ISO 27035 Information Security Incident Management

Duration: 2 Days

COURSE DESCRIPTION

This session is designed to provide participants with a comprehensive understanding and practical skills in implementing the frameworks outlined in ISO/IEC 27035-1:2023 and ISO/IEC 27035-2:2023 for effective information security incident management. The course format includes a series of hands-on activities where attendees will develop incident management policies, create response plans, and utilize tools and playbooks for managing security incidents.

COURSE OBJECTIVES

Attendees will achieve:

- An in-depth understanding of ISO/IEC 27035-1 and 27035-2 standards for incident management.
- Competencies in developing and implementing robust incident management policies and plans.
- Proficiency in using detection tools, establishing reporting mechanisms, and applying incident response playbooks.
- Enhanced ability to analyze incidents, manage escalation processes, and foster continuous improvement within their organizations.

COURSE OUTLINE

Day 1: Introduction to Incident Management and Planning

Morning Session: Introduction and Fundamentals

- **Overview:** Course introduction, overview of ISO/IEC 27035-1 & 27035-2, and discussion on the importance of structured incident management.
- Interactive session on developing incident management policies, with a focus on integration with corporate governance.

Afternoon Session: Planning and Preparation for Incident Management

- Hands-on creation of an incident response plan template, detailing clear processes and responsibilities.
- Development of escalation flows and priority criteria for various types of incidents using practical scenarios.

Day 2: Incident Detection, Response Tools, and Continuous Improvement

Morning Session: Detection Systems and Reporting Mechanisms

- Configuration of detection tools and establishment of reporting formats and protocols.
- Implementation and testing of incident reporting templates to ensure alignment with management policies.

Afternoon Session: Response Strategies and Learning from Incidents

- Application of incident response playbooks to real-world scenarios to determine actions and resource allocations.
- Analysis of a case study to extract lessons, identify improvements, and refine the incident response playbook.

Closing and Evaluation

- Comprehensive review of the course, emphasizing the practical application of content covered.
- Discussion on the implementation of learned techniques and strategies in participants' organizations.

- Recommendations on further resources for continuous learning and development in the field of incident management.

This course emphasizes practical, hands-on training, where participants engage actively with real-world scenarios and tools to master the nuances of information security incident management. By the end of the training, participants will be equipped with the necessary skills and knowledge to effectively manage and respond to security incidents, significantly enhancing their organizations' security posture.

WHO SHOULD ATTEND

- IT Managers and Security Managers
- Incident Response Team Members
- Risk Assessment and Management Professionals
- Information Security Consultants
- System and Network Administrators