Venzip

*ISO **27001** COMPLIANCE READINESS* **GUIDE**

For Startups, SaaS Companies & Growing Organizations

Venzip

STEP 1

PLAN YOUR ISMS IMPLEMENTATION

Before building your ISMS, create a roadmap. Define scope, budget, and timeline.

- [ ] Identify a PDCA (Plan-Do-Check-Act) process to find gaps and challenges
- [ ] Estimate certification costs relative to your organization's size
- [ ] Define the scope of work from planning through completion
- [ ] Use project management tools to track milestones and deadlines

STEP 2

DEFINE THE SCOPE OF YOUR ISMS

Decide which parts of your business the ISMS covers and communicate this to stakeholders.

- [ ] Determine which business areas, systems, and data are in scope
- [ ] Identify trust boundaries where protected data crosses systems
- [ ] Document and communicate the ISMS scope to all stakeholders

STEP 3

BUILD YOUR ISMS TEAM & ASSIGN ROLES

Assemble a cross-functional team with clear ownership and management support.

- [ ] Assign an information security leader or CISO
- [ ] Select engineers and compliance staff to implement controls
- [ ] Ensure senior leadership is involved for strategy and resource allocation
- [ ] Align the team on scope, planning steps, and individual responsibilities

STEP 4

CONDUCT AN ASSET INVENTORY

Identify and classify every information asset your ISMS will protect.

- [ ] Record information assets (data, databases, records, people)
- [ ] Record physical assets (laptops, servers, office locations)
- [ ] Record intangible assets (IP, brand, reputation)
- [ ] Assign each asset a classification level and an owner

STEP 5

PERFORM A RISK ASSESSMENT

Identify threats, evaluate likelihood and impact, and rank risks to prioritize treatment.

- [ ] Establish and document a risk management framework
- [ ] Identify scenarios where information or systems could be compromised
- [ ] Evaluate the likelihood and potential impact of each risk scenario
- [ ] Rank risks based on overall severity to the organization

Venzip

STEP 6

DEVELOP A RISK REGISTER & TREATMENT PLAN

Turn your risk assessment findings into an actionable plan with owners and timelines.

- [ ] Record all identified risks with impact, likelihood, and ranking
- [ ] Design a treatment response for each risk (mitigate, accept, transfer, avoid)
- [ ] Assign an owner to each risk and each mitigation activity
- [ ] Set target timelines and track progress of all treatment activities

STEP 7

COMPLETE THE STATEMENT OF APPLICABILITY

The SoA documents which Annex A controls apply to your ISMS and why.

- [ ] Review the 93 controls listed in ISO 27001 Annex A
- [ ] Select controls relevant to your identified risks and business context
- [ ] Justify inclusion or exclusion of each control in your SoA document

Venzip

STEP 8

IMPLEMENT CONTROLS & SECURITY POLICIES

Put your ISMS into action — assign control owners, draft policies, and build supporting documentation.

- [ ] Assign owners to each security control to be implemented
- [ ] Draft and approve key policies: Information Security,
- [ ] Access Control, Acceptable Use Establish procedures for incident management, change management, and business continuity
- [ ] Document the framework for maintaining and continually improving the ISMS

STEP 9

TRAIN EMPLOYEES & CONDUCT INTERNAL AUDIT

Security awareness training and an internal audit are required before your certification audit.

- [ ] Train all employees on security policies, threats, and their ISMS responsibilities
- [ ] Make security training part of onboarding for new hires
- [ ] Conduct an internal audit using staff not involved in ISMS development (or a third party)
- [ ] Share audit findings with the ISMS team and senior management
- [ ] Remediate any nonconformities identified before the external audit

Venzip

STEP 10

CERTIFICATION AUDIT & ONGOING COMPLIANCE

Select an accredited auditor and maintain your certification with annual surveillance audits.

- [ ] Select an independent, accredited ISO 27001 auditor
- [ ] Complete Stage 1 Audit (documentation review) and address any feedback
- [ ] Complete Stage 2 Audit (control testing and ISMS effectiveness evaluation)
- [ ] Address any nonconformities raised by the auditor
- [ ] Plan for annual surveillance audits and full re-certification every 3 years

SIGNS YOUR ORGANIZATION MAY BE READY FOR ISO 27001

- You work with enterprise clients that require security certifications
- Your company handles sensitive customer or employee data
- You want to build trust with partners, investors, and regulators
- You are preparing for SOC 2, HIPAA, or enterprise procurement reviews

NEED HELP PREPARING FOR ISO 27001?

Venzip helps startups and growing companies:

- Conduct ISO 27001 readiness assessments
- Build a compliant Information Security Management System
- Prepare documentation, policies, and controls for certification
- Automate evidence collection and continuous compliance monitoring
- Map shared controls across ISO 27001, SOC 2, HIPAA, and GDPR

BOOK A CONSULTATION

info@venzip.com

(604) 363-7138

www.venzip.com

Also Preparing for SOC 2?

Many organizations pursuing ISO 27001 also need SOC 2 compliance. Venzip helps you achieve both efficiently by mapping shared controls across frameworks — saving time, reducing duplication, and getting you audit-ready faster.

DOWNLOAD OUR SOC 2 READINESS CHECKLIST AT WWW.VENZIP.COM

Quick Reference: ISO 27001 Key Facts

Standard: ISO/IEC 27001:2022 (latest revision)

Focus: Information Security Management System (ISMS)

Annex A Controls: 93 controls across 4 themes (Organizational, People, Physical, Technological)

Certification Cycle: Stage 1 + Stage 2 audit, annual surveillance, re-certification every 3 years

Who Needs It: Any organization handling sensitive data or serving enterprise clients