



KIS | PRACTICAL SECURITY PRODUCTS

A FIELD GUIDE FOR IMPLEMENTATION

How to Use the KIS ISMS 22-Module Toolkit

A practical route from scope and risk to operating evidence, audit, and improvement.



FREE COMPANION PDF • RELEASE 1.0.0 • 15 OCTOBER 2026



22

NUMBERED MODULES

01–20

CORE ISMS SET

21–22

LIFECYCLE GUIDES

KIS working material | Tailor to your organization and validate against licensed requirements.

Start with a decision, then build evidence

This field guide gives a practical order for using the master manual, registers, and 22 module toolkits. It is designed for the executive sponsor, ISMS owner, process leads, and internal auditors working together.

The toolkit is a set of working documents. It will not implement controls by itself. Treat each module as a controlled draft: confirm scope, choose an owner, agree the local rule, approve it at the right level, operate it, keep evidence, and review whether the result works.

A useful first meeting ends with four decisions: the person accountable for the ISMS, the services and locations in scope, the risk acceptance authority, and the approved place where records will be kept. Leave detailed control drafting until those decisions are clear.

A 90-minute kickoff can produce a credible start:

- Name the executive sponsor, ISMS owner, risk owners, privacy/legal contact, and control owners.
- Agree which products, services, people, sites, suppliers, systems, and data the ISMS will cover.
- List customer, legal, regulatory, contractual, and other interested-party requirements with a source and owner.
- Set the risk method and the authority that can accept residual risk or approve exceptions.
- Create a secure evidence workspace with access, naming, retention, and deletion rules.
- Schedule the steering committee, evidence workshops, first risk review, and management review checkpoint.

DECISION GATE 1

Do not approve the scope until material interfaces and dependencies are visible. An excluded service or supplier may still affect security inside the boundary.

Keep this guide beside the editable master manual. The manual describes how the management system fits together; the modules provide focused procedure starters and evidence tools. Use the module PDFs as reading copies and edit the DOCX and XLSX files as working originals.

Understand the package before you tailor it

There are 22 numbered ISMS toolkits. The current shop has 24 product listings because it lists those 22 modules separately, plus the all-in-one bundle and a separate SME Incident Readiness Kit.

Asset	Use it for	Owner action
Master ISMS manual (DOCX + PDF)	Organizing document for clauses 4–10, governance, risk, SoA, operation, review, audit, and improvement.	Tailor scope, roles, policy, risk criteria, approval thresholds, and process interactions. Keep the DOCX controlled; use the PDF for reading.
Master working registers (XLSX)	Cross-module tracking for scope, risks, control applicability, policies, data flows, audits, actions, and evidence.	Agree one system of record. Protect access, set retention, and identify the owner of every live record.
Modules 01–20	Core implementation sequence for the management-system requirements and risk-based controls.	Use where a procedure, owner, operating record, or control evidence is needed. Combine procedures where that fits the organization's process.
Modules 21–22	Lifecycle companions for certification readiness, auditor evidence, surveillance, and continual improvement.	Use after the core system is operating and continue to use after certification or when preparing for external audit.
Free field guide	A sequence and working method for the whole package.	Download and share internally as orientation. The guide is public; protect the organization's own records separately.

PRODUCT COUNT

24 shop products = 22 numbered modules + 1 all-in-one bundle + 1 separate SME Incident Readiness Kit. The all-in-one package contains Modules 01–22; it is one product, not an additional numbered module.

A module pack may include editable Word policy/procedure material, a matching PDF, an Excel workbook, a PowerPoint briefing, a readme, and a module-specific implementation guide. The all-in-one product groups those packs with the master manual and master workbook. Check the included file list in the actual release ZIP, because release versions can change.

Follow the management-system cycle

The order matters: scope and obligations shape the risk assessment; risk treatment shapes the SoA and procedures; evidence and review test whether the controls operate.

01 Set context	02 Assess risk	03 Choose treatment	04 Operate controls	05 Evaluate evidence	06 Improve
-------------------	-------------------	------------------------	------------------------	-------------------------	---------------

Stage	What to produce	Exit question
01 Context and scope	Context and interested-party registers, approved scope, process map, obligations and dependencies.	Can an independent reader tell what is in scope, what is outside it, and why?
02 Risk assessment	Approved criteria and a consistent record of scenarios, impact, likelihood, risk owner and decision.	Can the organization reproduce the assessment and explain the decision?
03 Treatment and SoA	Treatment plan, risk-owner approvals and a justified applicability and implementation view.	Are selection, exclusion, residual risk, owner and status separately explained?
04 Operation	Tailored procedures, assigned roles, implemented controls and records from actual operation.	Is there dated evidence from the real process, not just a planned policy?
05 Evaluation	Measures, audit results, management decisions and action records.	Do the results trigger decisions, owners, due dates and verified closure?
06 Improvement	Corrective actions, lessons and controlled changes to the ISMS.	Did the response remove causes and reduce recurrence or impact?

Plan the sequence around risk and operating reality. The sample 12-week/90-day plan in this guide is a planning aid, not a promised certification timeline. A complex scope, outsourced service, legacy environment, or major remediation need may take longer.

Give people clear authority to decide

A steering committee turns evidence into accountable decisions. It should include people with authority over business priorities, security risk, technology, people, suppliers, privacy, and resources.

Role	Decision or responsibility	Useful record
Executive sponsor / top management	Set direction; approve policy and scope; provide resources; decide escalated risks within authority; review performance.	Approved policy, scope, risk appetite or criteria, meeting decisions, resourcing.
ISMS owner / coordinator	Maintain the management system, calendar, registers, evidence map, reporting, and controlled changes.	ISMS plan, action log, document register, dashboards, decision trace.
Risk owner	Own a business risk; validate impact; choose treatment with authority; accept residual exposure or escalate it.	Risk assessment, treatment decision, residual-risk approval, review trigger.
Control / process owner	Design and operate a safeguard; retain records; report failures; test operation; fix gaps.	Procedure, operating sample, measure, exception and corrective action.
Legal / privacy / HR / technology adviser	Interpret relevant duties and constraints in their expertise and flag changes; provide evidence and safeguards.	Obligation assessment, approved advice/action, privacy or personnel safeguards.
Internal auditor	Evaluate objectively against stated criteria; sample evidence; report results; follow up without auditing own work.	Audit program, plan, working papers, findings, conclusions.

A practical steering cadence is monthly during initial implementation, then quarterly or risk-led after the system stabilizes. Set the cadence based on risk and change. Every meeting should review prior actions, material context changes, risk and treatment status, objective and incident trends, supplier concerns, audit results, resource needs, and decisions. Send a short input pack in advance; record decisions, owners, due dates, rationale, and escalation.

Use the authority matrix below as a starting point, then replace it with a formally approved local delegation:

Decision	Prepared by	Approval route
Routine control procedure	Control owner with ISMS owner review	Delegated process authority; link to scope, risks and SoA.
Risk treatment / residual risk	Risk owner with control owner	Person with authority matching the risk threshold; escalate beyond delegated limit.
Policy, scope or material ISMS change	ISMS owner and affected business owners	Top management or documented delegate; communicate and set effective date.
Exception	Requesting owner, with impact and safeguards	Authorized risk owner, time-bound; record expiry and review.

Set context, obligations and the ISMS boundary

Use Modules 02 and 16 early. The boundary must describe the real service, people, technology, places, data, suppliers and interfaces that affect information security.

Begin with the business outcome the ISMS must protect. Document key services, customer promises, information assets, dependencies, sites, remote work, cloud platforms and outsourced operations. Interview service and technology owners, then test the draft against contracts, architecture, data flows and the way work is actually performed.

Boundary question	Capture	Evidence to confirm
Which services and outputs are in scope?	Products, services, business units, processes, customer commitments.	Service catalogue, org chart, process walkthrough, customer contract.
Where and by whom is work performed?	Sites, remote work, personnel, contractors and support locations.	Site list, HR/vendor records, access model and support arrangements.
Which systems and data support the service?	Applications, endpoints, networks, repositories, records and information classes.	Asset inventory, architecture/data-flow diagrams, system-owner confirmation.
Who can affect security across the boundary?	Suppliers, cloud providers, subprocessors, partners and customer interfaces.	Supplier inventory, contracts, data processing terms, shared-responsibility matrix.
Which requirements apply?	Legal, regulatory, contractual, customer and internal requirements; source, owner and review date.	Obligation register, legal/privacy review and contract clauses.
Is climate change relevant to context or interested-party requirements?	A reasoned relevance decision, supporting context and review trigger.	Decision record; business continuity, facilities, supplier or customer inputs where relevant.

BOUNDARY TEST

Trace one customer information item from collection to deletion. If a system, person, support location, supplier, or hand-off affects it, account for that dependency in the scope, risk assessment, control design, and evidence plan.

Keep exclusions explicit and evidence-backed. An exclusion is not a way to avoid a material dependency. Describe the interface and the safeguards that manage it. Revisit the scope when products, locations, providers, legal duties, data use, or organizational structure change.

Make risk decisions repeatable

Module 03 supplies an assessment method starter; Module 04 connects the result to treatment and the SoA. The organization must approve the scales and acceptance authority it will actually use.

Write risk scenarios as a cause, event and consequence. Identify the information or service affected and consider confidentiality, integrity and availability. Rate likelihood and impact using approved definitions, explain the evidence behind the rating, then assign a named risk owner. Do not treat a spreadsheet score as a decision by itself.

Example step	Illustrative entry for a small professional-services firm
Asset / service	Client engagement workspace containing project records and business contact details.
Scenario	A compromised staff account is used to download or alter client files before the activity is detected.
Cause / weakness	Credential theft plus an unreviewed privileged access route and incomplete alert triage.
Impact	Confidentiality breach, service disruption, contractual response effort, and possible regulatory assessment.
Treatment decision	Enforce stronger authentication, narrow privileged access, alert on unusual downloads, test response and retain review evidence.
Residual risk	Re-score after controls operate; record remaining exposure, evidence, owner decision and next review trigger.

If you use a likelihood-by-impact matrix, define the scale and bands before scoring. State impact dimensions, risk aggregation rules, uncertainty, acceptance thresholds, escalation, review cadence and who can approve. Use both routine and event-triggered reassessment, such as a major change, incident, new supplier, new data use, material obligation, or test result.

Keep a short decision trail: scenario, inherent/current state, existing safeguards, likelihood and impact rationale, risk rating, action and chosen treatment, owner, target date, residual rating, approval, evidence link and reassessment trigger. If evidence is unavailable, mark the assumption and assign a validation action.

DO NOT CONFUSE STATUS

Risk accepted, control applicable, control implemented, and control operating effectively are distinct statements. Record each separately and support each with its own decision or evidence.

Use the SoA as a reasoned control decision

The Statement of Applicability is the bridge between risk treatment and the control set. It should not be a checklist that marks all controls yes or no without rationale.

For each Annex A identifier in the master workbook, decide whether the control is necessary to treat risks or meet obligations. Compare the reference set against your selected controls. The SoA should show applicability, the reason for inclusion or exclusion, implementation status, owner, related risk or requirement, evidence location, and approval/review. Verify exact requirements and control wording in the licensed standard.

SoA field	Decision rule	Example
Applicability	Include when needed for risk treatment or obligations; otherwise record a specific, defensible exclusion rationale.	Applicable because remote access creates a material identity risk and customer contract requires controlled access.
Implementation status	Describe actual state separately from applicability; use local stages such as planned, partial, implemented, verified.	Implemented for employees; contractor review remains open with owner and due date.
Owner and timing	Name the accountable control owner, action owner and review date.	IT operations; complete contractor group by 30 June; review quarterly.
Evidence	Link to a controlled record that demonstrates operation, with date/range and custodian.	Quarterly access review record and sample of revoked accounts.
Residual risk / approval	Connect the decision to treatment and the authorized risk owner.	Risk owner accepts remaining exposure until supplier identity integration is complete.

A useful review reconciles four sources: the risk register, treatment plan, SoA, and control evidence. For each significant risk, confirm there is a clear path from risk to treatment and relevant control(s), owner, implementation evidence, residual-risk decision and review trigger. Conversely, investigate any control marked applicable with no risk, obligation or scope rationale.

The master workbook contains all 93 Annex A identifiers as original KIS comparison prompts; it is not official control text. Applicability is determined by the organization after considering risk and obligations. A selected control may not be the only safeguard needed, and an exclusion does not remove an applicable legal or contractual duty.

Collect evidence through more than one channel

Choose the method that proves the question with the least disruption and the right level of assurance. Record the method, date, participants, source, limitations and follow-up.

Method	Good use	Record and safeguard
Facilitated workshop	Map processes, identify dependencies, agree roles, walk through risk or data-flow decisions.	Agenda, attendees/roles, inputs, decisions, open actions, facilitator notes reviewed by the owner.
One-to-one interview	Understand a control operator's actual steps, hand-offs, exception route and record location.	Interviewee role, questions, notes validated for factual accuracy, evidence references; minimize personal data.
Group/team meeting	Compare how functions handle a shared process such as joiner access, incident triage or supplier change.	Purpose, participant roles, distinct views, agreed actions, owner and due date.
Email / offline submission	Collect approved policies, records or explanations when a workshop is not practical.	Retain source message or approved export in the evidence system; use approved secure transfer and access controls.
Shared drive / evidence portal	Collect controlled files and track evidence submissions across teams.	Use least-privilege access, version control, naming, owner, retention and deletion rules; avoid public links.
Teams / Zoom / online session	Remote workshop, screen-share walkthrough, interview or demonstration.	Confirm consent and recording rules; document evidence IDs and decisions. Do not record by default; store any approved recording securely.
System extract / log review	Verify access, backups, patches, vulnerabilities, alerts, incidents or configuration state.	Identify system, query, period, filters, completeness, custodian, time zone and integrity safeguards.
Observation / process walkthrough	Watch a normal transaction or control performed from trigger to closure.	Sample ID, date, observer, steps observed, deviations and follow-up evidence. Avoid unnecessary production changes.
Document and contract review	Confirm approvals, obligations, supplier terms, retention, response clauses and change history.	Controlled version, source, clause/requirement reference, reviewer and conclusion; protect confidential terms.
Sampling / reperformance	Test whether a selected population was handled consistently, such as leaver revocation or restore tests.	Population, selection basis, sample, expected result, actual result, exceptions and tester conclusion.

Use multiple methods for higher-risk assertions. For example, compare an access policy (design), an approved access request (implementation), system permissions (operation), and a leaver sample (effectiveness). A meeting statement alone rarely demonstrates consistent operation.

Keep evidence useful, safe and traceable

An evidence item should let a reviewer understand what happened, when, for which scope, who performed and reviewed it, what the result was, and where the authoritative record lives.

Evidence attribute	Check before accepting
Relevance	Does it directly support the control or requirement being assessed? Is the scope and period clear?
Reliability	Can the source and custodian be identified? Is it system-generated, approved, complete, and protected from alteration?
Sufficiency	Is the sample broad enough for the risk and assertion? Were failures, exceptions and adverse cases considered?
Timeliness	Does the evidence cover the review period and current system/process state?
Traceability	Can the item be linked to an evidence ID, owner, record location, date, related risk/control, and conclusion?
Confidentiality	Is collection minimized? Are secrets, credentials, customer data and personnel details redacted or access-restricted?

A sensible evidence identifier might be `M08-ACCESS-2026Q2-004`. The evidence index should point to the authoritative record, not duplicate everything. Use a controlled repository with role-based access, versioning, retention schedule, legal hold process and secure disposal. Do not place passwords, private keys, unredacted personal data, or raw sensitive production content in a general audit pack.

When evidence is collected by email or shared workspace, move the approved item into the record system and retain the source context needed to establish authenticity. For an interview, label it as inquiry evidence and corroborate important claims with an observation, sample or system record. If remote screen-sharing is used, note what was demonstrated, which account/environment was shown, who observed it, and any limitation.

EVIDENCE IS NOT A SCREENSHOT COUNT

A screenshot without context can be weak or misleading. Preserve source, time period, population, selection, result, reviewer, and exception details so the evidence can be independently understood.

Apply the module sequence: governance and protection

Core modules 01–20 support ISMS implementation; use them in the order that fits the organization's dependencies and risk priorities. The table is a routing map, not a mandatory policy-per-control design.

ID	Module	Main use / output
01	ISMS Policy and Governance	Set the leadership mandate, accountable roles, approvals, policy communication and exception authority.
02	Context, Scope and Interested Parties	Define internal and external context, obligations, interfaces, boundaries and the maintained scope statement.
03	Risk Assessment and Acceptance Method	Approve repeatable criteria, identify information-security risks, evaluate them and record risk-owner decisions.
04	Risk Treatment and Statement of Applicability	Select and justify treatments and controls, maintain the SoA and track implementation and residual-risk approvals.
05	Objectives, Measures and Improvement	Turn policy intent into measurable objectives, review results and track effective improvement.
06	Document and Record Control	Create, approve, identify, distribute, protect, retain and dispose of controlled documented information.
07	Asset Inventory, Classification and Acceptable Use	Assign owners and classification to information and supporting assets; define handling, use, return and disposal.
08	Identity, Access and Authentication	Authorize access through joiner, mover and leaver events, periodic review, authentication and privileged-access controls.
09	People Security and Remote Work	Set lawful, role-based personnel safeguards, awareness, confidentiality and secure remote-work rules.
10	Supplier and Cloud Security	Tier supplier risk, set contract safeguards, oversee cloud/shared responsibility and manage exit.
11	Physical Security and Equipment	Protect facilities and equipment through zones, visitor controls, secure handling and asset return.

Modules 01–04 establish direction, context, risk and treatment. Modules 05–06 set objectives and control the records that prove decisions. Modules 07–16 operationalize people, assets, suppliers, facilities, technology, resilience, incidents and privacy. Use the same owner and evidence conventions across all modules so that the master registers remain coherent.

Do not create unnecessary duplicate policies. An integrated policy can govern several processes when it stays clear, approved and usable. The organization must retain the records needed to show that required processes operate, regardless of how many documents it chooses to maintain.

Apply the module sequence: assurance and lifecycle

Modules 17–20 help complete, test and correct the system. Modules 21–22 extend that work into external-audit readiness and the continued operation of a certified management system.

ID	Module	Main use / output
12	Operations, Vulnerability and Configuration	Run controlled operational changes, hardening, vulnerability handling, logging and monitoring.
13	Cryptography and Key Handling	Choose encryption based on risk and obligations; govern key custody, rotation, recovery and destruction.
14	Backup, Continuity and Recovery	Set recovery requirements, protect backups, test restoration and coordinate continuity dependencies.
15	Incident and Evidence Handling	Report, triage, contain and learn from events while protecting reliable, traceable evidence.
16	Privacy and Data Sovereignty	Map personal and sensitive data flows, regions, transfers, retention, supplier access and applicable duties.
17	Secure Development and Change	Build security requirements into design, development, testing, deployment and change review.
18	Internal Audit	Plan impartial, risk-based audits, collect sufficient evidence, report findings and verify follow-up.
19	Management Review	Give top management an evidence-led view of ISMS suitability, adequacy, performance and decisions.
20	Nonconformity and Corrective Action	Contain issues, analyze causes, apply corrections, verify effectiveness and update the ISMS.
21	Certification Readiness and Auditor Evidence	Organize audit scope, evidence pathways, interviews, sampling and readiness actions.
22	Surveillance and Continual Improvement	Maintain the system after initial certification through surveillance planning, change triggers and improvement.

RELATIONSHIP TO THE 20-MODULE CORE

Modules 01–20 form the core implementation package. Modules 21 and 22 are distinct companion toolkits for certification readiness and surveillance/continual improvement. The updated all-in-one release includes all 22 numbered packages.

The series is modular. A small organization may use a single procedure to cover multiple topics; a complex organization may split work by service, location or risk. Keep the cross-reference between local procedures, the master manual, the SoA, risk records, and evidence index current.

Plan a practical 90-day first cycle

This illustrative schedule assumes a small organization with engaged owners and a manageable scope. Adjust it to risk, complexity, legal/contractual requirements and available evidence.

Window	Focus	Deliverables and decision gate
Weeks 1–2	Sponsor and governance; context; obligations; climate relevance; scope; evidence workspace.	Approved scope and roles; interested-party/obligation register; record-handling rules; steering calendar.
Weeks 3–4	Services, processes, assets, data flows and suppliers; risk criteria and acceptance authority.	Verified inventories; approved assessment method; risk owners assigned; initial risk workshop complete.
Weeks 5–6	Assess risks; choose treatment; prepare SoA and funded implementation actions.	Risk register, reasoned SoA, treatment plan, residual-risk approvals within authority.
Weeks 7–9	Tailor and operate priority safeguards; train affected people; collect routine evidence.	Approved procedures; operating samples; control owners; exceptions and measures in use.
Weeks 10–11	Evaluate objectives and control performance; test backup/response; conduct internal audit.	Audit program and report; test results; nonconformities and corrective actions.
Week 12	Management review; resource decisions; residual risks; improvement priorities.	Minutes and decisions; owners/dates; revised risk, SoA and ISMS plan.

Use decision gates rather than document completion as the progress measure. A document marked approved is only one part of implementation; collect evidence of communication, training where required, actual operation, testing and review.

At each gate, ask: What changed since the last review? What evidence is missing? Which risk could exceed tolerance? Which dependencies need another owner? What funding or leadership decision is blocking progress? What must be retested after a change?

Turn review results into action

Use Modules 18–20 for internal audit, management review and corrective action. Audit independence and clear follow-up help prevent self-confirmation and paper-only compliance.

Activity	Prepare	Do	Close
Internal audit	Risk-based program; criteria and scope; impartial competent auditor; sample plan; access and confidentiality rules.	Interview, observe, inspect records, sample and reperform. Separate fact, requirement, evidence and conclusion.	Report findings and strengths; assign owner and due date; verify correction and effectiveness; retain working papers.
Management review	Input pack: prior actions, context changes, objectives, incidents, audit, risk, control performance, interested-party feedback, resources and improvement.	Top management discusses whether the ISMS remains suitable, adequate and effective; decides changes and resources.	Record decisions, actions, owners and dates. Track to completion and check changed evidence at next review.
Corrective action	Contain the issue; preserve facts and evidence; determine impact and any notification need.	Correct the immediate problem; analyze causes; check similar processes; plan action proportionate to risk.	Verify the action works in operation; update risk, SoA, procedure, training or scope where needed; close with evidence.

A useful finding states the criteria, condition, objective evidence, risk/impact and expected next decision. Do not promise a legal notification deadline from this template; route the event to the organization's legal/privacy adviser and follow the applicable jurisdiction and contract. Track any decision not to notify with its rationale and approval where appropriate.

Management-review minutes should not be a transcript. Record the information considered, the decision made, the authority, resources or changes approved, and how the effectiveness of previous decisions will be checked.

Worked example: a fictional 80-person services firm

This scenario shows how the artefacts connect. Replace every assumption with verified facts and approved local decisions.

Northstar Advisory is a fictional 80-person firm delivering consulting projects to customers in Singapore and two regional markets. Staff work in one office and remotely. Client documents are stored in a cloud collaboration service; a payroll provider and managed IT supplier support operations. The company has contracts with confidentiality and breach-cooperation clauses. It has a small IT team and no dedicated compliance department.

Work	How Northstar uses the package	Evidence path
Scope and context	The sponsor approves the consulting service boundary, office/remote work, personnel, cloud workspace, managed IT, payroll dependency and customer interfaces. It records the reasoned climate-relevance decision.	Scope statement; process map; interested-party and obligations register; supplier and data-flow records.
Risk and SoA	The team assesses account compromise, supplier outage, accidental disclosure, loss of a laptop and failed recovery. Owners select treatments, document applicable controls and justify exclusions.	Risk assessment; approvals; treatment plan; completed SoA with status and evidence pointers.
Control operation	The firm operates access approvals/reviews, staff awareness, supplier review, endpoint configuration, backup restore tests, incident escalation and secure deletion.	Sampled requests, review outputs, training checks, supplier records, configuration/patch extracts, restore results, incident exercise and disposal record.
Evaluation	The internal auditor samples two joiners, one leaver, one restore, one supplier change and one incident/tabletop record. It raises a finding when leaver removal cannot be evidenced.	Audit plan, sample selection, evidence IDs, finding, containment and cause analysis.
Improvement	The process owner adds an HR-to-IT leaver notification step, an owner and a target time. A later sample verifies revocation and review of exceptions.	Updated procedure, role briefing, system records, effectiveness test and management review decision.

WHAT MAKES THE EXAMPLE AUDITABLE

Each decision links to a real owner, a defined scope, an approved method, a dated record, a review result and—when needed—a corrective action. The toolkit prompts the work; Northstar's own records would prove it.

Your first two working sessions

Finish with named decisions, not a pile of unassigned forms.

Session 1 — Sponsor and scope (90 minutes)

- Confirm the service outcome, executive sponsor, ISMS owner and steering members.
- Draw the first boundary: business units, services, people, sites, systems, suppliers, data and interfaces.
- List requirements and source documents; assign an owner and date to verify each one.
- Record assumptions, exclusions and unanswered questions as actions, not as settled facts.
- Approve the secure workspace, evidence ID convention, access groups and records owner.

Session 2 — Risk method and evidence planning (90–120 minutes)

- Agree impact dimensions, likelihood definitions, scoring rules, thresholds and escalation authority.
- Walk through one realistic service scenario; challenge the impact, cause and existing safeguard evidence.
- Assign risk owners and schedule module workshops with process/control owners.
- Select the first operating samples to collect: access, supplier, backup, incident, change or other priority controls.
- Set the steering review date and define what evidence or approvals must be ready for it.

Use a consistent evidence folder pattern, for example `ISMS / 01 Governance / 2026 / M01 / approved-policy-id`. Keep an index with the authoritative link, owner, period, classification, retention, related risk/control and test result. Restrict access to personnel with a business need; do not use personal email or uncontrolled public links.

Before closing either meeting, read each open action aloud. Confirm its owner, due date, acceptance criteria and escalation route. The ISMS owner updates the decision and action registers within the agreed service level.

Use the kit responsibly

The documents are original KIS planning aids. They do not substitute for the licensed standard, qualified professional advice, legal review, or operating evidence.

- Verify exact requirements and control text against a licensed copy of ISO/IEC 27001:2022 and applicable amendments. The official ISO catalogue lists the 2022 edition and Amendment 1:2024 climate-action changes.
- Check applicable laws, regulations, customer and supplier contracts, privacy obligations, data-location and transfer rules, employment requirements, retention, breach notification and sector-specific duties for the actual facts.
- Do not treat the starter SoA as the organization's final control decision. Make risk-based choices, document reasons and obtain approvals from authorized owners.
- A policy is not proof that a control is implemented. Collect dated operating evidence, test it, record exceptions and re-test corrections.
- Do not put secrets, private keys, live credentials or unnecessary personal/customer data in the toolkit, workshop notes or audit pack. Apply access, minimization, retention and secure disposal rules.
- No document, module count or completed checklist guarantees conformity or certification. The organization is responsible for its system; a certification body makes any independent certification decision.

Official reference	Use
ISO/IEC 27001:2022 catalogue	Confirm the edition, status and available amendment information. https://www.iso.org/standard/27001.html
ISO/IEC 27001:2022/Amd 1:2024	Check the published climate-action amendment and the organization's context/party requirements. https://www.iso.org/standard/88435.html

ONE-PAGE COMPLETION TEST

Can the organization show an approved scope; repeatable risk assessments; an SoA with reasons and status; risk treatment approvals; assigned process owners; operating records; objective evaluation; impartial audit; management decisions; and corrective action verified for effectiveness? If not, record the gap, owner, due date and evidence required.

Prepared by KIS Practical Security Products | Free companion guide | v1.0.0 | 15 October 2026

KIS is not affiliated with or endorsed by ISO or IEC. All company names and scenarios in this guide are fictional. Product contents are defined by the release ZIP supplied with the all-in-one product.