ISO 27001

What to Know

This is your high-level refresher on **ISO/IEC 27001**, the internationally recognized standard for managing information security. Whether you're preparing for an audit, building a secure cloud platform, or pursuing a cybersecurity role, ISO 27001 sets the foundation for aligning risk-based security practices with business goals.

This guide gives you a quick refresher focused on:

- **Cybersecurity controls** (access, encryption, monitoring)
- **Core structure of the standard**
- **Practical implementation** for IT, GRC, and DevSecOps teams

What Is ISO 27001?

- **ISO/IEC 27001** is an international standard for establishing, implementing, maintaining, and continually improving an **Information Security Management System (ISMS)**
- Published by the **ISO** and the **IEC**
- Focuses on **confidentiality, integrity, and availability** of data
- Applicable to **organizations of all sizes and industries**
- Auditable standard that leads to formal **certification**

Key Components of ISO 27001

Component	Description
ISMS	Framework for managing information security risks
Annex A Controls	93 reference security controls grouped into 4 themes
Risk-Based	Organizations define controls based on risk assessments
Improvement	Plan–Do–Check–Act (PDCA) model for ongoing improvement

ISO 27001:2022 Control Themes

The latest ISO 27001 revision (2022) reduced controls from 114 to 93 and organized them under 4 categories:

Theme	Description
Organizational	Policies, roles, HR security, supplier management, risk, compliance
People	Access control, user responsibilities, training
Physical	Physical security, equipment protection, secure work areas
Technological	Network security, logging, encryption, malware, system monitoring

Example Cybersecurity Controls

Common ISO 27001 Annex A controls in practice include:

- Role-based access control (RBAC) and segregation of duties
- Logging and monitoring of critical systems
- Encryption for data at rest and in transit
- Information classification policies and asset inventories
- Secure system engineering principles
- Business continuity and disaster recovery planning
- Incident response process and recordkeeping
- Secure disposal and equipment handling
- Formal user onboarding/offboarding processes

Organizations select controls based on their **Statement of Applicability (SoA)**, which justifies inclusion or exclusion of each control.

Risk Management Requirements

ISO 27001 requires organizations to:

- Identify and assess information security risks
- Determine acceptable levels of risk
- Select and implement appropriate controls
- Document a **risk treatment plan**
- Regularly review and update risk assessments

Risk management must be embedded in operational decisions and security planning.

Certification Process

To achieve ISO 27001 certification, organizations must:

1. Define scope of the ISMS
2. Conduct a risk assessment and select appropriate controls
3. Develop all required documentation (policies, procedures, SoA)
4. Implement controls and assign responsibilities
5. Undergo internal audits and management reviews
6. Pass a two-stage **external audit** by a certification body:
    - **Stage 1:** Documentation review and readiness
    - **Stage 2:** Full implementation and effectiveness audit

Certification is valid for **three years**, with **annual surveillance audits** and a full re-certification at the end of the cycle.

Enforcement and Compliance

Item	Details
Region	Global
Applicability	Any organization handling data or seeking security certification
Legal Requirement?	No — voluntary, but required in some contracts and industries
Report Format	Formal ISO 27001 certificate with audit findings
Validity	3 years (with annual reviews)
Recognized Standard?	Yes — considered equivalent or superior to SOC 2 in some markets

Why It Matters

- Aligns your security with a globally accepted, risk-based framework
- Supports trust in B2B, SaaS, fintech, healthcare, and cloud environments
- Helps meet overlapping requirements from GDPR, HIPAA, SOC 2, and NIST CSF
- Improves internal security governance and accountability