VERITAS ASSURANCE



ISO 27001 Made Practical: A Handbook for Understanding and Awareness

Information Security Management Systems - Practical Explanations, Business Examples and Illustrative Evidence

Standard edition: ISO/IEC 27001:2022, including Amendment 1:2024
Handbook version: 1.0
Prepared by: Veritas Assurance

Contact Veritas Assurance

Contents

A clause-by-clause guide to the handbook

WELCOME FROM VERITAS ASSURANCE 3
ABOUT THIS HANDBOOK 3
UNDERSTANDING ISO/IEC 27001 4
CORE INFORMATION-SECURITY CONCEPTS 6
UNDERSTANDING THE STRUCTURE: HLS AND HS 7
THE PROCESS APPROACH AND PDCA 9
CLAUSES 1 TO 3: SCOPE, REFERENCES AND TERMINOLOGY 11
CLAUSE 4 BUSINESS CONTEXT, REQUIREMENTS AND ISMS BOUNDARIES 12
CLAUSE 5 LEADERSHIP AND INFORMATION-SECURITY ACCOUNTABILITY 13
CLAUSE 6 RISK ASSESSMENT, TREATMENT AND OBJECTIVES 14
ANNEX A CONNECTING RISKS WITH NECESSARY CONTROLS 15
CLAUSE 7 RESOURCES, COMPETENCE AND CONTROLLED INFORMATION 17
CLAUSE 8 OPERATING THE ISMS AND REVIEWING RISK 18
CLAUSE 9 MONITORING, MEASUREMENT AND EVALUATION 19
CLAUSE 9 INTERNAL AUDIT AND MANAGEMENT REVIEW 20
CLAUSE 10 CONTINUAL IMPROVEMENT AND CORRECTIVE ACTION 21
YOUR ROLE IN THE INFORMATION SECURITY MANAGEMENT SYSTEM 22
PUTTING THE SYSTEM TOGETHER: LAUNCHING A PAYROLL SERVICE 23
QUICK REFERENCE AND GLOSSARY 24
CLOSING MESSAGE FROM VERITAS ASSURANCE 25
FURTHER READING AND DOCUMENT INFORMATION 25
DISCLAIMER 25

Welcome from Veritas Assurance

Information security depends on everyday decisions: who can open a customer file, how a supplier receives information, whether a backup can be restored and what happens when someone changes roles.

This ISO 27001 handbook explains how those decisions fit within an Information Security Management System, or ISMS.

Veritas Assurance has prepared it for readers who want to understand the standard through recognisable business situations. The examples connect information ownership, risk assessment, selected controls and performance evaluation.

The aim is practical awareness: understanding what needs protection, recognising relevant risks and knowing how your work contributes to the system.

About This Handbook

This handbook is intended for business owners, managers, employees, information owners, IT personnel, supplier coordinators, information-security teams and internal auditors.

You can read it in sequence or refer directly to a relevant clause.

Each main clause includes:

- A short explanation of its purpose.
- Plain-language subclause summaries.
- A specific business situation.
- Illustrative implementation and evidence.
- A key takeaway.

The examples include digital information, paper records, people, premises and external services. Information security extends beyond cybersecurity and the responsibilities of an IT department.

All scenarios are hypothetical. Suggested controls, records and methods are illustrative rather than universally mandatory arrangements.

This is a global awareness resource. Applicable legal, regulatory and contractual requirements need separate consideration.

The handbook does not replace formal training, demonstrate technical competence or provide a qualification. Read the disclaimer at the end before using it.

The standard’s formal designation is ISO/IEC 27001. “ISO 27001” is used in the handbook title as a familiar shorthand.

The technical basis is ISO/IEC 27001:2022, together with its 2024 climate-action amendment.

Understanding ISO/IEC 27001

ISO/IEC 27001 is an internationally recognized standard for Information Security Management Systems (ISMS), designed to help organizations protect sensitive information and manage information security risks systematically. ISO/IEC 27001:2022 provides a structured framework for identifying information security threats, assessing vulnerabilities, implementing security controls, and protecting the confidentiality, integrity, and availability of information. The standard applies to organizations of all sizes and industries and supports the management of risks associated with cyber threats, data breaches, unauthorized access, and other information security challenges.

Implementing ISO/IEC 27001 helps organizations protect business information, strengthen cybersecurity practices, reduce security risks, and improve data protection processes. It promotes risk-based security management, regulatory compliance, employee awareness, incident response, and continual improvement of information security controls. By adopting ISO/IEC 27001:2022, organizations can enhance customer trust, protect valuable information assets, strengthen their reputation, support business continuity, and demonstrate their commitment to information security and data protection.

Its purpose includes preserving three information-security properties.

Property	Practical meaning	Business illustration
Confidentiality	Information is accessible only to authorised people or entities.	Customer payroll files are restricted to approved personnel.
Integrity	Information remains accurate and complete.	Changes to supplier bank details receive appropriate verification and approval.
Availability	Authorised users can obtain information and use associated services when needed.	Essential order information remains recoverable after a system disruption.

The importance of each property depends on the information and its use.

Implementation and certification

Subject	Practical meaning
Implementing an ISMS	Establishing and operating arrangements addressing applicable ISO/IEC 27001 requirements.
Certification	Independent assessment and a certification decision within an agreed scope.
Technical security testing	Evaluation of particular systems or controls; it can support the ISMS but does not replace it.
Legal compliance	Meeting applicable obligations; certification does not automatically establish compliance with every privacy or security law.
Security assurance	Evidence about defined arrangements; certification does not guarantee that incidents cannot occur.

ISO and IEC develop standards. Certification bodies conduct certification activities. The organisation remains responsible for its information, processes and security decisions.

Core Information-Security Concepts

The following concepts introduce the handbook. They are an explanatory framework, not a separate official list of ISO/IEC 27001 principles.

Concept	Practical meaning	Everyday illustration
Information ownership	Assign responsibility for decisions concerning information and its protection.	A finance manager approves access to payment records.
Risk-based decisions	Select responses according to relevant risks and requirements.	Sensitive customer files receive controls reflecting the consequences of disclosure.
Appropriate access	Give people access suited to their responsibilities.	A temporary worker receives access only to the records needed for the assignment.
Reliable information handling	Protect information during collection, use, sharing, storage and disposal.	A team uses an approved transfer method for confidential documents.
Supplier responsibility	Understand security dependencies and agreed responsibilities.	A business checks its responsibilities when using a hosted application.
Incident readiness	Establish how concerns are reported, assessed and handled.	An employee knows where to report an unexpected request for sensitive information.
Evaluation and learning	Check whether arrangements work and address weaknesses.	Restore exercises identify gaps that successful backup messages did not reveal.

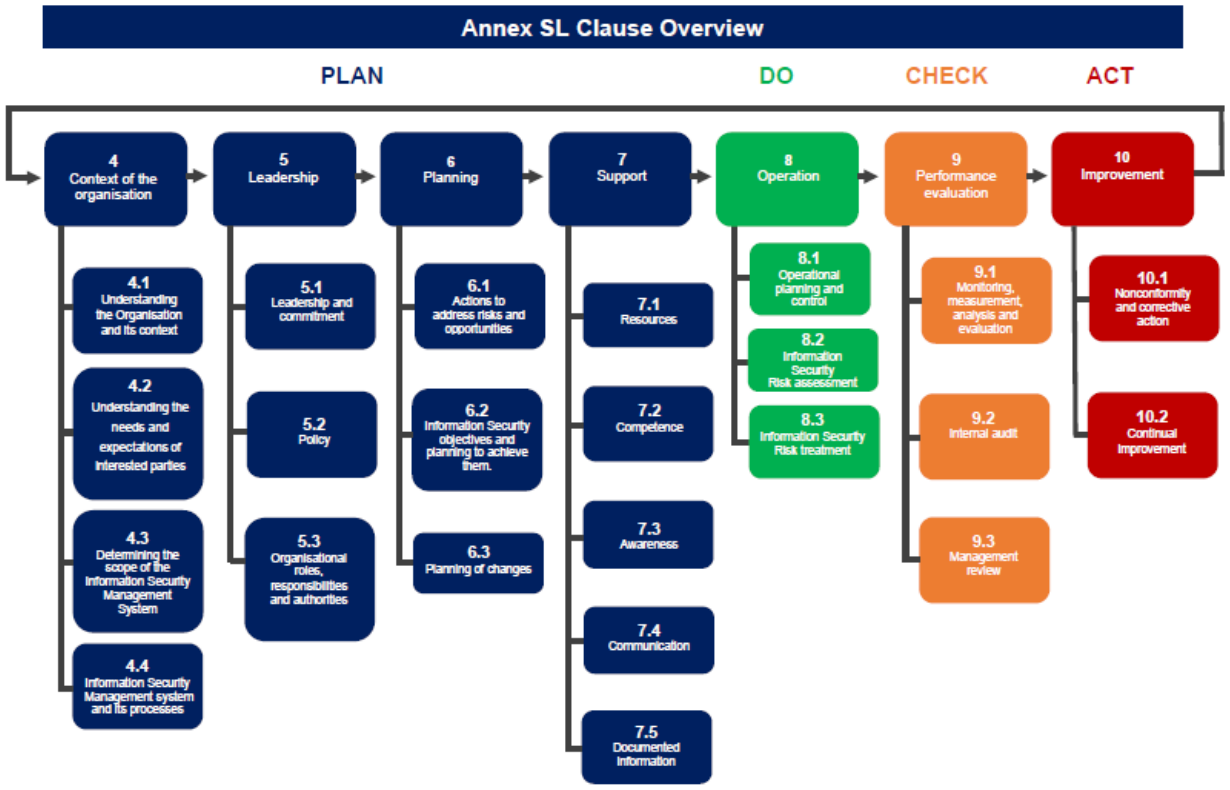
Key takeaway: Information security requires coordinated decisions across the organisation.

Understanding the Structure: HLS and HS

The High-Level Structure, or HLS, is the earlier term commonly associated with the shared management-system framework now generally described as the Harmonized Structure, or HS.

ISO/IEC 27001 uses the common structure while retaining its information-security requirements.

Clause	Main subject	Business question
1	Scope	What does the standard address?
2	Normative references	Which referenced publication supports its application?
3	Terms and definitions	What do the relevant terms mean?
4	Context	What affects the ISMS, and what does it cover?
5	Leadership	Who directs the system and takes responsibility?
6	Planning	Which risks, treatments and objectives need attention?
7	Support	What resources, competence and information are needed?
8	Operation	How are risk assessment, treatment and relevant processes operated?
9	Performance evaluation	How is effectiveness evaluated?
10	Improvement	How are weaknesses addressed and the system improved?



Where Annex A fits

Clauses 4 to 10 establish management-system requirements. Annex A provides a reference set of information-security controls used in the risk-treatment process.

Annex A does not replace the clauses. Completing a control checklist does not establish that the ISMS works.

Illustration of integration

A company may coordinate document control, management reviews and internal-audit planning across quality, environmental and information-security systems.

However, evaluating product conformity, environmental impacts and information-security risks requires different technical work.

Further information is available in ISO's management-system structure guidance.

The Process Approach and PDCA

The process approach

Information-security outcomes depend on connected activities.

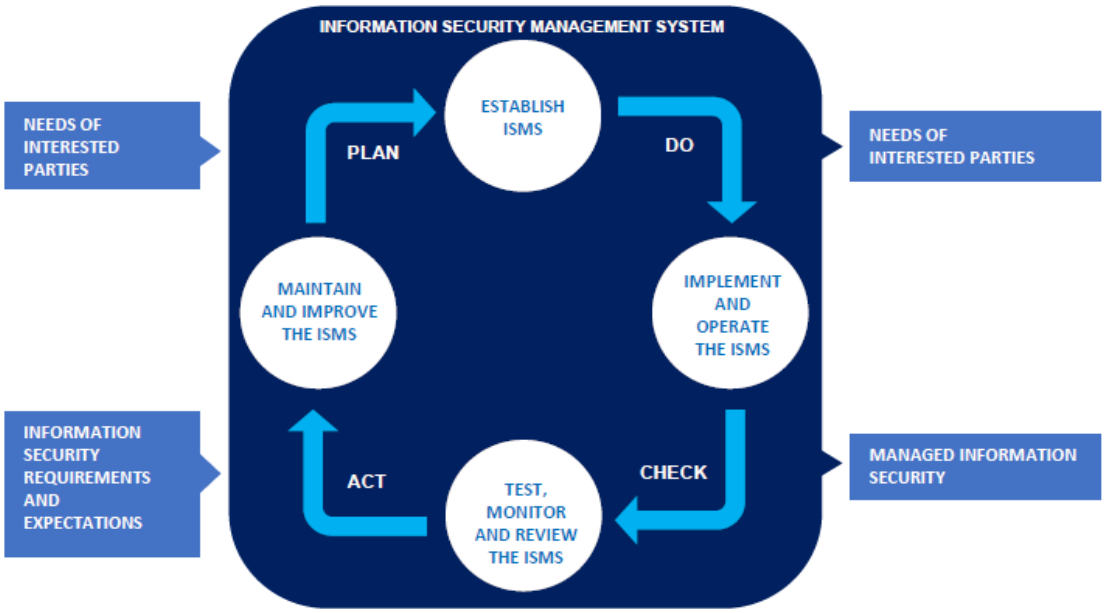
For example:

Customer requirement → information collection → access assignment → processing → approved sharing → retention or disposal

A secure application cannot address every risk if people routinely export information into an uncontrolled location.

For relevant processes, understand:

- What information is involved.
- Who owns the relevant decisions.
- Where information moves and is stored.
- Which requirements and risks apply.
- What controls are needed.
- How effectiveness will be evaluated.



The PDCA cycle

Plan–Do–Check–Act connects planning with implementation, evaluation and improvement.

Illustration: A recruitment company finds that candidate files are shared through inconsistent channels

Stage	What the organisation does	Possible evidence
Plan	Reviews information flows, access needs and disclosure risks, then establishes suitable sharing arrangements.	Risk assessment, responsibilities and a treatment plan.
Do	Implements the arrangements and explains them to relevant staff.	Configured controls, instructions and awareness activities.
Check	Samples actual sharing activity and reviews whether access remains appropriate.	Access-review results and handling checks.
Act	Addresses gaps and adjusts arrangements where necessary.	Corrective actions and subsequent evaluation.

Issuing an instruction is one action. Evaluation needs to establish whether people and systems follow it.

Key takeaway: Check the handling of real information, not only the existence of policies.

Clauses 1 to 3: Scope, References and Terminology

Clause 1 Scope

ISO/IEC 27001 addresses the establishment, operation, maintenance and continual improvement of an ISMS, including information-security risk assessment and treatment.

The organisation defines its ISMS boundaries while considering relevant dependencies and interfaces.

Requirements within Clauses 4–10 cannot be excluded when claiming conformity. Decisions about individual Annex A controls follow the risk-treatment and applicability process.

Example: A payroll provider scopes its payroll-processing service. It considers the people, applications, premises, information flows and external services supporting that service.

Clause 2 Normative references

ISO/IEC 27000 is the normative reference supporting the standard's information-security management terminology.

Consult the applicable authorised publication for the reference provisions.

ISO/IEC 27002 provides guidance on information-security controls. Its role differs from ISO/IEC 27001, which establishes ISMS requirements.

Clause 3 Terms and definitions

Term	Practical explanation	Illustration
Information asset	Information or a related resource that has value to the organisation.	Customer records and the application used to process them.
Threat	A potential cause of an unwanted security incident.	An attempt to obtain an employee's credentials.
Vulnerability	A weakness that could contribute to a security failure.	An account remaining active after its user leaves.
Risk owner	A person with responsibility and authority to manage a risk.	The manager accountable for risks affecting a business service.
Risk treatment	A selected response to an assessed risk.	Introducing suitable access controls and approval arrangements.
Residual risk	Risk remaining after treatment.	Remaining exposure after selected controls are implemented.
Statement of Applicability	A document recording necessary controls and relevant selection, implementation and exclusion information.	A controlled statement connecting controls with their justification and implementation status.

These are simplified explanations rather than formal definitions.

Clause 4 Business Context, Requirements and ISMS Boundaries

Why it matters

The ISMS should reflect the organisation's services, information, obligations and dependencies.

Illustrative business: An accounting firm processes client records using office systems and an external document platform.

Subclause	Meaning and specific application	Possible evidence
4.1 Organisational context	Understand relevant internal and external matters, including climate-change relevance. The firm considers remote working, supplier dependence and whether environmental disruption could affect information availability.	Context evaluation and resulting decisions.
4.2 Interested parties and requirements	Determine relevant parties, their requirements and which requirements the ISMS addresses. The firm reviews client commitments and applicable legal and regulatory requirements.	Reviewed requirements and assigned responsibilities.
4.3 ISMS scope	Define boundaries, interfaces and dependencies. The firm considers client processing, supporting personnel and its external platform.	Documented scope and relevant interface information.
4.4 ISMS processes	Establish and maintain connected processes. Client onboarding, access management, supplier review and incident handling receive coordinated responsibilities.	Process arrangements and implementation records.

For an already certified organisation adding services or locations, our ISO certification scope-extension guide explains the certification considerations.

Key takeaway: Scope should describe the business being protected and its important dependencies.

Clause 5 Leadership and Information-Security Accountability

Why it matters

Information-security decisions need business direction, resources and clear authority.

Illustrative business: A professional-services company discovers that departments use different arrangements for confidential client documents.

Subclause	Meaning and specific application	Possible evidence
5.1 Leadership commitment	Integrate information security into business management. Management assigns ownership and provides resources to address inconsistent handling.	Decisions, resource commitments and follow-up.
5.2 Information-security policy	Establish and communicate appropriate direction and commitments. The policy supports consistent decisions about protecting client information.	Approved policy and communication evidence.
5.3 Roles and authorities	Assign relevant responsibilities and reporting authority. Information owners approve business access, while technical personnel implement authorised changes.	Defined responsibilities and approval records.

Key takeaway: Technical personnel support security, but business owners also need to make and own decisions.

Clause 6 Risk Assessment, Treatment and Objectives

Why it matters

Planning connects security requirements and risks with justified decisions.

Illustrative business: A software company provides a customer order-management platform.

Subclause	Meaning and specific application	Possible evidence
6.1.1 Risks and opportunities generally	Determine matters affecting intended ISMS results. The company considers growth, service dependencies and weaknesses in security management.	Planning evaluations and actions.
6.1.2 Information-security risk assessment	Establish and apply suitable criteria and a consistent assessment process. The company evaluates unauthorised access, incorrect data changes and service interruption.	Assessment method, results and identified risk owners.
6.1.3 Information-security risk treatment	Select treatment options and necessary controls, compare them with Annex A and establish the required treatment information and approvals.	Treatment plan, Statement of Applicability and risk-owner approvals.
6.2 Information-security objectives	Establish suitable objectives and plans for achieving and evaluating them. The company sets an objective to improve timely removal of access after role changes.	Objectives, responsibilities, measures and progress results.
6.3 Planning changes	Carry out changes to the ISMS in a planned manner. The company reviews responsibilities and risk arrangements before expanding into another service.	Change planning and updated arrangements.

Illustrating a risk decision

Element	Example
Information or service	Customer order records.
Risk scenario	An inappropriate privileged account allows unauthorised changes.
Potential consequence	Incorrect orders, disrupted service and loss of customer confidence.
Possible treatment	Suitable access restrictions, approvals, reviews and monitoring.
Evaluation	Check that privileges remain justified and relevant changes are traceable.

The organisation determines its assessment method and criteria. ISO/IEC 27001 does not prescribe one universal scoring spreadsheet.

Key takeaway: Risk assessment should lead to treatment decisions, accountable owners and evaluation.

Annex A Connecting Risks with Necessary Controls

Annex A contains 93 reference controls grouped into four themes.

Theme	Number of controls	Illustrative application
Organisational	37	Define supplier responsibilities and information-handling arrangements.
People	8	Address awareness and responsibilities when people join, change roles or leave.
Physical	14	Control relevant access to premises and protect information in physical environments.
Technological	34	Apply suitable access, configuration, backup, logging and other technical arrangements.

The organisation determines necessary controls through risk treatment and relevant requirements. It then compares those controls with Annex A to check that necessary controls have not been overlooked.

Controls beyond Annex A may also be necessary. Organisations do not necessarily implement every Annex A control in the same way.

The Statement of Applicability

The Statement of Applicability, often shortened to SoA, records necessary controls, reasons for inclusion, implementation status and justification for excluded Annex A controls.

Applicability decision	Illustrative explanation
Why a control is necessary	It addresses an assessed risk or relevant requirement.
How implementation is represented	The statement accurately identifies whether the necessary control is implemented.
Why an Annex A control is excluded	The reason is justified against the organisation’s circumstances and requirements.
How decisions remain current	Changes in services, risks and obligations trigger appropriate review.

An “implemented” status needs support from actual operation. For example, a documented access-review arrangement should connect with completed reviews and action on inappropriate permissions.

For control guidance, consult ISO/IEC 27002.

Key takeaway: Annex A supports a reasoned treatment process; it does not replace understanding risk.

Clause 7 Resources, Competence and Controlled Information

Why it matters

People need suitable resources, understanding and reliable information to perform their security responsibilities.

Illustrative business: An architecture company shares project drawings with external partners.

Subclause	Meaning and specific application	Possible evidence
7.1 Resources	Provide resources needed for the ISMS. Management evaluates secure collaboration facilities, administration and review capacity.	Resource decisions and implemented arrangements.
7.2 Competence	Determine competence needs and evaluate actions taken. Administrators demonstrate responsibilities relevant to controlling partner access.	Competence evaluations and supporting records.
7.3 Awareness	Explain relevant policy, individual contributions and consequences of nonconformity. Project staff understand approved sharing arrangements.	Staff understanding and awareness activities.
7.4 Communication	Determine relevant internal and external communications. Staff know who handles security-related client enquiries and supplier notifications.	Communication responsibilities and correspondence.
7.5.1 Necessary documented information	Establish information required by the standard and needed for an effective system.	Relevant methods, plans and records.
7.5.2 Creating and updating information	Identify, review and approve information appropriately. A revised sharing instruction is checked before issue.	Approval and revision information.
7.5.3 Information control	Manage availability, protection, access, changes and retention. Staff can obtain current instructions while sensitive security records remain protected.	Access arrangements and controlled records.

Key takeaway: Awareness explains responsibilities; competence demonstrates the ability to perform them.

Clause 8 Operating the ISMS and Reviewing Risk

Why it matters

The organisation needs to operate its planned arrangements and revisit risk when circumstances change.

Illustrative business: A legal-services company moves case documents into a hosted collaboration service.

Subclause	Meaning and specific application	Possible evidence
8.1 Operational planning and control	Operate and control processes needed to meet ISMS requirements and implement planned actions. The company establishes migration, supplier and access arrangements.	Operating criteria, supplier requirements and completed checks.
8.2 Information-security risk assessment	Reassess risks at planned intervals and when significant changes are proposed or occur. The new service's access, availability and information-handling dependencies are evaluated.	Updated assessment results.
8.3 Information-security risk treatment	Implement the treatment plan and retain relevant results. Required configuration, approval and review arrangements are put into operation.	Treatment implementation and evaluation records.

Illustrating operation

Planned arrangement	What evidence could show
Approved access groups.	Actual permissions reflect approved responsibilities.
Defined supplier responsibilities.	Agreements and operating arrangements address relevant interfaces.
Recovery arrangements.	Relevant recovery activities have been evaluated.
Partner-access review.	Access is reviewed when a matter closes or responsibilities change.

Buying a service does not automatically establish that the organisation's own responsibilities have been addressed.

Key takeaway: Operating evidence should connect the assessment, treatment decision and actual control.

Clause 9 Monitoring, Measurement and Evaluation

Why it matters

The organisation needs to establish whether its security arrangements achieve their intended results.

Illustrative business: A managed-services provider reviews access management and recovery capability.

Subclause	Meaning and specific application	Possible evidence
9.1 Performance evaluation	Determine what to monitor, appropriate methods, responsibilities and timing, then evaluate results. The provider examines access-review quality and selected recovery outcomes.	Defined measures, analysis and conclusions.

Illustrating useful evaluation

Information collected	Question it helps answer
Access reviews completed.	Were permissions checked and inappropriate access resolved?
Backup jobs reported as successful.	Can required information be recovered under relevant conditions?
Security concerns reported.	Are reports assessed and followed through appropriately?
Treatment actions closed.	Did the actions achieve the intended risk response?

Activity counts can help, but they need interpretation. A high completion rate can conceal weak reviews or unresolved findings.

Key takeaway: Completing an activity and achieving its intended result are different questions.

Clause 9 Internal Audit and Management Review

Internal audits examine conformity and effective implementation. Management review considers the continuing suitability, adequacy and effectiveness of the ISMS.

Subclause	Meaning and specific application	Possible evidence
9.2.1 Internal-audit purpose	Evaluate the ISMS against applicable criteria. An auditor follows selected access changes from business approval through implementation.	Objective evidence and audit conclusions.
9.2.2 Audit programme	Establish suitable planning, scope, criteria, objectivity, reporting and follow-up. Important changes and previous results influence coverage.	Programme, reports and follow-up results.
9.3.1 Management review generally	Review the ISMS at planned intervals. Management considers whether it remains suitable for the services provided.	Review evidence.
9.3.2 Review inputs	Consider required information, including relevant changes, feedback, performance, risk assessment and treatment status.	Relevant review inputs.
9.3.3 Review results	Establish decisions concerning improvement and necessary ISMS changes. Management assigns resources to unresolved security needs.	Decisions, responsibilities and follow-up.

Key takeaway: Evaluation should influence business decisions rather than end with a completed report.

Clause 10 Continual Improvement and Corrective Action

Why it matters

The organisation needs to address failures, understand their causes and improve the system using evidence.

Illustrative business: A company's established supplier-review process requires security approval before renewing certain service agreements. A renewal proceeds without that approval.

The missed approval is a failure against the organisation's own arrangement. The company evaluates the consequences rather than assuming that a security incident has occurred.

Subclause	Meaning and specific application	Possible evidence
10.1 Continual improvement	Improve ISMS suitability, adequacy and effectiveness. The company strengthens the connection between supplier management and procurement.	Improvement decisions and evaluated results.
10.2 Response and correction	Address the nonconformity and relevant consequences. Responsible personnel complete the missed evaluation and determine whether further action is needed.	Nonconformity, review results and response records.
10.2 Cause evaluation and action	Determine why the failure occurred and whether similar issues exist. Investigation finds that renewal can proceed without the required security input.	Cause evaluation and implemented workflow changes.
10.2 Effectiveness and evidence	Check whether action worked and retain relevant information. Subsequent renewals are sampled to confirm that required reviews occur before approval.	Follow-up results and traceable records.

Completing the missed review corrects the immediate gap. Addressing the workflow weakness supports prevention of recurrence.

For further guidance, read managing nonconformities in ISO management systems.

Key takeaway: Corrective action should connect the cause, implemented change and effectiveness result.

Your Role in the Information Security Management System

Role	Practical contribution
Top management	Set direction, provide resources and evaluate effectiveness.
Information owners	Make relevant decisions about information access, handling and protection.
Risk owners	Take responsibility for assigned risks and relevant treatment decisions.
Managers	Apply security responsibilities within business processes.
Employees	Follow relevant arrangements and report concerns promptly.
IT and security personnel	Implement and evaluate assigned technical and security responsibilities.
Human resources	Coordinate relevant joining, role-change and leaving arrangements.
Purchasing and supplier coordinators	Address security requirements and external dependencies.
Facilities personnel	Support relevant physical and environmental protections.
Internal auditors	Evaluate evidence objectively and communicate conclusions.

Smaller organisations may combine roles. Responsibilities and decision authority should remain clear.

Putting the System Together: Launching a Payroll Service

A business-services company introduces a payroll-processing service for external customers.

Stage	What the company does	Relevant connection
Understand the service	Identifies information flows, customers, supporting systems and relevant obligations.	Clause 4: Context and scope.
Assign accountability	Establishes information, risk and process responsibilities.	Clause 5: Leadership.
Assess risk	Evaluates disclosure, incorrect processing and service-interruption scenarios.	Clause 6: Risk assessment.
Select treatment	Determines necessary controls, reviews Annex A and documents applicability decisions.	Clause 6: Treatment.
Provide support	Establishes competence, communication and controlled information.	Clause 7: Support.
Operate arrangements	Applies approved access, supplier and processing controls.	Clause 8: Operation.
Evaluate results	Reviews relevant monitoring, audits and risk information.	Clause 9: Evaluation.
Improve	Addresses weaknesses and checks whether changes achieve their intended result.	Clause 10: Improvement.

The service may depend on people, premises, applications and suppliers. The ISMS needs to address those connections.

Organisations preparing for independent assessment can also consult our ISO certification audit-preparation checklist.

Quick Reference and Glossary

Expression	Meaning in this handbook
ISMS	Information Security Management System.
Confidentiality	Protection against unauthorised access or disclosure.
Integrity	Protection of information accuracy and completeness.
Availability	Accessibility and usability when required by authorised users.
Control	An arrangement that maintains or modifies risk.
Risk acceptance	An informed decision to retain a risk under applicable criteria.
Residual risk	Risk remaining after treatment.
SoA	Statement of Applicability.
Security event	An occurrence requiring evaluation because it may indicate a security issue.
Corrective action	Action addressing a nonconformity's cause to prevent recurrence.

Clause reminder

4: Understand → 5: Lead → 6: Plan → 7: Support → 8: Operate → 9: Evaluate → 10: Improve

These activities interact continuously.

Closing Message from Veritas Assurance

A useful ISMS connects information-security decisions with the way the organisation works.

Use this handbook to discuss ownership, risk, responsibilities and evidence. Adapt the examples to your information, services, people and obligations.

Consult the authorised standard for the complete requirements.

To discuss independent certification assessment, contact Veritas Assurance with your activities, operating locations, proposed ISMS scope and relevant external dependencies.

Further Reading and Document Information

- ISO/IEC 27001 Official standard information
- ISO/IEC 27001:2022 / Amd 1:2024 Climate-action changes
- ISO/IEC 27002 Information-security control guidance
- ISO Management-system standards

Document purpose: Understanding and awareness.
Technical basis: ISO/IEC 27001:2022, including Amendment 1:2024.
Examples: Hypothetical and illustrative; no universal legal conditions, configurations or mandatory templates are implied.

Disclaimer

This handbook is independently prepared by Veritas Assurance for general understanding and awareness of ISO/IEC 27001. It is not an ISO or IEC publication, an official interpretation or a substitute for the authorised standard.

Clause and control descriptions are explanatory summaries and do not cover every requirement. Consult the applicable authorised publications when establishing requirements or evaluating conformity. ISO and IEC publications remain subject to their respective copyright protections.

All scenarios, evidence examples and suggested methods are hypothetical and illustrative. Their suitability depends on the organisation’s information, activities, services, risks, responsibilities and applicable requirements.

This handbook does not provide system-specific security architecture, incident-response instructions or legal advice. Obtain appropriate expertise before implementing technical or legal decisions.

Using this handbook does not establish conformity, guarantee certification, demonstrate complete legal compliance or guarantee protection from security incidents. Certification decisions depend on applicable assessment, review and decision arrangements.