



# Institute of Risk Management

## Information Systems Risk

### Syllabus and Detailed Learning Outcomes

#### Overall Module Aims

To provide a clear, well-structured and interesting treatment of why and how organisations are vulnerable to loss, destruction, damage, unauthorised access and misuse of business information (BI). The textbook will provide a logical path through the understanding of BI threats, attacks and consequences, controls and countermeasures to the establishment of a proactive and professional BI culture. Formal, manual and computer-based and informal information systems will be considered as will the common business information technologies.

#### The Organisational Context

- Describe the main features of an organisation and describe common organisational purposes
- Able to analyse organisational environments using the PESTLE framework
- List the main elements of organisation structure and identify key managerial roles.
- Discuss theories on corporate strategy – what it is and how it may be developed
- Understand key theories on decision-making
- Identify the need and mechanisms used in organisations to co-ordinate and control people at work.

#### Business Information Systems

- Explain how information management delivers value to an organisation
- Identify the relationship between data, information and knowledge
- Describe and evaluate information quality in terms of its characteristics
- Identify systems and their components and identify what is meant by an information system
- Classify types of Business Information System
- Identify how information is used in business, particularly in support of decision-making, control and co-ordination
- Specify which components of a communications system are necessary to exchange information
- Within and between businesses; explain the basic components and terminology of networks, including the internet; identify the benefits available through the introduction of computer networks and explain the broad implications of the internet on the marketplace

- Describe the role of information technology in organisational activities explaining how information, information systems and IT support the attainment of competitive advantage.

### **Organisational Risk Management**

- Discuss the meaning and components of risk and related constructs
- Identify sources and types of business risk
- Determine why it is important for organisations to consider risk
- Explain the Risk Management Process
- Contrast different ways of handling business risk at the strategic level.
- Identify sources of new risk theory, standards and codes
- Appreciate methods used to control / prevent business risk
- Explain what Business Continuity Management (BCM) is and describe the BCM process.

### **Security – An Introduction**

- Describe what is meant by security
- Explain the relevance of confidentiality, integrity, availability and trust to business
- Identify common security controls, countermeasures and technologies
- Explain the concept of access control in the physical, procedural and logical control sense
- Explain the concept of layered security and discuss security control strategies that blend access control and surveillance techniques to protect organisations.

### **Business Information Risk – Threats, Hazards & Vulnerabilities**

- Identify common business information risks
- Describe BIR threats
- Explain why organisations are vulnerable to BIR's
- Discuss the concept of hazard in relation to the way organisations may use information to conduct business.

### **Business Information Risk – Controls and Countermeasures**

- Identify common methods to reduce the likelihood of BIR
- Identify how BIRs may be controlled upon and following loss in a manner seeking to reduce business harm
- Compare and contrast a range of IS security technologies
- Discuss the product security process and explain the benefits of building security into product design
- Review the need to control BIR and the purpose of controls and countermeasures.

### **Business Information Risk Management**

- Discuss The application of the risk management process to the problem of managing business information systems risk
- Discuss techniques for identifying and assessing business information systems risk
- Appreciate the importance of judgement in the processes of risk assessment and control selection
- Appreciate factors impacting BIS risk decision making in organisations
- Explain how organisations may develop strategies to manage BIR.

### **Business Information Risk – Codes, Standards & Legislation**

- Identify key sources of knowledge about BIR
- Describe the impact of legislation on BIR

- Compare and contrast a range of general risk management standards
- Discuss the content of a selection of Information Security Risk Standards
- Identify information security best practice.

### **Software – Business User Risks**

- Describe the components of a database
- Understand the importance of databases to business and how to secure and protect them
- Describe the concepts of a database integrity
- Describe the common risks associated with the use of business software and databases.

### **The Digital Organisation & Information Security**

- Identify what is meant by the digital organisation
- Appreciate why organisations are making greater use of internet technologies
- Compare and contrast the internet, intra and extranets from an information risk perspective
- Describe the major threats to computer networks
- List the common security technologies, controls and countermeasures used to protect internet technologies
- Compare and contrast the information security requirements of the traditional and digital organisation.

### **The Risk & Security Organisation**

- Compare and contrast different risk and security roles and responsibilities in organisations
- Evaluate different options for structuring organisational risk and security resources when considering BIR
- List the common information system security roles and responsibilities
- Compare and contrast operational and strategic security roles
- Review different modes of operation as an organisational risk specialist
- Discuss the implications of empowerment, autonomy, decentralisation and organisational culture as contextual factors influencing security organisation and decision making.

### **The Risk & Security Aware Organisation**

- Identify what is meant by organisational and professional culture
- Explain what is meant by a security culture
- Discuss the advantages and disadvantages of security awareness initiatives
- Identify how a security culture may be developed
- Discuss employee loyalty, motivation and commitment and explain their relevance to BIR exposure and control.