

ISO 27001 CHEAT SHEET

ISO 27001 OVERVIEW

ISO 27001 is an international standard for Information Security Management Systems (ISMS), providing a framework to identify, manage, and reduce security risks.

ISO KEY PRINCIPLES

CONFIDENTIALITY

Ensuring information is accessible only to authorized individuals

INTEGRITY

Maintaining the accuracy and reliability of data.

AVAILABILITY

Ensuring information is accessible when needed.

RISK BASED APPROACH

Identifying and mitigating security risks.

CONTINUOUS IMPROVEMENT

Regularly updating security measures.

BENEFITS

COST SAVING

Helps reduce the financial impact of security breaches.

PREPAREDNESS

The standard encourages organizations to regularly review and update their ISMS.

CIA TRIAD

Ensure Data confidentiality, integrity, availability.

COVERAGE

ISO 27001 applies to all types of information (digital or physical)

ATTRACTING BUSINESS

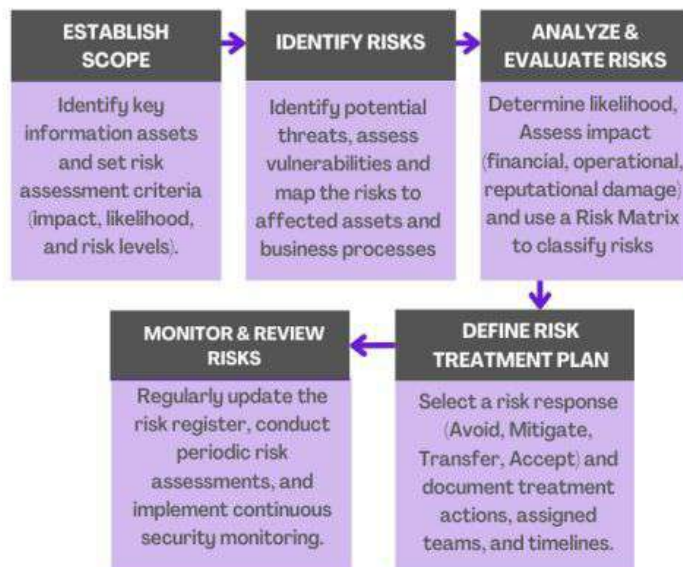
Attract new business opportunities by showcasing commitment to information security.

ISO-27001:2013 V/S ISO-27001:2022

CATEGORY	ISO 27001:2013	ISO 27001:2022
Annex A Controls	114 controls in 14 Domains	93 controls in 4 Domains
New Controls	None	Threat Intelligence, DLP, Data Masking, Web Filtering, etc.
Merged & Updated	Several fragmented controls	Redundant controls combined
Risk Approach	Compliance-driven, static risk treatment	Dynamic Risk management
Business Continuity	Less detailed on IT system resilience.	New control on ICT readiness for business continuity.



RISK ASSESSMENT



COMPLIANCE IN SECURITY INCIDENTS



ASSESS THE INCIDENT

Identify type & impact.

CONTAIN THE INCIDENT

Stop further damage.

RESTORE & SECURE

Take corrective actions



- 🚨 **Notify Affected Parties** – Inform users about potential risks.
- 📄 **Report to Authorities** – Follow legal & regulatory requirements.

KEY SECURITY PRINCIPLES

ACCESS CONTROL

Restrict unauthorized access.

DATA ENCRYPTION

Protect sensitive information.

INCIDENT RESPONSE PLAN

Ensure readiness for cyber threats.

EMPLOYEE AWARENESS

Maintain accurate and up-to-date personal data.

AUDIT & COMPLIANCE CHECKS

Regular assessments for improvement.

NEW CONTROLS IN ISO 27001:2022

- Threat Intelligence
- ICT Readiness for Business Continuity
- Physical Security Monitoring
- Configuration Management
- Data Masking
- Information Deletion
- Secure Coding
- Data Leakage Prevention
- Monitoring Activities
- Web Filtering
- Information Security for the Use of cloud Services

ISO KEY CLAUSES

- Context of the Organization
- Leadership
- Planning
- Support
- Operation
- Performance Evaluation
- Improvement

ISO 27001 AUDIT ISSUES & FIXES

LACK OF RISK ASSESSMENT

Conduct & document a thorough risk analysis.

WEAK ACCESS CONTROLS

Implement strong password policies & role-based access.

UNPATCHED SYSTEMS

Regularly update OS, applications, and firmware.

LACK OF SECURITY AWARENESS

Conduct periodic employee training.

DATA SECURITY & PRIVACY MEASURES

DATA ENCRYPTION

Implement encryption techniques to protect personal data from unauthorized access.

Restrict access based on least privilege and role-based access control (RBAC)

ACCESS CONTROLS

REGULAR DATA BACKUPS

Maintain regular backups of personal data to prevent loss or corruption

Add an extra layer of protection by requiring multiple forms of verification before granting access
MFA