SLIIT

Discover Your Future

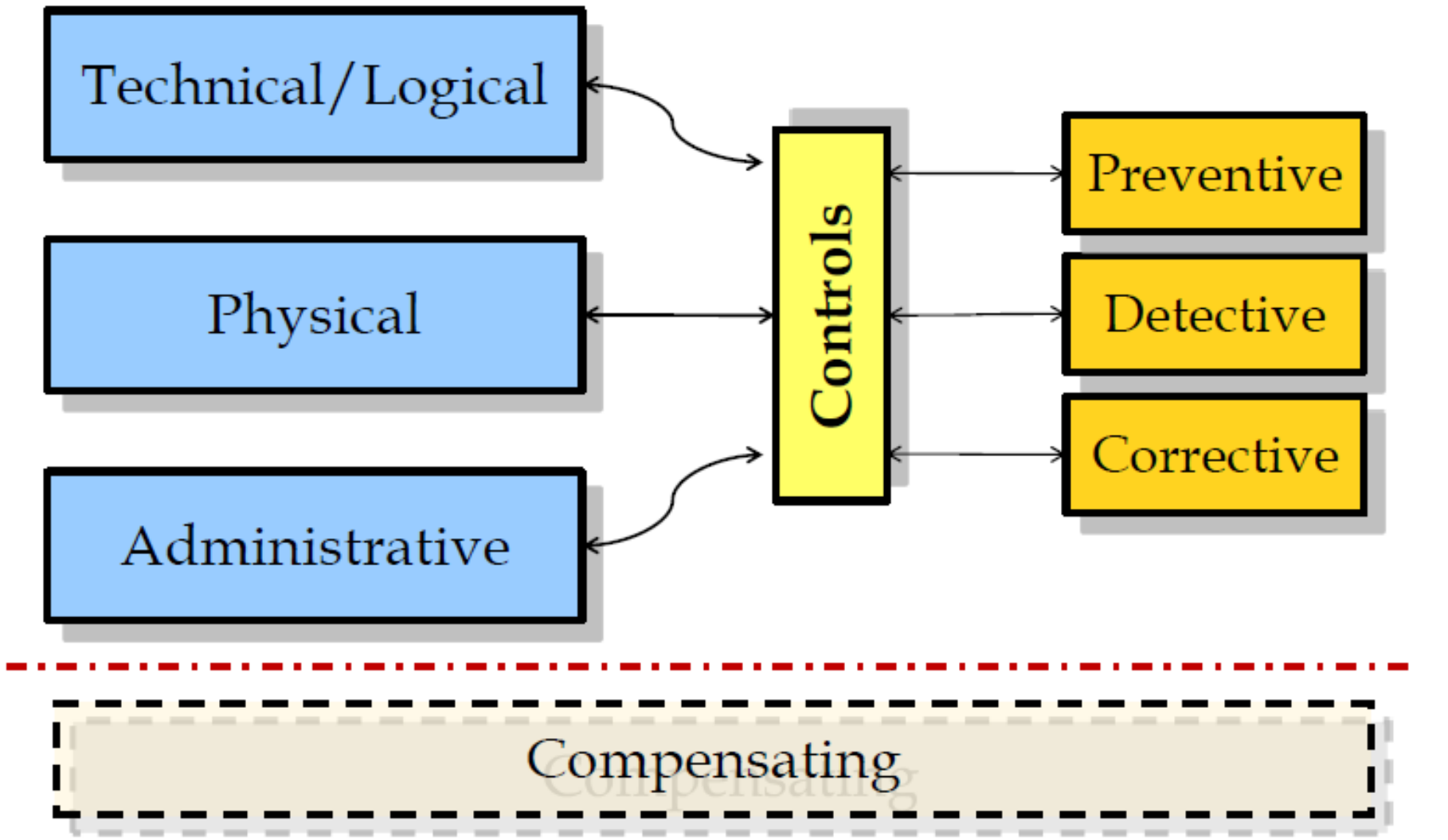
IE2022 – Introduction to Cyber Security

Lecture - 03

Security Controls and Risk Management

Mr. Amila Senarathne

Security Controls



Security Controls

Computer/information security controls are often divided into three distinct categories

- Physical controls
- Technical/Logical controls
- Administrative controls

Physical Controls

The Physical control is the implementation of security measures in a defined structure used to deter or prevent unauthorized access to sensitive material.

- Surveillance cameras
- Motion or thermal alarm systems
- Security guards
- Picture IDs
- Locked and dead-bolted steel doors
- Network segregation
- Work area separation

Technical Controls

The Technical control uses technology as a basis for controlling the access and usage of sensitive data throughout a physical structure and over a network.

- Encryption
- Smart cards
- Network authentication
- Access control lists (ACLs)
- File integrity auditing software

.

Administrative Controls

Administrative controls define the human factors of security. It involves all levels of personnel within an organization and determines which users have access to what resources and information by such means as:

- Training and awareness
- Disaster preparedness and recovery plans
- Personnel recruitment and separation strategies
- Personnel registration and accounting
- Policy and procedures

Controls categorized : By functionality

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

Preventive Controls

Designed to discourage errors or irregularities from occurring. They are proactive controls that help to ensure departmental objectives are being met.

- Separation of duties
- Security of Assets (Preventive and Detective)
- Planning/testing
- Proper hiring practices
- Proper processing of terminations
- Approvals, Authorizations, and Verifications

Detective Controls

Designed to find errors or irregularities after they have occurred.

- Monitoring Systems
- Log reviews
- Bugler Alarm
- File Integrity checkers
- Security reviews and audits
- Performance evaluations

Deterrent Controls

Intended to discourage potential attackers and send the message that it is better not to attack, but even if you decide to attack we are able to defend ourselves.

- Notices of monitoring logging
- Visible practice of sound information security management.

Corrective Controls

Designed to correct the situation after a security violation has occurred. Although a violation occurred, not all is lost, so it makes sense to try and fix the situation.

- Procedure to clean a virus from an infected system
- A guard checking and locking a door left unlocked by a careless employee
- Updating firewall rules to block an attacking IP address

Recovery Controls

Somewhat like corrective controls, but they are applied in more serious situations to recover from security violations and restore information and information processing resources.

- Disaster recovery and business continuity mechanisms
- Backup systems and data
- Emergency key management arrangements and similar controls.

Compensating Controls

- Intended to be alternative arrangements for other controls when the original controls have failed or cannot be used.
- When a second set of controls addresses the same threats that are addressed by another set of controls, the second set of controls are referred to ad compensating controls.

Risk Management

What is risk?

- Life is full of risk. We all manage risk consciously or automatically in life.
- Risk is the possibility of damage happening, and the ramifications of such damage should it occur.

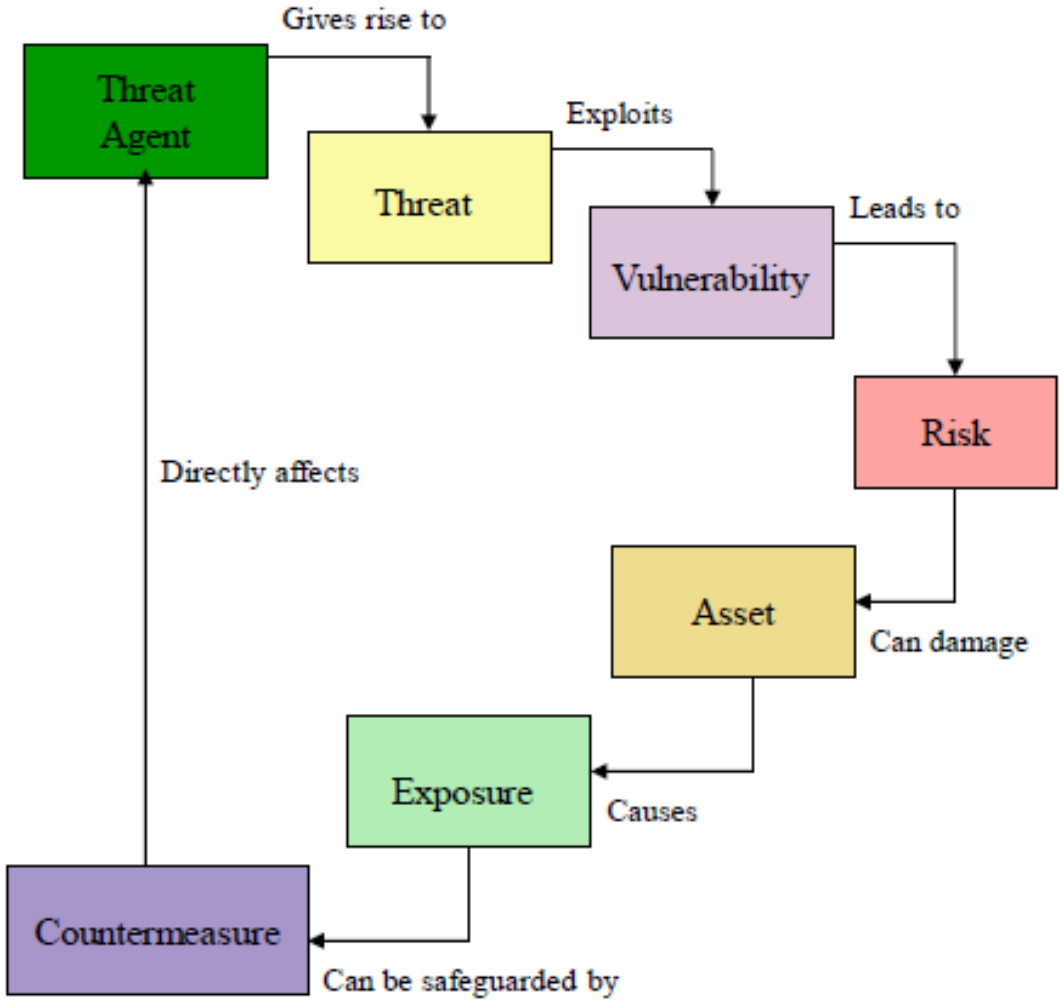
Information Risk Management (IRM) is the *process of identifying and assessing risk, reducing* it to an acceptable level, and implementing the right mechanisms to maintain that level.

- Risk can be mitigated, but cannot be eliminated (which is usually not an option in the commercial world, where controlled (managed) risk enables profits)

Risk Management Terms

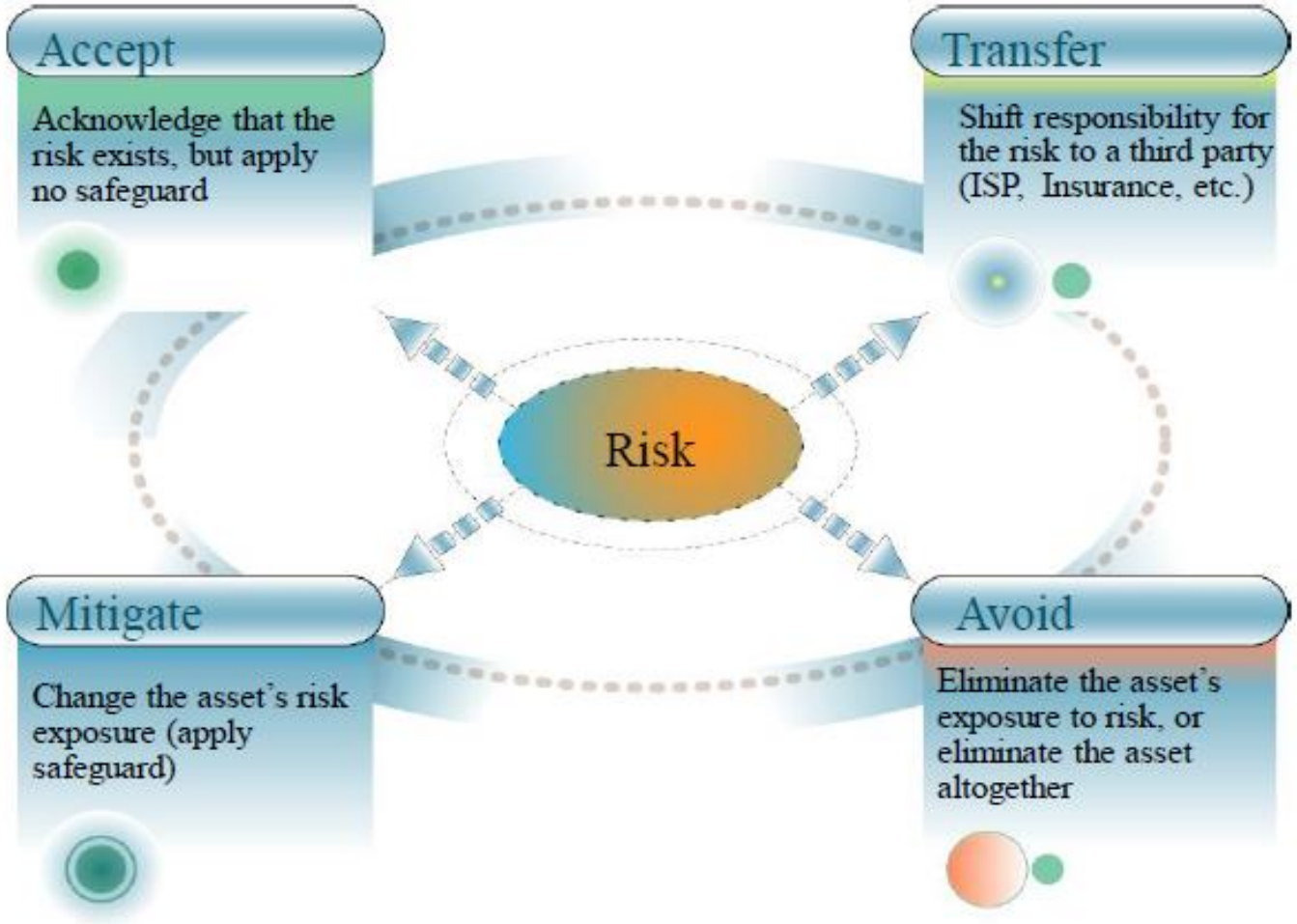
- Vulnerability – a system, network or device weakness
- Threat – potential danger posed by a vulnerability
- Threat agent – the entity that identifies a vulnerability and uses it to attack the victim
- Risk – likelihood of a threat agent taking advantage of a vulnerability and the corresponding business impact
- Exposure – potential to experience losses from a threat agent
- Countermeasure – put into place to mitigate the potential risk

Understanding Risk

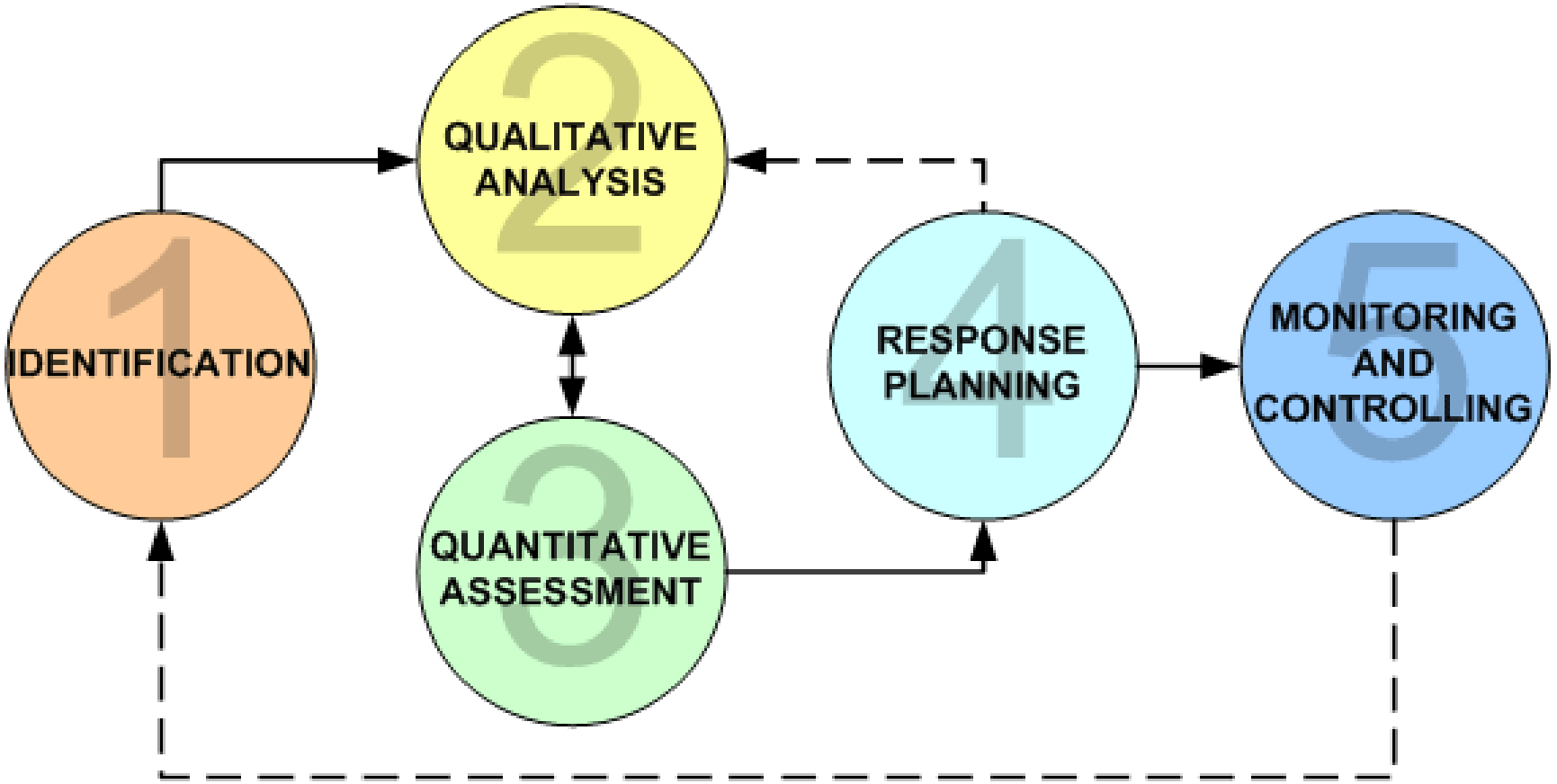


*A **threat agent** gives rise to a **threat** that exploits a **vulnerability** and can lead to a **security risk** that can damage your **assets** and cause an **exposure. This can** be counter-measured by a safeguard that directly affects the threat agent.*

Managing Risks



Risk Management Process



Quantitative Risk Analysis

- **Exposure Factor(EF)** = Percentage of asset loss caused by identified threat (0-100%)
- **Single Loss Expectancy (SLE)** = Asset Value x EF

  e.g. Rs. 50,000 x 20% = Rs. 10,000
- **Annualized Rate of Occurrence (ARO)** = Frequency a threat will occur within a year
- **Annualized Loss Expectancy (ALE)** = SLE x ARO
- **Safeguard Cost/Benefit** = ALE before Safeguard - ALE After Safeguard - Annual Cost of Safeguard

Comprehensive Security Model