INSIGHTS INTO ISO/IEC 27001

INFORMATION SECURITY MANAGEMENT SYSTEM

What is ISO/IEC 27001?

ISO/IEC 27001 is the leading international standard for information security management. It can be applied to commercial, governmental and not-for-profit organizations, and specifies the requirements for establishing, implementing, maintaining and continually improving an information security management system (ISMS). It is a risk-based and risk-driven standard and is the only known auditable standard for ISMS."

Why is ISO/IEC 27001 important for my business?

Your organization may not consider its information to be vulnerable or targeted for attack but disruptions to business IT processes can cripple your operations and allow your competitors to gain market share. ISO/IEC 27001 offers a systematic and well-structured approach that will protect the confidentiality of your information, ensure the integrity of business data and improve the availability of your business IT systems.

Business benefits include:

A structured, globally recognized information security methodology that identifies & mitigates threats.

Protection from the threat of hacking, data loss & breach of confidentiality, & ensure you can recover faster from such attacks.

Plans that ensure your operations will continue in the event of man-made and natural disasters.

6 Steps to ISO/IEC 27001 Certification

Step 1
Develop and define the scope of the ISMS.

Step 2
Develop an implementation plan.

Step 3
Perform a pre-audit or a gap assessment.

Step 4
TÜV SÜD to perform Stage 1 audit.

Step 5
TÜV SÜD to perform Stage 2 audit. The organization will close any non-conformances.

Step 6
Receive the audit report and certificate after approval by the Certification Body, and initiate annual or six monthly surveillance audits.

Learn more about TÜV SÜD America's ISO Certifications

www.tuvsud.com/en-us