ISO/IEC 27000

Overview & vocabulary

Type: Overview | Certifiable: No | Focus: Concepts

Defines the core concepts and terms used across the ISO/IEC 27000 family and ISMS work.

When you need it

You want shared language across scope, policies, and risk discussions.

Who uses it

Anyone new to ISO security standards; project teams and stakeholders.

Typical outputs

Common definitions, aligned terminology, consistent documentation wording.

ISO/IEC 27001

ISMS requirements (certifiable)

Type: Requirements | Certifiable: Yes | Focus: ISMS

Specifies requirements to establish, implement, maintain and continually improve an ISMS.

When you need it

You need a structured ISMS or customers request ISO 27001 certification.

Who uses it

Organisations building governance, roles, processes, and evidence.

Typical outputs

Scope, risk method, SoA, objectives, controls evidence, internal audits.

ISO/IEC 27002

Controls reference & guidance

Type: Guidance | Certifiable: No | Focus: Controls

Provides a catalogue of information security controls and guidance for implementation.

When you need it

You select and implement controls and justify choices in the SoA.

Who uses it

Security teams, control owners, and implementers.

Typical outputs

Control mapping, implementation notes, ownership and operational evidence.

ISO/IEC 27003

How to implement ISO 27001

Type: Guidance | Certifiable: No | Focus: Implementation

Provides guidance on implementing an ISMS in line with ISO/IEC 27001 clauses.

When you need it

You want a practical implementation approach and sequencing.

Who uses it

First-time implementers and teams structuring an ISMS programme.

Typical outputs

Implementation plan, roles, milestones, deliverables checklist and approach.

ISO/IEC 27004

Measurement & performance evaluation

Type: Guidance | Certifiable: No | Focus: Metrics

Guides how to monitor, measure, analyse and evaluate ISMS performance and effectiveness.

When you need it

You define KPIs/KRIs and support ISO 27001 performance evaluation.

Who uses it

ISMS managers, governance teams, and management review owners.

Typical outputs

Metrics catalogue, monitoring plan, dashboards, trends and evaluation records.

ISO/IEC 27005

Information security risk management

Type: Guidance | Certifiable: No | Focus: Risk

Guidance on managing information security risks and aligning risk work with ISMS needs.

When you need it

You build a risk method for assessment, treatment and review.

Who uses it

Risk owners, security leads, and ISMS implementers.

Typical outputs

Risk criteria, risk register, treatment plan, residual risk decisions and review.

ISO/IEC 27006-1

Rules for certification bodies

Type: Requirements | Certifiable: No | Focus: Certification bodies

Specifies requirements for bodies providing audit and certification of ISMS against ISO/IEC 27001.

When you need it

You choose a certification body or validate its accreditation approach.

Who uses it

Certification bodies and accreditation bodies; informed customers may reference it.

Typical outputs

Competence criteria, certification process requirements, impartiality expectations.

ISO/IEC 27007

ISMS auditing guidance

Type: Guidance | Certifiable: No | Focus: Internal audit

Guidelines for managing an ISMS audit programme and conducting ISMS audits.

When you need it

You plan and execute internal audits and track corrective actions.

Who uses it

Internal auditors, audit programme managers, ISMS owners.

Typical outputs

Audit programme, audit plans, findings, evidence trails, follow-up actions.

ISO/IEC 27017

Cloud security controls guidance

Type: Guidance | Certifiable: No | Focus: Cloud security

Cloud-specific guidance on implementing controls for cloud service customers and providers.

When you need it

Your service relies on cloud or you provide cloud services.

Who uses it

Cloud/SaaS teams defining shared responsibility and cloud controls.

Typical outputs

Cloud control mapping, shared responsibility statements, cloud evidence pack.

ISO/IEC 27018

PII protection in public cloud

Type: Guidance | Certifiable: No | Focus: Cloud privacy

Guidance for protecting personally identifiable information (PII) in public cloud environments.

When you need it

You process customer PII in public cloud services (as a provider/processor).

Who uses it

SaaS/cloud services handling PII and privacy commitments.

Typical outputs

PII protection controls, privacy commitments, supporting evidence for customers.

ISO/IEC 27701

Privacy Information Management (PIMS)

Type: Requirements | Certifiable: Yes | Focus: Privacy management

Requirements and guidance for a Privacy Information Management System for PII controllers and processors.

When you need it

You want structured privacy governance aligned to security management.

Who uses it

Organisations acting as PII controllers and/or processors.

Typical outputs

PIMS policies, privacy roles, PII inventory, DPIA approach, privacy controls.

ISO/IEC 27035-1

Incident management foundation

Type: Guidance | Certifiable: No | Focus: Incident response

Core concepts, principles and process for information security incident management.

When you need it

You formalise detection, response, recovery and lessons learned.

Who uses it

SOC/IR teams, security operations, and ISMS owners.

Typical outputs

IR policy, playbooks, triage workflow, comms plan, post-incident review.

ISO/IEC 27036

Supplier relationships security

Type: Guidance | Certifiable: No | Focus: Third parties

Guidance to address information security risks in supplier and outsourcing relationships.

When you need it

You rely on vendors, subprocessors, or an extended supply chain.

Who uses it

Procurement, vendor management, security and risk teams.

Typical outputs

Supplier security requirements, due diligence, contract clauses, monitoring.

Need help applying it?

WHAT WE OFFER

Services

At RisQera, we focus on practical security governance. We support organisations through ISO projects with clear methods and evidence

ISO/IEC 27001 Implementation

Build or improve your ISMS from scope definition to certification readiness.

ISO/IEC 27001 Internal Audit

Independent internal audits to assess gaps and prepare for external audits.

ISO/IEC 27005 & ISO/IEC 42001

Risk management and AI governance support, aligned with ISO standards.

Contact: info@risqera.com

Follow risQera on LinkedIn

risQera | Beyond Risk