ISO 27001 - INFORMATION SECURITY MANAGEMENT SYSTEM STANDARD

OVERVIEW

ISO 27001 is an internationally recognized standard for Information Security Management Systems (ISMS). It sets the framework for protecting sensitive information and managing security risks.

#1

BENEFITS

Offers enhanced security, regulatory compliance, improved customer trust, and effective risk management.

#2

KEY COMPONENTS

Consists of key components like policies, risk assessment, security controls, objectives, and management reviews, forming a holistic approach to information security.

#3

RISK MANAGEMENT

Emphasizes a risk-based approach, where organizations identify, assess, and prioritize information security risks and then take measures to mitigate or accept them.

#4

SECURITY CONTROLS

Provides 14 categories of security controls, including access control, cryptography, and incident response, to help organizations protect their information assets.

#5

CERTIFICATION PROCESS

The certification process involves several steps, including an initial assessment, implementing controls, conducting internal audits, and achieving external certification through accredited bodies

#6

CONTINUOUS IMPROVEMENT

Promotes a culture of continuous improvement. Organizations regularly review and enhance their ISMS to adapt to evolving security threats and changes in the business environment.

#7