

# Information and Network Security

Information Security Governance and  
Risk Management

# Agenda

- Basic Concepts
- Types of Controls
- Risk Analysis and Management
  - Quantified Risk Analysis
  - Risk Management Strategies
- Other Functions of Domain

# Basic Concepts of Information Security

- Asset
- Vulnerability
- Threat
- Threat Agent
- Exposure Factor/Impact
- Risk
- Control/Counter Measure/Safeguard

- Asset
  - Anything that is of value for an organization
  - E.g. Information, Software, Hardware, Human
- Vulnerability
  - A weakness /defect in a system or absence of a safeguard
- Threat
  - A threat is a potential danger for an Asset
  - Its an event that if happen will adversely affect an Asset

- Threat Agent
  - The entity which causes threat to happen is threat agent.
  - E.g. an intruder in a system, Malware, Nature
- Exposure Factor/Impact
  - Percentage of asset loss caused by threat
- Risk
  - Likelihood of threat agent exploiting a vulnerability and its impact on asset
  - Risk ties the likelihood, vulnerability and threat to the resulting business impact.

# Security Controls

- Control/Safeguard/Counter Measure
  - A control is implemented to mitigate the Risk.
  - E.g. Fire Extinguisher, Password Policy, Firewall
- **Types of Controls**
  - **Physical Controls**
    - Guards, Identity Badges, Smoke Detector etc
  - **Logical Controls**
    - Administrative Controls
      - Policies and Procedures
    - Technical Controls
      - Firewall, IDS, Antivirus, Port Binding etc.

# Administrative Controls

- Policy
  - A policy is a general statement produced by senior management that dictates what role security will play in organization or what is acceptable and not acceptable generally.
  - Policies are usually broad documents that require procedures to implement them.
- Standards
  - A standard refer to mandatory activities, actions or rules.
  - E.g. ISO 9001, ISO 27001 etc.

# Policies, Procedures, Baselines, Guidelines

- Baselines
  - The term baseline refers to a point in time that is used as a comparison for future changes.
  - Baselines are also used to define the minimum level of protection required.
  - In security, specific baselines can be defined per system type, which indicates the necessary settings and the level of protection being provided



# Guidelines

- Guidelines are recommended actions and operational guides.
  - Industry best practices falls in this category

# Types of Controls (Functionalities)

- Deterrent
- Preventive
- Corrective
- Recovery
- Detective
- Compensating

# Control Functionalities

- Six different control functionalities are as follows:
  - **Deterrent** Intended to discourage a potential attacker
  - **Preventive** Intended to avoid an incident from occurring
  - **Corrective** Fixes components or systems after an incident has occurred
  - **Recovery** Intended to bring the environment back to regular operations
  - **Detective** Helps identify an incident's activities and potentially an intruder
  - **Compensating** Controls that provide an alternative measure of control

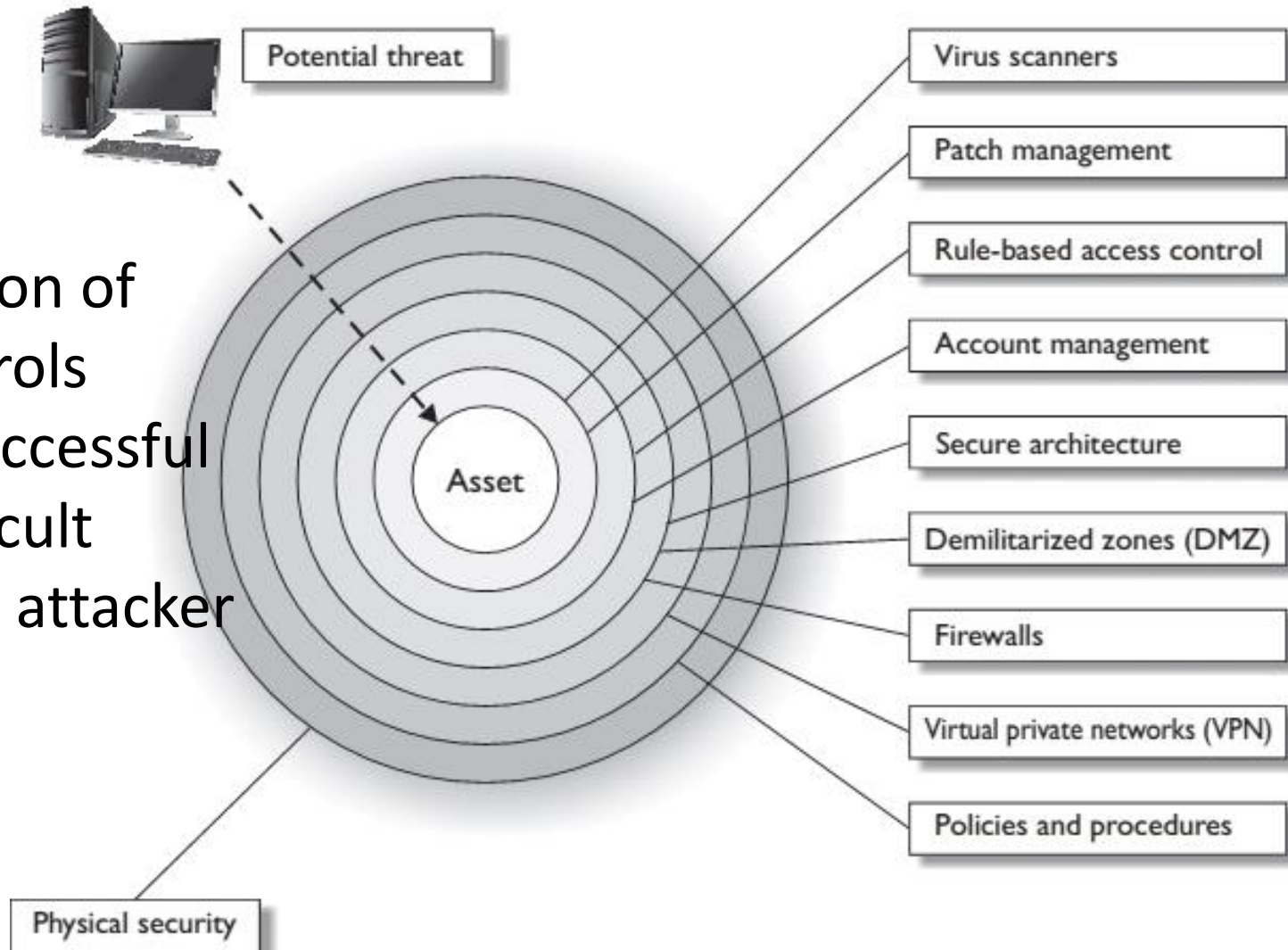
# Control Functionalities

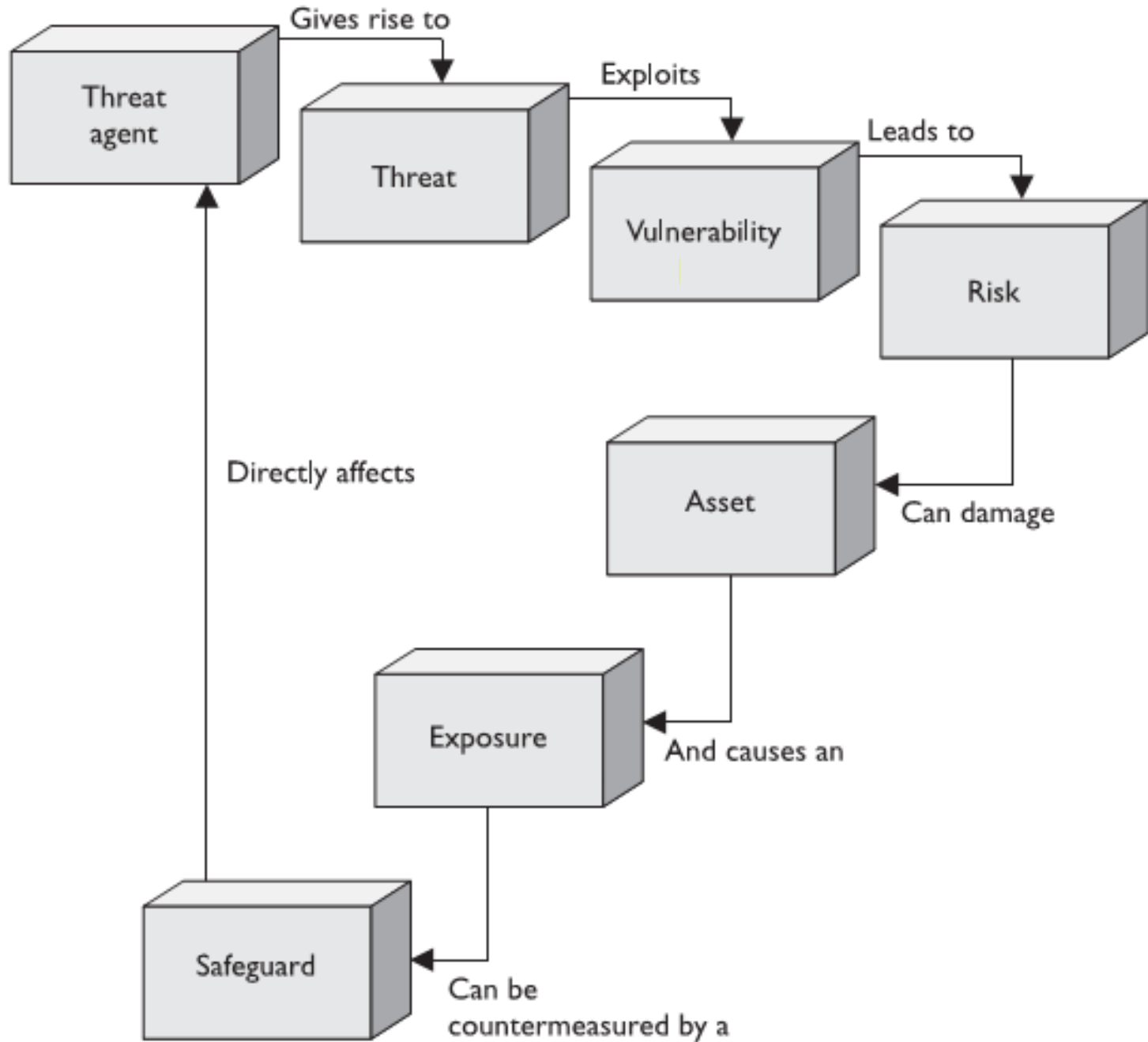
- Preventive: administrative
  - Policies and procedures
  - Effective hiring practices
  - Pre-employment background checks
  - Controlled termination processes
  - Data classification and labeling
  - Security awareness
- Preventive: Physical
  - Badges, swipe cards
  - Guards, dogs
  - Fences, locks, mantraps
- Preventive: Technical
  - Passwords, biometrics, smart cards
  - Encryption, secure protocols, call-back systems, database views, constrained
  - user interfaces
  - Antimalware software, access control lists, firewalls, intrusion prevention system

# Defense in Depth

Controls are implemented in layers to ensure defense in depth.

Implementation of multiple controls so that the successful breach is difficult to achieve for attacker



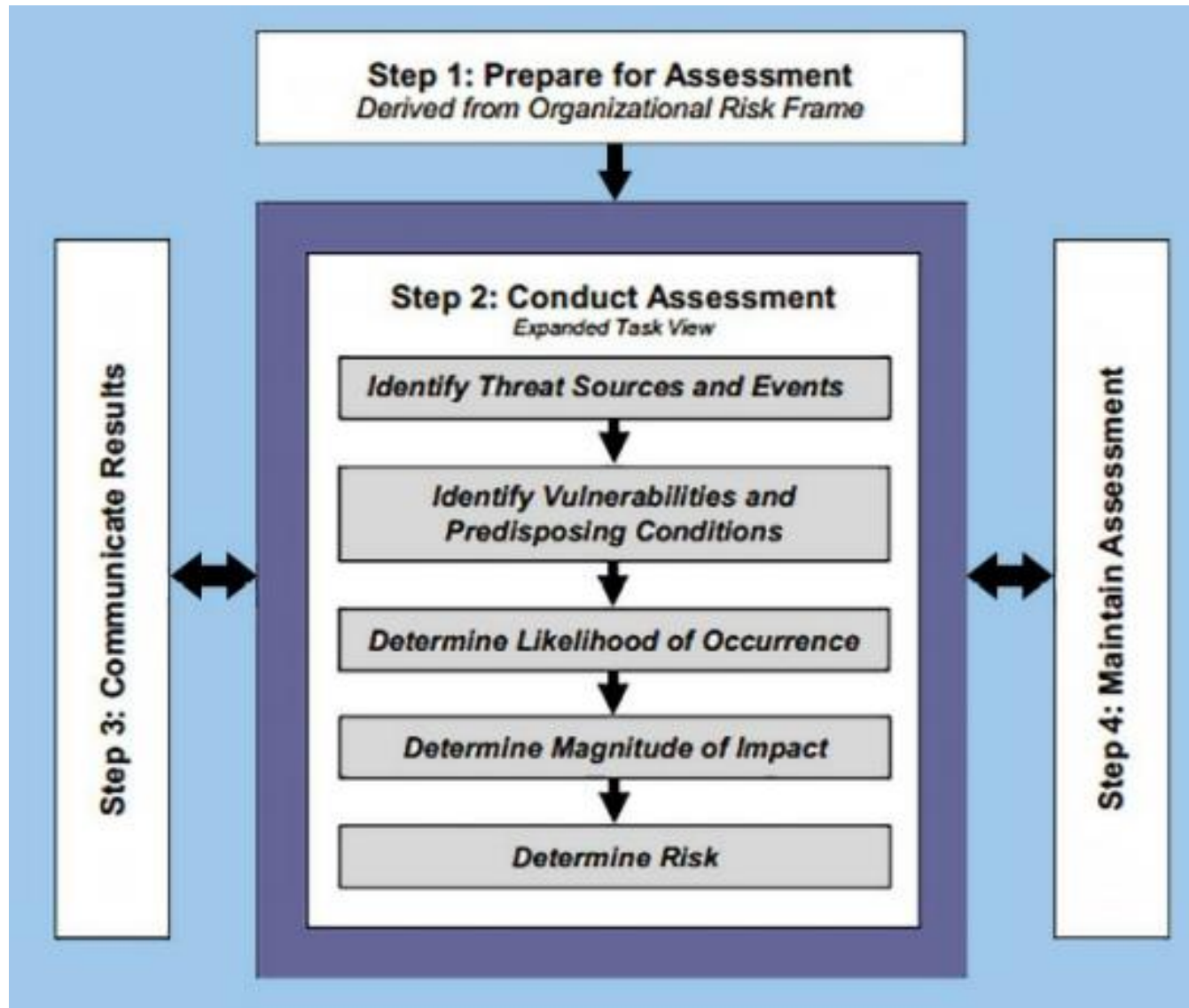


**Relationship between discussed concepts**

# Risk Analysis and Management

- Risk
  - Risk is the likelihood of occurrence of a threat and the damage it causes to the assets.
- Risk = *Likelihood of occurrence of a threat x Impact*

# NIST Risk Assessment Framework





# Risk Analysis

- Before Managing Risk, you have to analyze what risks are prevalent to your organization.
- A Risk analysis consist of four phases:
  - 1. Asset Identification**
  - 2. Vulnerabilities and Threats to Assets**
  - 3. Quantified Likelihood of threat and its impact on asset**
  - 4. Cost of Countermeasures**
- Risk Analysis provides a cost/benefit comparison of Risk and cost of countermeasure

# Quantified Risk Analysis

- The objective is to assign dollar value to risk.
- **SLE**
  - defined as the difference between the original value and the remaining value of an asset after a single impact of a threat.
  - **SLE** = asset value (in \$) × exposure factor as a %
- **ARO**
  - Measures the likelihood of threat
  - an estimate of how often a threat will be successful in exploiting a vulnerability over the period of a year
- **ALE**
  - $ARO * SLE$
- Once we have a value of Risk, we can decide how we want to manage risk.

- **Cost benefit analysis (CBA)** Also known as an economic feasibility study, the formal assessment and presentation of the economic expenditures needed for a particular security control, contrasted with its projected value to the organization.
- **single loss expectancy (SLE)** In a cost-benefit analysis, the calculated value associated with the most likely loss from an attack. The SLE is the product of the asset's value and the exposure factor.
- **exposure factor (EF)** In a cost-benefit analysis, the expected percentage of loss that would occur from a particular attack.
- **annualized rate of occurrence (ARO)** In a cost-benefit analysis, the expected frequency of an attack, expressed on a per-year basis.
- **annualized loss expectancy (ALE)** In a cost-benefit analysis, the product of the annualized rate of occurrence and single loss expectancy.

# Risk Management Strategies

- Risk Acceptance
- Risk Avoidance
- Risk Transfer
- Risk Mitigation

# Other Functions of Information Security Management

- Personnel Security
  - Properly hiring and managing personnel
- Security Awareness and Trainings
- Security Monitoring and Audits

# Information Security Auditing

- Verification of implementation and Proper working of control
- Auditing is performed against some benchmark i.e. Standard or Guidelines
  - E.g. ISO 27000 Information Security Management System requirements

- System characterization
- Threat identification
- Vulnerability identification
- Control analysis
- Likelihood determination
- Impact analysis
- Risk determination
- Control recommendations
- Results documentation

