

Lead Security Incident professional

Schedule of the Training Course

Duration: 04 Days

Course Agenda and Contents -

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

- Fundamental concepts of Information security and its associated Standards & frameworks.
- Introduction of Information Security Incident Management concepts.
- Relation between Information security Incident Management and Business continuity.
- Processes of ISO/IEC 27035 and related ethical & legal issues.

Day – 2: Designing and preparing an Information Security Incident Management Plan.

- Planning and preparation of Information Security Incident Management Process.
- Establishing the context and develop understanding of Information Security Incident Management objectives.
- Policies and Procedures for the successful Information security incident management plan.
- Developing understanding of functions of security Incident Management Plan.

Day – 3: Implementing the Incident Management process and handling Information Security incidents.

- Steps in implementation of Information security Incident Management process.
- Planning and execution of Communication, Responses and Reporting.
- Assessing and decision-making process.
- Lessons Learned.

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

- Competence testing and evaluating performance of incident managers.
- Developing insights on Monitoring, Corrective actions, and Continual improvement of the Information Security Incident Management plan.
- Closing of training program.

*****End of Document*****