UNIVERSITY OF Southampton
Electronics and Computer Science

COMP6236
Software Engineering and Cyber Security
Security Risk Analysis

Dr Mu Yang

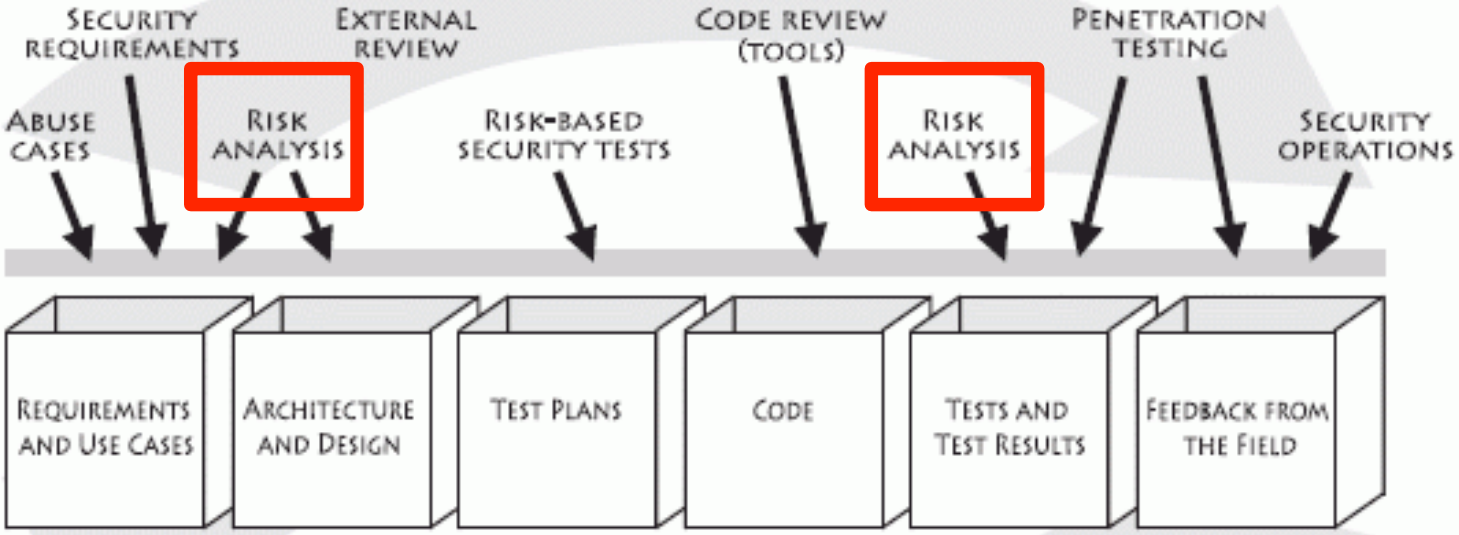
This Week

- Introduction to Risk Analysis
  - Why Risk Analysis?
  - What is Risk Analysis?
- CORAS
  - Language
  - Process
  - Tool
- CORAS Exercise

Learning outcomes

- At the end of this week you will be able to:
  - Identify security threats
  - Evaluate the risks represented by security threats
  - Identify mitigations for the risks

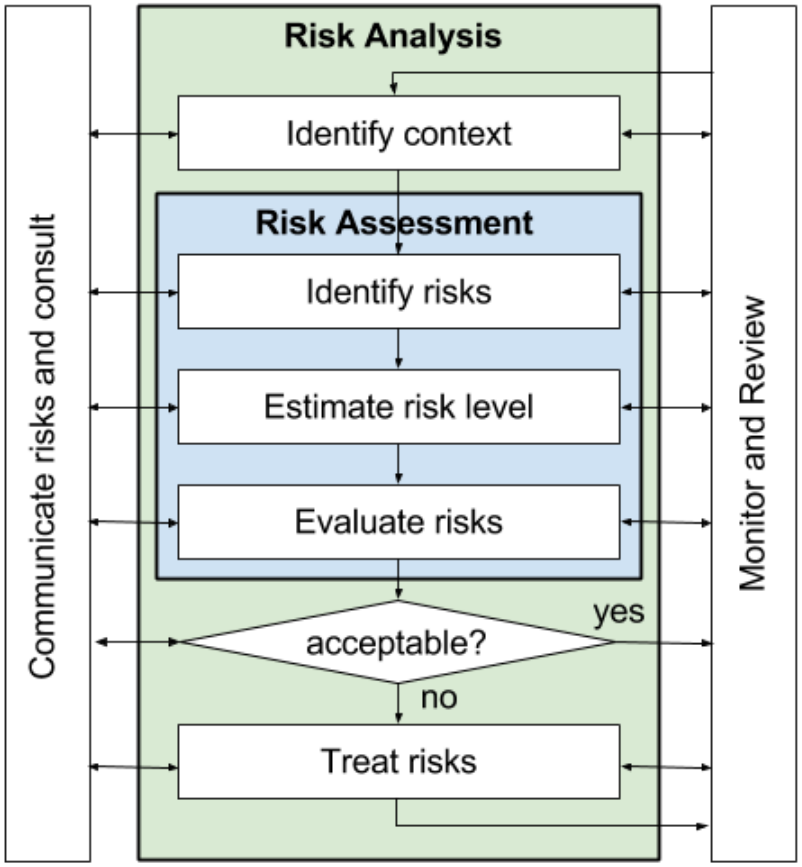
Why Risk Analysis?



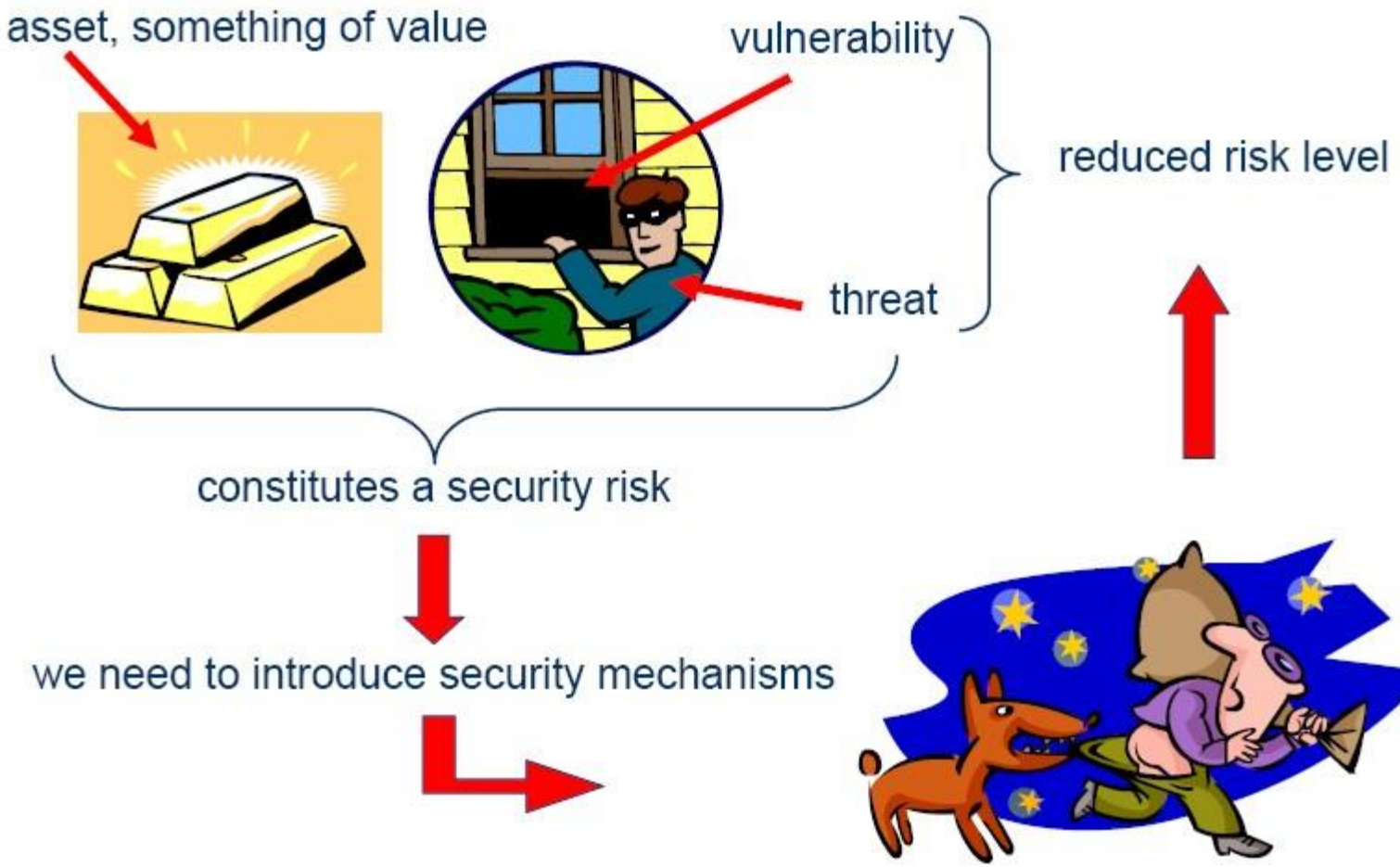
Need to prioritize because you can't perfectly secure everything…secure the most risky

What is Risk Analysis?

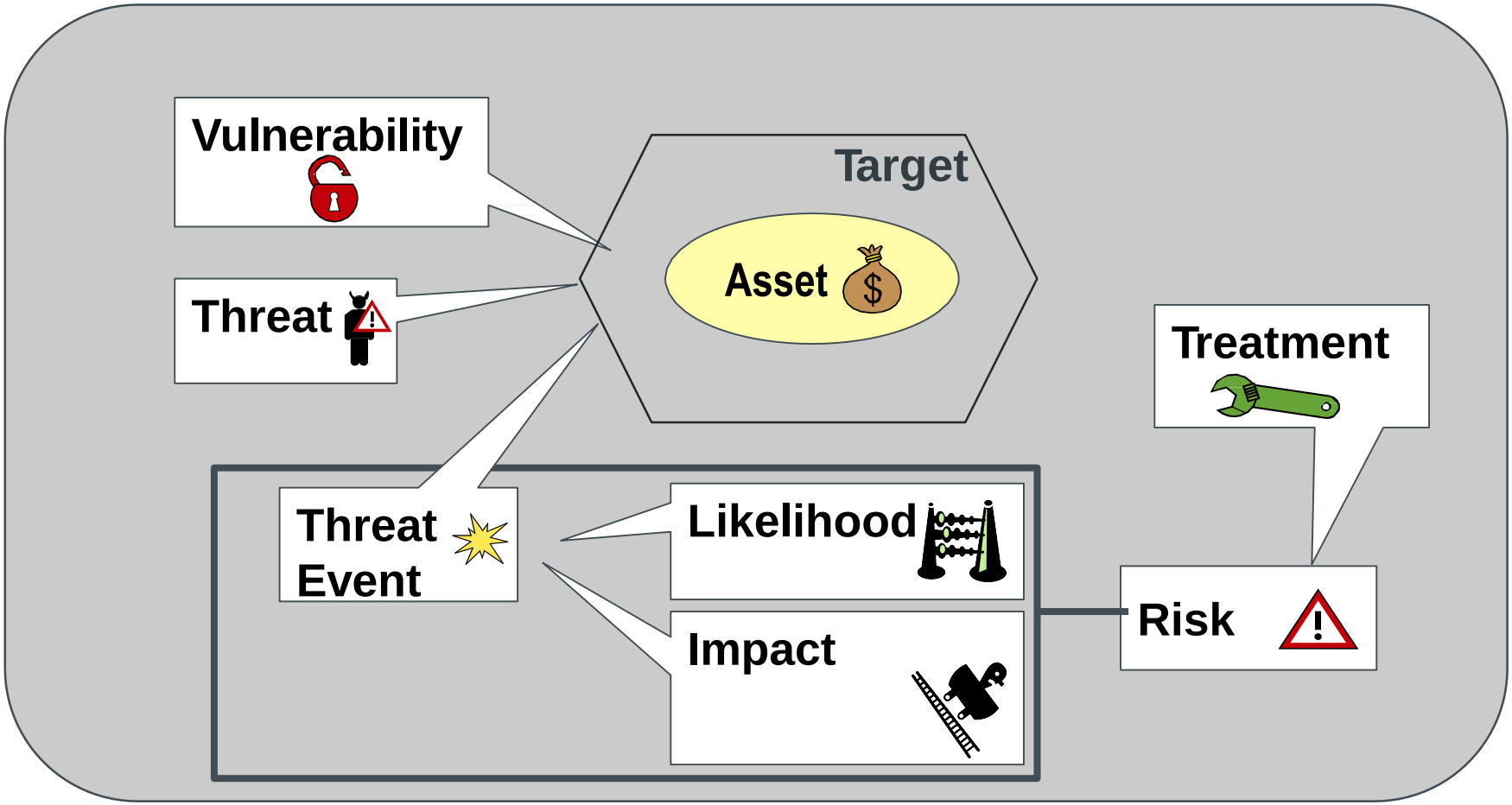
- **Risk Management -** Activity of performing a number of discrete risk analysis exercises to identify, track and mitigate risks throughout SDLC
- **Risk Analysis -** Activity of identifying and ranking risks at some stage of the SDLC
- **Risk Assessment –** Activity of identifying and evaluating risks



Elements of Risk Analysis



Elements of Risk Analysis



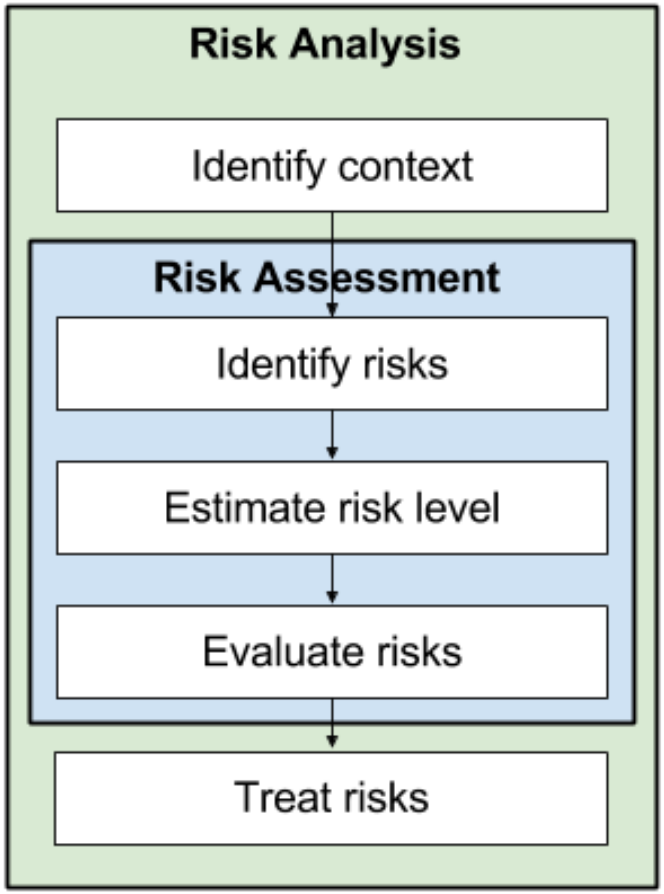
Elements of Risk Analysis

- **Threat**
  - Entity who causes the threat
- **Threat Event**
  - Event or circumstance with potential adversely impact to organizational assets
- **Threat Scenario**
  - Set of discrete threat events that cause harm
- **Vulnerability**
  - Weakness that could be exploited by a threat

Elements of Risk Analysis

- **Likelihood**
  - Probability that a threat event will occur
- **Adverse Impact/Consequence**
  - Magnitude of the harm caused by a threat event
- **Risk**
  - Function of Likelihood and Adverse Impact/Consequence
- **Treatment**
  - An appropriate measure to reduce risk level

Risk Analysis Process



Context Identification

- Characterise target of analysis
  - What is the focus and scope of the analysis?
- Identify and value assets
- Specify risk evaluation criteria
  - There will always be risks, but what losses can the client tolerate?

Risk Identification

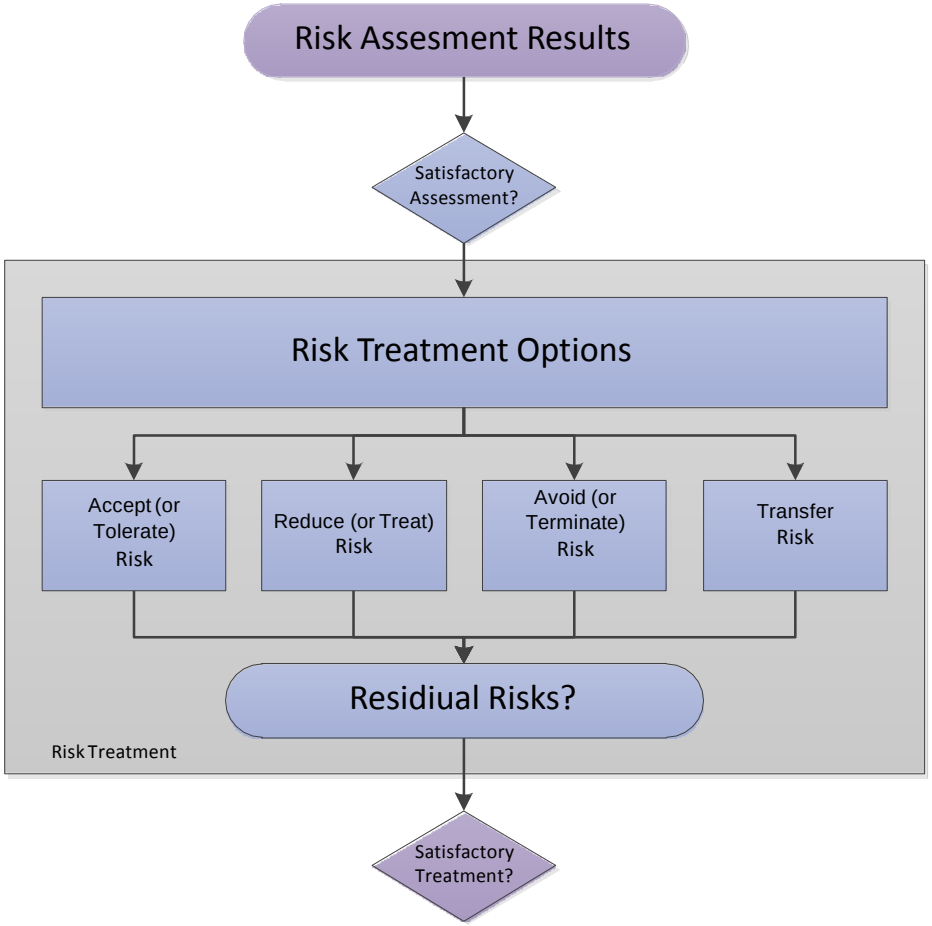
- Identify threats to assets through structured brainstorming
  - Involving system owners, users, developers, domain experts, risk analysis expert
- Identify vulnerabilities of assets
  - Questionnaires and checklists
  - e.g Is equipment properly physically protected against unauthorized access to data or data loss?

Risk Evaluation

- We cannot completely eliminate all risks
- Determine which risks need treatment
  - We need to know how serious they are so we can prioritize
- Risk level is determined based on analysis of the likelihood and impact of a threat event
  - **Quantitative** values: e.g loss of 1M£, 25% chance per year
  - **Qualitative** values: e.g, high, medium, low

Risk Treatment

- Four options
  - Accept
  - Treat
  - Avoid or Terminate
  - Transfer
- Identify treatments for unaccepted risks
- Evaluate and prioritize different treatments



Security Risk Analysis Methods

- **International Standards**
  - ISO 27001 (process) + ISO 27005 (treatments)
  - ISO 31000
  - NIST SP800-30 (process) + NIST SP 800-53(treatments)
- **National Standards**
  - IT-Grundschutz (Germany)
  - Magerit (Spain)
- **Standards-based**
  - OCTAVE
  - CORAS

A Case Study

In one region of the country, an experimental telemedicine system has been set up. A dedicated network between the regional hospital and several primary health care centres (PHCC) allows a general practitioner (GP) to conduct a cardiological examination of a patient (at the PHCC) in cooperation with a cardiologist located at the hospital. During an examination, both of the medical doctors have access to the patient's health record, and all data from the examination is streamed to the cardiologist's computer.

The National Ministry of Health is concerned whether the patient privacy is sufficiently protected, and hires a risk analysis consultancy company to conduct a risk analysis of the cardiology system with particular focus on privacy. The consultancy company appoints a team of two consultants to do the job. They are in the following referred to as "the analysts" and assigned the roles of risk analysis leader and risk analysis secretary, respectively.

Summary

- **Risk management** is one of the pillars to build secure software
  - Continuous process to identify, track and mitigate security risks
  - Several risk analysis exercises at different stages of SDLC
- **Risk analysis** is the activity to identify, assess, and mitigate security risks
- **Risk assessment** is the activity to evaluate security risks
  - Risk = Likelihood x Impact

Reading Material

- Chapter 16. Stallings, Brown. Computer Security
- Chapters 1 and 2. Lund, Solhaug, Stolen. Model-Driven Risk Analysis. The CORAS approach, Springer.
- NIST SP 800-30 – Guide for Conducting Risk Assesments. Available at http://csrc.nist.gov/publications/nistpubs/800-30-rev1/sp800_30_r1.pdf.
- NIST SP 800-53 – Security and Privacy Controls for Federal Information Systems and Organizations. Available at http://csrc.nist.gov/publications/nistpubs/800-53A-rev1/sp800-53A-rev1-final.pdf.