€TRAINING

ISO IEC 27002 Information Security Controls

ISO IEC 27002 Information Security Controls

Introduction:

ISO/IEC 27002 outlines best practices for implementing effective information security controls within organizations. It focuses on safeguarding data confidentiality, integrity, and availability while ensuring compliance with global information security standards. This training program provides comprehensive instruction on implementing and managing information security controls effectively. Through it, participants will be equipped with the knowledge and skills needed to safeguard organizational information assets and mitigate security risks.

Program Objectives

At the end of this program, participants will be able to:

- Establish information security controls and control rules in accordance with ISO/IEC 27002 standards.
- Explore of the methods and processes employed in the establishment and efficient administration of information security controls
- Acquire the knowledge required to assist a business in organizing, putting into place, and administering information security measures.
- Recognize the value of risk management in identifying the best information security controls.
- Assist firms in continuously enhancing their information security management system.

Targeted Audience:

- Managers or consultants who want to establish information security controls in an ISMS built on ISO/IEC 27001.
- Personnel in charge of preserving an organization's information security, compliance, risk, or governance.
- IT consultants or professionals who want to learn more about information security.
- Members of an information security or ISMS deployment team.

Program Outline:

Unit 1:

Introduction to ISO/IEC 27002 Information Security Controls:

- Understanding the importance of information security controls.

- Overview of ISO/IEC 27002 standards.
- Identifying the scope and objectives of information security controls.
- Exploring the relationship between ISO/IEC 27001 and ISO/IEC 27002.
- Introduction to the structure and content of ISO/IEC 27002.

Unit 2:

Governance and Management of Information Security Controls:

- How to establish an information security management system ISMS.
- Defining roles, responsibilities, and governance structures.
- Implementing policies, procedures, and processes for information security.
- Conducting risk assessments and managing risk.
- Monitoring, measuring, and reviewing the effectiveness of information security controls.

Unit 3:

Asset Management and Access Control:

- Identifying and classifying information assets.
- Implementing controls for the management of information assets.
- Enforcing access controls and user management.
- Managing privileged access and user responsibilities.
- Monitoring techiques and auditing access to information assets.

Unit 4:

Operational Security and Incident Management:

- How to implement controls for secure operations.
- Managing secure configuration and change management.
- Ensuring the protection of information during operations.
- Incident management and response procedures.
- Business continuity planning and disaster recovery.

Unit 5:

Compliance, Audit, and Continual Improvement:

- Ensuring compliance with legal, regulatory, and contractual requirements.
- Conducting internal and external audits of information security controls.
- Monitoring and reviewing compliance with ISO/IEC 27002 standards.
- Implementing corrective and preventive actions.
- Continually improving the effectiveness of information security controls.