

# IT and Information Risk Management Training Course



Are you effectively securing your organisation's IT systems that store, process, or transmit organisational information?

Is your IT risk management plan tailored to the specific risk profile of your business and being coordinated across all functional and business units?

Research has shown that IT Risk is an area that no-one really wants to take responsibility for – the IT Managers believe that it is an audit function, and the internal auditors believe that it is an IT function...however, your stakeholders require that your data is secure and that all possibilities for fraud are minimised and that any potential loopholes are closed.

With the release of King II and IT Governance frameworks, requirements for risk management and new international standards entering the market, the pressure is mounting to ensure that all your IT risks are identified and the necessary action is taken – be this to mitigate them, accept or ignore them. So, how safe is your IT system? What are the risks that your organisation is being exposed to?

The solution to this challenge is to establish an effective risk management process that protects the organisation, not just its IT assets, and provides it with the ability to perform its mission. Risk management is the process of identifying and assessing risk and taking preventive measures to reduce it to an acceptable level. However, it is critical that you develop an effective risk management programme that assesses and mitigates risks within your IT systems and better manages these IT-related mission risks.

As an IT manager or head of an organisational unit, you are also expected to minimise any potential negative impact on your organisation by implementing a risk management process that identifies the appropriate controls for providing the mission-essential security capabilities.

## Course Objectives

This 3-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

## Who will benefit?

- IT Risk and Security Managers
- IT Technology and Systems Managers
- IT Auditors
- IT Operations Managers
- IT Project Managers



## What you will learn

On completion of the course, delegates will be able to:

- Determine the importance & application of IT risk management
- Successfully establish the steps for developing an IT risk management strategy
- Manage risk treatment & assessment
- Conduct an business impact analysis
- Assess all threats & vulnerabilities in order to create a risk response strategy
- Effectively apply risk control measures
- Examine & identify information classification schemes

## About the Trainer

**Maiendra Moodley** is a former Technical Security Advisor within the Infrastructure Renewal and Service Delivery Division of the Business Systems and Technology department at the South African Reserve Bank. He is currently a partner at a well-known consulting company. Maiendra's professional experience includes having served as a senior systems auditor and a security architect with a leading retail bank, supervising IT LAN support services, to being a panellist and examiner on the IT program of a national tertiary institution. Other positions that he has held range from serving as a trainee accountant to a senior risk consultant. He is presently studying for his Masters in Security Studies at the University of Pretoria and is a member of the American Society of Industrial Security and a former Director of the Computer Society of South Africa.

## **Course Content**



### **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

### **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

### **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

### **Reviewing information & IT & information security fundamentals**

- Concept of confidentiality
- Principle of integrity
- Concept of availability
- Analyse terms such as accountability, non-repudiation, authenticity, identification & reliability
- Theory of information assurance

### **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

### **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

### **Evaluating the impact of IT risk on your organisation's assets**

- Identify various types & the value of tangible assets
- Examine various types & the value of intangible assets

### **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)

### **Setting the scope**

- Determine the overall scope of an IT risk management framework
- Establish the limits of the scope

### **Conducting a business impact analysis**

- Identify the parties involved in a business impact analysis
- Assess the relevant approach for the type of organisation & 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

### **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
- Analyse statistical or historic data to predict likelihood
- Perform a threat & vulnerability assessment

## **ANALYTIX**

MLC House • 1st Floor • 50 Sixth Road • Hyde Park • 2196

PO Box 413988 • Craighall • 2024

www.analytix.co.za • info@analytix.co.za

## Course Content (Continue)



### **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

### **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

### **Adopting IT risk management methodologies**

- Analyse IT risk management tools
- Use the appropriate IT risk management tool
  - Key threats & vulnerabilities
  - Recommended remedial action

### **Creating a risk reporting plan**

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

### **Developing a decision-making process**

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

### **Applying a risk treatment process**

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

### **Implementing a risk monitoring process**

- Undertake periodic reviews
- Apply ongoing reporting of the IT risk management status

### **Analysing 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

### **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 organisation
- Understand the differences between standard information classification schemes
- Create an information classification scheme for confidential & strictly confidential information

### **In-house Training**

All Analytix Courses are available in-house, should your organisation have a number of people or multiple sets to train. The cost advantages & the ability to discuss & resolve organisational issues are two major attractions of such training.

### **Consulting services**

Analytix also offers consulting services to support the implementation of IT and Information Risk Management programmes.

Other services include Corporate and IT Governance, ISO 27001 compliant ISMS implementation, IT maturity assessments, security certification assistance & performance management.

## **Register Today**

**Tel: 0861 ANALYTIX or 0861 262 598**

**Fax: +27 (011) 447 4192**

**Email: [info@analytix.co.za](mailto:info@analytix.co.za)**

**Web site: [www.analytix.co.za](http://www.analytix.co.za)**

### **ANALYTIX**

MLC House • 1st Floor • 50 Sixth Road • Hyde Park • 2196

PO Box 413988 • Craighall • 2024

[www.analytix.co.za](http://www.analytix.co.za) • [info@analytix.co.za](mailto:info@analytix.co.za)