underway	Information-security-specific guidance for ISMS audit programmes, audits and auditor competence
ISO/IEC 17021-1:2015	Published edition at the research date	Requirements for bodies providing audit and certification of management systems
ISO/IEC 27006-1:2024	Published first edition	Additional requirements for bodies providing audit and certification of ISMSs

Recheck the official sources before using this material for a public release or certification application. A new audit programme and a material sector-source decision also warrant a current check, as does a materially updated edition of this guide. Obtain the certification body's current programme directly from an authoritative source. Verify its accreditation and the status of the intended certificate. Then establish the applicable audit arrangements, finding rules and rules for using certification marks.

The toolkit and this guide do not reproduce the requirements of ISO/IEC 27001. The implementation team needs authorized access to the standards and other sources it adopts. The organization's source system

should identify the adopted edition and any amendment. It should name the source owner and the licensed location, explain the access conditions, and assign responsibility for monitoring change.

Authority reminder

- ISO/IEC 27001 provides management-system requirements.
- ISO/IEC 27002 provides control guidance.
- ISO/IEC 27005 and ISO/IEC 27004 provide guidance within their stated subjects.
- ISO 19011 and ISO/IEC 27007 provide audit guidance within their scopes.
- ISO/IEC 17021-1 and ISO/IEC 27006-1 apply to certification bodies within their scopes.
- Applicable law, regulation, contract, scheme and sector sources require their own applicability and interpretation.
- The organization supplies its facts, decisions, operation and evidence.
- The certification body controls its audit findings and certification decision.
- ISO itself does not certify organizations.

Appendix D: Complete ClausePass27001 resource atlas

This atlas accounts for all 133 files in the toolkit release covered by this guide. The identifier is a navigation label used in the book; it does not replace the filename or the organization's document identifier. Open a resource when the stated work arises. Do not complete every file by default.

The destination column uses M1 through M12 for the field-guide modules; Capstone means Module 12 and Laboratory D. An atlas entry is only a route to the resource. The organization still decides whether to adopt it and which record will be authoritative. It must also assign approval authority and establish the evidence behind any populated content.

Toolkit root

Source	Resource	Manual destination
CP-SRC-001	00 Start Here.docx	M1
CP-SRC-002	00 Welcome to ClausePass 27001.docx	M1

01 Implementation Planning

Source	Resource	Manual destination
CP-SRC-003	00 Start Here.docx	M2–M3
CP-SRC-004	01 Initial Implementation Decisions.docx	M2–M3
CP-SRC-005	02 Implementation Planning and Governance.docx	M2–M3
CP-SRC-006	03 Evidence and Readiness Decisions.docx	M2–M3
CP-SRC-007	04 Deciding Whether to Pursue Certification.docx	M2–M3
CP-SRC-008	05 ISO IEC 27001 Implementation Planning Record.docx	M2–M3
CP-SRC-009	06 Implementation Planning and Coordination.docx	M2–M3
CP-SRC-010	07 ISMS Implementation Lifecycle.docx	M2–M3
CP-SRC-011	08 ISO IEC 27001 Implementation Sequence.pptx	M2–M3
CP-SRC-012	09 Leadership Kickoff Workshop.pptx	M2–M3
CP-SRC-013	10 Leadership and Implementation Discussion Cards.docx	M2–M3

Source	Resource	Manual destination
CP-SRC-014	11 Control Ownership and Evidence.docx	M2–M3
CP-SRC-015	12 Technology Responsibilities and Evidence.docx	M2–M3

02 Scope and Governance

Source	Resource	Manual destination
CP-SRC-016	00 Start Here.docx	M3
CP-SRC-017	01 Context and Governance.docx	M3
CP-SRC-018	02 ISMS Scope and External Interfaces.docx	M3
CP-SRC-019	03 Context, Scope and Governance Approval Workshop.pptx	M3
CP-SRC-020	04 ISMS Operating Model.docx	M3
CP-SRC-021	05 First ISMS Operating Cycle and Issue Recovery.docx	M3

03 Policies, Standards and Procedures

Source	Resource	Manual destination
CP-SRC-022	00 Start Here.docx	M6
CP-SRC-023	CP-POL-001 - AI and Emerging Technology Security Policy.docx	M6
CP-SRC-024	CP-POL-002 - Governance Roles and Responsibilities Policy.docx	M6
CP-SRC-025	CP-POL-003 - Information Security Policy.docx	M6
CP-SRC-026	CP-POL-004 - Intellectual Property and Confidentiality Policy.docx	M6
CP-SRC-027	CP-POL-005 - Asset Management Policy.docx	M6
CP-SRC-028	CP-POL-006 - Data Masking and Data Loss Prevention Policy.docx	M6
CP-SRC-029	CP-POL-007 - Information Classification Policy.docx	M6
CP-SRC-030	CP-POL-008 - Information Transfer Policy.docx	M6
CP-SRC-031	CP-POL-009 - Privacy and PII Protection Policy.docx	M6

Source	Resource	Manual destination
CP-SRC-032	CP-POL-010 - Records Retention and Disposal Policy.docx	M6
CP-SRC-033	CP-POL-011 - Acceptable Use and Remote Working Policy.docx	M6
CP-SRC-034	CP-POL-012 - Endpoint and Removable Media Policy.docx	M6
CP-SRC-035	CP-POL-013 - Human Resources Security Policy.docx	M6
CP-SRC-036	CP-POL-014 - Cloud Services Security Policy.docx	M6
CP-SRC-037	CP-POL-015 - Supplier Security Policy.docx	M6
CP-SRC-038	CP-POL-016 - Backup and Recovery Policy.docx	M6
CP-SRC-039	CP-POL-017 - Malware Protection and Endpoint Detection Policy.docx	M6
CP-SRC-040	CP-POL-018 - Web Filtering and Internet Access Policy.docx	M6
CP-SRC-041	CP-POL-019 - Access Control and Identity Management Policy.docx	M6
CP-SRC-042	CP-POL-020 - Cryptography and Key Management Policy.docx	M6
CP-SRC-043	CP-POL-021 - Network and Communications Security Policy.docx	M6
CP-SRC-044	CP-POL-022 - Secure Development Lifecycle Policy.docx	M6
CP-SRC-045	CP-POL-023 - Physical and Environmental Security Policy.docx	M6
CP-SRC-046	CP-STD-001 - Secure Configuration Baseline Standard.docx	M6
CP-SRC-047	CP-STD-002 - Authentication, MFA and Secrets Standard.docx	M6
CP-SRC-048	CP-PRC-001 - Control Assurance and Security Testing Procedure.docx	M6
CP-SRC-049	CP-PRC-002 - Document and Record Control Procedure.docx	M6
CP-SRC-050	CP-PRC-003 - Evidence Collection and Preservation Procedure.docx	M6
CP-SRC-051	CP-PRC-004 - Legal and Regulatory Compliance Procedure.docx	M6
CP-SRC-052	CP-PRC-005 - Objectives and Compliance Review Procedure.docx	M6

Source	Resource	Manual destination
CP-SRC-053	CP-PRC-006 - Risk Assessment and Treatment Procedure.docx	M6
CP-SRC-054	CP-PRC-007 - Supplier Assurance Procedure.docx	M6
CP-SRC-055	CP-PRC-008 - Capacity and Performance Management Procedure.docx	M6
CP-SRC-056	CP-PRC-009 - Change and Configuration Management Procedure.docx	M6
CP-SRC-057	CP-PRC-010 - Clock Synchronization Procedure.docx	M6
CP-SRC-058	CP-PRC-011 - Logging, Monitoring and Detection Procedure.docx	M6
CP-SRC-059	CP-PRC-012 - Threat Intelligence Procedure.docx	M6
CP-SRC-060	CP-PRC-013 - Vulnerability and Patch Management Procedure.docx	M6
CP-SRC-061	CP-PRC-014 - Privileged Access Management Procedure.docx	M6
CP-SRC-062	CP-PRC-015 - Application Security Testing Procedure.docx	M6
CP-SRC-063	CP-PRC-016 - Security in Project Management Procedure.docx	M6
CP-SRC-064	CP-PRC-017 - Source Code Repository and Secrets Procedure.docx	M6
CP-SRC-065	CP-PRC-018 - Test Data and Environment Management Procedure.docx	M6
CP-SRC-066	CP-PRC-019 - Business Continuity and ICT Readiness Procedure.docx	M6
CP-SRC-067	CP-PRC-020 - Incident Response Procedure.docx	M6
CP-SRC-068	CP-PRC-021 - Secure Disposal and Reuse of Equipment Procedure.docx	M6
CP-SRC-069	04 Managing Policies and Procedures.docx	M6
CP-SRC-070	05 Policy and Procedure Decisions Workshop.pptx	M6
CP-SRC-071	06 Policy System Operating Model.docx	M6
CP-SRC-072	07 Policy Adoption, Exceptions and Change.docx	M6

04 Risk and Statement of Applicability

Source	Resource	Manual destination
CP-SRC-073	00 Start Here.docx	M4–M5
CP-SRC-074	01 Risk Management and the Statement of Applicability.docx	M4–M5
CP-SRC-075	02 Information Security Risk Method.docx	M4–M5
CP-SRC-076	03 Risk and Statement of Applicability Decisions Workshop.pptx	M4–M5
CP-SRC-077	04 Risk Decisions and Reassessment.docx	M4–M5

05 ISMS Registers, Plans and Logs

Source	Resource	Manual destination
CP-SRC-078	00 Start Here.docx	M7–M10
CP-SRC-079	01 Maintaining ISMS Registers, Plans and Logs.docx	M7–M10
CP-SRC-080	Asset Register.xlsx	M7–M10
CP-SRC-081	Backup and Restore Test Log.xlsx	M7–M10
CP-SRC-082	Business Continuity and Recovery Test Register.xlsx	M7–M10
CP-SRC-083	Business Impact and Continuity Requirements Register.xlsx	M7–M10
CP-SRC-084	Change Register.xlsx	M7–M10
CP-SRC-085	Context, Interested Parties and Scope Register.xlsx	M7–M10
CP-SRC-086	Evidence Register.xlsx	M7–M10
CP-SRC-087	Exceptions and Waivers Register.xlsx	M7–M10
CP-SRC-088	Findings, Nonconformity and Corrective Action Register.xlsx	M7–M10
CP-SRC-089	Internal Audit Plan and Checklist.xlsx	M7–M10
CP-SRC-090	ISMS Implementation Plan and Action Tracker.xlsx	M7–M10
CP-SRC-091	ISO 27001 Gap Assessment.xlsx	M7–M10
CP-SRC-092	Legal, Regulatory and Contractual Requirements Register.xlsx	M7–M10
CP-SRC-093	Management Review Actions and Performance Register.xlsx	M7–M10
CP-SRC-094	Master Document Register.xlsx	M7–M10

Source	Resource	Manual destination
CP-SRC-095	Risk Register and Risk Treatment Plan.xlsx	M7–M10
CP-SRC-096	Security Incident Register.xlsx	M7–M10
CP-SRC-097	Security Objectives and KPI Register.xlsx	M7–M10
CP-SRC-098	Statement of Applicability.xlsx	M7–M10
CP-SRC-099	Supplier Register and Assessment.xlsx	M7–M10
CP-SRC-100	Training and Awareness Register.xlsx	M7–M10
CP-SRC-101	User Access Register and Access Review.xlsx	M7–M10
CP-SRC-102	Vulnerability and Patch Register.xlsx	M7–M10

06 Evidence, Internal Audit and Improvement

Source	Resource	Manual destination
CP-SRC-103	00 Start Here.docx	M9–M10
CP-SRC-104	01 Evidence, Internal Audit and Improvement.docx	M9–M10
CP-SRC-105	02 Resolving Evidence and Audit Issues.docx	M9–M10
CP-SRC-106	03 Management Review Decisions Workshop.pptx	M9–M10

07 Certification Preparation

Source	Resource	Manual destination
CP-SRC-107	00 Start Here.docx	M11
CP-SRC-108	01 Certification Planning and Lifecycle.docx	M11
CP-SRC-109	02 Certification Audit Coordination and Findings.docx	M11
CP-SRC-110	03 Certification Readiness Decision Workshop.pptx	M11

08 Sector Guidance

Source	Resource	Manual destination
CP-SRC-111	00 Start Here.docx	M12
CP-SRC-112	01 Sector Context and Source Use.docx	M12

Source	Resource	Manual destination
CP-SRC-113	02 Sector Review Questions.docx	M12
CP-SRC-114	03 Resolving Sector-Source Conflicts.docx	M12
CP-SRC-115	04 Sector Applicability Decisions Workshop.pptx	M12

09 Worked Examples

Source	Resource	Manual destination
CP-SRC-116	00 Start Here.docx	Capstone
CP-SRC-117	01 Hearthline Example Overview.docx	Capstone
CP-SRC-118	02 FICTIONAL EXAMPLE - Hearthline End-to-End ISMS Example.docx	Capstone
CP-SRC-119	03 Fictional Example Review Workshop.pptx	Capstone
CP-SRC-120	FICTIONAL EXAMPLE - Hearthline Worked ISMS Records.xlsx	Capstone
CP-SRC-121	01 FICTIONAL EXAMPLE - Hearthline Data Services Implementation Chronology.docx	Capstone
CP-SRC-122	02 FICTIONAL EXAMPLE - Hearthline Context, Scope and Governance.docx	Capstone
CP-SRC-123	03 FICTIONAL EXAMPLE - Hearthline Policy and Procedure Adaptation.docx	Capstone
CP-SRC-124	04 FICTIONAL EXAMPLE - Hearthline Risk Management and Statement of Applicability.docx	Capstone
CP-SRC-125	05 FICTIONAL EXAMPLE - Hearthline Evidence, Internal Audit and Improvement.docx	Capstone
CP-SRC-126	06 FICTIONAL EXAMPLE - Hearthline Certification Preparation.docx	Capstone
CP-SRC-127	07 FICTIONAL EXAMPLE - Hearthline Sector Context and Source Applicability.docx	Capstone
CP-SRC-128	01 FICTIONAL EXAMPLE - HDS-POL-041 - Information Security and Decision Authority Policy.docx	Capstone
CP-SRC-129	02 FICTIONAL EXAMPLE - HDS-STD-041 - Authentication and Service Credential Standard.docx	Capstone
CP-SRC-130	03 FICTIONAL EXAMPLE - HDS-PRC-041 - Customer Incident Communication Procedure.docx	Capstone

Source	Resource	Manual destination
CP-SRC-131	01 FICTIONAL EXAMPLE - Asterline Implementation Chronology.docx	Capstone

10 License and Release

Source	Resource	Manual destination
CP-SRC-132	00 Start Here.docx	M1–M12
CP-SRC-133	01 ClausePass 27001 Commercial Terms.docx	M1–M12

Atlas reconciliation

The release is accounted for when CP-SRC-001 through CP-SRC-133 are present once, each file resolves within the preserved toolkit, and every adopted resource has an organizational owner or an explicit reason for not being adopted. A later toolkit release requires a new inventory and comparison; do not reuse this atlas as proof that the later release is unchanged.

For fictional resources, the fictional label is part of the control boundary. For commercial terms, the named source remains authoritative. A template or workbook acquires record status only through organizational adoption and use. Its presence in this atlas proves no more than inventory and routing.

Turn the Guide Into a Working ISMS

Get your clausepass27001 toolkit