Day 1 : Introduction to Information Security Incident Management concepts as recommended by ISO/IEC 27035

- Course objectives and structure
- Standards and regulatory frameworks
- Information Security Incident Management
- ISO/IEC 27035 core processes
- Fundamental principles of Information Security
- Linkage to business continuity
- Legal and ethical issues

Day 2 : Designing and preparing an Information Security Incident Management plan

- Initiating an Information Security Incident Management Process
- Understanding the organization and clarifying the information security incident management objectives
- Plan and prepare
- Roles and functions
- Policies and procedures

Day 3 : Enacting the Incident Management process and handling Information Security incidents

- Communication planning
- First implementation steps
- Implementation of support items
- Detecting and reporting
- Assessment and decisions
- Responses
- Lessons learned
- Transition to operations

Day 4 : Monitoring and continual improvement of the Information Security Incident Management plan

- Further analysis
- Analysis of lessons learned
- Corrective actions
- Competence and evaluation of incident managers
- Closing the training

Day 5 : Certification Exam