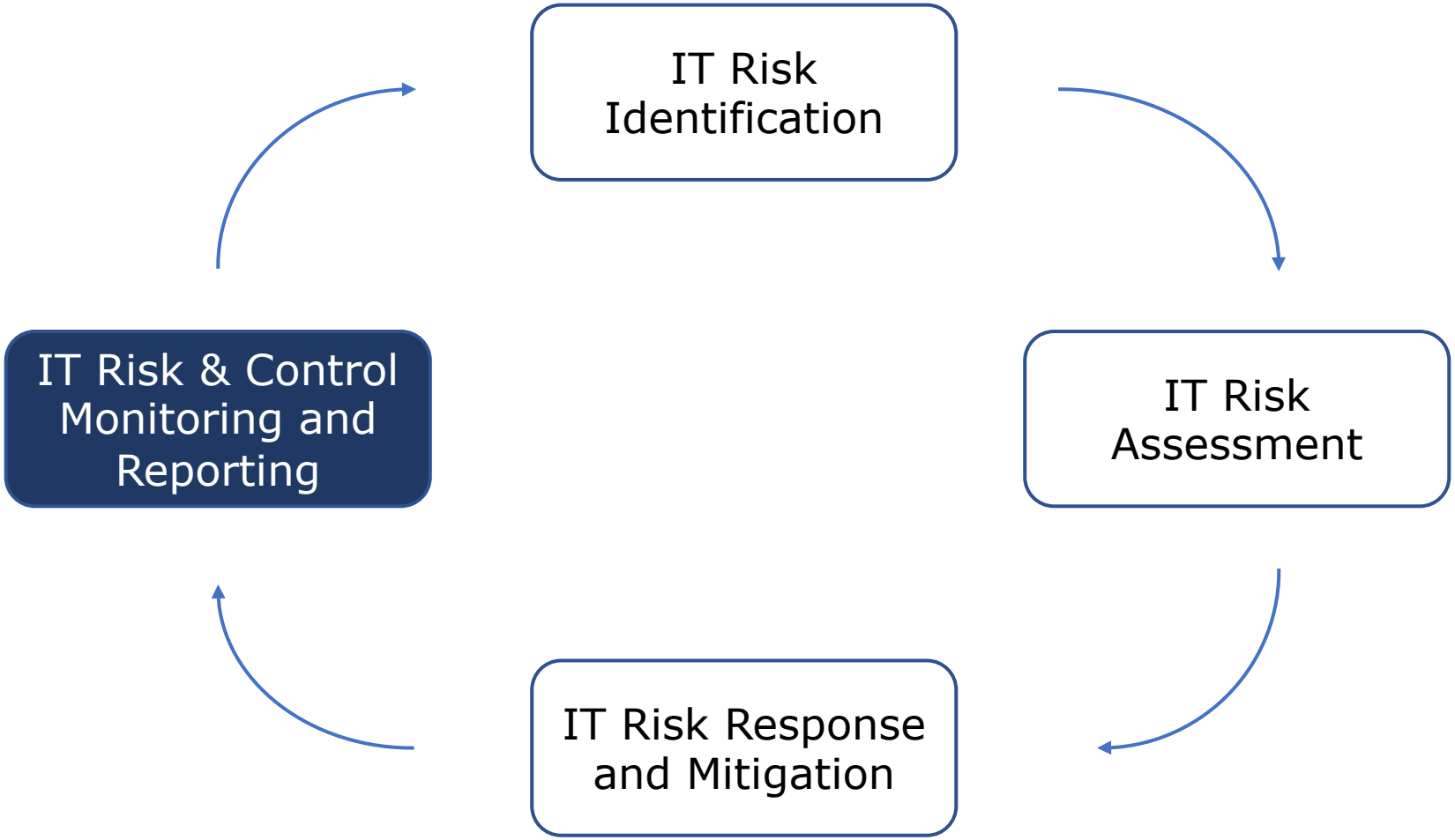
Chapter 4: Risk & Control Monitoring & Reporting

IT 727-A & OL – Managing Cybersecurity Risk

Dr. Ibrahim Waziri Jr.

IT Risk & Control Monitoring & Reporting



4.0 Overview & Objective

Continuously monitor and report on IT risk and controls to relevant stakeholders to ensure the continued efficiency and effectiveness of the IT risk management strategy and its alignment to business objectives.

4.1 Key Risk Indicators (KRI)

KRIs allow organizations to:
- Measure the level of risk
- Compare to risk thresholds
- Alert to risk reaching or approaching an unacceptable level of risk
- Tracking mechanism

KRI Selection:
- Select a meaningful set of controls to monitor
- Consistent areas to measure
- Good indicators of health of risk management program
- Areas that can be influenced by management

SMART Metrics
- **S**pecific
- **M**easurable
- **A**ttainable
- **R**elevant
- **T**imely

KRI Effectiveness:
- Impact
- Effort
- Reliability
- Sensitivity
- Repeatable

KRI Optimization:
- Sensitivity
- Timing
- Frequency
- Corrective Action

4.2 Key Performance Indicators

Examples of KPIs:

- Network Availability
- Customer Satisfaction
- Number of Resolved Complaints …

4.3 Data Collection and Extraction Tools & Techniques

Internal Data Sources :

- Prior Risk Assessment
- Project Documents
- Tickets
- Audit & Incident Reports
- Event & Activity Logs etc.

External Data Sources:

- Media Reports
- CERT & CIRTs
- Regulatory Bodies
- Peer Organizations etc.

4.4 Monitoring Controls

- Provide feedback to improve risk response
- Verify that controls are working correctly and mitigating risk

Monitoring Controls is a process that has six steps:

- Identify and confirm risk control owners and stakeholders
- Engage with stakeholders and communicate the risk and objectives for monitoring and reporting
- Align and continually maintain the information security monitoring approach with enterprise approach.
- Establish the information security monitoring process and procedure.
- Agree on a lifecycle management and change control process for information security monitoring and reporting.
- Request, prioritize and allocate resources for monitoring information security.

Types of Monitoring:

- Self-assessment
- Automated assessment
- Third party audits
  - Internal
  - External

4.5 Control Assessment Types

- Audits
- Vulnerability Assessments
- Penetration Test
- Third-Party Assurance

4.6 Results of Control Assessments

Maturity Model Assessments

Capability Maturity Model

5 Optimized
4 Predictable
3 Established
2 Managed
1 Performed
0 Incomplete

4.7 Changes to IT Risk Profile

Annual (or organization-defined) review of monitoring an reporting program

Summary

- Proper and effective management of risk is essential to protecting the assets of the organization.
- Risk management is a never-ending process.
- IT risk and controls should be monitored continuously to ensure that they are adequate and effective

Risk Management Framework - Complete