

ISO 27001 CERTIFICATION AND INFORMATION SECURITY MANAGEMENT SYSTEM (ISMS) REGISTRATION

ISO/IEC 27001 is the internationally recognized standard for Information Security Management Systems (ISMS). It provides a model for risk assessment, security design and implementation, and security management.



INTERNAL BENEFITS OF ISO 27001

- ✔ Increase revenue without additional capital outlay
- ✔ Provides a framework for Information Security customized to the needs of the organization and its customers
- ✔ Risk-based vs. controls-based
- ✔ Must cover legal, regulatory, contractual, industry, and self-imposed requirements
- ✔ Can provide assurance equivalent to SSAE 18
- ✔ Produces a well-documented, managed, governed, and continuously improving Information Security program
- ✔ Provides structure for information security and business improvement processes
- ✔ Provides a common method to define information security processes and document them for use in training, controlling, and improving them
- ✔ Provides tools to establish and maintain effective customer focus

BENEFITS OF ISMS IMPLEMENTATION

Corporate governance and oversight

Focus on critical information in any form

Greater visibility and control of information security costs

Avoid "silo" approach to implementing controls

Independent 3rd party validation of due diligence

Shorten sales cycle

Direct ROI on information security

Demonstrated assurance

Consistent and persistent controls

WHAT IS IT?

The ISO 27001 standard specifies implementation and management guidelines to help keep your digital and paper information safe.

An ISMS is a systematic approach to managing sensitive company information in all its forms so that it remains secure. It includes people, processes and IT systems by applying a risk management process.

ISO 27001 certification focuses on data security and risk management. The specification requires that a company strictly follow a set of rigorous business practices and policies in multiple areas (not just information technology) that have been developed to facilitate data security, systems availability and integrity, limit vulnerabilities, manage risks and perform other steps to ensure reasonable data security.