PACIFIC CERTIFICATIONS

ISO/IEC 27001:2022

INFORMATION SECURITY MANAGEMENT SYSTEM

Implementation Guide

Practical implementation resource

A clause-by-clause guide to establishing, operating and preparing an Information Security Management System (ISMS) for independent certification assessment.

Includes ISO/IEC 27001:2022/Amd 1:2024 climate-action considerations

Edition 1 | 2026

How to Use This Guide

This guide provides practical, educational guidance for organizations establishing an Information Security Management System. It is not a replacement for the official standard and should be used together with a licensed copy of ISO/IEC 27001:2022 and relevant guidance standards.

Impartiality statement

Pacific Certifications provides independent assessment and certification services. As a certification body, Pacific Certifications does not design, implement or operate a client's ISMS. Organizations may implement internally or engage an independent consultant.

Recommended reading sequence

1. Understand the purpose, scope and expected outcomes of an ISMS.
2. Complete an initial gap analysis against Clauses 4-10 and Annex A.
3. Define the implementation plan, responsibilities, resources and milestones.
4. Build and operate the ISMS using risk-based decisions.
5. Verify effectiveness through monitoring, internal assessment and management review.
6. Address findings and prepare for the certification process.

Contents at a glance

Section	Coverage
1	ISO/IEC 27001 fundamentals and business case
2	Implementation roadmap and governance
3	Clauses 4-10 implementation guidance
4	Information security risk assessment and treatment
5	Annex A control themes and Statement of Applicability
6	Operational evidence, internal assessment and management review
7	Certification readiness, checklists and 90-day plan

1. Understanding ISO/IEC 27001:2022

ISO/IEC 27001 specifies requirements for establishing, implementing, maintaining and continually improving an Information Security Management System. The ISMS protects information through a coordinated system of governance, risk management, operational controls, monitoring and improvement.

Core security objectives

Objective	Practical meaning
Confidentiality	Information is accessible only to authorized persons, systems or processes.
Integrity	Information remains accurate, complete and protected from unauthorized modification.
Availability	Information and supporting services are accessible when required by authorized users.

What the standard expects

- An ISMS aligned with organizational purpose and strategic direction.
- A defined scope covering relevant business activities, information, technologies, locations and dependencies.
- A repeatable risk assessment and risk treatment process.
- Selection and justification of controls, recorded in a Statement of Applicability.
- Clear leadership accountability, resources, competence and communication.
- Evidence that controls and processes operate effectively and improve over time.

> **Important distinction**
> ISO/IEC 27001 certifies the management system. It does not guarantee that an organization will never experience a cyber incident, data breach or service disruption.

2. Benefits of an Effective ISMS

Benefit	Expected organizational value
Risk visibility	A consistent view of threats, vulnerabilities, impacts, ownership and treatment priorities.
Customer confidence	Structured assurance that information security risks are governed and monitored.
Contract readiness	Stronger responses to security questionnaires, tenders and supply-chain requirements.
Regulatory alignment	A framework for identifying and managing legal, regulatory and contractual obligations.
Incident resilience	Defined detection, response, communication, recovery and learning processes.
Operational consistency	Documented responsibilities, access controls, change controls and security practices.
Continual improvement	Performance data and corrective action support better security decisions over time.

Common implementation mistakes

- Treating ISO/IEC 27001 as an IT-only project rather than an organization-wide management system.
- Selecting Annex A controls before understanding risk.
- Creating excessive documents that are not used in daily operations.
- Defining a scope that excludes important dependencies, people or systems.
- Relying on policies without evidence of implementation and effectiveness.
- Failing to connect security objectives with measurable business outcomes.

3. ISMS Implementation Roadmap

Phase	Key activities	Typical outputs
1. Initiate	Confirm sponsorship, purpose, scope concept and resources.	Project charter; governance structure; implementation plan.
2. Understand	Analyze context, interested parties, obligations, assets and processes.	Context register; interested-party register; preliminary scope.
3. Assess risk	Define criteria; identify, analyze and evaluate risks.	Risk methodology; risk register; risk owners.
4. Treat risk	Select treatments and controls; obtain owner approvals.	Risk treatment plan; Statement of Applicability.
5. Implement	Develop required processes, controls, training and records.	Policies; procedures; technical and organizational evidence.
6. Operate	Run controls and collect performance data.	Logs; reviews; incidents; supplier records; training evidence.
7. Verify	Conduct internal assessment and management review.	Assessment report; management review minutes; action plan.
8. Improve	Correct nonconformities and strengthen effectiveness.	Corrective actions; updated risks; improved controls.
9. Certify	Complete Stage 1 and Stage 2 certification assessments.	Certification decision and ongoing surveillance program.

Timeline note

Implementation duration varies according to organizational size, scope, complexity, regulatory obligations, current maturity and resource availability. A fixed timeline should not be assumed.

4. Context of the Organization - Clause 4

4.1 Internal and external issues

Identify issues that can affect the ISMS and its intended outcomes. Consider business strategy, technology architecture, threat environment, workforce model, outsourcing, customer commitments, legal change and organizational culture. The organization must also determine whether climate change is a relevant issue.

Internal issues	External issues
Business objectives, governance and risk appetite	Cyber threat landscape and geopolitical conditions
Legacy systems and technical debt	Laws, regulations and contractual obligations
Skills, staffing and security culture	Cloud, data-center and critical supplier dependencies
Mergers, acquisitions and restructuring	Customer expectations and market requirements
Remote work and physical locations	Climate-related disruptions affecting facilities, utilities or suppliers

4.2 Interested parties and requirements

- Customers and data subjects
- Regulators and law-enforcement authorities
- Employees, contractors and temporary workers
- Shareholders, owners and governing bodies
- Cloud providers, processors, suppliers and business partners
- Insurers, banks and other assurance stakeholders

4.3 Defining the ISMS scope

The scope must be maintained as documented information and clearly identify boundaries and applicability. Include organizational units, locations, products and services, business processes, information assets, technologies, interfaces and dependencies. Any exclusion must not undermine the organization’s ability to achieve intended ISMS outcomes.

4.4 Establishing the ISMS

Define the processes needed for the ISMS, their interactions, responsibilities, criteria, resources, monitoring and improvement arrangements. Integrate the ISMS into existing business processes wherever practical.

5. Leadership - Clause 5

5.1 Leadership and commitment

- Ensure the information security policy and objectives align with strategic direction.
- Integrate ISMS requirements into business processes and decision-making.
- Provide adequate people, technology, time and financial resources.
- Promote risk-based thinking and effective information security management.
- Support relevant roles and hold management accountable for results.
- Review whether the ISMS achieves its intended outcomes.

5.2 Information security policy

The policy should be appropriate to the organization, provide a framework for objectives and include commitments to satisfy applicable requirements and continually improve the ISMS. It must be documented, communicated, understood and available to relevant interested parties as appropriate.

5.3 Roles, responsibilities and authorities

Role	Typical accountability
Top management	Direction, resources, policy approval and overall ISMS accountability.
ISMS manager / coordinator	Coordinate the system, reporting, reviews and improvement activities.
Risk owners	Approve risk ratings, treatments and residual risk decisions.
Control owners	Implement, operate, monitor and improve assigned controls.
Asset owners	Classify information and define handling and access requirements.
All personnel	Follow security requirements and report events, weaknesses and incidents.

Evidence examples

Approved policy, governance terms of reference, role descriptions, delegated authorities, management communications, budget decisions and leadership review records.

6. Planning - Clause 6

6.1 Risks and opportunities

Plan actions to address both information security risks and broader ISMS risks and opportunities. Information security risk assessment and treatment requirements are detailed in Clauses 6.1.2 and 6.1.3.

6.2 Information security objectives

Objective example	Measure	Owner	Target
Improve timely access reviews	Percentage completed by due date	IT Operations	>= 98% quarterly
Reduce phishing susceptibility	Simulation failure rate	Security Manager	< 5%
Improve incident response	Mean time to contain priority incidents	Incident Manager	< 4 hours
Strengthen supplier assurance	Critical suppliers reviewed	Procurement	100% annually

6.3 Planning changes

Changes to the ISMS must be planned. Consider purpose, consequences, integrity of the system, resources, responsibilities, dependencies and communication. Relevant changes include new technology, cloud migrations, acquisitions, office moves, outsourced processes and significant regulatory changes.

Planning principle
Objectives should be measurable where practicable, monitored, communicated, updated and supported by defined actions, owners, resources, deadlines and evaluation methods.

7. Information Security Risk Assessment

Define the methodology first

- Risk identification method and risk scenarios.
- Likelihood and consequence scales.
- Risk calculation or evaluation method.
- Risk acceptance criteria and authority levels.
- Rules for consistency, repeatability and comparability.
- Frequency and triggers for reassessment.

Recommended risk workflow

7. Identify information, services, systems, people, facilities and third-party dependencies.
8. Identify credible threat events and vulnerabilities or weaknesses.
9. Describe potential consequences for confidentiality, integrity, availability and other business objectives.
10. Assess likelihood and impact using approved criteria.
11. Determine inherent risk and assign a risk owner.
12. Evaluate against acceptance criteria and prioritize treatment.
13. Reassess residual risk after treatment and obtain approval.

Field	Example
Risk scenario	Unauthorized access to customer records through compromised privileged credentials.
Asset/process	Customer relationship management platform.
Potential impact	Confidentiality breach, regulatory notification, service disruption and reputational damage.
Existing controls	MFA, privileged access management, logging and access reviews.
Treatment	Strengthen session monitoring and reduce standing privileges.
Residual risk decision	Accepted by designated risk owner subject to quarterly monitoring.

8. Risk Treatment and the Statement of Applicability

Risk treatment options

Option	Meaning
Modify	Implement or strengthen controls to reduce likelihood or impact.
Avoid	Stop or change the activity creating the risk.
Share	Transfer or share elements through insurance, contracts or service arrangements.
Retain	Accept the risk with informed authorization and monitoring.

Statement of Applicability (SoA)

The SoA is a central ISMS document. It records necessary controls, the justification for inclusion, whether each control is implemented and justification for any Annex A control considered unnecessary. Controls may also come from laws, contracts, industry frameworks or the organization's own requirements.

SoA field	What to record
Control reference	Annex A or other control identifier.
Control title	Clear name consistent with the source framework.
Applicability	Applicable / not applicable.
Justification	Risk, legal, contractual, business or other reason.
Implementation status	Implemented, partially implemented or planned.
Evidence / owner	Responsible owner and principal evidence sources.

Key rule

Annex A is a reference set for comparison. Control selection must be driven by the organization's risk treatment needs and applicable requirements, not by automatically implementing every control.

9. Support - Clause 7

7.1 Resources

Determine resources required to establish, operate, monitor and improve the ISMS. Consider security personnel, system administrators, independent assessors, tools, logging capacity, training, testing and supplier assurance.

7.2 Competence and 7.3 Awareness

- Define competence requirements for security-relevant roles.
- Verify qualifications, experience and practical capability.
- Maintain evidence of training and competence evaluation.
- Ensure personnel understand the policy, their contribution and consequences of nonconformity.
- Provide role-specific training for administrators, developers, incident responders, procurement and management.

7.4 Communication

Communication	Audience	Trigger/frequency	Owner
Security awareness	All personnel	On joining and periodically	HR / Security
Incident escalation	Response team and management	On defined severity thresholds	Incident Manager
Customer notification	Affected customers	Contractual or legal trigger	Legal / Account Owner
Supplier requirements	Relevant providers	Contracting and review cycle	Procurement

7.5 Documented information

Control creation, review, approval, versioning, access, distribution, storage, retention and disposition. Protect sensitive ISMS records from unauthorized access, alteration or loss. Documents may be digital, paper, workflow records, tickets, dashboards, diagrams or other controlled formats.

10. Operation - Clause 8

8.1 Operational planning and control

Plan, implement and control the processes needed to meet information security requirements and carry out risk treatment. Establish criteria, operate processes under controlled conditions and retain evidence that activities were performed as planned.

Operational controls commonly expected

- Identity and access management, including joiner-mover-leaver processes.
- Secure configuration, vulnerability management, patching and change control.
- Backup, restoration testing, resilience and continuity arrangements.
- Logging, monitoring and detection of security events.
- Secure development and application change practices.
- Supplier onboarding, contractual security requirements and monitoring.
- Information classification, handling, retention and secure disposal.
- Physical security, visitor management and environmental safeguards.

8.2 and 8.3 Risk assessment and treatment in operation

Perform risk assessments at planned intervals and when significant changes occur. Implement the approved risk treatment plan and retain results. Reassess risks after incidents, major changes, new vulnerabilities, supplier changes or shifts in legal and threat conditions.

Outsourced processes

Outsourcing does not transfer accountability. The organization must define, communicate and monitor security requirements for externally provided processes, products and services.

11. Annex A Control Themes

ISO/IEC 27001:2022 Annex A contains 93 controls grouped into four themes. These controls align with ISO/IEC 27002:2022 guidance and provide a reference set for risk treatment comparison.

Theme	Controls	Implementation focus
A.5 Organizational	37	Policies, governance, roles, threat intelligence, suppliers, incidents, continuity, legal and compliance.
A.6 People	8	Screening, terms of employment, awareness, remote work, disciplinary processes and confidentiality.
A.7 Physical	14	Perimeters, entry, secure areas, equipment protection, media, utilities and disposal.
A.8 Technological	34	Endpoints, access, authentication, malware, vulnerabilities, backup, logging, networks, development and cryptography.

Control implementation test

- Is the control justified by risk or another requirement?
- Is there a named owner with authority and resources?
- Is the control integrated into operational workflows?
- Is there reliable evidence that it operates?
- Is performance monitored and reviewed?
- Are exceptions approved, time-bound and risk-assessed?
- Has effectiveness been evaluated after changes or incidents?

12. Selected Annex A Implementation Guidance

Control area	Practical implementation evidence
Information security policies	Approved policy set, review schedule, communication and acknowledgements.
Threat intelligence	Defined sources, relevance criteria, analysis records and action tracking.
Cloud services	Due diligence, shared-responsibility mapping, configuration baselines, exit and data-return arrangements.
Identity management	Unique identities, lifecycle workflows, privileged accounts, periodic reviews and segregation.
Vulnerability management	Asset coverage, scanning, triage, remediation SLAs, exceptions and verification.
Logging and monitoring	Log source inventory, retention, alert rules, escalation, review and time synchronization.
Secure development	Security requirements, code review, testing, dependency controls and environment separation.
Incident management	Classification, roles, response plans, evidence preservation, communication and lessons learned.
ICT readiness for continuity	Recovery objectives, resilient architecture, backups, testing and improvement.
Supplier security	Risk tiering, contractual clauses, performance review, change notification and termination controls.

13. Performance Evaluation - Clause 9

9.1 Monitoring, measurement, analysis and evaluation

Measure	Possible indicator
Access control	Overdue access reviews; orphaned accounts; privileged account usage.
Vulnerability management	Critical vulnerabilities past SLA; mean remediation time; coverage.
Security awareness	Completion rate; simulation outcomes; repeat failures.
Incident management	Incident volume by severity; time to detect, contain and recover.
Supplier assurance	Critical supplier review completion; unresolved high-risk findings.
Continuity	Backup success; restoration test success; recovery exercise results.
Risk treatment	Overdue actions; residual risks above appetite; treatment effectiveness.

9.2 Internal assessment

Conduct internal assessments at planned intervals to determine whether the ISMS conforms to organizational and ISO/IEC 27001 requirements and is effectively implemented and maintained. Assessors should be objective and impartial and should not assess their own work where this would compromise independence.

9.3 Management review

- Status of previous review actions.
- Changes in context and interested-party requirements.
- Security performance, trends and objective achievement.
- Nonconformities, corrective actions and assessment results.
- Risk assessment results and risk treatment progress.
- Resource adequacy and opportunities for improvement.

14. Improvement - Clause 10

10.1 Continual improvement

Continually improve the suitability, adequacy and effectiveness of the ISMS. Improvement may result from performance trends, incidents, testing, technological change, stakeholder feedback, internal assessments and management review.

10.2 Nonconformity and corrective action

14. React to the nonconformity and control or correct it.
15. Address consequences and protect affected information or services.
16. Determine the root cause and whether similar issues exist elsewhere.
17. Implement proportionate corrective action.
18. Review whether the action was effective.
19. Update risks, controls and documented information where necessary.

Record	Minimum content
Issue description	What requirement was not fulfilled and objective evidence.
Immediate correction	Action taken to contain or correct the issue.
Cause analysis	Why the issue occurred, including systemic factors.
Corrective action	Action designed to prevent recurrence.
Owner and deadline	Accountability and due date.
Effectiveness review	Evidence that recurrence risk was reduced.

15. Required and Common Documented Information

Category	Typical documents and records
Required core documents	ISMS scope; information security policy; risk assessment process; risk treatment process; objectives; Statement of Applicability; risk treatment plan.
Required evidence	Risk assessment results; risk treatment results; competence evidence; monitoring results; internal assessment program and results; management review results; corrective actions.
Common governance documents	ISMS manual or process map; roles matrix; legal and contractual register; asset ownership rules; exception process.
Common operational documents	Access control, incident response, backup, vulnerability, supplier, change, secure development, classification and continuity procedures.
Common records	Access reviews; vulnerability reports; incident tickets; backup tests; supplier reviews; training records; change approvals; recovery exercises.

Documentation principle

Document only what is necessary for effective control, consistency and evidence. A concise process that personnel use is stronger than a large document set disconnected from operations.

16. Certification Readiness Checklist

Readiness area	Confirmation criteria	Status
Scope and context	Scope is clear; internal/external issues, interested parties and requirements are current.	☐ Ready ☐ Action
Leadership	Policy, responsibilities, resources and leadership involvement are evident.	☐ Ready ☐ Action
Risk management	Methodology is repeatable; risks have owners; treatment and residual-risk decisions are approved.	☐ Ready ☐ Action
Statement of Applicability	All necessary controls are identified, justified and status is accurate.	☐ Ready ☐ Action
Objectives	Objectives are measurable, monitored and linked to business needs.	☐ Ready ☐ Action
Operational controls	Controls operate consistently and have sufficient evidence.	☐ Ready ☐ Action
Competence and awareness	Role competence and awareness activities are recorded and evaluated.	☐ Ready ☐ Action
Monitoring	Relevant security and ISMS performance indicators are reviewed.	☐ Ready ☐ Action
Internal assessment	Full scope and applicable requirements have been assessed objectively.	☐ Ready ☐ Action
Management review	Required inputs and decisions are documented.	☐ Ready ☐ Action
Corrective action	Issues have root-cause analysis, action and effectiveness verification.	☐ Ready ☐ Action
Readiness	No unresolved critical gaps prevent the ISMS from achieving intended outcomes.	☐ Ready ☐ Action

17. Typical Certification Process

Stage	Purpose
Application and scope confirmation	Confirm organization profile, scope, sites, workforce, activities and certification requirements.
Assessment planning	Determine duration, competence, sampling and delivery arrangements.
Stage 1 assessment	Review ISMS design, scope, documented information, readiness and planning for Stage 2.
Stage 1 follow-up	Address identified concerns and confirm readiness.
Stage 2 assessment	Evaluate implementation, effectiveness and evidence across the defined scope.
Corrective action review	Review actions for any nonconformities identified.
Independent certification decision	Authorized personnel review assessment evidence and make the certification decision.
Surveillance assessments	Periodic assessments verify continued conformity and effectiveness.
Recertification	A comprehensive reassessment is completed before the certification cycle ends.

Certification-body independence

Pacific Certifications evaluates conformity and effectiveness as an independent certification body. Certification cannot be guaranteed in advance and remains subject to successful completion of the required assessment and certification decision processes.

18. Practical 90-Day Implementation Planner

Period	Priority activities	Outputs
Days 1-15	Appoint sponsor and team; define project plan; conduct initial gap review; develop scope concept.	Project plan; governance; gap report; draft scope.
Days 16-30	Analyze context, interested parties, obligations, information and dependencies; approve policy.	Context and requirements registers; policy; scope.
Days 31-45	Approve risk methodology; conduct risk assessment; assign risk owners.	Risk criteria and risk register.
Days 46-60	Develop risk treatment plan and SoA; confirm control owners; prioritize critical gaps.	Treatment plan; SoA; implementation actions.
Days 61-75	Implement priority controls; deliver awareness; establish monitoring and evidence collection.	Operational procedures, training and records.
Days 76-85	Operate and test controls; complete internal assessment; address immediate findings.	Assessment report and corrective actions.
Days 86-90	Conduct management review; confirm readiness and remaining actions.	Management review record; readiness plan.

This planner is illustrative. Organizations should adjust sequencing and duration based on their risk profile, maturity, scope and available resources.

19. Frequently Asked Questions

Is ISO/IEC 27001 only for technology companies?

No. Any organization that depends on information can implement an ISMS, regardless of sector or size.

Must every Annex A control be implemented?

No. Controls are selected based on risk treatment and applicable requirements. The SoA must justify applicability and exclusions.

Is a specific risk assessment method required?

No. The method must be defined, consistent, repeatable and capable of producing comparable results.

Can the ISMS cover only part of an organization?

Yes, provided the scope is clear, justified and does not create misleading boundaries or exclude essential dependencies.

Does certification prove that no breach will occur?

No. Certification provides confidence that a structured management system is implemented and evaluated, not a guarantee against incidents.

How much documentation is required?

Enough to operate the ISMS effectively, support consistency and retain required evidence. The standard does not require a traditional manual.

How often should risks be reviewed?

At planned intervals and when significant changes, incidents, threats, vulnerabilities or obligations arise.

What is the role of ISO/IEC 27002?

It provides implementation guidance for information security controls and supports control design, but certification is against ISO/IEC 27001.

How does Amendment 1:2024 affect implementation?

The organization must determine whether climate change is a relevant issue, and relevant interested parties may have climate-related requirements.

How can Pacific Certifications support organizations?

Pacific Certifications can provide independent certification assessments, surveillance and recertification services after the organization has implemented its ISMS.

20. Final Implementation Principles

- Start with business risk, not a list of controls.
- Keep the ISMS scope accurate and connected to real dependencies.
- Make risk and control ownership visible.
- Integrate security activities into normal business workflows.
- Use evidence to evaluate effectiveness, not merely document existence.
- Treat suppliers and cloud services as active risk dependencies.
- Learn from incidents, near misses, testing and performance trends.
- Ensure leadership decisions are visible in priorities and resources.
- Maintain the ISMS as the organization, technology and threat environment change.

Ready for independent assessment?

Before applying for certification, confirm that the ISMS has been implemented, operated, internally assessed and reviewed by top management, with corrective actions underway or completed as appropriate.

Contact Pacific Certifications

For information about the ISO/IEC 27001:2022 certification process, scope confirmation, assessment planning or quotation requirements, contact support@pacificcert.com or visit www.pacificcert.com.

Disclaimer: This guide is an educational implementation resource and does not reproduce the full text of ISO/IEC 27001. Organizations should obtain an authorized copy of the standard and determine applicable legal, regulatory and contractual requirements.