



Information Security Management

Course Introduction:

An overview of functions relevant to management-oriented security focus. While information has become more easily accessible and readily available, the associated risks and security threats have not only increased in number, but also complexity. As a result, the importance of ensuring that an enterprise's information is protected has also increased. It is now more important than ever for executives to ensure that their IT security managers have the expertise needed to reduce risk and protect the enterprise. This comprehensive course provides participants with the knowledge and tools to design, develop, implement and manage an effective security management program.

Course Objectives:

- Participants will learn how to establish and maintain an IT governance framework aligned with business objectives, identify and manage information security risks, and develop and manage a capability to respond to and recover from disruptive and destructive information security events.
- Builds on technical security skills.
- Provides a strong base for building a successful career in managing information security.
- Focuses on managing security, including development and implementation of best practices

Who Should Attend?

- Information security practitioners
- Information security consultants
- Information security managers

Course Outline:

Information Security Governance

- Information Security Manager's Responsibility
- Information Security Governance
- Governance Owner / Sponsor
- Review of Key Security Concepts
- Information Security Governance – Specific Tasks
- Info Security Strategy
- Align Information Security Strategy with Corporate Governance
- Governance Components
- Business Case for Information Security
- Legal and Regulatory Issues

- Drivers Affecting the Organization and Their Security Impact
- Management Commitment
- The Security Organization – Roles
- COBIT Security Baseline
- Communication & Reporting Channels
- Security Steering Committee

Information Risk Management

- Information Security Risk Management
- NIST 800-30: Risk Assessment Activities
- Risk Management – Specific Tasks
- Information Asset Classification
- Developing a Risk Management Program
- Risk Management Standard
- Organization Risk Profile
- Risk Assessment Process
- Alternative Approach to Risk Management
- Business Impact Assessments
- Threat & Vulnerability Evaluations
- Mitigation Strategies and Prioritization
- Integration Into Life Cycle Processes
- Security Baselines as an Alternative
- Risk Management Reporting

Information Security Program Development

- Information Security Program Management – Tasks
- Information Security Manager Responsibilities
- Alignment with Assurance Programs
- Security Resources
- Security Architectures
- Information Security Policy
- Security Policy Framework
- Security Awareness Program
- IT Procedures and Guidelines
- Business Process Procedures and Guidelines
- Information Security Baseline
- Security Metrics

Information Security Program Management

- Information Security Management – Specific Tasks
- Manage Internal and External Security Resources
- Security Due Diligence Activities
- Liaison Activities with Service Providers
- Ensure Processes and Procedures Comply With Policy and Standards
- Procedures / Rules of Use
- Security Controls Needed in Contracts
- Controlling Outsourcer Security
- System Development / Acquisition
- Security Advice and Guidance
- Security Design Services
- Security Awareness Training
- Vulnerability and Penetration Testing
- Security Logging and Monitoring
- Non-Compliance Issues

Incident Management & Response

- Response Management – Overview & Tasks
- Security Incidents
- Escalation and Communication Processes
- Incident Response Plans
- Incident Investigations
- Live Response
- Forensics
- Integrate Incident Response with BCP
- Key DRP/BCP Steps
- Response and Recovery Teams
- Testing
- Response Management

Course Fees:

To be advice as per course location. This rate includes participant's manual, Hands-Outs, buffet lunch, coffee/tea on arrival, morning & afternoon of each day.

Course Methodology:

A variety of methodologies will be used during the course that includes:

- (30%) Based on Case Studies
- (30%) Techniques
- (30%) Role Play
- (10%) Concepts
- Pre-test and Post-test
- Variety of Learning Methods
- Lectures
- Case Studies and Self Questionnaires
- Group Work
- Discussion
- Presentations

Course Certificate:

International Center for Training & Development (ICTD) will award an internationally recognized certificate(s) for each delegate on completion of training.

Course Timings:

Daily Course Timings:

08:00 - 08:20	Morning Coffee / Tea
08:20 - 10:00	First Session
10:00 - 10:20	Coffee / Tea / Snacks
10:20 - 12:20	Second Session
12:20 - 13:30	Lunch Break & Prayer Break
13:30 - 15:00	Last Session