CYS 403 – Security Risk Management, Governance and Control

Intended Learning Outcomes

- CLO 1: Evaluate the issues and concerns indicative to protecting information, systems and users.

Agenda

- The Shangri-La of Risk Management
- Applying Risk Management to cyber security
- Qualitative vs. Quantitative risk management

Risk?

Definition of risk

- **Risk is the possibility of losing something of value.**

Risk is the **probability that a threat will turn into a disaster**.

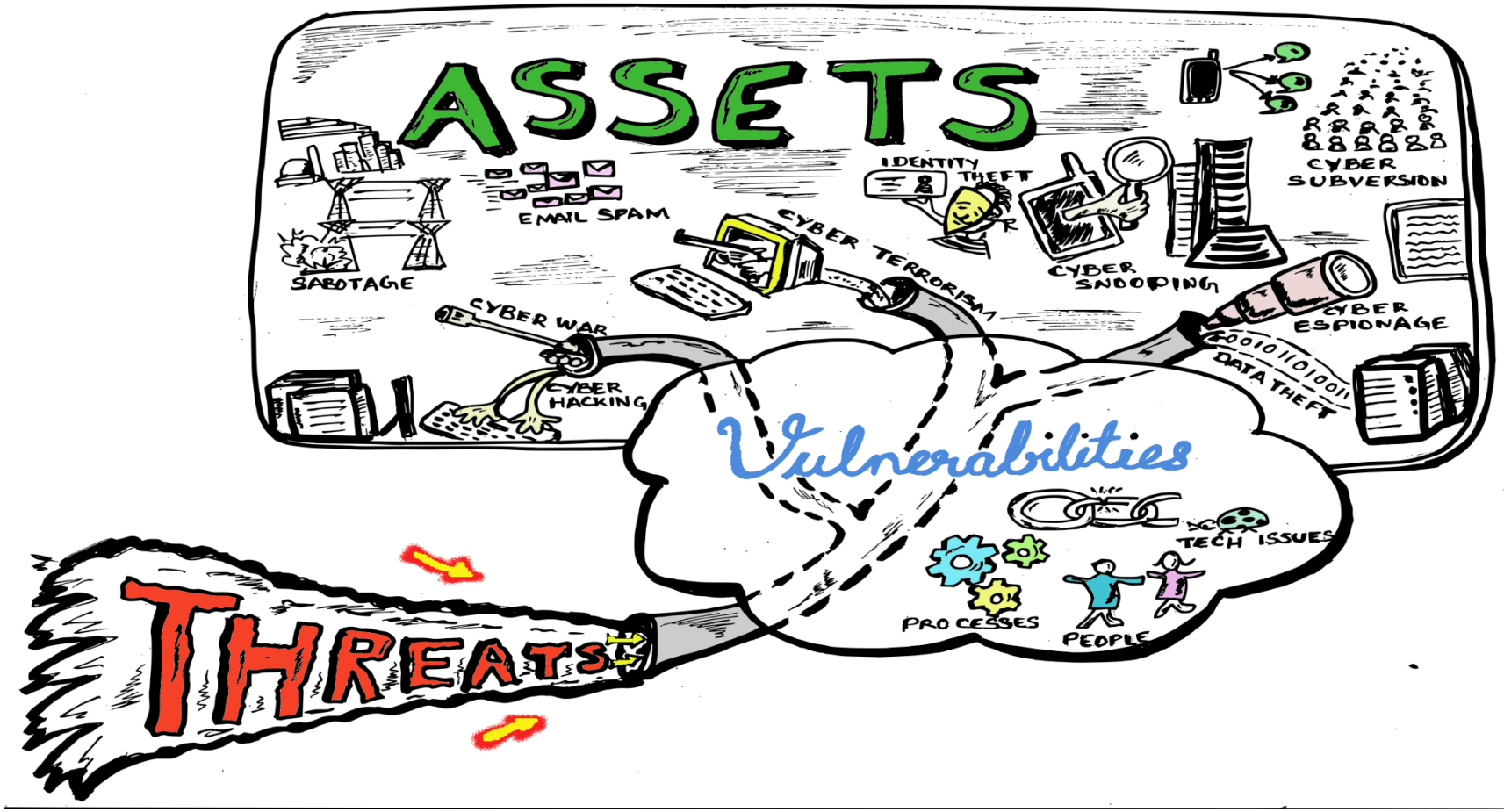
Vulnerability(weakness) and hazards are not dangerous, taken separately. But if they come together, they become a risk or, in other words, the probability that a disaster (ruin) will happen.

Definition of Risk

- *Risk* is a function of the *likelihood* of a given *threat-source's* exercising a particular potential *vulnerability*, and the resulting *impact* of that adverse event on the organization assets.

NIST SP 800-30

Risk is


ASSETS
EMAIL SPAM
IDENTITY THEFT
CYBER SUBVERSION
SABOTAGE
CYBER TERRORISM
CYBER SNOOPING
CYBER ESPIONAGE
CYBER WAR
CYBER HACKING
DATA THEFT
Vulnerabilities
TECH ISSUES
PROCESSES
PEOPLE
THREATS

Some terms and concepts

- **Asset** - Something that is valued by the organization to accomplish its goals and objectives.
- **Threat** - Any potential danger to information or an information system.
- **Attack**: Any actual danger to information or an information system.

Some terms and concepts

- Examples of threats include, but are not limited to:
  - Unauthorized access
  - Hardware failure
  - Utility failure
  - Loss of key personnel
  - Human errors
  - Neighboring hazards
  - Tampering
  - Dissatisfied employees

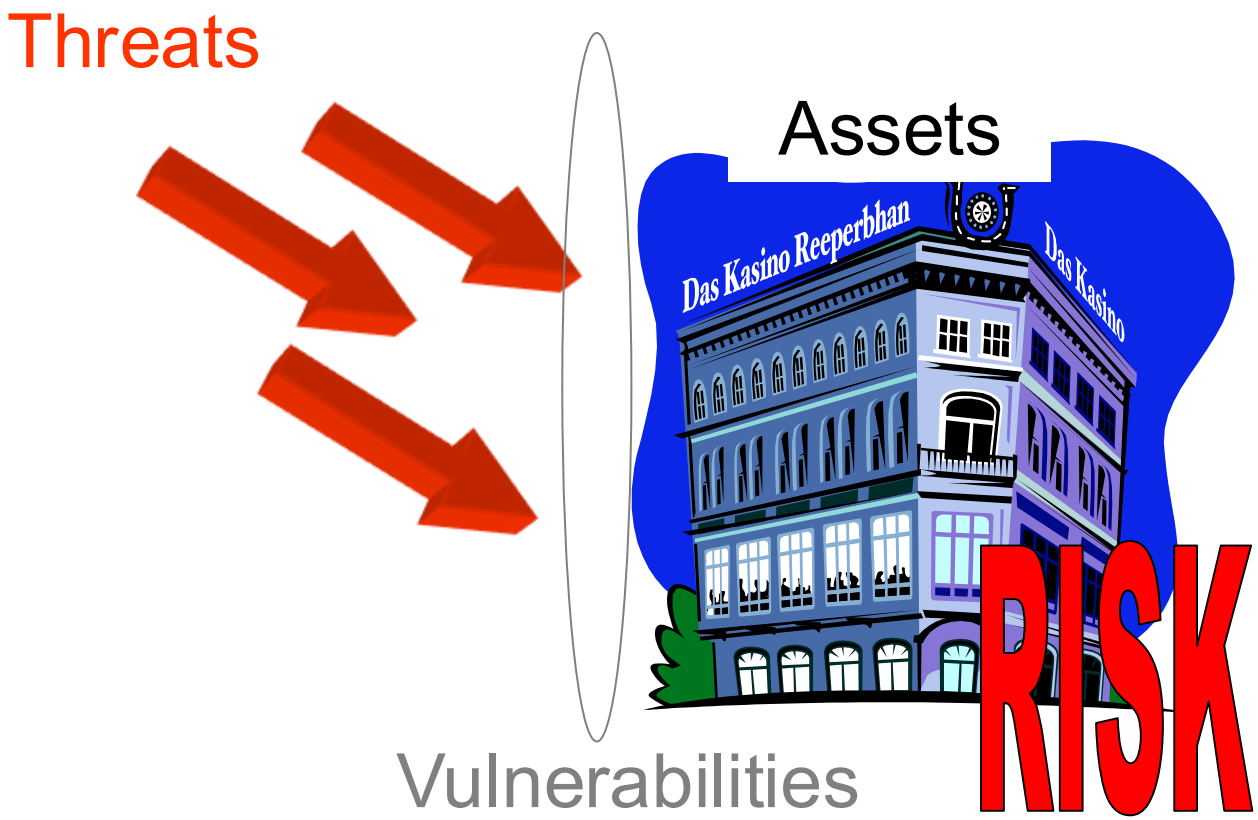
Some terms and concepts

- **Threat Agent** - Anything that has the potential of causing a threat.
- **Attacker**: Anything that has the actual cause of attack.
- **Vulnerability**: - Is any weakness that could be exploited. Vulnerabilities exist in every IT system, product and application.
- **Exposure** - An opportunity for a threat to cause loss.

Some terms and concepts

- **Countermeasures and Safeguards**: Are those measures and actions that are taken to protect systems.
- **Residual Risk** : Is the amount of risk remaining after countermeasures and safeguards are applied.

Risk Factors



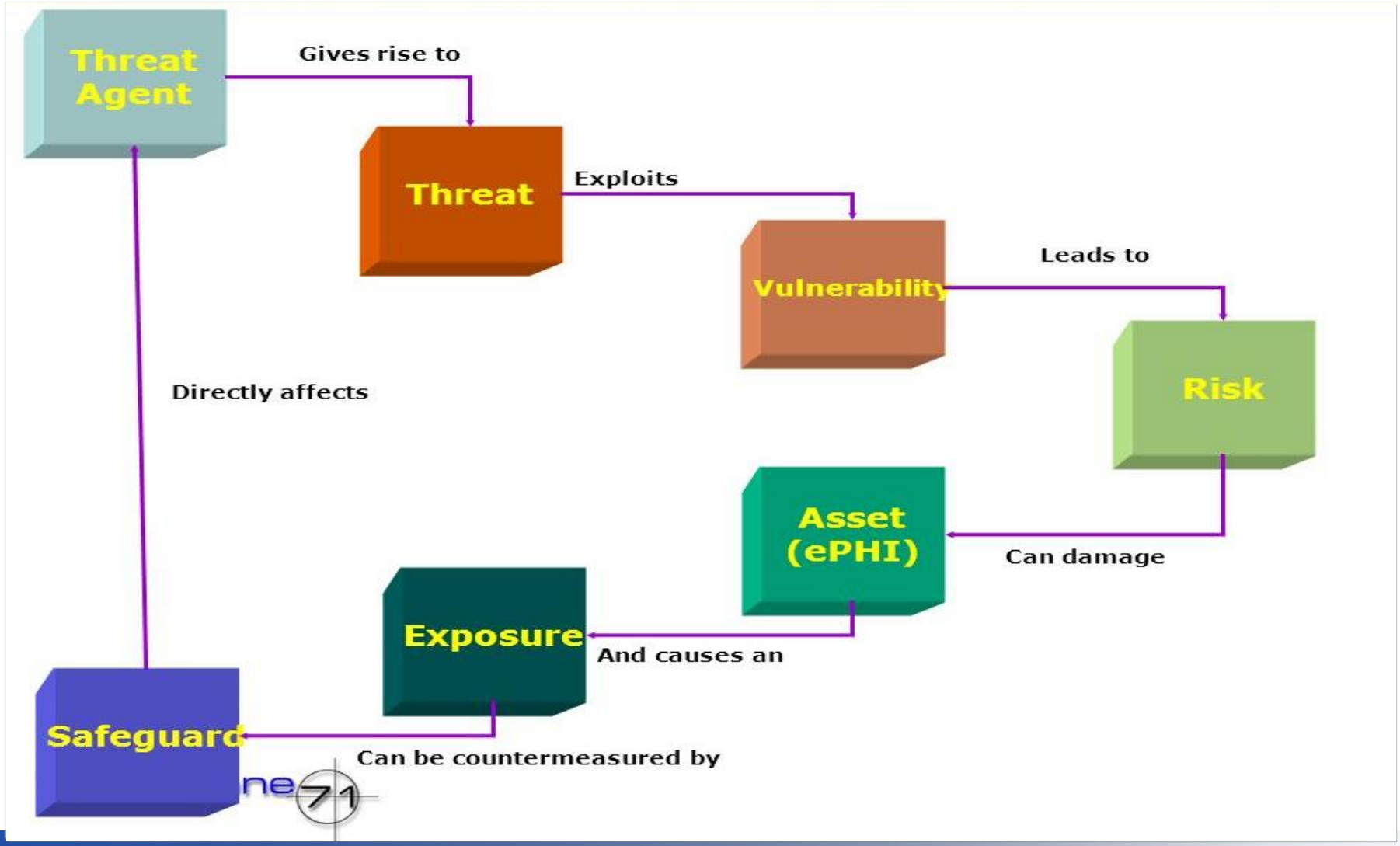
Risk Factors

Threats

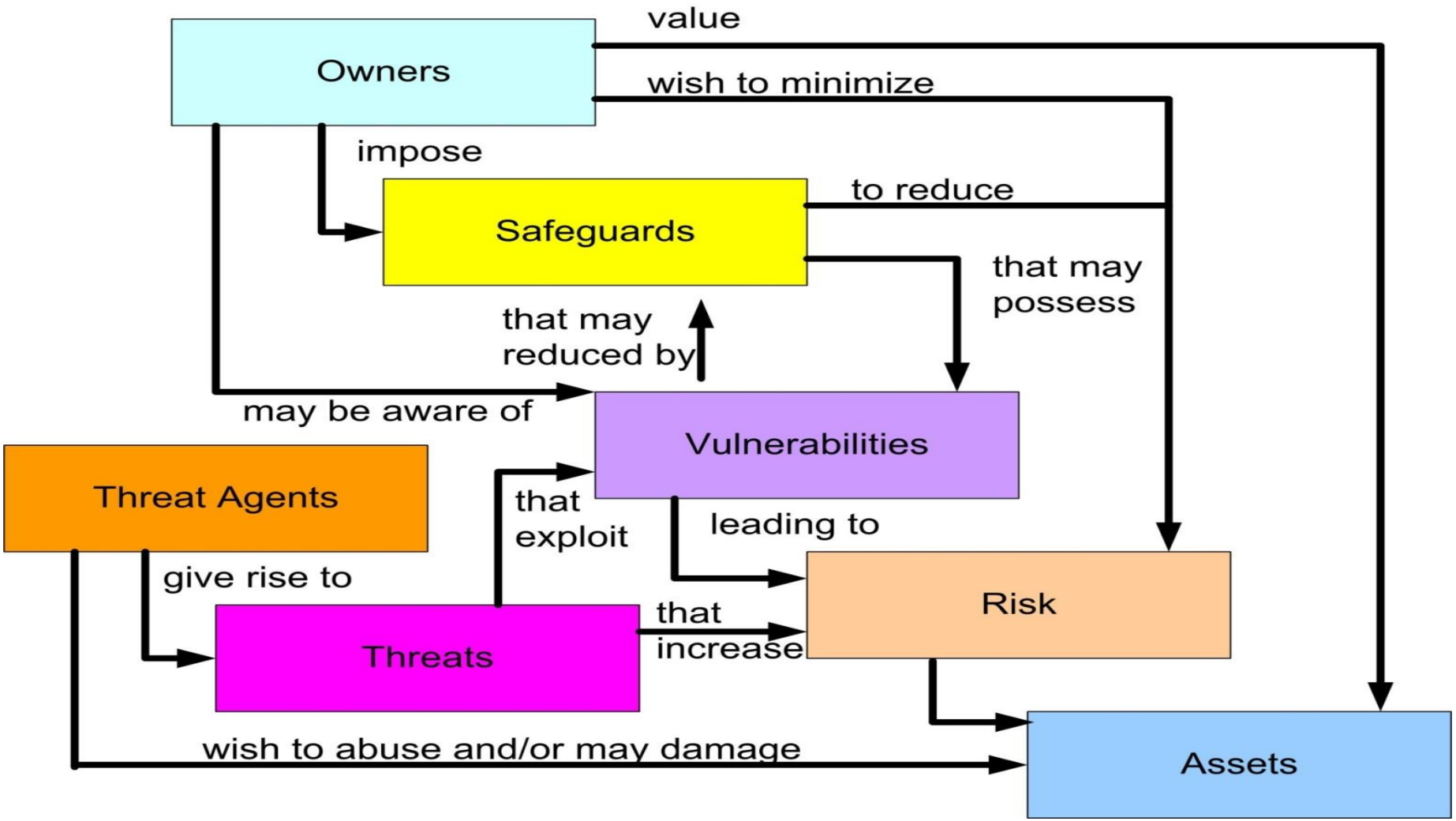
Assets

RESIDUAL RISK

Understanding Risk



Risk Management Concept Flow



An Overview on Risk Management

- Organizations must design and create safe environments in which business processes and procedures can function
- Risk management is the process of identifying and controlling risks facing an organization
  - Risk identification is the process of examining an organization's current information technology security situation
  - Risk Assessment is the process of evaluating the risks to find a suitable control.
  - Risk control is applying controls to reduce risks to an organization's data and information systems

An Overview on Risk Management

- **Know yourself**: identify, examine, and understand the information and systems currently in place
- **Know the enemy**: identify, examine, and understand threats facing the organization
- Responsibility of each community of interest within an organization to manage risks that are encountered

Risk Management

- The purpose of Risk Management is to identify potential cyber risks
  - Before they occur
  - Across the life of the product or project
  - So that risk-handling activities may be planned and invoked as needed

Risk Management

- **Risk Management** identifies and reduces **Risks** (Threats, Vulnerabilities, & impact on asset Value)
- **Mitigating controls: Safeguards & countermeasures** reduce risk
- Residual Risk should be set to an **acceptable level**

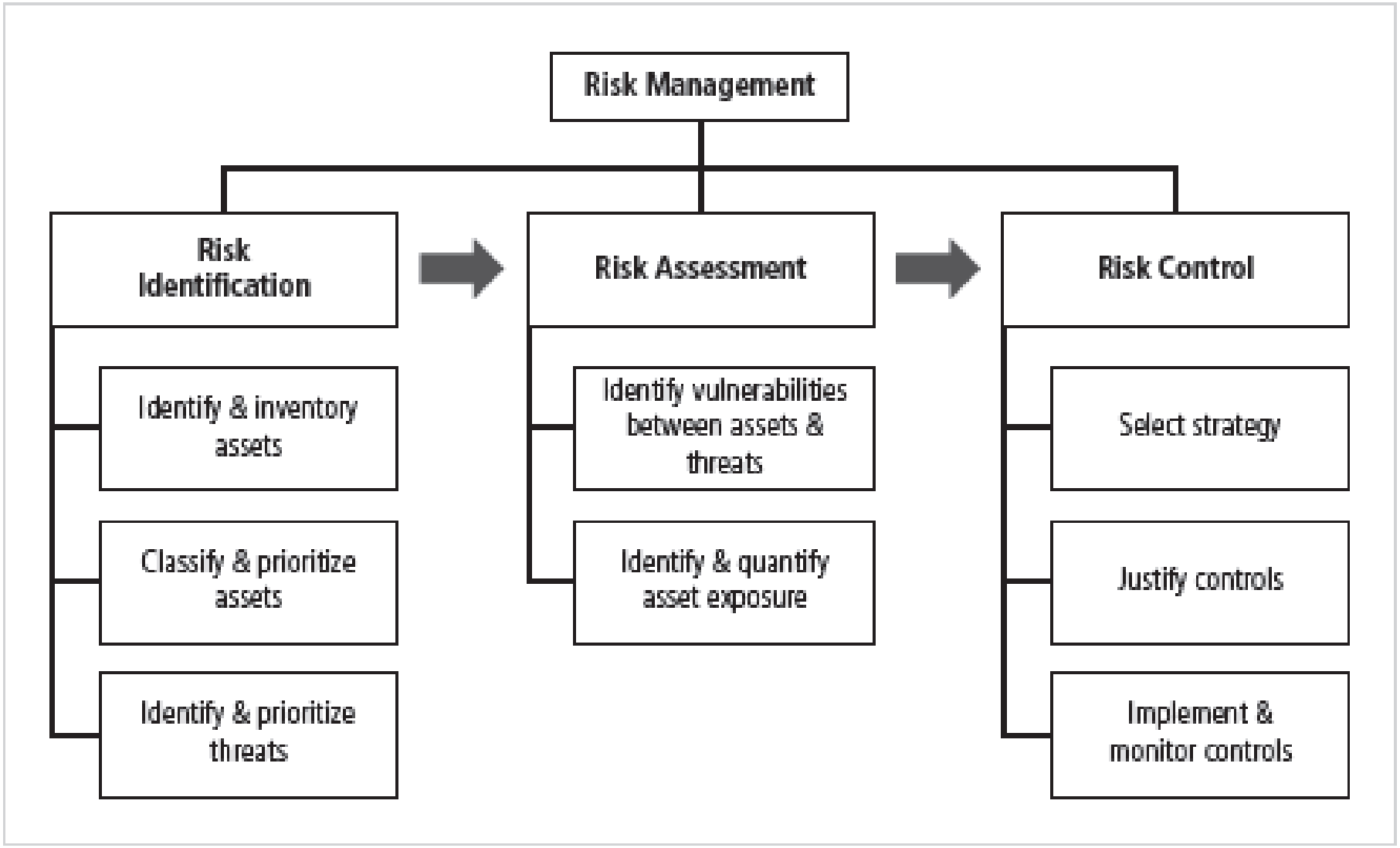
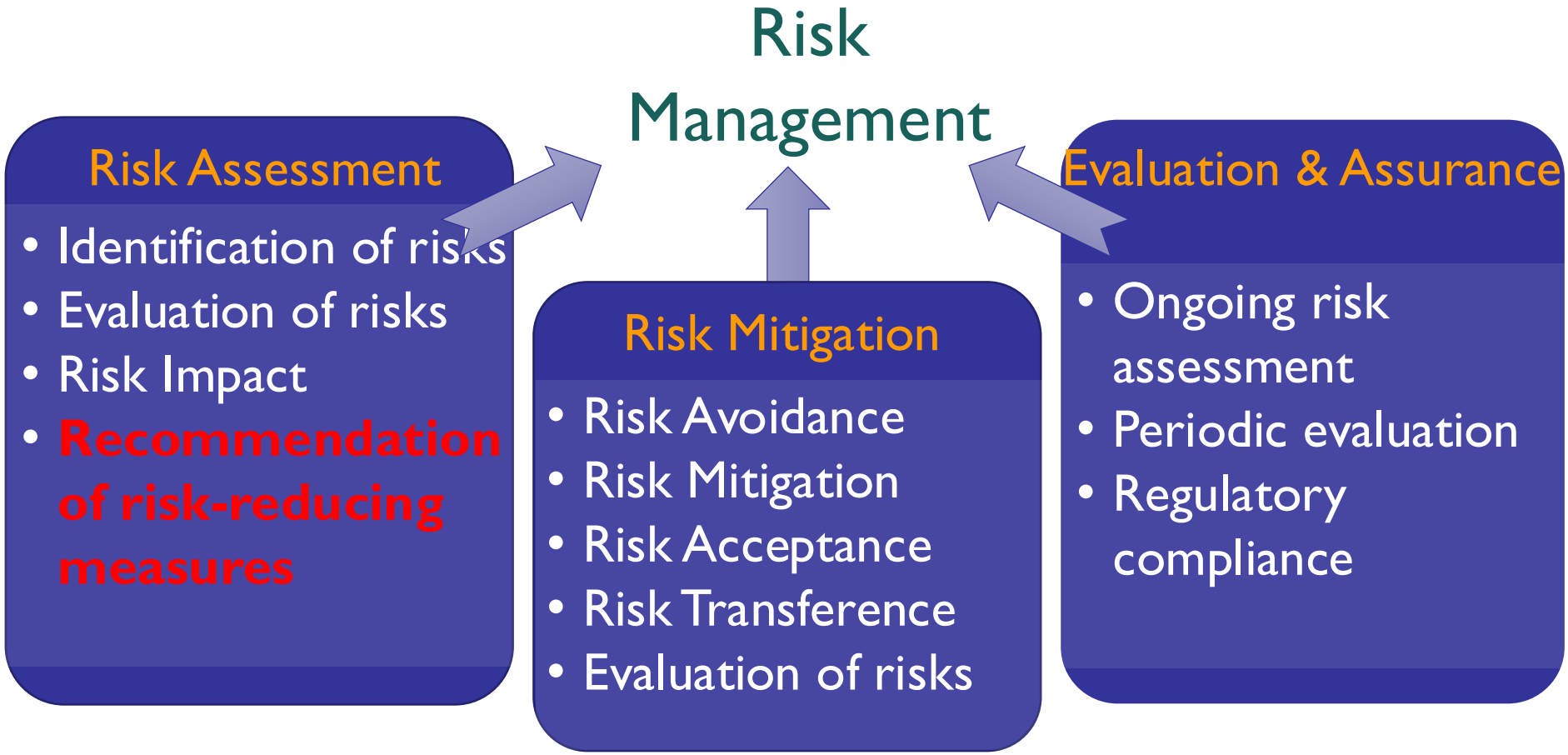


Figure 4-1 Components of Risk Management

The Risk Equation

Risk= Probability (threat, vulnerability, impact)



Risk Management Steps

- **Step 1: Identify the Risk.**
  - uncover, recognize and describe risks that might affect your system or its outcomes. There are a number of techniques you can use to find risks. During this step you start to prepare your Risk Register.

- Interview with SME's
- Brainstorming
- Delphi Technique
- Nominal Group Technique
- Crawford Slip
- Analogy
- SWOT
- Cause & Effect Diagram

Risk Management Steps

- **Step 2: Analyze the risk.**
  - Once risks are identified you determine the likelihood and impact of each risk. You develop an understanding of the *nature of risk and its potential to affect the business objectives*. This information is also input to your Risk Register.

Risk Management Steps

- **Step 3: Evaluate & Rank the Risk.**
  - You evaluate & rank the risk by determining the ***risk Score***, which is the combination of likelihood and impact.
  - You make decisions about whether the risk is acceptable or whether it is serious enough to warrant treatment.
  - These risk rankings are also added to your Risk Register.

Risk Management Steps

- **Step 4: Risk Control.**
  - This is also referred to as Risk Response Planning. During this step you assess your highest ranked risks and set out a plan to *treat or modify these risks to achieve acceptable risk levels*.
  - You create risk mitigation strategies, preventive plans and contingency plans in this step (DRP, BCP, IRP,...).
  - you add the risk treatment measures for the highest ranking or most serious risks to your Risk Register.

Risk Management Steps

- **Step 5: Monitor and Review the risk.**
  - This is the step where you take your Risk Register and use it to *monitor, track and review risks*.

Risk Register Sample

ID	Date raised	Risk description	Likelihood of the risk occuring	Impact if the risk occurs	Severity *Rating based on impact & likelihood.*	Owner *Person who will manage the risk.*	Mitigating action *Actions to mitigate the risk e.g. reduce the likelihood.*
1	[enter date]	Project purpose and need is not well-defined.	Medium	High	High	Project Sponsor	Complete a business case if not already provided and ensure purpose is well defined on Project Charter and PID.
2	[enter date]	Project design and deliverable definition is incomplete.	Low	High	High	Project Sponsor	Define the scope in detail via design workshops with input from subject matter experts.
3	[enter date]	Project schedule is not clearly defined or understood	Low	Medium	Medium	Project Manager	Hold scheduling workshops with the project team so they understand the plan and likelihood fo missed tasks is reduced.

Automated Tools for Risk Management

- Aims to minimize manual effort
- Can be time consuming to setup
- Perform calculations quickly

Qualitative versus Quantitative

- Two types of Risk Analysis
  - Quantitative Risk Analysis
  - Qualitative Risk Analysis
- Both provide unique capabilities
- Both are often required to get a full picture

Quantitative Risk Analysis

- Assign independently objective numeric monetary values
- Fully quantitative if all elements of the risk analysis are quantified
- Sometimes, Difficult to achieve
- Requires substantial time and personnel resources

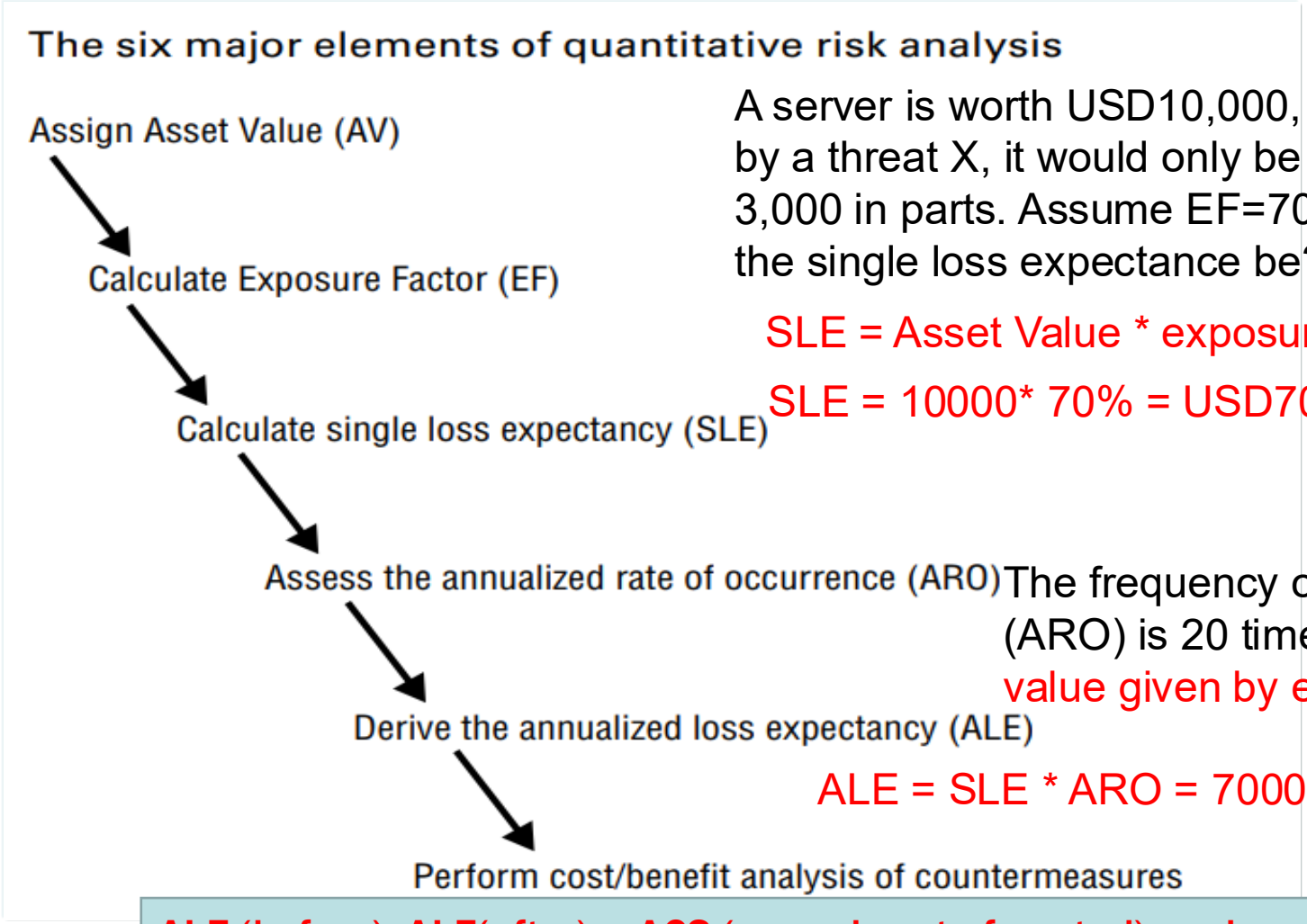
RISK = MONEY

Quantitative Analysis Steps

- Three primary steps
  - Determining Asset Value
  - Estimate potential losses
  - Conduct a threat analysis (prob. & impact)
  - Determine annual loss expectancy

Risk ID	Risk Name	Description	Risk Type	Probability	Impact	Expected Value
001	Availability of Senior Designers	Two senior designers needed to work on the front end design.	Threat	60%	$50,000	$30,000
002	Delivery Overrun for Driver module	Driver module is found to be more complex and might result in schedule overrun.	Threat	55%	$68,000	$40,800
004	Need of separate automation software	Automation software is needed to run 100,000 test cases for stability check.	Threat	58%	$55,000	$33,000

Real example



A server is worth USD10,000, if it was attacked by a threat X, it would only be worth USD 3,000 in parts. Assume EF=70%. What would the single loss expectance be?

SLE = Asset Value * exposure factor

SLE = 10000* 70% = USD7000

The frequency of threat in a year (ARO) is 20 times (subjective value given by experts)

ALE = SLE * ARO = 7000 * 20= SR140000

ALE (before)- ALE(after) – ACS (annual cost of control)= value of control

140000- 50000 – 30000= 60000 (value of control)

Ranked Risk Worksheet

Asset	Asset Impact or Relative Value	Vulnerability	Vulnerability Likelihood	Risk-Rating Factor
Customer service request via e-mail (inbound)	55	E-mail disruption due to hardware failure	0.2	11
Customer order via SSL (inbound)	100	Lost orders due to web server hardware failure	0.1	10
Customer order via SSL (inbound)	100	Lost orders due to Web server or ISP service failure	0.1	10
Customer service request via e-mail (inbound)	55	E-mail disruption due to SMTP mail relay attack	0.1	5.5
Customer service request via e-mail (inbound)	55	E-mail disruption due to ISP service failure	0.1	5.5
Customer order via SSL (inbound)	100	Lost orders due to Web server denial-of-service attack	0.025	2.5
Customer order via SSL (inbound)	100	Lost orders due to Web server software failure	0.01	1

Qualitative Risk Analysis

- Scenario Oriented
  - Does not attempt to assign absolute numeric values to risk components
- Purely qualitative risk analysis is possible

Qualitative Risk Analysis Critical Factors

- Rank seriousness of threats and sensitivity of assets
- Perform a carefully reasoned risk assessment

Risk Levels (AS/NZ 4360 Standard)

	Consequence:				
	Insignificant	*Minor*	*Moderate*	*Major*	*Catastrophic*
Likelihood:	*1*	*2*	*3*	*4*	*5*
A (almost certain)	H	H	E	E	E
B (likely)	M	H	H	E	E
C (possible)	L	M	H	E	E
D (unlikely)	L	L	M	H	E
E (rare)	L	L	M	H	H

E	Extreme Risk: Immediate action required to mitigate the risk or decide to not proceed
H	High Risk: Action should be taken to compensate for the risk
M	Moderate Risk: Action should be taken to monitor the risk
L	Low Risk: Routine acceptance of the risk

5 top Qualitative RA Techniques

- Delphi Technique
- SWIFT Analysis: “Structured What-If”
- Decision Tree Analysis
- Bow-tie Analysis
- Probability/Consequence Matrix
-

Qualitative Risk Analysis

- Risk Register
- Probability-Impact (PI) Matrix
- Risk Catergorization
- Expert Judgement

Quantitative Risk Analysis

- Sensitivity Analysis
- Decision Tree Analysis
- Scenario Analysis
- Latin Hyper Cube Simulation
- Monte Carlo Simulation

Quantitative vs. Qualitative

TABLE 2.2 Comparison of quantitative and qualitative risk analysis

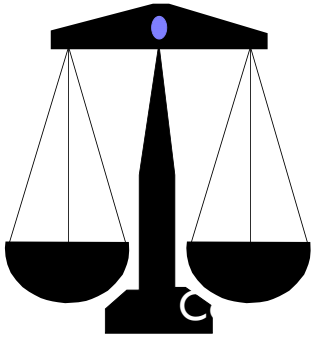
Characteristic	Qualitative	Quantitative
Employs complex functions	No	Yes
Uses cost/benefit analysis	No	Yes
Results in specific values	No	Yes
Requires guesswork	Yes	No
Supports automation	No	Yes
Involves a high volume of information	No	Yes
Is objective	No	Yes
Uses opinions	Yes	No
Requires significant time and effort	No	Yes
Offers useful and meaningful results	Yes	Yes

Risk Mitigation Options

- Risk Acceptance :
  - *if cost is higher than the expected loss*
- Risk Reduction :
  - *implement countermeasure to reduce the risk impact.*
- Risk Transference:
  - *outsource or transfer to third party.*
- Risk Avoidance
  - *Stop the activities that are having the risks.*

The Right Amount of Security

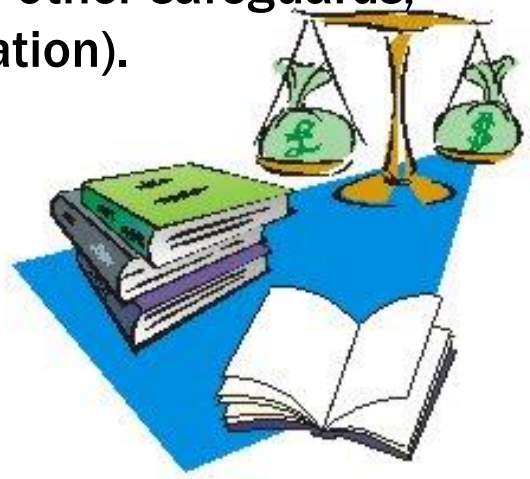
- Cost/Benefit Analysis - balance between the cost to protect and asset value
- Before we proceed with CBA, we must understand the:
  - Adversary, means, motives, and opportunity
  - Asset value (more than just cost)
  - Threats Analysis
  - Vulnerabilities Analysis
  - Resulting Risk
  - Countermeasures
  - Risk tolerance :
    - Risk appetite



Security is a Balancing Act!

Countermeasure Selection Principles

- Based on a cost/benefit analysis
- Cost must be justified by the potential loss
- Accountability: *who is responsible?*
- Absence of Design Secrecy:
  - Changeability of safeguards, interoperability with other safeguards, confidence in the design (common criteria evaluation).
- Audit Capability
  - Can be tested and audited.



Countermeasure Selection Principles

- Vendor Trustworthiness
- Independence of Control and Subject
  - segregation of duties
- Universal Application
- Compartmentalization and Defense in Depth
- Isolation, Economy, and least Common Mechanism

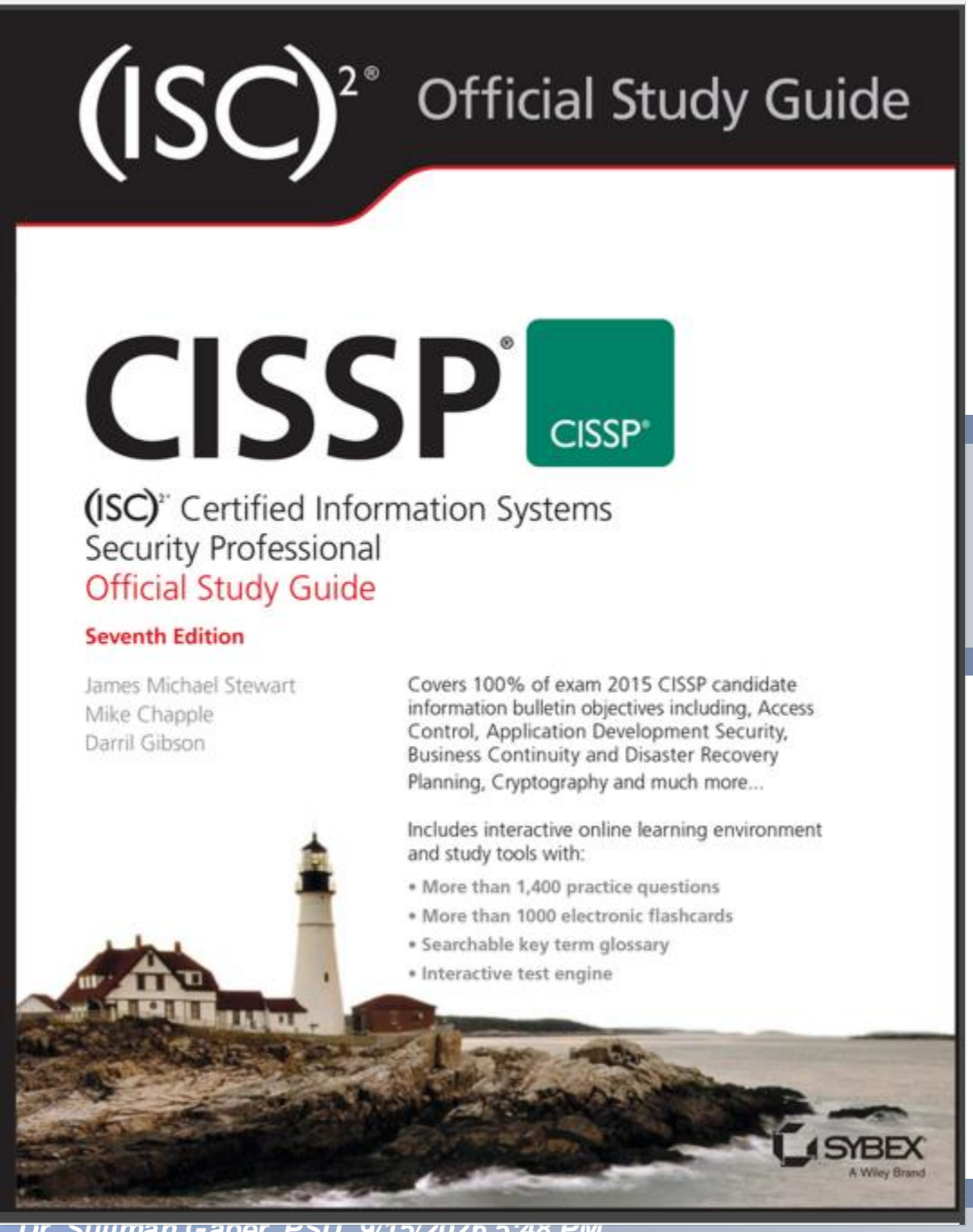
Countermeasure Selection Principles

- Acceptance and Tolerance by Personnel
- Minimum Human Intervention
- Sustainability
- Reaction and Recovery
- Override and Fail-safe Defaults
- Residuals and Reset

Types of Security Controls

- Directive Controls. Often called administrative controls, these are intended to advise employees of the behavior expected of them during their interfaces with or use the organization's information systems.
- Preventive Controls. Included in preventive controls are physical, administrative, and technical measures intended to prevent actions violating policy or increasing risk to system resources.
- Detective Controls. Detective controls involve the use of practices, processes, and tools that identify and possibly react to security violations.
- Corrective Controls. Corrective controls also involve physical, administrative, and technical measures designed to react to detection of an incident in order to reduce or eliminate the opportunity for the unwanted event to recur.
- Recovery Controls. Once an incident occurs that results in the compromise of integrity or availability, the implementation of recovery controls is necessary to restore the system or operation to a normal operating state.


ASSESS RISK
IDENTIFY RISK
RISK MANAGEMENT PROCESS
CONTROL RISK
REVIEW CONTROLS



Chapter 2: Personnel Security and Risk Management Concepts

Preparation Exam for CISSP: https://www.simplilearn.com/cissp-exam-prep-free-practice-test