ISO/IEC 27035 Information Security Incident Management

Course Outline

Module 1: Introduction to ISO/IEC 27035
- Overview of ISO/IEC 27035 and its importance
- Role of incident management in information security
- Relation to other ISO/IEC standards (e.g., ISO/IEC 27001)

Module 2: Incident Classification and Identification
- Identifying and classifying information security incidents
- Incident categorization and severity assessment
- Early warning signs and indicators

Module 3: Incident Response Planning
- Developing an incident response plan
- Establishing an incident management team
- Legal and regulatory considerations

Module 4: Incident Handling and Response
- Incident handling phases (preparation, detection, containment, eradication, recovery, lessons learned)
- Escalation procedures and decision-making during an incident
- Coordinating response efforts

Module 5: Digital Evidence Preservation
- Preserving digital evidence during incident response
- Chain of custody and forensic considerations
- Legal admissibility of evidence

Module 6: Incident Reporting and Communication
- Internal and external incident reporting requirements
- Communicating with stakeholders, including regulatory bodies and law enforcement
- Managing public relations during incidents

Module 7: Post-Incident Analysis and Lessons Learned
- Conducting post-incident analysis and root cause analysis
- Lessons learned and continuous improvement
- Updating incident response plans based on findings

Module 8: Case Studies and Best Practices
- Real-world examples of effective incident management
- Best practices from organizations with mature incident response programs

Module 9: Action Plan and Implementation
- Developing an action plan for implementing ISO/IEC 27035 practices within

participants' organizations
- Steps to initiate and sustain effective incident management practices

Module 10: Q&A and Course Evaluation
- Opportunity for participants to ask questions and seek clarification
- Course evaluation and feedback collection