Chapter 4

About Me

- Raniel Misra (SM AGSA)
- CISA
- Member of the ISF and ISACA
- Family man and crazy about running and cricket

Chapter 4

- What can you tell me about it?

- What do you think are key?

- Why is Chapter 4 important?

- How can I help?

- Set your targets like running a marathon….

- Make sure you practice….

- Never give up….

- Gain an understanding by reading…..

- Gain knowledge of the Core

- Practice….

Information systems operations and support

Information Systems Operations

- Management of IS Operations
- Infrastructure support including computer operations
- Technical support/ helpdesk
- Scheduling
- Controlling input/ output of data
- Quality assurance
- Change control and release management
- Configurations management
- Program library management system and control software
- Problem management procedures
- Performance monitoring and management
- Capacity monitoring and planning
- Management of physical and environmental security
- Information security management

Information systems hardware

- Computer hardware components and architectures
- Hardware maintenance program
- Hardware monitoring procedures
- Capacity management

IS Architecture and Software

- Operating systems

- Access control software

- Data communications software

- Data management

- Database management systems

- Tape and disk management systems

- Utility programs

- Software licensing issue

IS Network Infrastructure

- Enterprise network architectures
- Types of networks
- Network services
- Network standards and protocols
- LAN/WAN and Network models
- Network administration and control
- Applications in the networked environment

Chapter 5

Introduction

- Addresses key components that ensure confidentiality, integrity and availability (CIA) on information Assets.

- The chapter evaluates design, implementation and monitoring of logical and physical access controls to ensure CIA.

- The chapter also evaluates network security, environmental controls and processes and procedures used to store, retrieve, transport and dispose of confidential assets.

- The chapter describes the various methods and procedures followed by organizations and focuses on the auditors role in evaluating these procedures.

Importance of Information Security Management

- Key elements of information security management
  - Senior management commitment and support
  - Policies and procedures
  - Organization
  - Security awareness and education
  - Monitoring and compliance
  - Incident handling and response

Importance of information security management

- Information security management roles and responsibilities
  - IS security steering committee
  - Executive management
  - Security advisory framework
  - Chief privacy officer
  - Chief information security officer
  - Process owners
  - External parties
  - Security administrator
  - Security specialist
  - IT Developers
  - IS Auditors

Importance of information security management

- Inventory and classification of information assets

Effective control requires a detailed inventory of information assets

The inventory record of each information asset should include:

- A clear and distinct identification the assets
- Its relative value to the organization
- Its location
- Its security risk classification
- Its asset group
- Its owner
- Its designated custodian

Importance of information security management

- System access permission
- Mandatory and discretionary access controls
- Privacy management issues and the role of IS auditors
- Critical success factors to information security management
- Information security and external parties
- Third party agreements
- Computer crime issues and exposures
- Security incident handling and response

Logical access

- Logical access exposures (Data leaks, Viruses, Worms)
- Social Engineering
- Paths of logical access
- Logical access control software
- Identification and authentication
- Logon IDs and Passwords
- Token devices, One time passwords
- Biometrics
- Single sign on
- Authorization issues
  - Access control lists
  - Logical access security administration
  - Remote access security
  - Mobile technology
- Storing, retrieving, transporting and disposing of confidential information

Network infrastructure security

Communications networks (wide area or local area networks) generally include devices connected to the network as well as programs and files supporting the network operations.

- LAN Security
- Client Server Security
- Wireless security
- Internet threats and security
- Internet security controls
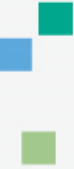- Firewall security systems
- Encryption

What are the types of audits?

Why would you audit?

Thank you
Presenter details: Raniel Misra
Contact details: ranielm@agsa.co.za