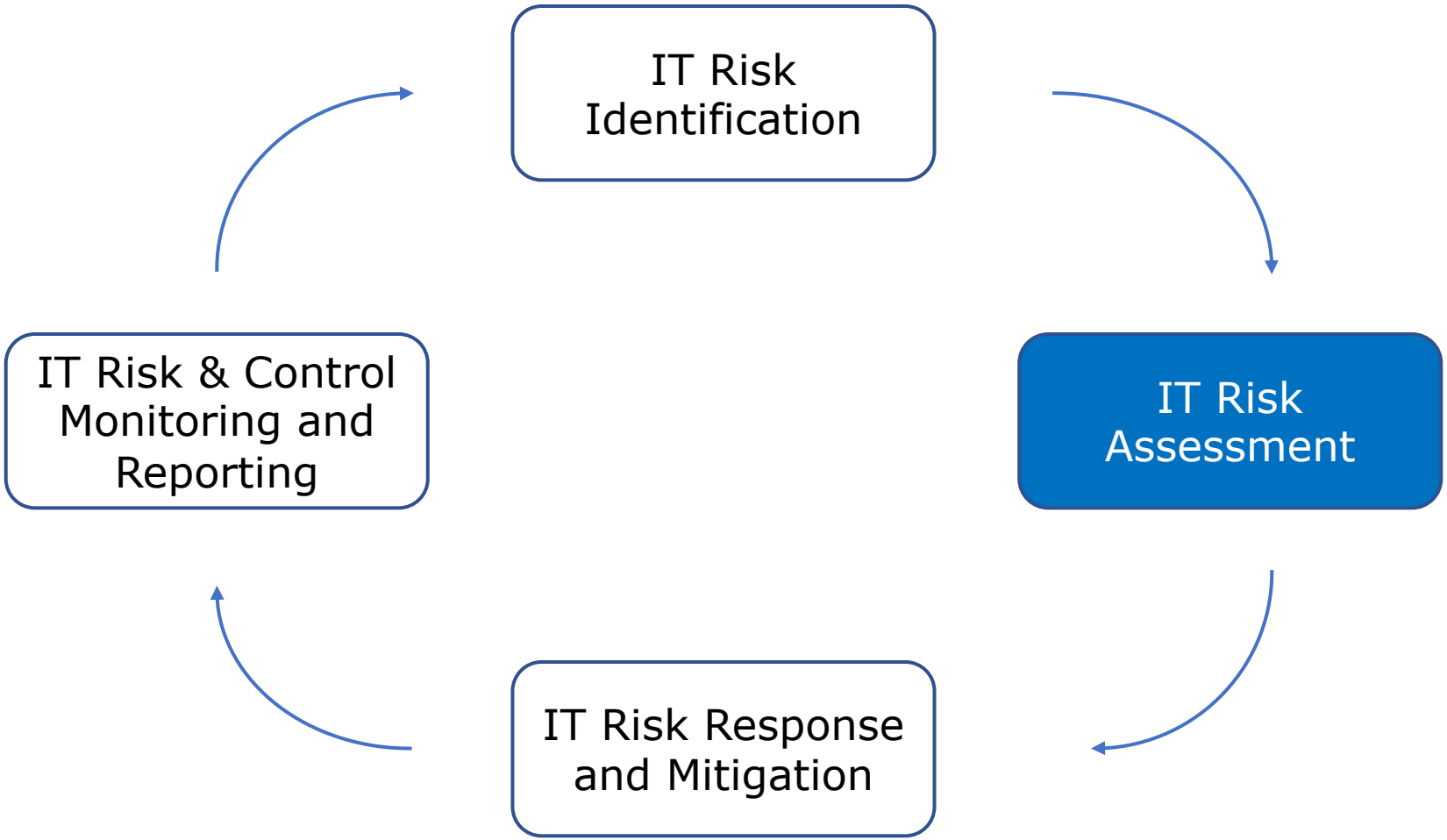
Chapter 2: IT Risk Assessment

IT 727-A & OL – Managing Cybersecurity Risk

Dr. Ibrahim Waziri Jr.

IT Risk Management Life Cycle



Recap: Risk Identification vs. Risk Assessment

Risk Identification	Risk Assessment
Identification of threats, vulnerabilities and assets	Evaluate the potential effect of risk
Risk Documentation	Evaluate probabilities of an adverse event
	Document critical business operations

2.0 Overview, Objective & Output

Objective:

- Identify and assess risk assessment techniques
- Analyze risk scenarios
- Identify current state of controls
- Assess gaps between current and desired state of the IT risk environment
- Communicate IT risk assessment results to relevant stakeholders
- Understand relationship between the risk and enterprise risk appetite and tolerance

Output:

- Information used to respond to risk in an appropriate and cost-effective manner.

2.1 Risk Assessment Techniques

- Bayesian Analysis
- Bow Tie Analysis
- Brainstorming/Structured or Semi-structured Interview
- Cause and Consequence Analysis
- Cause-and-effect Analysis
- Checklists
- Delphi Method
- Environmental Risk Assessment
- Event Tree Analysis
- Fault Tree Analysis
- Hazard Analysis and Critical Control Points (HACCP)
- Hazard and Operability Studies (HAZOP)
- Human Reliability Analysis (HRA)
- Layer of Protection Analysis (LOPA)
- Markov Analysis
- Monte Carlo Simulation
- Preliminary Hazard Analysis
- Reliability-Centered Maintenance
- Root cause Analysis
- Scenario Analysis
- Sneak Circuit Analysis
- Structured "What if" Technique (SWIFT)
- **Business Impact Analysis (BIA)**

2.2 Analyzing Risk Scenarios

During Risk Identification, risk scenarios are developed and used to identify and describe potential risk events.

- Organizational Structure and Culture
- Policies, Standards and Procedures
  - High-Level Policies
  - Functional Policies
- Architecture
- Technology
- Controls

2.3 Current State of Controls

Objectives:

- Ensure that controls were installed/implemented as designed
- Ensure that the controls are working correctly
- Ensure that the controls are producing the desired result
- Mitigating risk

Concerns:

- Misconfigured controls
- Lack of monitoring
- Wrong control
- Ability to bypass a control
- Lack of documentation

Categories of Controls:

- Preventive
- Deterrent
- Directive
- Detective
- Corrective
- Compensating

Controls Measurement

- Audit – Logs etc.
- Business Continuity Plans (DRPs)
- Capability Maturity Models Controlled Test
- Incident Reports
- IT Operation & Management Evaluation
- Enterprise Architecture Assessment
- Vulnerability Assessment & Penetration Test
- Third Party Assessments – External Audits, Compliance Verification

2.4 Changes In The Risk Environment

Emerging Technologies

Industry Trends

2.5 Project and Program Management

IT Projects fail for various reasons, including:

- Unclear or changing requirements
- Scope creep
- Lack of budget
- Lack of skilled resources
- Problems with technology
- Delays in delivery of supporting elements/equipment
- Unrealistic time lines (push to marketing)
- Lack of progress reporting

Lack of good **project management** can lead to:

- Loss of business
- Boss of competitive advantage
- Low morale among staff members
- Inefficient processes
- Lack of testing of new systems or changes to existing systems
- Impact on other business operations
- Failure to meet SLAs or contractual requirements
- Failure to comply with laws and regulations

System development and IT Project Support: SDLC – System Development Life Cycle

Phase 1: Initiation
Phase 2: Development or Acquisition
Phase 3: Implementation
Phase 4: Operation and/or Maintenance
Phase 5: Disposal

2.6 Risk and Control Analysis

- Data Analysis
  - Cause and Effect Analysis
  - Free fault Analysis
  - Sensitivity Analysis
- Threat and Misuse Case Modeling
- Root Cause Analysis
- Gap Analysis
- Predicting Risk

2.7 Risk Analysis Methodologies

Quantitative
- Monetary value of risk
- Cost of single risk event
- Frequency of risk events (usually calculated annually)
- Cost of risk averaged per year - Justifies cost of controls

Qualitative
- Scenario-based
- Non-monetary elements of risk
- Risk levels by identified by comparing likelihood with impact
  - Range of risk level (Very Low, Low, moderate, High, Very High)

Semi-Quantitative
- Combination of Quantitative and Qualitative risk methods – associates money with range of risk levels

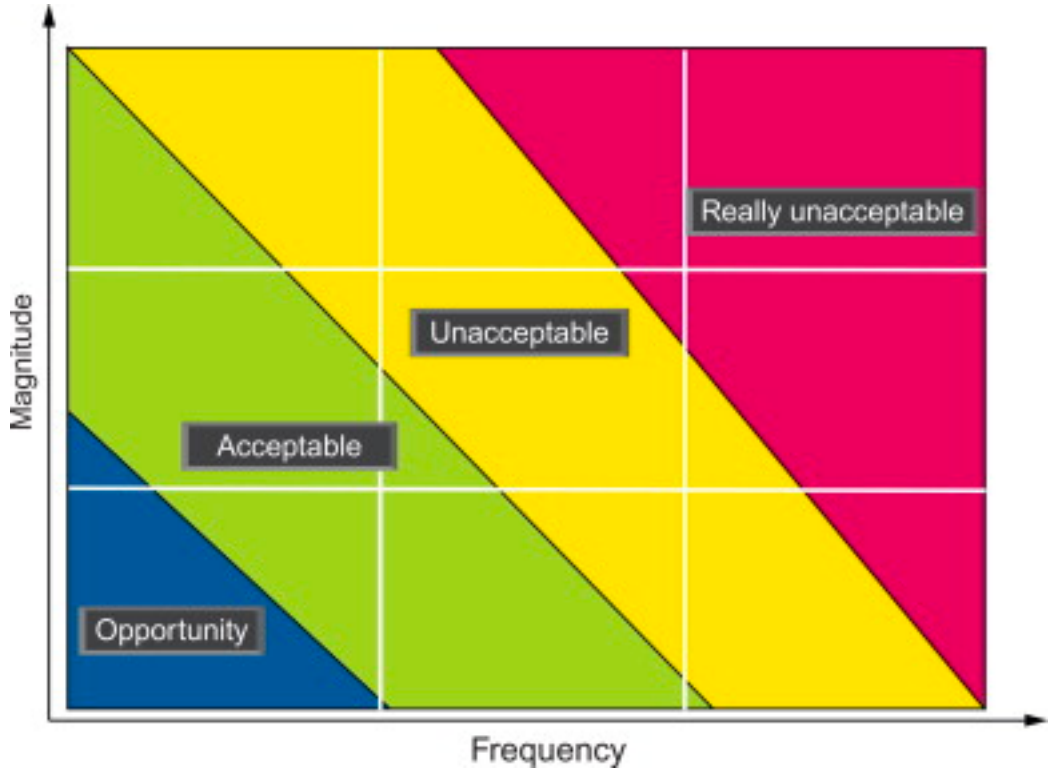
2.8 Risk Ranking

OCTAVE – Operationally Critical Threat Asset and Vulnerability Evaluation
Phases:

- Phase 1: Organizational evaluation
- Phase 2: Technological evaluation
- Phase 3: Strategy and Plan Development

Risk Appetite Bands:

- Risk within risk appetite is "acceptable"
- Risk outside of the risk appetite but within the risk tolerance is "unacceptable"
- Risk outside of the risk tolerance is "really unacceptable"



Risk Ownership –

- Links each risk to responsible individuals

2.9 Documenting Risk Assessment

Update the risk register with the risk assessment result

2.10 Summary

The risk practitioner must assess and determine the severity of each risk facing the organization.

All risk must be identified, assessed and reported to senior management.