€TRAINING

Information Security Management System ISMS

Information Security Management System ISMS

Introduction:

In today's digital landscape, security of information assets is crucial for organizations. With the increasing volume and complexity of cyber threats, establishing robust measures to safeguard sensitive information has become imperative. ISO/IEC 27001 provides a framework to ensure the confidentiality, integrity, and availability of information assets. This training program ISMS provides a comprehensive framework for organizations to address these challenges effectively, and it offers guidelines and best practices for establishing, implementing, maintaining, and continually improving an Information Security Management System.

Program Objectives:

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

- Recognize the significance of ISO/IEC 27001 in enhancing organizational information security.
- Plan and establish an effective Information Security Management System ISMS.
- Perform key security controls and risk mitigation measures within an ISMS framework.
- Maintain and continuously improve the ISMS to align with organizational changes and compliance needs.
- Develop robust incident management and response procedures to address security threats.

Targeted Audience:

- Information Security Professionals.
- IT Managers and Professionals.
- Compliance Officers.
- Risk Management Professionals.
- Consultants.
- Business Owners and Managers.

Program Outlines:

Unit 1:

Introduction to ISO/IEC 27001:

- Understand the importance of information security management.
- Explore the key principles and requirements of ISO/IEC 27001.
- Recognize the benefits of implementing an ISMS.
- Identify common misconceptions about ISO/IEC 27001.
- Learn about the role of ISO/IEC 27001 in organizational security frameworks.

Unit 2:

Establishing an ISMS:

- Learn how to plan and initiate the implementation of an ISMS.
- Identify stakeholders and define the scope of the ISMS.
- Develop policies, procedures, and controls to address information security risks.
- Establish roles and responsibilities for ISMS implementation.
- Determine the resources required for implementing an ISMS.

Unit 3:

Implementing an ISMS:

- How to implement security controls and measures to mitigate risks.
- Processes of monitoring, measuring, and evaluating the effectiveness of the ISMS.
- Techniques for developing documentation to support the ISMS implementation.
- Learn how to conduct risk assessments and treatment activities.

Unit 4:

Maintaining and Improving an ISMS:

- Develop strategies for continuous improvement of the ISMS.
- Importance of regular reviews and audits to ensure compliance and effectiveness.
- Techniques for monitoring changes in the organization and updating the ISMS accordingly.
- Engage top management in the maintenance and improvement of the ISMS.

Unit 5.

Incident Management and Response:

- Incident response plan development and procedures.
- Establish roles and responsibilities for managing and responding to security incidents.
- How to conduct post-incident analysis and implement measures to prevent recurrence.
- Importance of training personnel on incident management procedures.
- Ensure regular review and update of the incident response plan and procedures.