ASSALAMU'ALAIKUM

Chapt 3
IT Risk Management Imperatives & Opportunities

DR. RAHMAD KURNIAWAN, ST., MIT., MTA., CISDV.

Outline

- Purpose of Risk Management
- Risk Management Process in IT

Purpose of Risk Management

- **Cyber attacks** continue to be a source of significant exposure to organizations of all types
- Practitioners of information security are all well aware that exposure to risk is ever-changing and that it is also **hard to assess**.
- Risk is a quantitative measure of the **potential damage** caused by a threat, by a vulnerability, or by an event (malicious or non malicious) that affects the set of IT assets owned by the organization.

..Cont

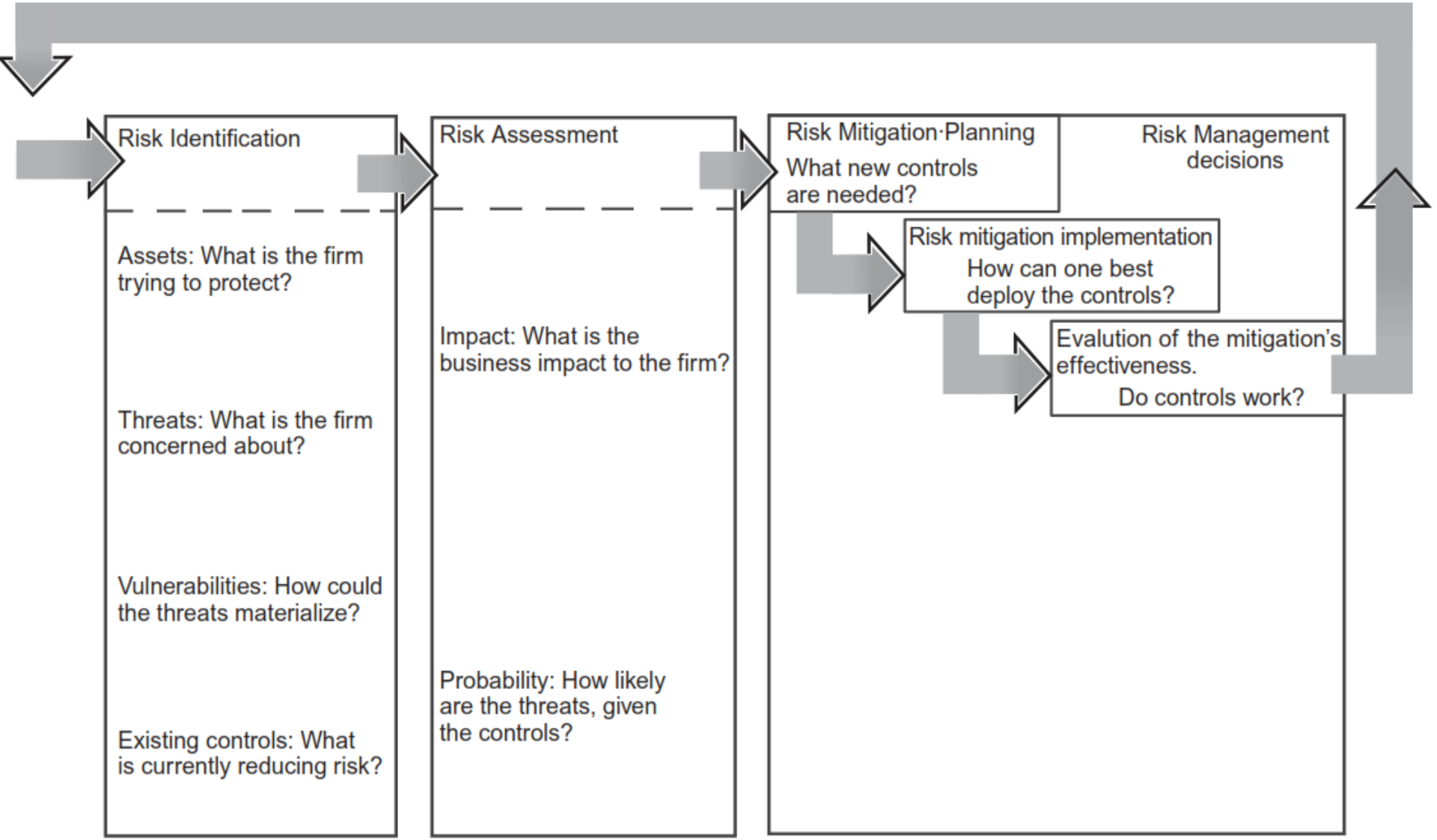
- **Confidentiality**
  - A breach of confidentiality occurs when a person knowingly accesses a computer without authorization or exceeding authorized access.
- **Integrity**
  - A breach of integrity occurs when a system or data has been accidentally or maliciously modified, altered, or destroyed without authorization.
- **Availability.**
  - A breach of availability occurs when an authorized user is prevented from timely, reliable access to data or a system, e.g., DoS attack.

..Cont

- **IT risk management → The process of reducing IT risk**
  - A process is a well-defined, repeatable sequences of activities
- **Process:**
  - (Ongoing) identification of threats, vulnerabilities, or (risk) events impacting the set of IT assets owned by the organization
  - Risk assessment (also called risk analysis)
  - Risk mitigation planning
  - Risk mitigation implementation
  - Evaluation of the mitigation's effectiveness

Risk identification	The process of identifying threats, vulnerabilities, or events (malicious or nonmalicious, deterministic/planned, or random) impacting the set of IT assets owned by the organization.
Risk assessment	The process of calculating quantitatively the potential damage and/or monetary cost caused by a threat, a vulnerability, or by an event impacting the set of IT assets owned by the organization. Identification of the potential damage to the IT assets and/or to the business processes based on previous internal and external events, input from subject matter experts, and audits. Specifically, this entails (a) quantifying the potential damage, and (b) quantifying the probability that damage will occur.
Risk mitigation planning	Process for controlling and mitigating IT risks. It typically includes cost–benefit analysis, and the selection, implementation, test, and security evaluation of safeguards. This overall system security review considers both effectiveness and efficiency, including impact on the mission and constraints due to policy, regulations, and laws [STO200201].
Risk mitigation implementation	Deploying and placing in service equipment and/or solution identified during the risk mitigation planning phase, or actuating new corrective processes.
Evaluation of the mitigation's effectiveness	Monitoring the environment for effectiveness against the previous set of threats, vulnerabilities, or events, as well as determining if new/different threats, vulnerabilities, or events results from the modifications made to the environment.

Risk Management Process



❖ Thank you