ISO/IEC 27001:2022 GAP ANALYSIS TEMPLATE

Information Security Management Systems | Downloadable Website Resource

Use this template to compare your current information security practices against ISO/IEC 27001:2022 requirements and identify gaps before certification assessment.

Prepared for organizations planning ISO/IEC 27001:2022 certification, information security management system readiness review, internal evaluation, risk treatment review, or Annex A control readiness assessment.

Pacific Certifications provides independent third-party certification services. This template is intended as an educational and self-assessment resource and does not replace the formal certification assessment process.

Contact: support@pacificcert.com | www.pacificcert.com

How to Use This Gap Analysis Template

- Review each ISO/IEC 27001:2022 clause and compare it with existing policies, processes, risk assessments, statement of applicability, control evidence, monitoring records, and management review outputs.
- Record available evidence and identify missing documentation, weak implementation, incomplete risk treatment, unclear ownership, or gaps in Annex A control coverage.
- Assign responsibilities, target dates, and priority levels so the organization can track closure before certification assessment.
- Use the results to prepare a structured action plan, improve ISMS readiness, and strengthen information security governance, risk management, and operational control.

Suggested Status Definitions

Status	Meaning
Compliant	Requirement is documented, implemented, monitored, and supported by objective evidence.
Partially Compliant	Some controls or records exist, but implementation is incomplete, inconsistent, or not fully evidenced.
Gap Identified	Requirement is missing, weak, undocumented, not implemented, or not aligned with the organization's information security risks.
Not Applicable	Requirement or control is not applicable based on ISMS scope, risk assessment, business context, and statement of applicability. Justification should be recorded.

Pacific Certifications
INSPECTION & CERTIFICATION

Gap Analysis Summary

Complete this summary before or after the clause-wise review to capture the ISMS profile and overall readiness level.

Organization Name	
Location(s) / Site(s)	
ISMS Scope	
Business Activities Covered	
Information Assets / Critical Services	
Applicable Legal, Regulatory and Contractual Requirements	
Cloud / IT / Outsourced Services in Scope	
Number of Employees / Users Covered	
Review Date	
Reviewed By	

Overall Readiness Rating

Area	Strong	Needs Improvement	Critical Gap
ISMS Documentation	☐	☐	☐
Implementation Evidence	☐	☐	☐
Risk Assessment and Treatment	☐	☐	☐
Annex A Controls	☐	☐	☐
Monitoring and Improvement	☐	☐	☐

ISO/IEC 27001:2022 Clause-Wise Gap Analysis Worksheet

Use this worksheet during document review, ISMS interviews, process walkthroughs, information asset review, risk assessment review, control evidence review, and management system readiness evaluation. The clause descriptions are summarized for self-assessment purposes.

Clause Area	Gap Analysis Questions	Evidence to Review	Status	Gap / Risk Noted	Corrective Action / Next Step	Owner	Target Date
4.1 Context of the organization	Has the organization identified internal and external issues affecting the ISMS and information security objectives?	Context analysis, business risks, threat landscape, strategic review, external obligations	☐ C ☐ PC ☐ Gap ☐ N/A				
4.2 Interested parties	Are interested parties and their information security requirements identified and reviewed?	Interested party register, client requirements, regulator requirements, contracts, stakeholder needs	☐ C ☐ PC ☐ Gap ☐ N/A				
4.3 ISMS scope	Is the ISMS scope documented with clear boundaries, locations, activities, assets, technology, interfaces, and exclusions?	ISMS scope statement, process map, sites, asset groups, network/service boundaries	☐ C ☐ PC ☐ Gap ☐ N/A				
4.4 ISMS processes	Are ISMS processes established, implemented, maintained, and continually improved?	Process interaction map, procedures, records, responsibilities, ISMS operating model	☐ C ☐ PC ☐ Gap ☐ N/A				
5.1 Leadership and commitment	Does top management demonstrate accountability and support for ISMS effectiveness?	Management communications, objectives, resource decisions, review outputs, governance records	☐ C ☐ PC ☐ Gap ☐ N/A				
5.2 Information security policy	Is the information security policy approved, communicated, available, maintained, and aligned with business purpose?	Approved policy, communication records, version control, employee awareness evidence	☐ C ☐ PC ☐ Gap ☐ N/A				
5.3 Roles and responsibilities	Are ISMS roles, responsibilities, authorities, and reporting lines defined and communicated?	RACI matrix, job descriptions, committee terms, appointment letters, reporting structure	☐ C ☐ PC ☐ Gap ☐ N/A				
6.1 Risks and opportunities	Are risks and opportunities that affect ISMS intended outcomes identified and addressed?	Risk methodology, risk register, opportunity log, treatment plans, action trackers	☐ C ☐ PC ☐ Gap ☐ N/A				
6.1.2 Information security risk assessment	Is a repeatable risk assessment process defined with criteria for risk acceptance and analysis?	Risk assessment procedure, risk criteria, asset/threat/vulnerability records, risk results	☐ C ☐ PC ☐ Gap ☐ N/A				
6.1.3 Risk treatment and SoA	Are risk treatment actions selected and is the Statement of Applicability complete and justified?	Risk treatment plan, Statement of Applicability, control selection rationale, residual risk approvals	☐ C ☐ PC ☐ Gap ☐ N/A				
6.2 Information security objectives	Are measurable information security objectives established at relevant functions and levels?	Objectives, KPIs, plans, responsibilities, monitoring results, review records	☐ C ☐ PC ☐ Gap ☐ N/A				
6.3 Planning of changes	Are ISMS changes planned in a controlled manner considering purpose, consequences, resources, and responsibilities?	Change records, impact assessments, approvals, implementation plans, communication evidence	☐ C ☐ PC ☐ Gap ☐ N/A				
7.1 Resources	Are adequate resources available for ISMS implementation, control operation, monitoring, and improvement?	Budget, staffing, security tools, outsourced service support, infrastructure resources	☐ C ☐ PC ☐ Gap ☐ N/A				
7.2 Competence	Are personnel competent for roles affecting information security and ISMS performance?	Competency matrix, training records, qualification records, awareness assessments	☐ C ☐ PC ☐ Gap ☐ N/A				

Clause Area	Gap Analysis Questions	Evidence to Review	Status	Gap / Risk Noted	Corrective Action / Next Step	Owner	Target Date
7.3 Awareness	Are personnel aware of policy, their contribution, security obligations, and consequences of nonconformity?	Awareness records, induction material, campaigns, acknowledgement records, phishing simulations where used	☐ C ☐ PC ☐ Gap ☐ N/A				
7.4 Communication	Are internal and external ISMS communications defined, including what, when, with whom, and how to communicate?	Communication matrix, incident communication plan, client/regulator communication records	☐ C ☐ PC ☐ Gap ☐ N/A				
7.5 Documented information	Are ISMS documents and records controlled for approval, access, retention, changes, and protection?	Document control procedure, master list, version records, retention controls, access rights	☐ C ☐ PC ☐ Gap ☐ N/A				
8.1 Operational planning and control	Are ISMS processes operated as planned and are outsourced processes controlled?	Operational procedures, control monitoring records, outsourced process records, change records	☐ C ☐ PC ☐ Gap ☐ N/A				
8.2 Risk assessment execution	Are information security risk assessments performed at planned intervals and when significant changes occur?	Risk assessment schedule, updated risk register, review evidence, change-triggered assessments	☐ C ☐ PC ☐ Gap ☐ N/A				
8.3 Risk treatment execution	Are risk treatment plans implemented, tracked, and reviewed for effectiveness?	Risk treatment tracker, control implementation evidence, residual risk approvals, SoA updates	☐ C ☐ PC ☐ Gap ☐ N/A				
9.1 Monitoring, measurement, analysis and evaluation	Are ISMS performance and control effectiveness monitored, measured, analyzed, and evaluated?	Monitoring plan, security KPIs, control testing results, incident trends, dashboards	☐ C ☐ PC ☐ Gap ☐ N/A				
9.2 Internal audit	Are internal audits planned and conducted against ISO/IEC 27001:2022 and organizational ISMS requirements?	Internal audit program, audit reports, auditor competence, findings, follow-up records	☐ C ☐ PC ☐ Gap ☐ N/A				
9.3 Management review	Does management review the ISMS at planned intervals with required inputs and outputs?	Management review agenda, minutes, decisions, actions, resource needs, improvement outputs	☐ C ☐ PC ☐ Gap ☐ N/A				
10.1 Continual improvement	Are opportunities identified and actions taken to continually improve the ISMS?	Improvement register, trend analysis, management actions, control enhancement records	☐ C ☐ PC ☐ Gap ☐ N/A				
10.2 Nonconformity and corrective action	Are nonconformities managed with correction, root cause analysis, corrective action, and effectiveness review?	Nonconformity records, root cause analysis, corrective action tracker, closure evidence	☐ C ☐ PC ☐ Gap ☐ N/A				

Pacific Certifications
INSPECTION & CERTIFICATION

Annex A Control Readiness Review

Review Annex A controls based on the organization's risk assessment and Statement of Applicability. The control areas below are grouped according to ISO/IEC 27001:2022 Annex A control themes for practical gap analysis.

Annex A Theme	Control Readiness Questions	Evidence to Review	Status	Gap / Action Required	Owner	Target Date
A.5 Organizational controls	Are governance, policies, roles, segregation of duties, contact with authorities, threat intelligence, project security, asset inventory, acceptable use, access return, classification, information transfer, supplier security, cloud services, incident management, business continuity, legal compliance, privacy, IPR, record protection, independent review, and documented operating procedures addressed where applicable?	Policies, SoA, governance records, asset inventory, supplier controls, contracts, incident procedures, continuity plans, legal/privacy records	☐ C ☐ PC ☐ Gap ☐ N/A			
A.6 People controls	Are screening, employment terms, awareness, disciplinary process, remote working, confidentiality, and post-employment responsibilities controlled where applicable?	HR procedures, screening records, employment terms, awareness records, NDA/confidentiality records, remote work controls	☐ C ☐ PC ☐ Gap ☐ N/A			
A.7 Physical controls	Are physical security perimeters, entry controls, secure offices, physical monitoring, environmental threats, secure areas, clear desk/screen, equipment security, off-premises assets, storage media, cabling, maintenance, and disposal controlled where applicable?	Access logs, visitor records, CCTV/security records, equipment registers, media handling, maintenance and disposal records	☐ C ☐ PC ☐ Gap ☐ N/A			
A.8 Technological controls	Are user endpoint devices, privileged access, access rights, authentication, capacity, malware protection, vulnerability management, configuration, information deletion, data masking, DLP, backup, logging, monitoring, clock sync, secure coding, test information, network security, web filtering, cryptography, change management, secure development, outsourced development, testing, protection against leakage, and technical resilience addressed where applicable?	Access reviews, IAM records, vulnerability scans, backup tests, logs, monitoring evidence, secure configuration, encryption records, change records, development controls	☐ C ☐ PC ☐ Gap ☐ N/A			

Pacific Certifications
INSPECTION & CERTIFICATION

Gap Closure Action Plan

Use this section to prioritize actions and track closure before applying for ISO/IEC 27001:2022 certification.

Priority	Gap / Issue	Action Required	Responsible Person	Due Date	Closure Evidence	Status

Key ISMS Evidence Checklist

- ISMS scope, context review, interested party register, information security policy, ISMS roles and responsibilities, and process interaction records.
- Information asset inventory, risk assessment methodology, risk register, risk treatment plan, Statement of Applicability, and residual risk acceptance records.
- Annex A control evidence such as access control reviews, vulnerability records, backup tests, logging and monitoring evidence, incident records, supplier controls, cloud service controls, and physical security records.
- Competence and awareness records, communication records, internal audit records, management review outputs, nonconformity records, corrective action records, and continual improvement actions.
- Legal, regulatory, contractual, privacy, data protection, intellectual property, and information transfer requirements applicable to the ISMS scope.

Certification Readiness Notes

Organizations should close major documentation and implementation gaps before certification assessment. Particular attention should be given to ISMS scope definition, risk assessment and treatment, Statement of Applicability justification, Annex A control implementation evidence, internal audit, management review, incident management, supplier controls, access control, vulnerability management, and continual improvement records.

For ISO/IEC 27001:2022 certification support, application review, and quotation, contact Pacific Certifications at support@pacificcert.com.

Call to Action

Ready to begin ISO/IEC 27001:2022 Certification? Email support@pacificcert.com or visit www.pacificcert.com to request application support, certification cost evaluation, and downloadable resources.

Pacific Certifications
INSPECTION & CERTIFICATION