WHITE PAPER

What is ISO?

A Complete Guide

Understand the International Organization for Standardization: its history, the key security certifications relevant to technology organizations, the ISO 27001:2022 certification journey, and how ISO compliance can be a strategic differentiator.

Version 1.0

Prepared By Lorikeet Security

lorikeetsecurity.com

OVERVIEW

1. Executive Overview

ISO is an independent, non-governmental international body that develops and publishes standards across virtually every industry. For technology organizations, ISO/IEC 27001 — the Information Security Management System (ISMS) standard — is the most strategically significant certification, providing a globally recognized framework for managing information security risk.

> **Current Standard: ISO/IEC 27001:2022**
>
> ISO/IEC 27001:2022 updated Annex A controls from 114 to 93, reorganized across four themes. Organizations have until October 2025 to transition from 2013 certifications.

HISTORY

2. History of ISO

Year	Milestone
1947	ISO founded in Geneva, Switzerland, succeeding the International Federation of National Standardizing Associations.
1987	ISO 9001 (Quality Management Systems) published — one of the most widely adopted standards globally.
1995	ISO/IEC 17799 (Code of Practice for Information Security) published — the precursor to ISO 27001.
2005	ISO/IEC 27001:2005 formally published as the first dedicated ISMS certification standard.
2013	ISO/IEC 27001:2013 released with structural revisions and alignment to the Annex SL high-level structure.
2022	ISO/IEC 27001:2022 released, updating and consolidating Annex A controls across four themes.

STANDARDS

3. Key ISO Standards for Technology Organizations

Standard	Description
ISO/IEC 27001	Information Security Management System. The flagship cybersecurity certification governing how organizations manage security risk across people, processes, and technology.

Standard	Description
ISO/IEC 27002	Code of practice for information security controls. Provides implementation guidance for Annex A controls. Not a certifiable standard — used as supporting guidance.
ISO/IEC 27017	Cloud security controls. Extends ISO 27002 with cloud-specific guidance for providers and customers.
ISO/IEC 27018	Protection of PII in public clouds. Relevant for providers processing personal data under GDPR.
ISO/IEC 27701	Privacy Information Management System (PIMS). GDPR-aligned extension to ISO 27001.
ISO 9001	Quality Management Systems. Often required alongside ISO 27001 in enterprise procurement.
ISO 22301	Business Continuity Management. Governs organizational resilience and continuity planning.

STRUCTURE

4. ISO 27001:2022 — Annex A Control Themes

Annex A provides 93 controls across four themes:

Theme	Controls	Coverage
Organizational Controls (5.1–5.37)	37	Policies, roles, threat intelligence, supplier security, and incident management.
People Controls (6.1–6.8)	8	Screening, onboarding, awareness training, and remote working.
Physical Controls (7.1–7.14)	14	Physical perimeters, entry controls, equipment security, and secure disposal.
Technological Controls (8.1–8.34)	34	Endpoints, access rights, malware protection, logging, encryption, and vulnerability management.

JOURNEY

5. The Certification Journey

- Gap Assessment: Identify current-state gaps against ISO 27001 clauses and Annex A controls. Produces a prioritized remediation roadmap.

- ISMS Design and Implementation: Define ISMS scope, develop the Statement of Applicability (SoA), implement controls, and train personnel.
- Internal Audit: Conduct an internal audit of the ISMS to identify non-conformities before the external audit.
- Stage 1 Audit — Documentation Review: Certification body reviews ISMS documentation and confirms Stage 2 readiness.
- Stage 2 Audit — Certification: On-site or remote audit verifying controls are implemented and operating effectively.
- Certification Issued: Certificate valid for three years with annual surveillance audits and full recertification at cycle end.

BUSINESS VALUE

6. Business Value of ISO/IEC 27001

Benefit	Description
Sales Acceleration	ISO 27001 is a standard vendor requirement in enterprise procurement. Certified organizations progress security reviews faster.
Risk Reduction	The PDCA cycle and mandatory risk treatment process drive continuous improvement and reduce incident likelihood and impact.
Regulatory Alignment	ISO 27001 controls map directly to GDPR, SOC 2, HIPAA, and NIS2, enabling efficient multi-framework programs.
Talent Attraction	Certification signals organizational commitment to security, attracting security-conscious employees and partners.
Insurance Positioning	Underwriters increasingly use ISO 27001 certification as a positive factor contributing to lower premiums.

HOW WE HELP

7. How Lorikeet Security Supports ISO 27001

- Control 8.8 (Vulnerability Management): Penetration testing provides evidence of systematic vulnerability identification and remediation.
- Control 8.25–8.29 (Secure Development): Web application and API assessments validate secure SDLC practices.
- Control 5.7 (Threat Intelligence): Assessment findings provide actionable threat intelligence tied to your specific technology stack.
- Control 5.24 (Incident Management): Penetration test findings can validate and stress-test incident response playbooks.

Get Started

Contact Lorikeet Security at lorikeetsecurity.com to integrate our assessments into your ISO 27001 certification roadmap with audit-ready evidence packages.