



Enterprise-Ready Made Simple: Free ISO 27001 Checklist by Riskora.io



The 'ISO 27001' is an information security standard adopted by organisations across the globe.

The ISO 27001 framework is highly detailed and may seem complex to the uninitiated.

In this article we'll break down the ISO 27001 framework into its core pillars. Each pillar focuses on protecting a specific part of your ISMS (information security management system).

By simplifying each pillar into practical, actionable steps, ISO 27001 compliance becomes faster, clearer, and less overwhelming.

Use this checklist to assess your organisational readiness, start closing the gaps, and build trust with your clients.

Using this checklist:

- Tick off what's implemented; highlight what needs work.
- Collect evidence (documents, logs, training records) for each completed item.
- Use the checklist as proof of your enterprise-readiness when approaching large clients.

Pillar 1 Documentation

Ensure these documents are prepared and updated regularly. Strong documentation is key to an effective ISMS, allowing you to keep your system structured, traceable, and sustainable.

- Information Security Policy
- IS (information security) Context, Requirements, and Scope Manual
- Statement of Applicability (SoA)
- Acceptable Use & Cyber Security Policies
- Risk Assessment and Treatment Procedure
- Business Continuity & Incident Management Plans
- Network Security & Access Control Policies
- Change Management & Secure Development Guidelines
- Human Resources Security Policy
- Third-Party and Cloud Usage Policies
- Data Protection, Physical & Environmental Security Policies
- Information Classification and Labelling Procedure
- Non-conformity and Corrective Action Procedure

Optional but recommended:

Information Backup Policy / Cryptography Policy / Document Control / Asset & Media Handling / Governance and Management Review Procedures

Pillar 2 Core ISO 27001 Standard Requirements

- Define ISMS boundaries that reflect your business priorities and stakeholder expectations
- Demonstrate leadership commitment and assign clear roles & responsibilities
- Set measurable ISMS objectives based on risk assessment outcomes
- Establish an awareness and communication strategy for staff and partners
- Maintain an organised documentation control system
- Define metrics/KPIs (key performance indicators) to measure ISMS performance
- Ensure continual improvement through internal audits, management reviews, and corrective actions

Pillar 3 Organisational Controls

- Define clear information-security roles, responsibilities, and segregation of duties
- Maintain communication channels with authorities, regulators, and industry groups
- Establish threat-intelligence processes to identify and mitigate emerging risks
- Maintain an asset inventory with ownership, classification, and lifecycle tracking
- Define processes for access control, authentication, and least-privilege management
- Implement supplier-risk management and periodic reviews of SLAs
- Ensure secure configuration and use of cloud services
- Implement a structured incident-management process (detection → response → lessons learned)
- Maintain and test a business continuity plan
- Continuously monitor compliance with legal, contractual, and privacy requirements
- Safeguard intellectual property and personal data (PII)
- Schedule independent reviews to verify ISMS effectiveness

Pillar 4 People Controls

As well as being the strongest defence, employees can sometimes be the weakest link. These controls ensure employees and contractors understand and uphold security responsibilities.

- Conduct background screenings before granting data access
- Include NDA and security clauses in employment agreements
- Deliver regular awareness training and refreshers on security best practices
- Establish a clear disciplinary and incident-reporting process
- Apply formal access revocation when staff leave or change roles

Pillar 5 Physical Controls

Physical measures protect your premises, equipment and information from unauthorised access or interference.

- Define secure perimeters and control physical entry (locks, visitor logs, supervision)
- Apply a “clean desk / clear screen” policy
- Protect and position equipment securely, especially off-premises devices
- Safeguard and dispose of storage media appropriately
- Protect power, cabling, and supporting utilities from damage or tampering

Pillar 6 Technological Controls

Technology controls protect digital assets and data in your organisation in an increasingly connected world.

Here are some examples of technical controls to enforce:

- Secure user devices; manage privileged access; enforce MFA and least privilege
- Guard against malware; maintain vulnerability management and patching
- Apply encryption for data at rest and in transit, use secure configurations
- Maintain backups and test recovery regularly, design redundancy into critical systems
- Track, log, and monitor all access and changes; maintain audit trails
- Filter web traffic and separate development, test, and production environment
- Prevent data leakage, control use of privileged utilities and software installations
- Follow a secure development lifecycle with defined app-security requirements and testing

Book a consultation with us - <https://riskora.io/>

Book a consultation with us!

riskora.io