

Risk Assessment & ISO 27001

Understand your risks, build an ISMS and get ready for certification

Customers, investors and regulators increasingly want proof that you manage information security deliberately. A security questionnaire from an enterprise customer, or obligations under India's DPDP Act, can stall a deal or a launch if you cannot show how risks are identified and treated.

ISO/IEC 27001 is the international standard for an information security management system (ISMS). Certification shows that security is governed, measured and improved, with controls chosen to fit your actual risks.

SentryArk helps you get there, from a first risk assessment and gap analysis to a working ISMS and an audit-ready organisation, without burying your team in paperwork.

RISK ASSESSMENT AND MANAGEMENT

We identify the information assets that matter to your business, the threats they face and the weaknesses that expose them. Each risk is rated on likelihood and impact, and we help you decide how to treat it, with owners and timelines your management can track.

- Asset and data inventory
- Threat and vulnerability analysis
- Risk rating and register
- Risk treatment planning
- Third-party and vendor risk
- Board-level risk reporting

ISO 27001 IMPLEMENTATION

We guide you through the standard step by step: defining scope, writing policies that match how you work, selecting Annex A controls and producing the Statement of Applicability. Because our team also runs penetration tests and a SOC, the technical controls we recommend are ones we know work in practice.

We prepare you for certification with an internal audit and management review, and support you through the external audit itself.

ASSESSMENT DETAILS AND METHODOLOGY

Our approach follows ISO/IEC 27001:2022 and the risk management guidance in ISO/IEC 27005. Each stage produces documents you own and can keep improving after the engagement ends.

Scoping and gap analysis	01	We agree the ISMS scope and compare current practice with clauses 4 to 10 and the Annex A controls, showing what exists and what is missing.
Risk assessment	02	We inventory assets, assess threats and vulnerabilities, rate each risk and record it in a risk register with a named owner.
Risk treatment and controls	03	We help select and implement controls, write policies and procedures, and prepare the Statement of Applicability.
Internal audit and review	04	An independent internal audit and management review find gaps, and corrective actions are closed before the auditors arrive.
Certification support	05	We support you through the stage 1 and stage 2 audits, help answer auditor findings and plan for surveillance audits.

The engagement includes

- Gap analysis report
- Statement of Applicability
- Internal audit report
- Risk register and treatment plan
- ISMS policies and procedures
- Certification audit support

ABOUT SENTRYARK

SentryArk is a team of security engineers, SOC analysts and offensive security specialists. Our consultants hold OSCE, CRT0, CEH and ISMS certifications. We have secured 20+ organisations, assessed 8K+ devices and 30+ applications, and reported 250+ vulnerabilities. Because the same team attacks and defends, our advice reflects how real attackers operate.