IT and Information Risk Management Training Course for Bankers

COURSE CONTENT

Course Objectives Download

This 2-day, practical hands-on training workshop is designed for IT Risk managers and IT practitioners who deal with the complexities of developing an IT risk management programme in order to reduce IT infrastructure and process cost, and at the same time, quantify and prioritise IT risk for bringing it under control. The objective is to provide attendees with the necessary perspective, knowledge and skills to understand the essential elements and benefits of applying effective IT risk management and to learn how it assists:

- Management in ensuring that the appropriate resources are effectively applied in order to achieve the mission
- Users in ensuring that proper controls are applied to address integrity, confidentiality, and availability of the IT systems and data that they own
- IT professionals in promoting IT policy adherence and maintain security of the IT systems

COURSE CONTENT

1. **Determining the need for information risk management**
   - Use of IT risk management in an organisation
   - Importance & application of IT risk management
   - Regulatory framework governing IT risk management
   - Clarify when IT risk management should be used
2. **Establishing the context of risk in the business**
   - Why businesses must take account of risk
   - Business benefits of IT & information risk management
   - Determine the consequences of no IT & information risk management
3. **Overview of the IT & information risk management requirements stipulated by the relevant International Frameworks & Standards**
   - ISO 27001 Information Security Standard
   - COBIT IT Governance Framework with specific reference to:
     - PO9
     - DS4
     - DS5
   - BS 25999 Business Continuity Management Standard
   - PAS 77 IT Service Continuity Standard

4. **Reviewing information & IT & information security fundamentals**
    - Concept of confidentiality
    - Principle of integrity
    - Concept of availability
    - Analyze terms such as accountability, non-repudiation, authenticity, identification & reliability
    - Theory of information assurance
5. **Developing an IT risk management strategy**
    - Perform a high-level risk assessment
    - Establish the business risk appetite & criteria for risk acceptance
    - Verify the business information security requirements
    - Assess the industry or sector legal & regulatory requirements
    - Determine the appropriate IT risk categories & information classification scheme for information systems
    - Identify the relevant industry or sector IT risk management standards
    - Establish the critical methods of treating risk
    - Back testing action plans
6. **Examining the purpose of IT risk management, risk assessment & risk treatment**
    - IT risk management & ownership
    - What is risk assessment?
    - Understanding the concept of risk treatment
7. **Evaluating the impact of IT risk on your organization's assets**
    - Identify various types & the value of tangible assets
    - Examine various types & the value of intangible assets
8. **Outlining IT risk management terminology**
    - Assess the meaning of:
        - Threats & hazards
        - Vulnerabilities & proximity
        - Likelihood or probability
        - Risk
        - Controls
        - Risk treatment
        - Risk reduction
        - Risk transfer
        - Risk avoidance
        - Risk acceptance (tolerance)
9. **Setting the scope**
    - Determine the overall scope of an IT risk management framework
    - Establish the limits of the scope
10. **Conducting a business impact analysis**

- Identify the parties involved in a business impact analysis
- Assess the relevant approach for the type of organization & event/incident
- Differences between qualitative & quantitative analyses
- Generic business impact analyses
- Application of property loss control
- Formulate a business interruption cost in terms of confidentiality, integrity & availability
- Applications of cost of failure analyses
- What is 'worst-case scenarios' analysis
- Conduct a business impact analysis

11. Assessing all threats & vulnerability

- Differences between threats & hazards
- Common threats & hazards
- How to determine potential threats
- How to identify potential vulnerabilities
- What is the motivation for threats & the responsibility for causing them
- Relevant criteria for assessing probability
- Indicate a suitable impact / likelihood scale
- Analyze statistical or historic data to predict likelihood
- Perform a threat & vulnerability assessment

12. Determining a risk response strategy

- How to apply a risk matrix
- Quantify the results of a risk assessment
- Identify the key risks for treatment & those that will be accepted

13. Applying IT risk management controls

- Identify suitable controls to treat the key risks from the previous matrix
- Using best practice frameworks, e.g. COBIT, ISO 27001 & PAS 77 considering appropriate controls
- Advantages & disadvantages of root cause analysis
- Types of controls appropriate for people, physical, procedural & technical

14. Adopting IT risk management methodologies

- Analyze IT risk management tools
- Use the appropriate IT risk management tool
- Differences between qualitative & quantitative analyses
- Generic business impact analyses
    - Key threats & vulnerabilities
    - Recommended remedial action

15. 15.Creating a risk reporting plan

- Reporting requirements on an IT risk management program
- Produce various reports
  - Important areas of risk
  - Key business impacts

16. Developing a decision-making process

- Risk acceptance
- Risk avoidance
- Risk transfer
- Risk reduction
- Risk register

17. Applying a risk treatment process

- Appropriate requirements for managing the risks identified
- Assess business continuity & disaster recovery as additional methods of treating risk
- Differences between qualitative & quantitative analyses
- Produce a treatment plan to:
  - Review selected controls
  - Agreement of actions
  - Establishment of ownership
  - Accountability & responsibility
  - Setting of realistic time scales
  - Gaining business approval

18. Implementing a risk monitoring process

- Undertake periodic reviews
- Apply ongoing reporting of the IT

Risk management status

1. Analyzing the classification process

- Understand the importance of IT & information classification
- Explain the process for identifying & documenting IT assets
- Understand the verification process through the interviewing of information owners
- Apply a process of confidentiality, integrity & availability in the development of an IT classification scheme
- Explain the requirements for a periodic review of information & its classifications
- Examining classification issues
- Determine requirements for setting information classification
- Evaluate appropriate information storage
- Assess appropriate information disposal, transfer, transmission & processing

2. Typical classification schemes

- Determine the main differences between various classifications
- Identify similarity & meaning of terms depending on the classification scheme in use
- Assess the importance of handling sensitive information from another organization
- Understand the differences between standard information classification schemes
- Create an information classification scheme for confidential & strictly confidential information