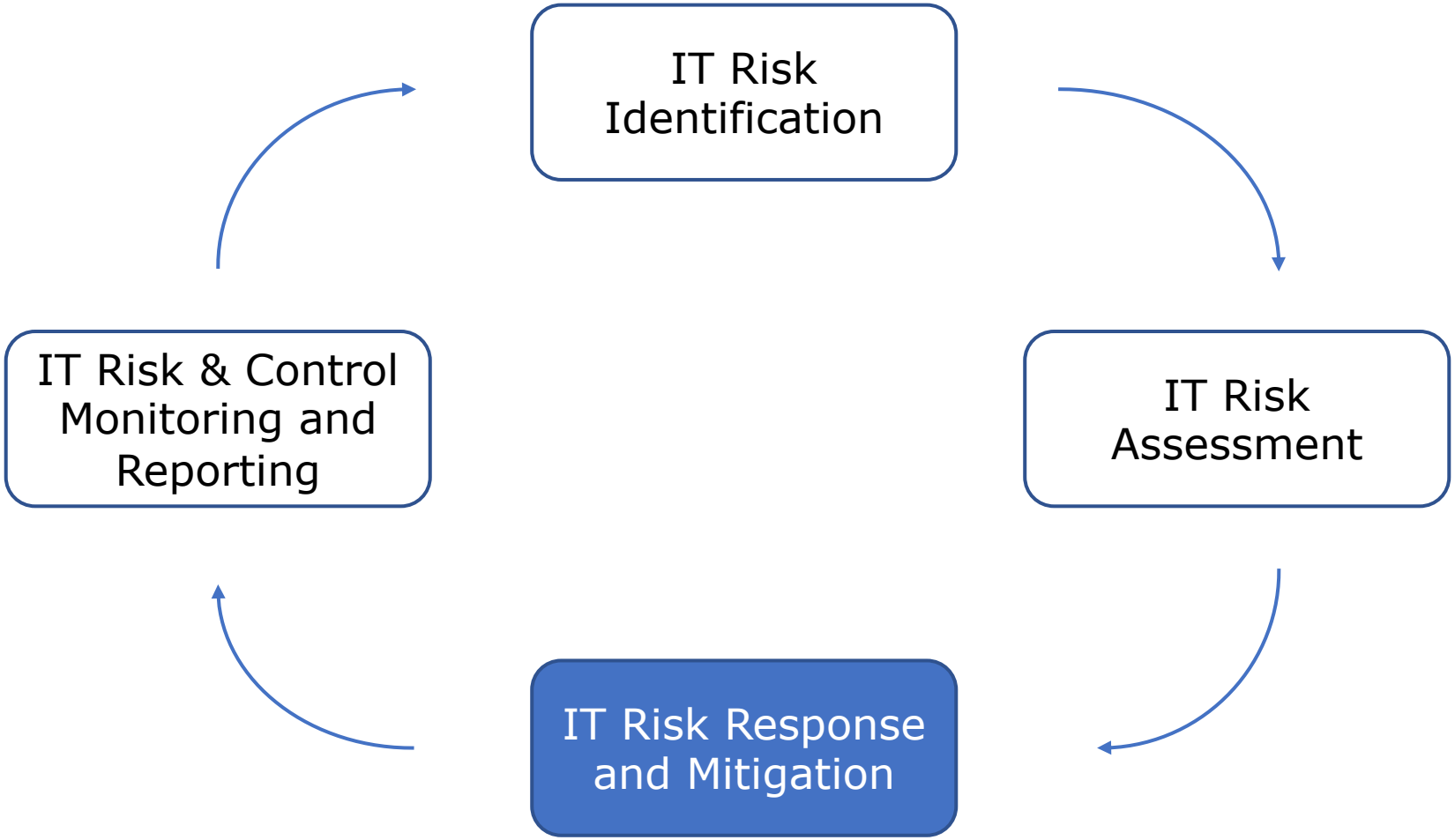
Chapter 3: IT Risk Response & Mitigation

IT 727-A & OL – Managing Cybersecurity Risk

Dr. Ibrahim Waziri Jr.

IT Risk Management Life Cycle



3.0 Overview & Objective

Overview:

- The risk response process requires management to make the decisions regarding the correct way to respond to, and address risk.

Objective:

- Develop risk action plan based on different risk response options
- Discuss the need for performing a cost benefit analysis when determining a risk response
- Define various parameters for risk response selection

3.1 Aligning Risk Response with Business Objectives

Risk response is based on the risk on the risk assessment report and risk register documented during the identification and assessment phase.

Management considers the recommendations from the report and register to:

- Determines best response
- Develops action plan
- Meet compliance requirements and business goals

3.2 Risk Response Options

- Risk Acceptance
- Risk Mitigation
- Risk Avoidance
- Risk Transfer (sharing)

3.3 Risk Response Analysis Technique

Risk Response Factors:

- Priority of risk
- Availability of controls
- Cost, etc.

Types of analysis:

- Cost Benefit Analysis
- Return on Investment (ROI)

3.4 Vulnerabilities Associated with New Controls

- A new lock may keep authorized people out
- A new control may fail resulting in denial of service
- A new control may present a new attack surface that could be exploited
- An unreasonable control may frustrate users and cause them to bypass the control

3.5 Developing a Risk Action Plan

Strategy and timeframe to address risk

3.6 Business Process Review – Tools & Techniques

Business Review Process steps:

- Document & evaluate current business processes
- Identify potential changes
- Schedule and implement changes
- Feedback and evaluation

3.7 Control Design and Implementation

Risk Mitigation is accomplished through the use of controls.

Control Groups:
- Managerial
- Technical
- Physical Controls

Control Types:
- Compensating
- Corrective
- Detective
- Deterrent
- Preventive

3.8 Control Monitoring and Effectiveness

SIEM

(Security Information and Event Management)

3.9 Types of Risk

- Inherent Risk
- Residual Risk
- Current Risk

3.10 Control Activities, Practices & Metrics

- Information Security
  - Change Control
  - System Authorization
  - Asset Inventory & Configuration Management
- Third Party Management
  - Managed Service Provider
  - Cloud Service Provider
- Data Management
  - Identity Management
  - Segregation of Duties
  - Job Rotations
  - Access Controls
  - Cryptography etc.

3.11 Systems Control Design & Implementation

- Testing
  - Application Testing
  - System Test
  - Network Test etc.

- Changeover (Go-Live)
  - Parallel Changeover
  - Phased Changeover
  - Abrupt Changeover

3.12 Impact of Emerging Technologies on Controls

- Unproven operations
- Undiscovered vulnerabilities
- New threat vectors
- Lack of skills and training
- Business interruption

3.13 Control Ownership

- Ownership of controls
- Ownership of risk response
- Ownership of risk response plans
- Ownership of reporting and compliance

Summary

- Be aware of risk
- Be aware of changes to risk
  - New threats
  - New vulnerabilities
  - Environmental changes
  - Changes in asset value
  - Changes in control effectiveness