

Course Title

IT Risk Management

Course Introduction

The ability to accurately analyse, assess and manage the risk to business information systems has always been the central issue in information security. The increasing emphasis on corporate governance, and compliance with standards such as ISO 27001 and BS 25999, has further underlined the importance of knowing and managing risk. This course helps the candidates to understand the overall concept of Risk Management and then managing the IT or information risks.

Target Group

- Security and risk management practitioners involved in the practical implementation of risk analysis and management for information systems.
- Business managers and risk decision makers who need a good understanding of information risk analysis, assessment and management disciplines in order to make business risk decisions aligned with corporate governance principles.

Course Duration

3 days (8 hours/day)

Learning Level

Advanced



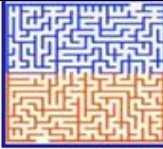
Course Objectives

The aim for this course is:

- To help the attendees to form an understanding on the overall concept of Risk Management with an emphasis on IT Risk Management
- To clearly deliver the different aspects of Risk Management such as Assets management, Qualitative, Quantitative Risk management etc.,
- To make the attendees understand the Business Impact Analysis.
- To provide the candidates with different Risk Treatment options, Monitoring and Controlling of Risks.

This course will also equip delegates with the skills to:

- Carry out a business impact analysis (BIA)
- Carry out a threat & vulnerability assessment
- Identify risks that require treatment and recommend suitable controls
- Produce a Risk Report and Treatment Plan for business managers
- Produce (or improve) an Information Classification scheme.



Course Outline

Controlling Access to Information Systems

- Control Data Access
- Control System Access
- Determine an Access Control Administration

Networking Systems and Telecommunications

- Design Data Networks
- Provide Remote Access to a Data Network
- Secure a Data Network
- Manage a Data Network

Defining Security Management

- Determine Security Management Goals
- Classify Information
- Develop a Security Program
- Manage Risk

Creating Applications Security

- Perform Software Configuration Management
- Implement Software Controls
- Secure Database Systems

Performing Cryptography

- Apply a Basic Cipher
- Select a Symmetric Key Cryptography Method
- Select an Asymmetric Key Cryptography

Securing System Architecture

- Evaluate Security Models
- Choose a Security Mode
- Provide System Assurance

Executing Operations Security

- Control Operations Security
- Audit and Monitor Systems
- Handle Threats and Violations



Performing Business Continuity Planning

- Sustain Business Processes
- Perform Business Impact Analysis
- Define Disaster Recovery Strategies
- Test the Disaster Recovery Plan

Applying Physical Security

- Control Physical Access
- Monitor Physical Access
- Establish Physical Security Methods
- Design Secure Facilities

Applying Law, Investigations, and Ethics

- Interpret Computer Crime Laws and Regulations
- Apply the Evidence Life Cycle

Contact Us

Phone: 09712 4456466
Fax: 0971 2 4456656
Email: bhavani@nbizinfosol.com
Mobile: 0506156289