Protective Security Management

Security Risk Management

Introduction to Risk Management

Outlines

- Overview of Risk Management
- What is Risk Management
- General Risk Management Model

Objectives

- Explain the definition and purpose of risk management.
- Define important terms associated with risk management.
- Describe the general risk management model.
- Describe an example of risk management in daily situations.

Overview of Risk Management

Risk Management? No, never heard of it. Can you pass me that wrench.

Overview of Risk Management

- Risk management can be described as a decision-making process.
- Effective risk management avoids costly oversights and unexpected problems.
- Industry best practices state that effective risk management involves treating it as an ongoing process

Overview of Risk Management

- Risk management is an essential element of management.
- It encompasses all the actions to:
  - Reduce complexity.
  - Increase objectivity.
  - Identify important decision factors.

Overview of Risk Management

- Businesses need to take risks to retain their competitive edge.
- As a result, risk management must be done as part of managing any project.
- To succeed, one needs to manage risks better.
- Risk management is both a skill and a task.
- Depending on the size of the project and the amount of risk involved, risk management can be simple or complex.

Understanding Risk Management

Key terms in Risk Management:

- **Risk** - the possibility of suffering a loss.
- **Risk management** - the decision-making process of identifying threats and vulnerabilities and their potential impacts.
- **Risk assessment (or risk analysis)** - the process of analyzing an environment to identify the threats, vulnerabilities, and mitigating actions to determine the impact of an event on a project, program, or business.

Understanding Risk Management

Key terms (continued):

- **Asset** - a resource or information required by an organization to conduct its business.
- **Threat** - any circumstance or event that may cause harm to an asset.
- **Vulnerability** - the characteristic of an asset that can be exploited by a threat to cause harm.
- **Impact** - the loss when a threat exploits a vulnerability.

Understanding Risk Management

Key terms (continued):

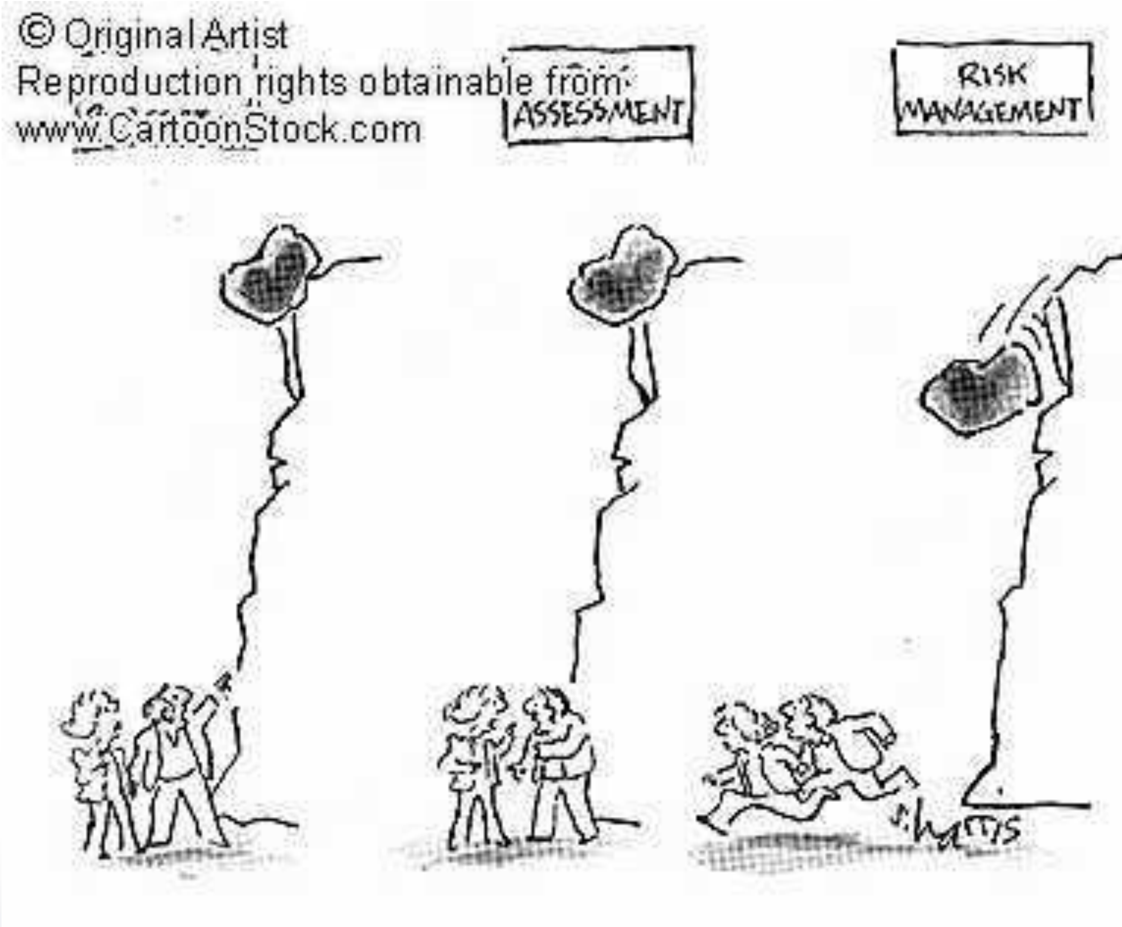
- **Control** (countermeasure or safeguard) - a measure to detect, prevent, or mitigate the risk associated with a threat.
    - It describes a variety of processes, procedures, or tools for reducing risk to an acceptable level.
    - When a risk is identified, the organization must
        - assess its potential impact
        - prioritize its importance
        - identify the options for managing the risk
        - assess the business value of introducing a mitigating control.
    - Specifically, controls are security tools, programs, policies, restrictions, and other methods used to mitigate identified risks.

Understanding Risk Management

Key terms (continued):

- **Mitigate** - action taken to reduce the likelihood of a threat occurring.
- **Qualitative risk assessment** - the process of subjectively determining the impact of an event that affects a project, program, or business.
- **Quantitative risk assessment** - the process of objectively determining the impact of an event that affects a project, program, or business.

What is Risk Management



© Original Artist
Reproduction rights obtainable from:
www.CartoonStock.com

Risk Management

- The dictionary defines **risk** as the possibility of suffering harm or loss.
- *Buku Arahan Keselamatan* defines risk management as:
  - A systematic and logical process to identify, analyze, value, overcome vulnerabilities and carry out surveillance in order to enable the Government Ministries, Departments and Agencies to ensure an excellent and a continuous service delivery system to achieve the organization’s objectives

Risk Management

- University of Manchester Risk Management Framework
  - **Risk** is a major factor to be considered during the management of any project and can be defined as a combination of constraint and uncertainty.
  - The term exposure relates to the sum of the likelihood multiplied by the impact (i.e. the likelihood of the risk occurring multiplied by the impact that risk would have if it did occur).
  - The aim of **Risk Management** is to manage that exposure by taking action to keep exposure to an acceptable level in a cost effective way.

Risk Management

- University of Manchester Risk Management Framework (cont)
  - Risk Management at the project level focuses on keeping unwanted risks to an acceptable minimum. It is important to plan how risks will be managed from the project start-up (investigation stage).
  - Risk Management is seen as an integral part of the decision-making process which adds value rather than increase burdens.
  - Risk Management embedded into the decisions making process will make it easier to achieve its objectives

Risk Management

- Carnegie Mellon University’s Software Engineering Institute (SEI) defines **continuous risk management** as: processes, methods, and tools for managing risks in a project.
- It provides a disciplined environment for proactive decision-making to:
  - Assess what could go wrong (risks).
  - Determine which risks are important.
  - Implement strategies to deal with those risks.

Risk Management

- **Definition by Wikipedia**
  - **Risk management** is the human activity which integrates recognition of risk, risk assessment, developing strategies to manage it, and mitigation of risk using managerial resources.
  - The strategies include transferring the risk to another party, avoiding the risk, reducing the negative effect of the risk, and accepting some or all of the consequences of a particular risk.

Risk Management

- **Definition by Wikipedia (cont)**
  - Objective of *risk management* is
    - to reduce different risks related to a preselected domain to the level accepted by society.
  - It may refer to numerous types of threats caused by environment, technology, humans, organizations and politics.
  - On the other hand it involves all means available for humans, or for a risk management entity (person, staff, organization).

Risk Management

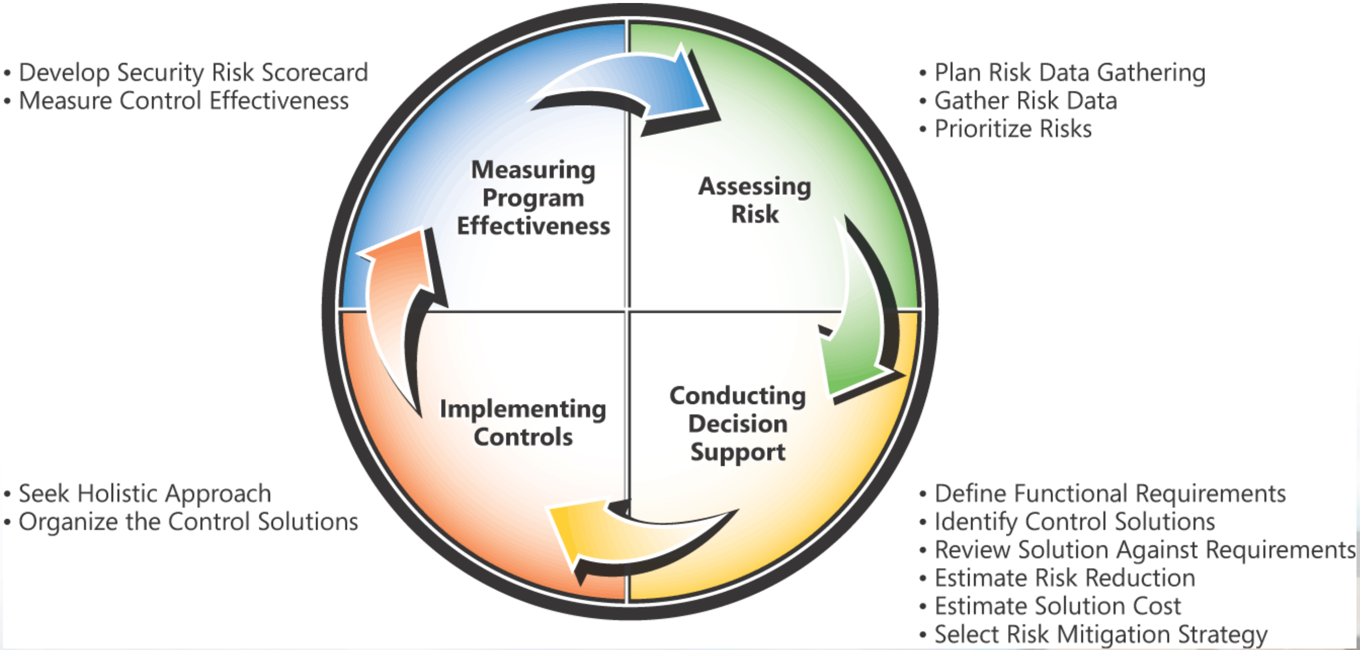
- **Definition by National Institute of Standards & Technology (NIST)**
  - A process that allows IT managers to balance the operational & economic costs of protective measures – to protect IT systems & data

Risk Management
= Risk Assessment + Risk Mitigation + (Evaluation + Assessment)

  - Risk Assessment (RA) = identification & evaluation of risks & impacts
  - Risk Mitigation/Treatment = prioritize, implement & maintain appropriate risk reducing measures (recommended from RA)

Risk Management

- Microsoft Security Risk Management
  - defined risk management as an ongoing process with four primary phases:



- Develop Security Risk Scorecard
- Measure Control Effectiveness

- Plan Risk Data Gathering
- Gather Risk Data
- Prioritize Risks

- Seek Holistic Approach
- Organize the Control Solutions

- Define Functional Requirements
- Identify Control Solutions
- Review Solution Against Requirements
- Estimate Risk Reduction
- Estimate Solution Cost
- Select Risk Mitigation Strategy

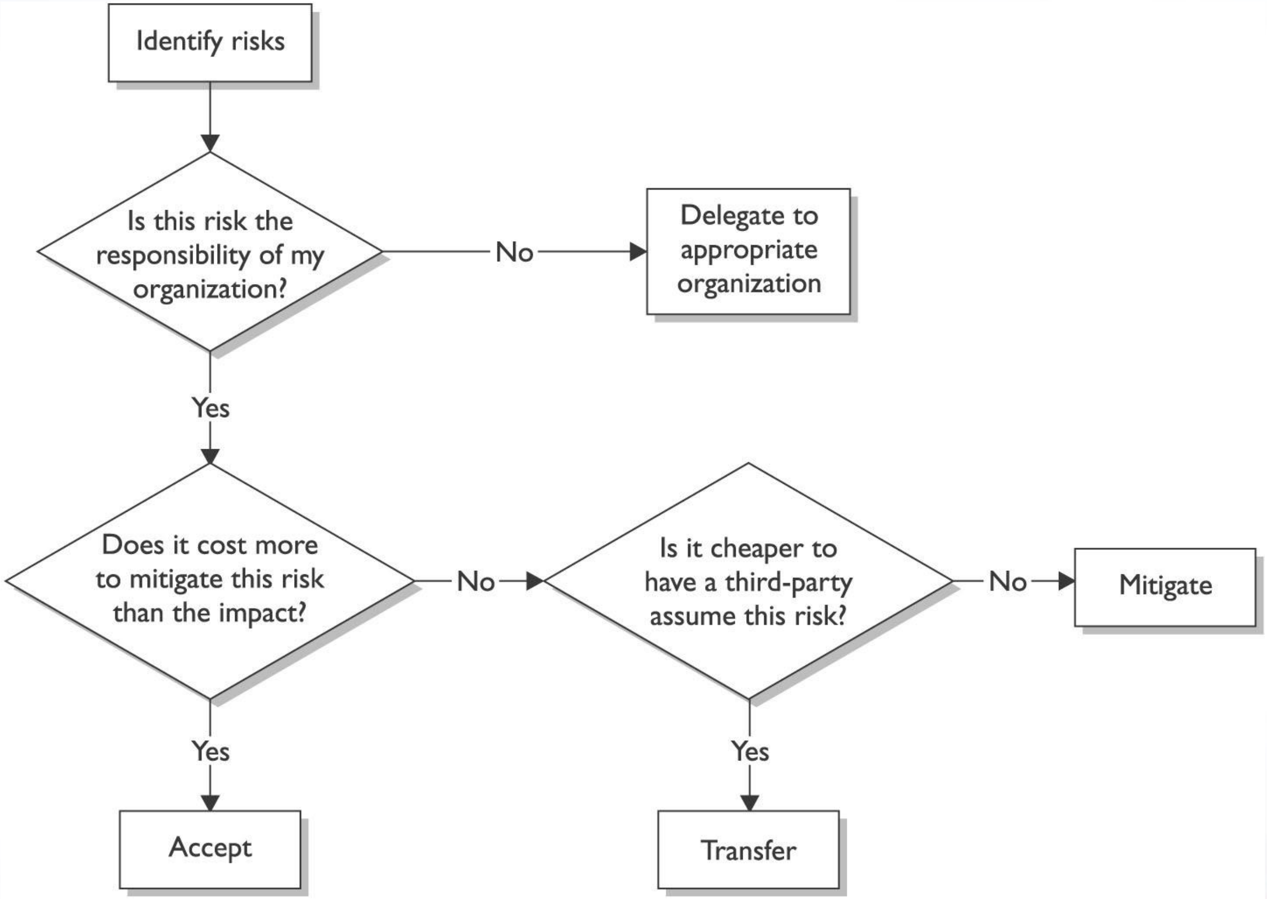
Risk Assessment and Treatment

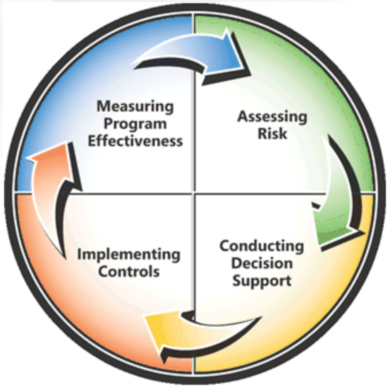
- Definition by ISO 17799:2005 Code of Practice for Info Sec Mgmt
  - Risk Assessment
    - identify, quantify & criteria for risk acceptance & objectives relevant to organization
    - Include systematic approach to estimate the magnitude of risks (risk analysis) & compare the estimated risks against risk criteria to determine the significance of the risks (risk evaluation)
    - Decide on the criteria of acceptable risks e.g. risk is low or the cost of treatment is not cost effective

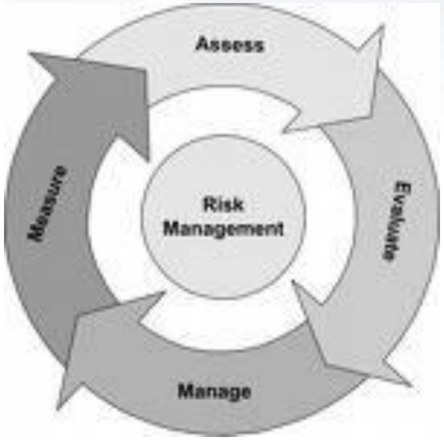
Risk Management vs Risk Assessment

	Risk Management	Risk Assessment
Goal	Manage risks across business to acceptable level	Identify and prioritize risks
Cycle	Overall program across all four phases	Single phase of risk management program
Schedule	On going	As needed

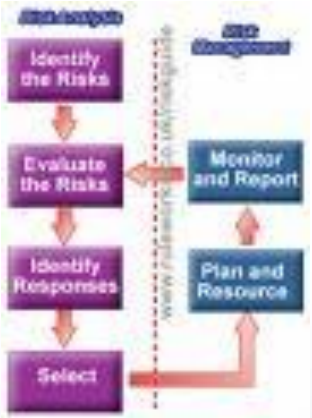
Risk Management


Identify risks
Is this risk the responsibility of my organization?
No
Delegate to appropriate organization
Yes
Does it cost more to mitigate this risk than the impact?
No
Is it cheaper to have a third-party assume this risk?
No
Mitigate
Yes
Accept
Yes
Transfer





General Risk Management Model



External Risks:
Internal Risks:
Corporate Strategy
Risk Management: Holistic Approach
Firm Culture
Management Infrastructure
Corporate Governance

Risk Management Model

- There are several risk management models for managing risk through its various phases.
- The chosen models should align with the business objectives and strategies.

Risk Management Model

- General risk management model includes the following steps:
  1. Asset identification.
  2. Threat assessment.
  3. Impact definition and quantification.
  4. Control design and evaluation.
  5. Residual risk management.

Risk Management Model

- Asset Identification (Phase 1)
  - In this step, the assets, systems, and processes that need protection need to be identified and classified, as they are vulnerable to threats.
  - This classification helps to prioritize assets, systems, and processes and to evaluate the costs of addressing the associated risks.

Risk Management Model

Asset Identification (cont)

- Assets include:
  - Inventory and buildings.
  - Cash.
  - Information and data.
  - Hardware and software.
  - Products & Services
  - Documents
  - Personnel.
  - Brand recognition and organization reputation.

Risk Management Model

- Threat Assessment (Phase 2)
  - Threats can be defined as any circumstance or event with the potential to harm an asset.
  - In this step, the possible threats and vulnerabilities associated with each asset and the likelihood of their occurrence is identified.

Risk Management Model

Threat Assessment (cont)

- Examples of threat:
  - Natural disasters
  - Man-made disasters
  - Terrorism
  - Errors
  - Malicious damage or attacks
  - Fraud
  - Theft
  - Equipment or software failure

© Original Artist
Reproduction rights obtainable from
www.CartoonStock.com

© Mike Baldwin / Cornered

Risk Management Model

Threat Assessment (cont)

- Vulnerabilities are characteristics of resources that can be exploited by a threat to cause harm.
- Examples of vulnerabilities include:
  - Unprotected facilities.
  - Unprotected computer systems.
  - Unprotected data.
  - Insufficient procedures and controls.
  - Insufficient or unqualified personnel.

Risk Management Model

- Impact Definition & Quantification (Phase 3)
  - When a threat is realized, it turns risk into impact.
  - An impact is the loss created when a threat exploits a vulnerability.
  - Impacts can be either tangible or intangible.

Risk Management Model

Impact Definition & Quantification (cont)

- Tangible impacts include:
  - Direct loss of money.
  - Endangerment of staff or customers.
  - Loss of business opportunity.
  - Reduction in operational efficiency or performance.
  - Interruption of a business activity.

Risk Management Model

Impact Definition & Quantification (cont)

- Intangible impacts include:
  - Breach of legislation or regulatory requirements.
  - Loss of reputation or goodwill (brand damage).
  - Breach of confidence.

Risk Management Model

- Control Design & Evaluation (Phase 4)
  - Controls are designed to control risk by reducing vulnerabilities to an acceptable level.
  - Controls can be actions, devices, or procedures.
  - They can be:
    - Preventive controls - prevent the vulnerability from being exploited by a threat, thus causing an impact.
    - Detective controls - detect a vulnerability that has been exploited by a threat so that action can be taken.

Risk Management Model

- Residual Risk Management (Phase 5)
  - Any risks that remain after implementing controls are termed residual risks.
  - Residual risks can be further evaluated to identify where additional controls are required to further reduce risk.
  - Business process reengineering or organizational changes can create new risks or weaken existing control activities.

END OF SESSION

Topics that have been covered:

- **Overview of Risk Management**
- **What is Risk Management**
- **General Risk Management Model**