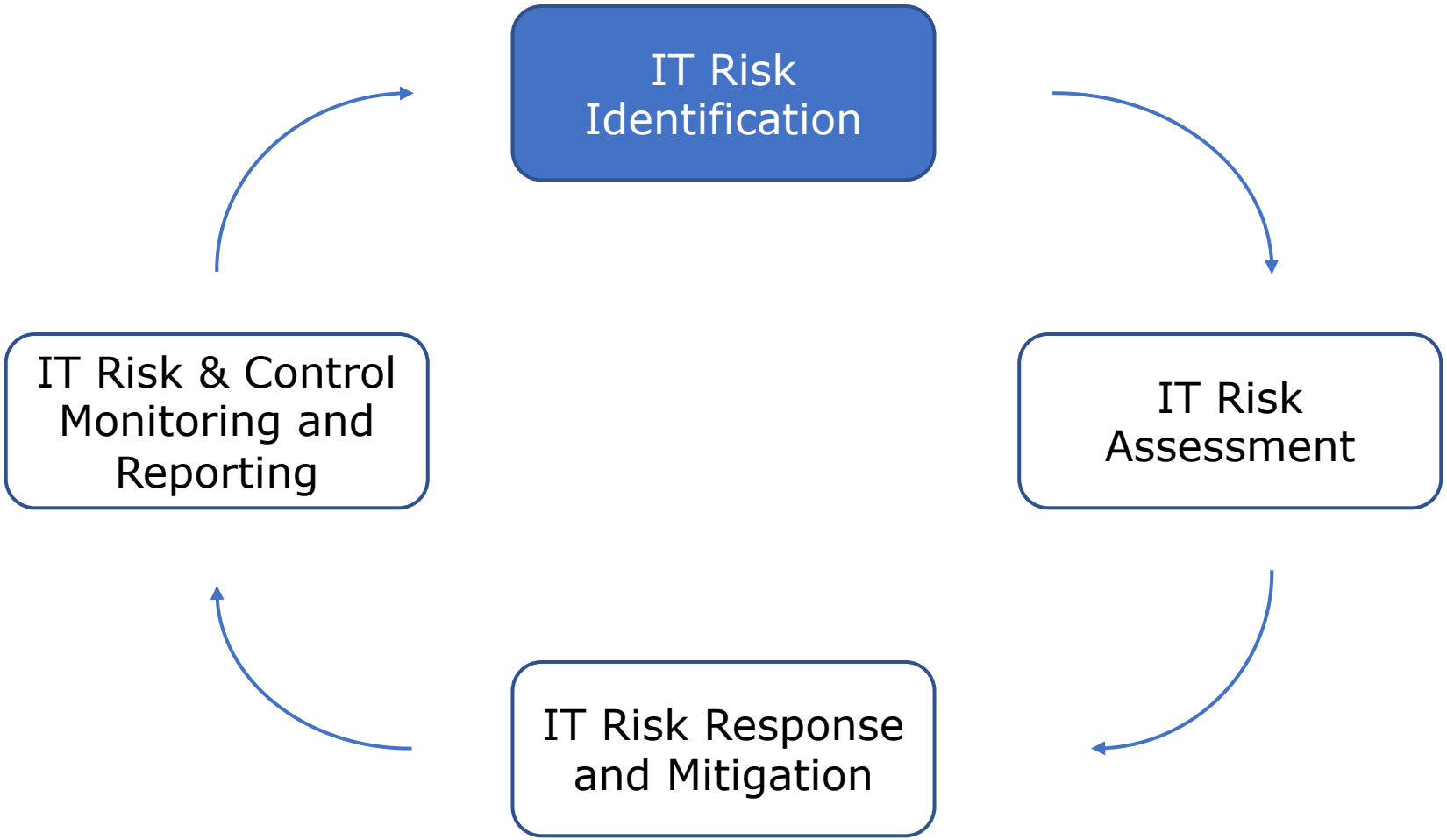
Chapter 1: IT Risk Identification

IT 727-A & OL – Managing Cybersecurity Risk

Dr. Ibrahim Waziri Jr.

IT Risk Management Life Cycle



Objective, Methodology & Output

Objective:

- To identify IT risk to assets being protected
- To enable IT risk management execution
- To support business objectives
- Understand consequences of risk events etc.

Output:

- List of risk scenarios with their consequences related to assets and business processes

1.1 Risk Capacity, Appetite & Tolerance

Risk Capacity: Objective amount of loss an enterprise can tolerate without its continued existence being called into question.

Risk Appetite: Number of standards and policies to contain the risk level within the boundaries set by the risk appetite.

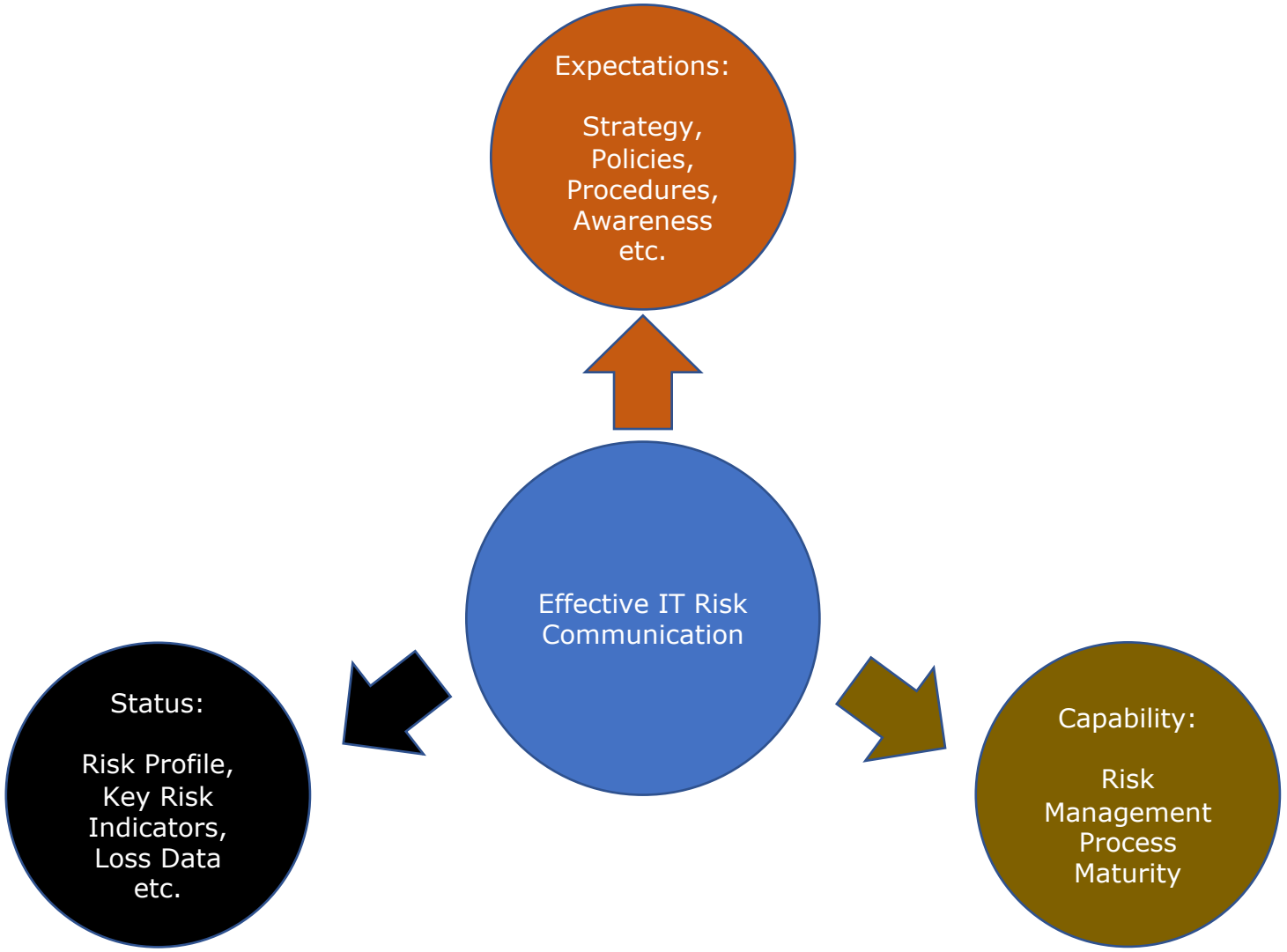
Risk Tolerance: Deviations from risk appetite (which are not desirable) but are known to be sufficiently below the risk capacity that acceptance of risk is still possible.

1.2 Risk Culture and Communication

Risk Culture: Willingness to embrace, cautiously accept or avoid risk

Elements of Risk Culture

1.2 Risk Culture and Communication



Risk Communication Components

1.3 Elements of Risk

Risk Factors	Vulnerabilities (Weakness)
• External Context • Internal Context • Risk Management Capabilities • IT-Related Capabilities	• Network • Physical • Technology (Cloud, Networks, Apps & Web-facing services • Supply Chain **Vuln Info Sources:** National Vulnerability Database (NVD), Open Web Applications Security Project (OWASP), Common Weakness Enumeration (CWE) **Testing:** Application Security Testing, Vulnerability Assessment, Penetration Testing
Assets	**Likelihood & Impact**
• People • Intellectual Property • Information • Brand • Reputation • Customers	Probability of risk event happening. • Motivation • Skill • Visibility • Impact on business, organization, asset etc.

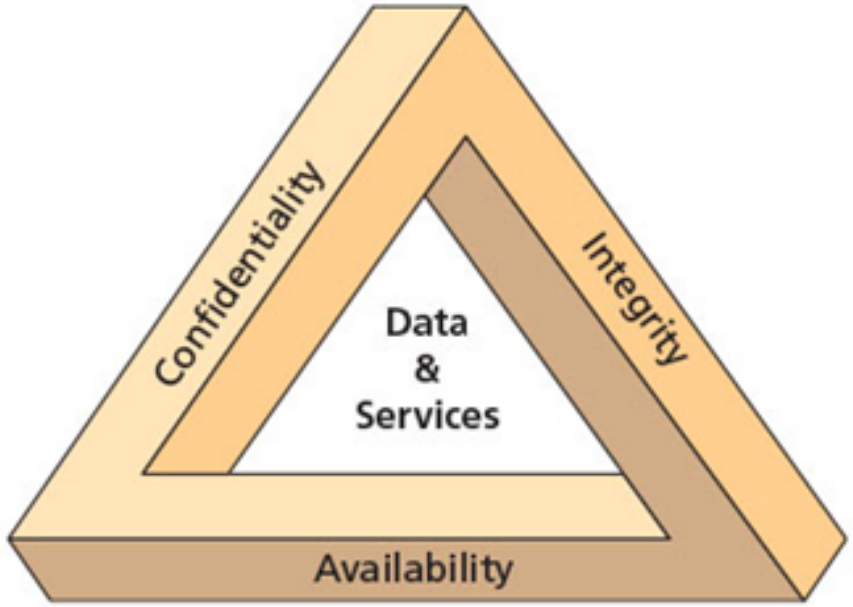
1.4 Info Sec Risk Concept & Principles

Confidentiality

Integrity

Availability

Nonrepudiation



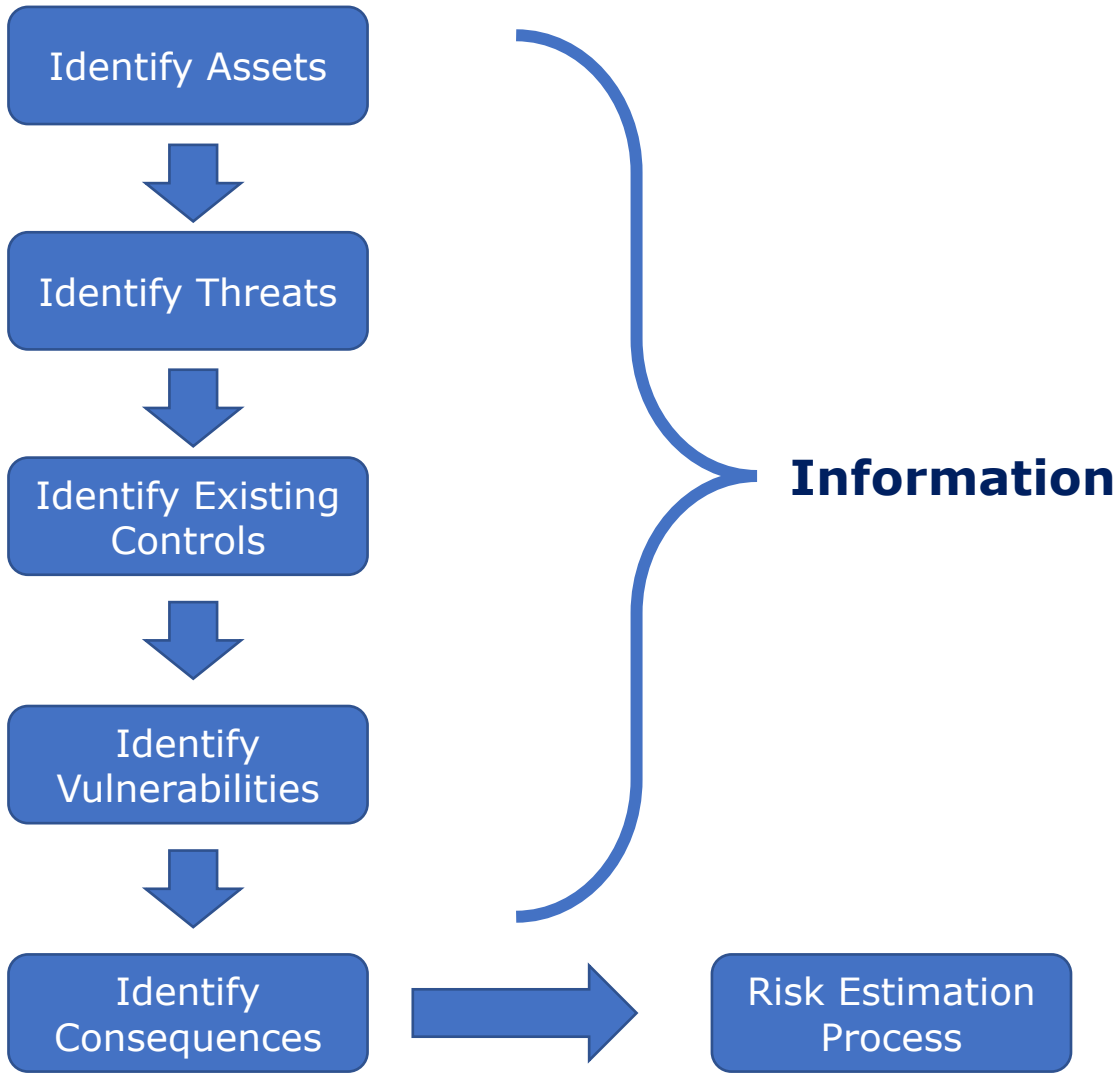
1.5 IT Risk Strategy of the Business

- Business-related IT Risk Types
- Senior Management support
- Alignment with Business goals and objectives
- Organizational structures
  - RACI (Responsible, Accountable, Consulted, Informed)
- Organizational Culture, Ethics and Behavior
- Laws, Regulations, Standards and Compliance
- Establish an approach to Risk Management
  - NIST 800-37
  - ISO 31000

1.6 IT Areas of Concern for the Risk Practitioner

- Hardware
  - CPU, Motherboards, RAM, ROM etc.
- Software (Applications)
  - Patches, API, Lack of IO Validations, Access Controls, SDLC etc.
- Operating Systems
  - Lack of interoperability, complexity
- Environmental Controls
  - Power, HVAC, Water, Secure Operational Areas
- Platforms & Topologies
  - Centralized, Peer-to-peer, middleware
- Networking Components
  - Cabling, Switches, Routers, Firewalls, Wireless Access Points etc.

1.7 Methods of Risk Identification



Risk Identification Process

Information Gathering

Historical

- What has happened previously

Systematic

- Expert opinion
- Examine a business process to identify possible points of failure
- Interviews

Inductive (Theoretical) analysis

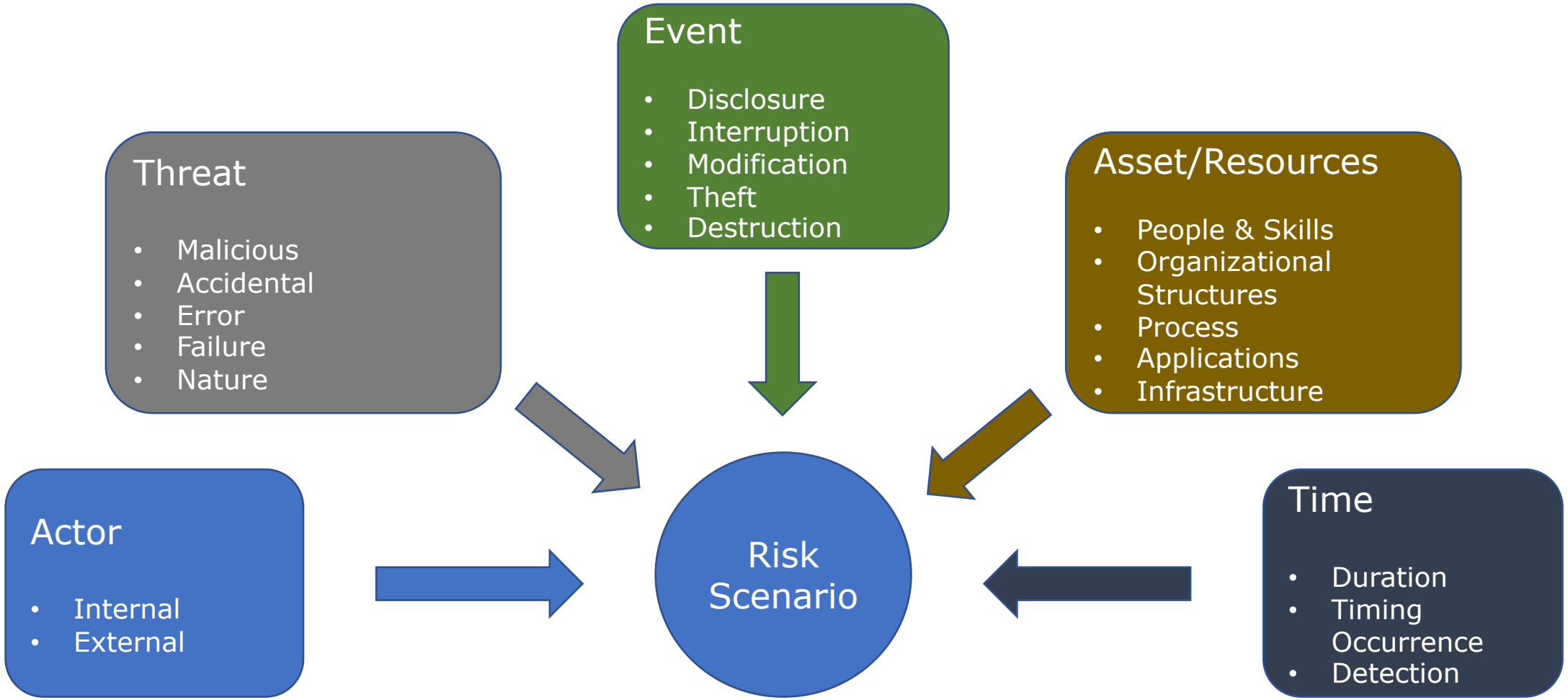
- New technology or process review to determine points of attack (e.g. PenTest)

Guides for Risk Classification

- COBIT 5 for Risk
- COSO
- ISO 31000
- NIST SP800-39
- ISO 27005
- NIST 800-30

1.8 IT Risk Scenarios

Risk scenario is a description of an IT-related event that can lead to a business impact.



Risk Scenario Structure

1.9 Ownership, Accountability & Responsibility

Ownership

- Accept or deny risk

Accountability

- Ensure risk is owned and managed

Responsibility

- Handle risk, update risk register, etc.

1.10 IT Risk Register

Document and track all identified risk in one place. IT Register consolidates all information about risk into one central repository

- Risk ID
- Description
- Risk Owner
- Risk Scenario (Actor, Threat Type, Event, Asset/Resource, Timing)
- Risk Category
- Impact
- Risk Response Types
- Response Owner
- Response Description

1.11 Risk Awareness

- Ensure risk is understood and well-known
- IT risks are identified
- The enterprise recognizes and manages risk
  - Risk Factors
  - Risk Impacts
  - Risk Controls

1.12 Summary

- The risk practitioner must ensure that is risk is identified in order to support the following steps of risk assessment and response
- Requires understanding business goals, management priorities and operational risks
- Creation of risk register

?

What is the purpose of Risk Identification?

VALUE