



What is ISO 27001

- ISO 27001:2022 is an ISO standard that provides requirements for an information security management system (ISMS)
- Written by the best security experts
- Allows organisations to be certified by a certification body
- The most popular information security standard

How Does ISO 27001 Work?

- ISO 27001 manages information security
- Based on risk management process
- Identify and evaluate risks
- Implement security controls
- Includes policies, access controls, encryption, etc.
- Reduces likelihood of security breach
- Protects sensitive information



ISO 27001 Family of Standards

ISO 27000 : Overview and vocabulary

ISO 27001 : Information security management System requirements

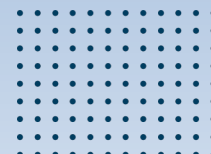
ISO 27002 : Code of practice for information security controls

ISO 27003 : Information security management System implementation guidance

ISO 27004 : Information security management System measurement

ISO 27005 : information security risk management

ISO 27007 : Guidelines for Information security management Systems auditing



How is ISO 27001 organized?

- **Main part**
 - 11 clauses
 - 0-3 Definition of the standard
 - 4-10 Information Security Requirements
- **Annex A**
 - 4 Categories
 - 93 security controls





What is an ISMS?

Information Security Management System

- Establish, Implement, Operate, Monitor, Review, Maintain and Improve Information Security
- Policies, procedures, practices
- Uses risk Management processes
- Systematic Approach
- Protect and secure information assets
- Minimize risk and ensure business continuity

Use Case : HealthBridge



HealthBridge Clinic is a growing small-to-medium sized healthcare provider

ISO 27001 Implementation will help in :

- Regulatory Compliance
- Enhancing Reputation
- Improving Security Posture
- Streamlining Processes
- Building Trust with Patients
- Facilitating Business Growth

