NETWORK SECURITY ASSESSMENT AND AUDIT

LECTURE 9

"It's tough to make predictions, especially about the future."
Yogi Berra, Niels Bohr

UTeM
UNIVERSITI TEKNIKAL MALAYSIA MELAKA
DR ZAHEERA BINTI ZAINAL ABIDIN

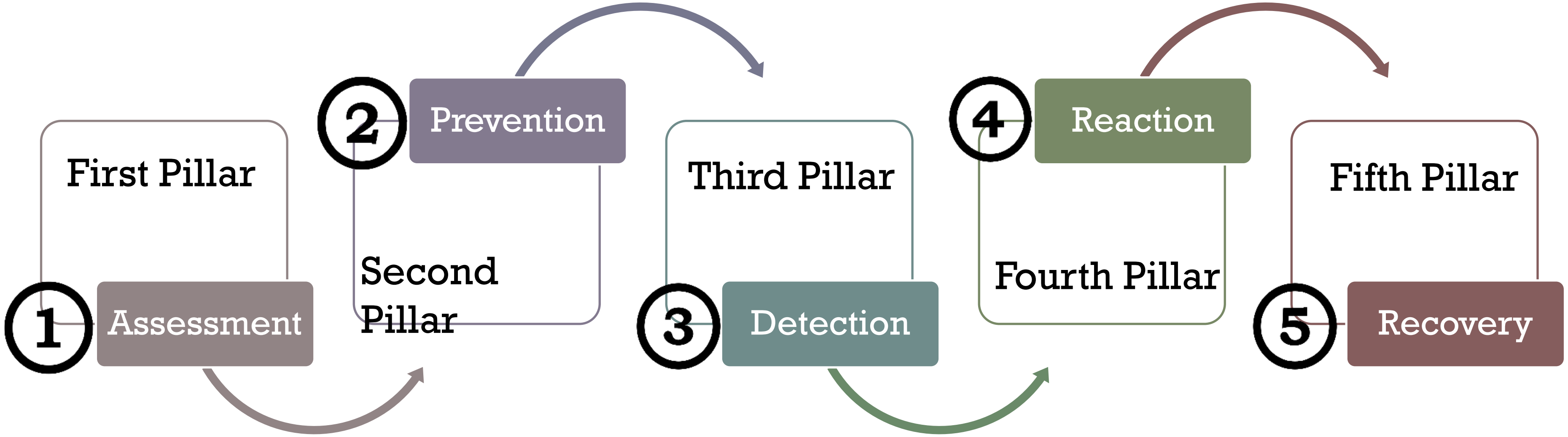
CONTENT

- INTRODUCTION
- NETWORK SECURITY AUDITING - 5 PRINCIPLES OF NETWORK SECURITY AUDIT
- RISK ASSESSMENT
- RISK MITIGATION

LEARNING OBJECTIVES

- Student need to perform Network Security Audit and Assessment, by following Standard ISO 27002
- Understand the importance of good project risk management
- Understand what risk is and describe different tolerances for risk
- Identify common sources of risk on network security project management and develop strategies for reducing them
- Describe common risk conditions that occur in each project area
- Explain various techniques for quantifying risk and calculate expected monetary values of projects
- Describe how software tool can assist in network security project management

NETWORK SECURITY AUDITING PRINCIPLE



First Pillar

1 Assessment

2 Prevention

Second Pillar

Third Pillar

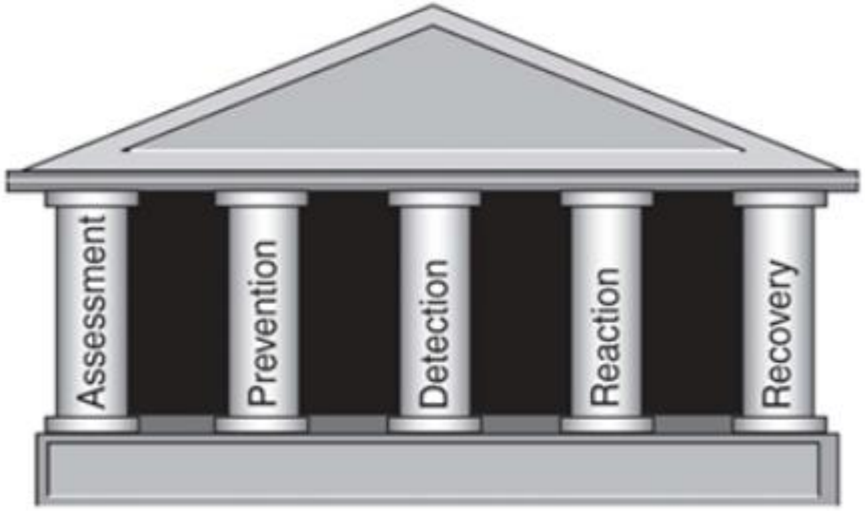
3 Detection

4 Reaction

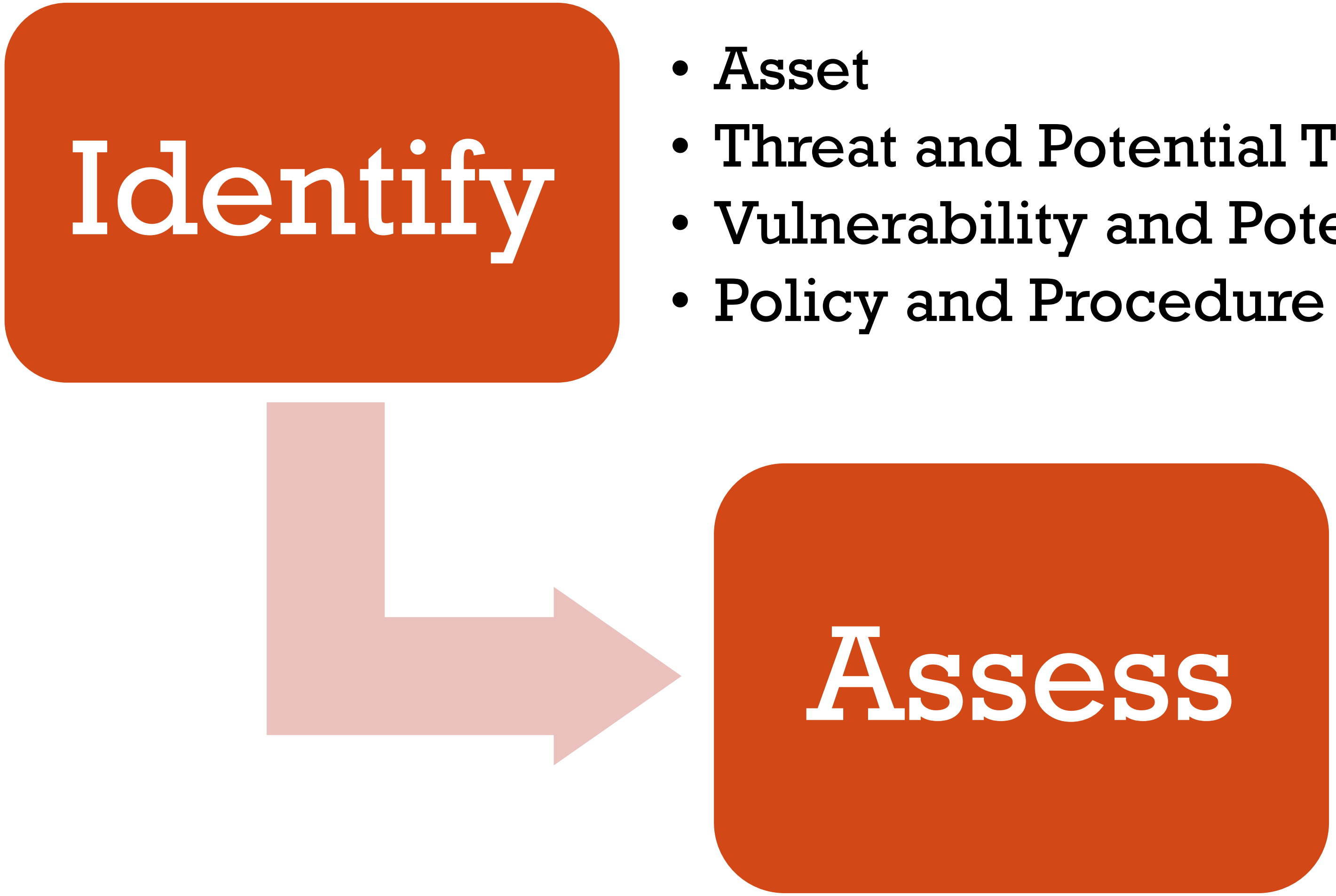
Fourth Pillar

Fifth Pillar

5 Recovery



ASSESSMENT



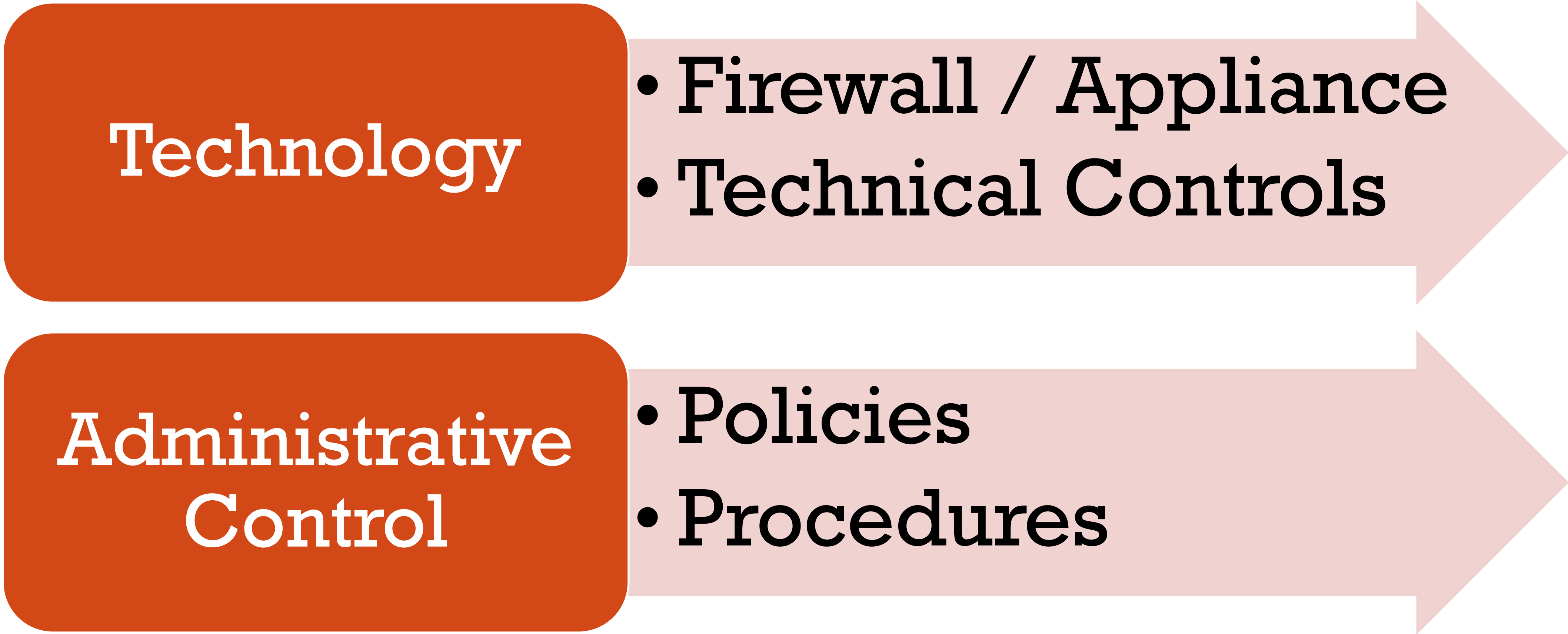
Identify

- Asset
- Threat and Potential Threat
- Vulnerability and Potential Vulnerability
- Policy and Procedure

Assess

- Measure the category level of asset, threat, vulnerability, policy and procedure based on the percentage

PREVENTION



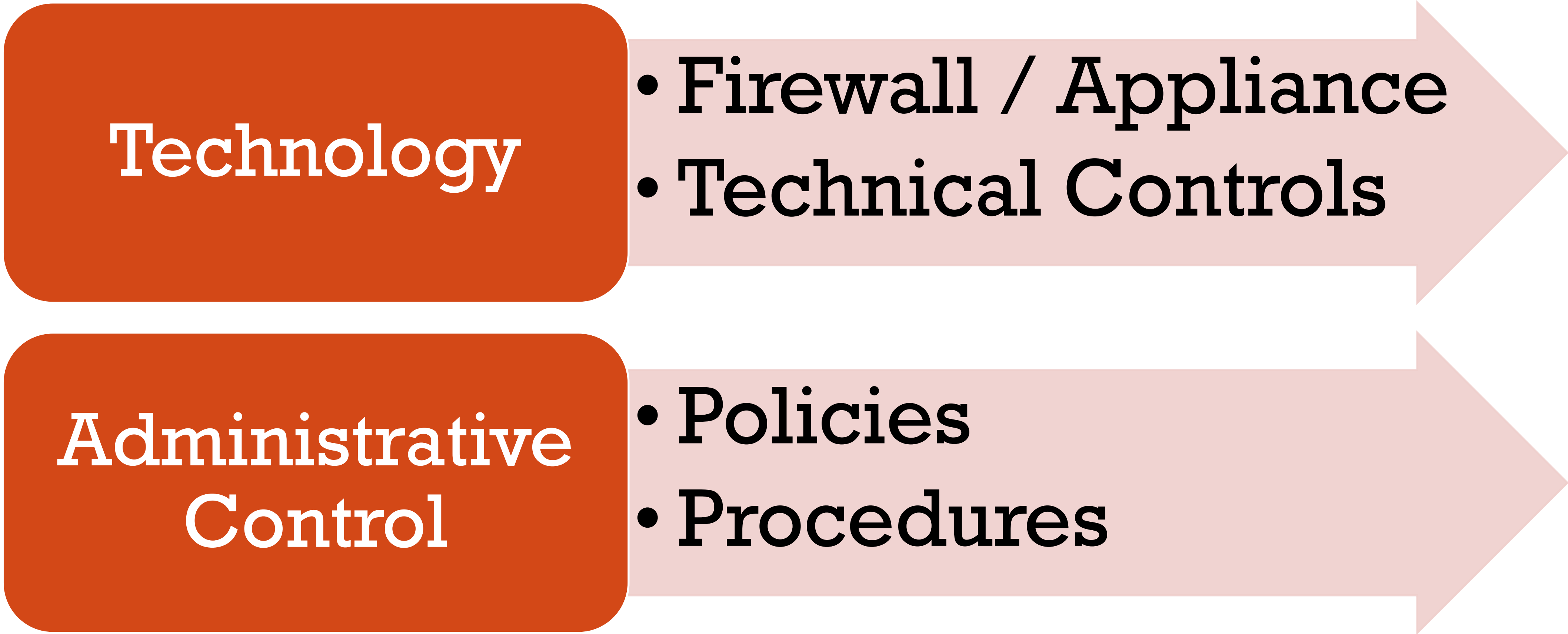
Technology

- Firewall / Appliance
- Technical Controls

Administrative Control

- Policies
- Procedures

DETECTION



Technology

- Firewall / Appliance
- Technical Controls

Administrative Control

- Policies
- Procedures

REACTION

- When prevention and detection are effective, reaction time is greatly reduced. No one wants to find out that they have a breach, but if you do have a compromise you need to do something about it now! Reaction is the aspect of security that is most concerned with time. The goal is to minimize the time from detection to response so that exposure to the incident is minimized. Fast reaction depends on prevention and detection to provide the data and context needed to recognize a security breach. Of course, just knowing about a compromise doesn't help if you haven't planned out in advance what to do. This planned and coordinated response is called incident handling. Some companies have a dedicated incident-handling team that can move in at a moments notice to reduce exposure time. Not everyone has the budget for these types of teams. Even if your company doesn't have a dedicated team, some forethought and planning can mean the difference between everyone falling all over themselves trying to figure out what to do next and restoring key services.

- Automated response through technology is an important tool that reduces your reaction time to a security incident. But as good as automated response technologies are, you still need skilled people to handle the incident to ensure that the incident is real and not a hiccup on the wire. How quickly and efficiently incidents are handled is one of the most important tests to the effectiveness of a company's security program. When the alarms go off, how you react can make all of the difference in the world!

RECOVERY

- When your company has an eCommerce system that simply must be available to your customers or it processes hundreds of thousands of dollars in sales a minute, downtime is relatively easy to quantify. Recovery is where you play detective to determine what went wrong so that you can get the systems back on line without opening up the same vulnerability or condition that caused the problem in the first place. Do you patch the exploited vulnerability and recover the data from backup or do you have a bigger flaw in security controls that allowed the incident to occur? What was the reason that the system was compromised? How did the technical controls fail? Was there a misconfiguration? The recovery phase doesn’t end with bringing the system back online. There is also the post-mortem aspect that determines what changes need to be made to processes, procedures, and technologies to reduce the likelihood of this type of vulnerability in the future. As an auditor, you must ensure that the organizations you audit have a plan for recovery that addresses these issues.

TOOLS FOR NETWORK SECURITY AUDITING

Network Scanning

- NMAP (Wired)
- Wireshark (Wireless)

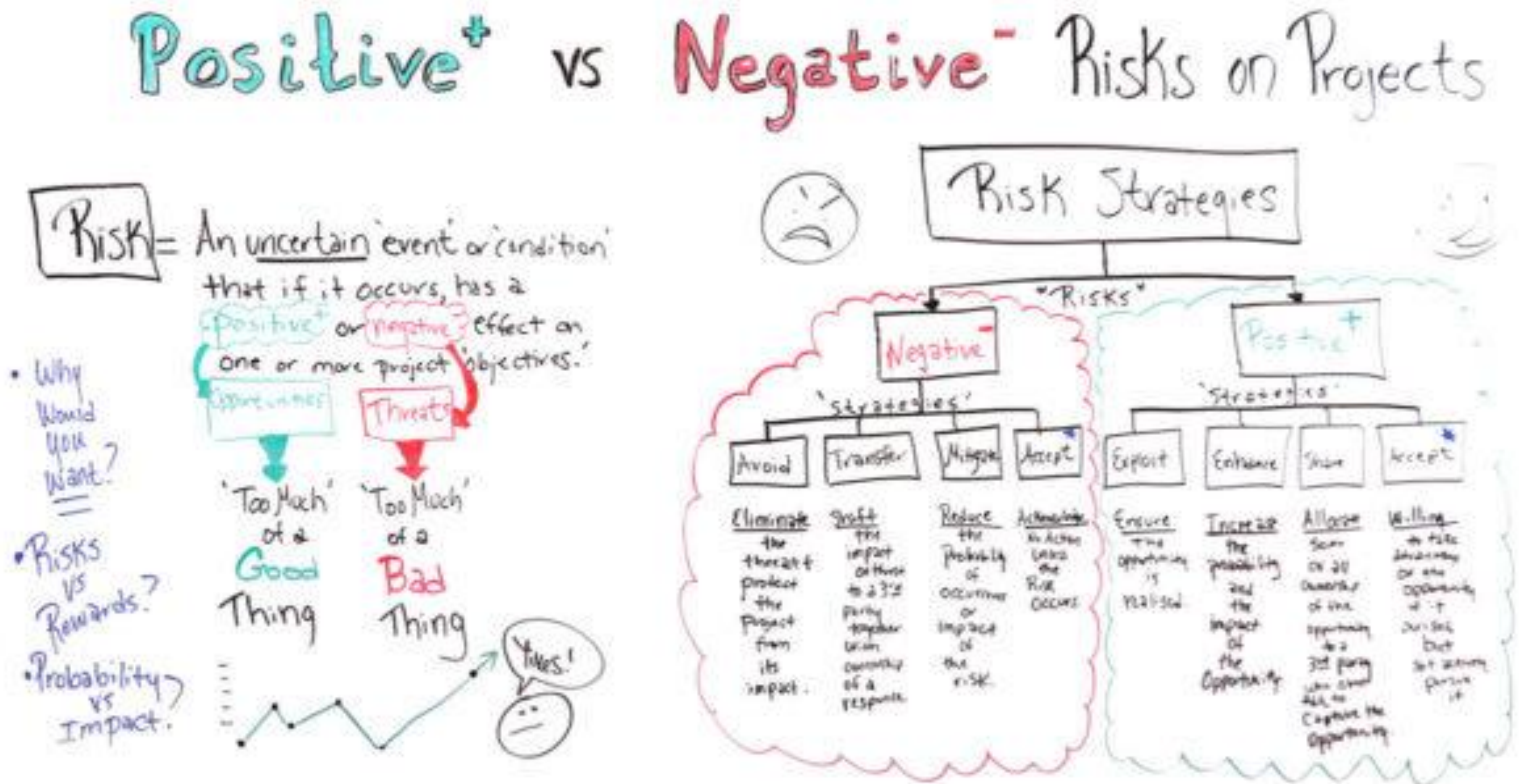
Vulnerability Assessment Tool

- Nessus

11

RISK MANAGEMENT

DR ZAHEERA BINTI ZAINAL ABIDIN



Positive+ vs Negative- Risks on Projects

Risk = An uncertain 'event' or 'condition' that if it occurs, has a 'positive' or 'negative' effect on one or more project 'objectives.'

- Why Would you Want?
- Risks vs Rewards?
- Probability vs Impact.

Avoid: Eliminate the threat & protect the project from its impact.

Transfer: Shift the impact of threat to a 3rd party together with ownership of a response.

Mitigate: Reduce the probability of occurrence or impact of the risk.

Accept: Acknowledge No Action unless the Risk occurs

Exploit: Ensure the opportunity is realised

Enhance: Increase the possibility and the impact of the Opportunity

Share: Allocate some or all ownership of the opportunity to a 3rd party who is best able to capture the opportunity

Accept: Willing to take advantage of the opportunity if it arises but not actively pursue it

DEFINITION OF RISK MANAGEMENT – 1

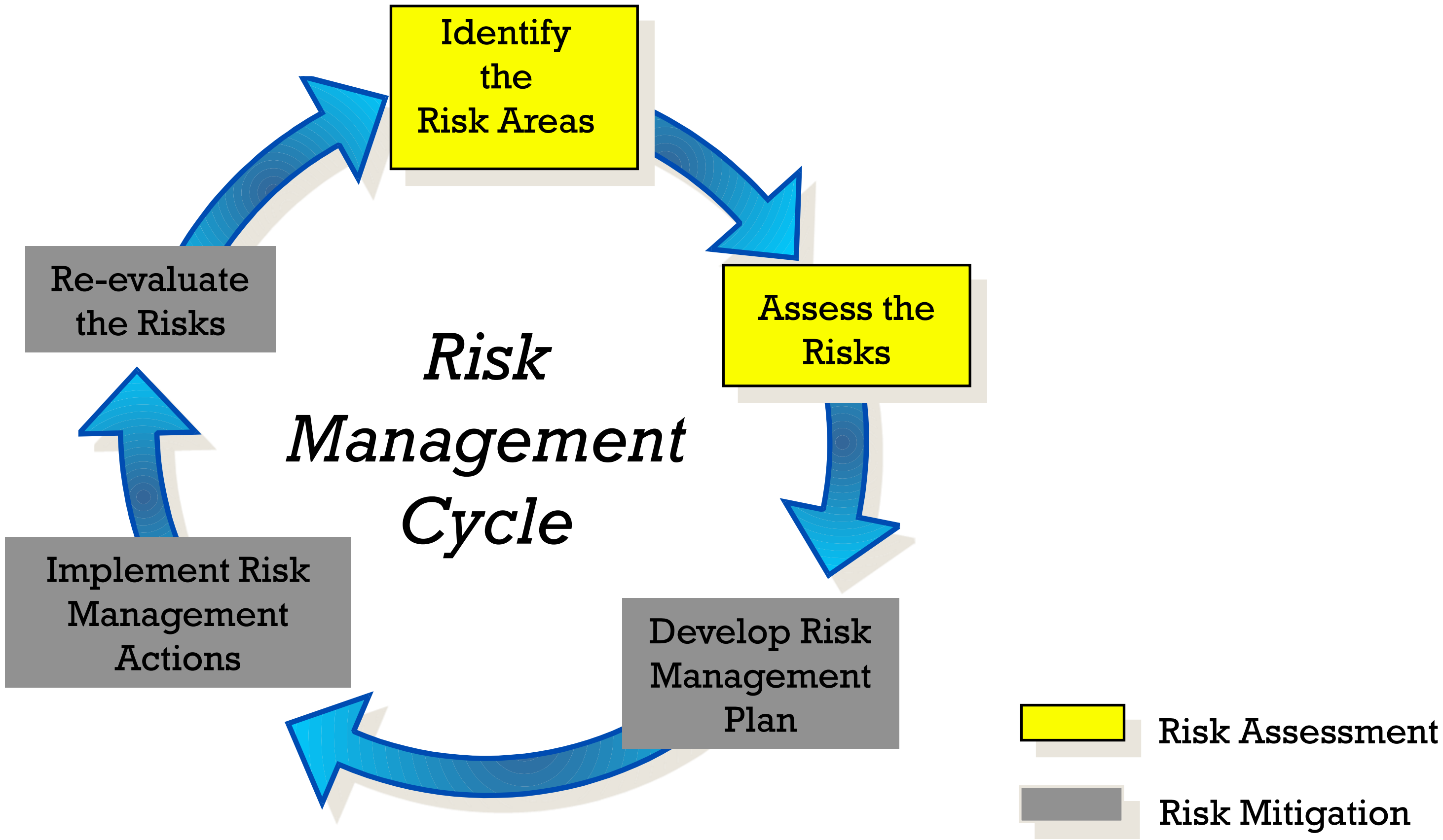
- Project risk management is the art and science of identifying, assigning and responding to risk throughout the life of a project which meet the project objectives.
- Risk management has a positive impact on selecting projects, determining the scope of projects and developing realistic schedules and cost estimation. It helps project stakeholders understand the nature of the project, involves team members in defining strengths and weaknesses, and helps to integrate the other project management knowledge areas.
- What is risk? Risk is the possibility of loss or injury. Thus, project risk involves understanding potential problems that might occur on the project and how it may impede project success.
- On the other hand, risk management is like an insurance.

DEFINITION OF RISK MANAGEMENT – 2

- The process concerned with identification, measurement, control and minimization of security risks in information systems to a level commensurate with the value of the assets protected.
- The likelihood that a particular threat using a specific attack, will exploit a particular vulnerability of a system that results in an undesirable consequence.
- Threat is any circumstance or event with the potential to cause harm to an information system in the form of destruction, disclosure, adverse modification of data, and/or the denial of service.

(Definition from National Information Systems Security (INFOSEC) Glossary, NSTISSI No. 4009, Aug. 1997)

RISK MANAGEMENT LIFE CYCLE



Identify the Risk Areas

Assess the Risks

Develop Risk Management Plan

Implement Risk Management Actions

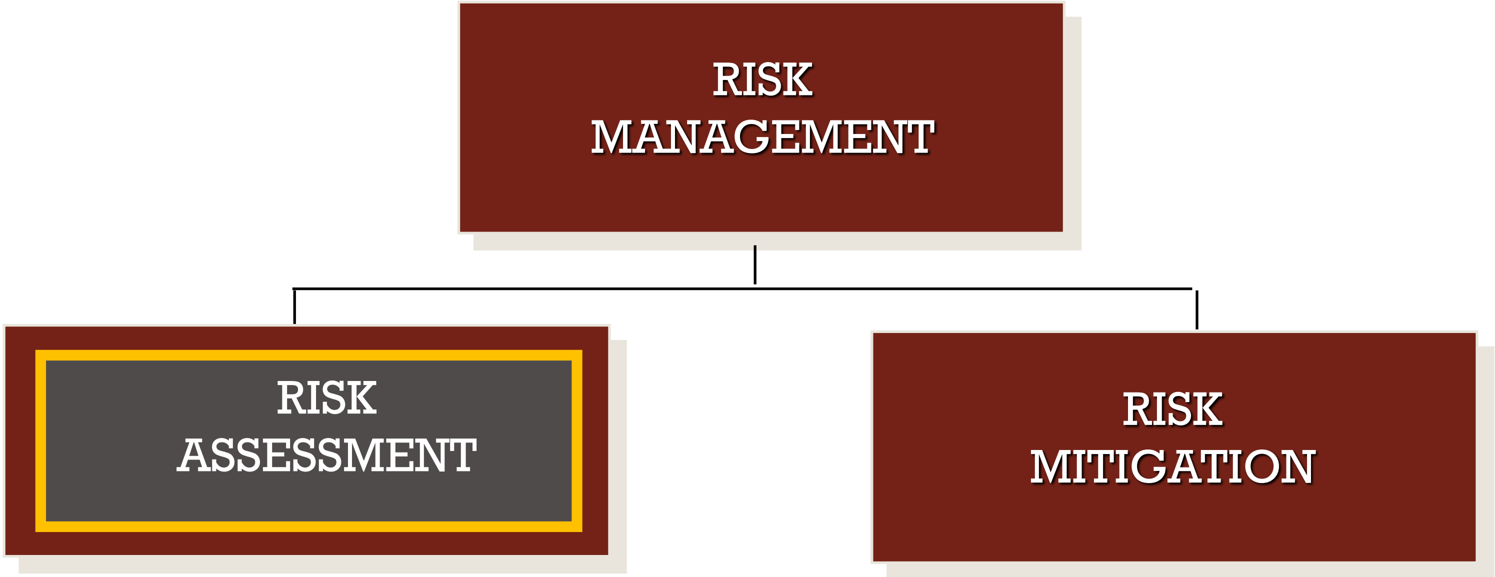
Re-evaluate the Risks

Risk Management Cycle

🟨 Risk Assessment

▨ Risk Mitigation

CLASSIFICATION IN RISK MANAGEMENT



RISK MANAGEMENT

RISK ASSESSMENT

RISK MITIGATION

RISK ASSESSMENT

- Risk Assessment:
  - Asset, Threat and Vulnerabilities Identification
  - Asset, Threat and Vulnerabilities Analysis

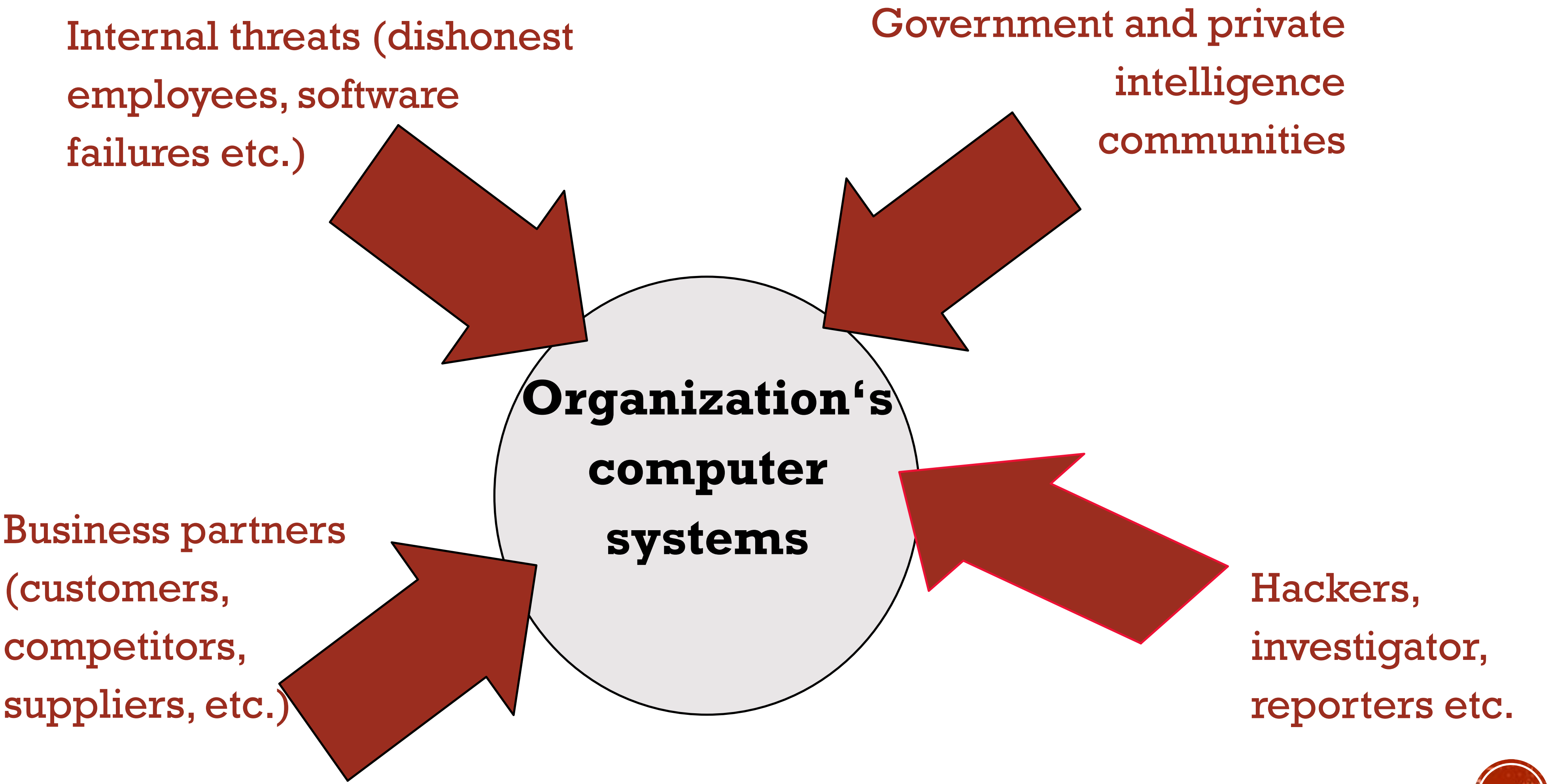
RISK IDENTIFICATION

- Risk identification is the process of gaining an understanding of potential unsatisfactory outcomes which are associated with particular project.
- Perform the risk identification checklists in the form of flowchart, interviews, power point presentation (excel) and diagrams.
- Identify the potential risk based on area such scope, time cost and quality as in Table 1.

TABLE 1: POTENTIAL RISK BASED ON AREA

Area	Risk Conditions
Integration	Inadequate planning: poor resources allocation; poor integration management; lack of post-project review
Scope	Poor definition of scope /work packages; incomplete definition of quality requirements; inadequate scope control
Time	Errors in estimating time / resources availability; poor allocation and management of float; early release of competitive products
Cost	Estimating errors; inadequate productivity, cost, change or contingency control; poor maintenance, poor security
Quality	Poor attitude towards quality; substandard design; inadequate quality assurance program
Human Resources	Poor conflict management; absence of leadership; poor project organization
Communications	Lack of consultation with key stakeholders; careless in communication
Risk	Ignoring risk; unclear assignment of risk; poor insurance management
Procurement	Unenforceable conditions or contract clauses; adversarial relations

ASSET, THREAT & VULNERABILITY ASSESSMENT



Internal threats (dishonest employees, software failures etc.)

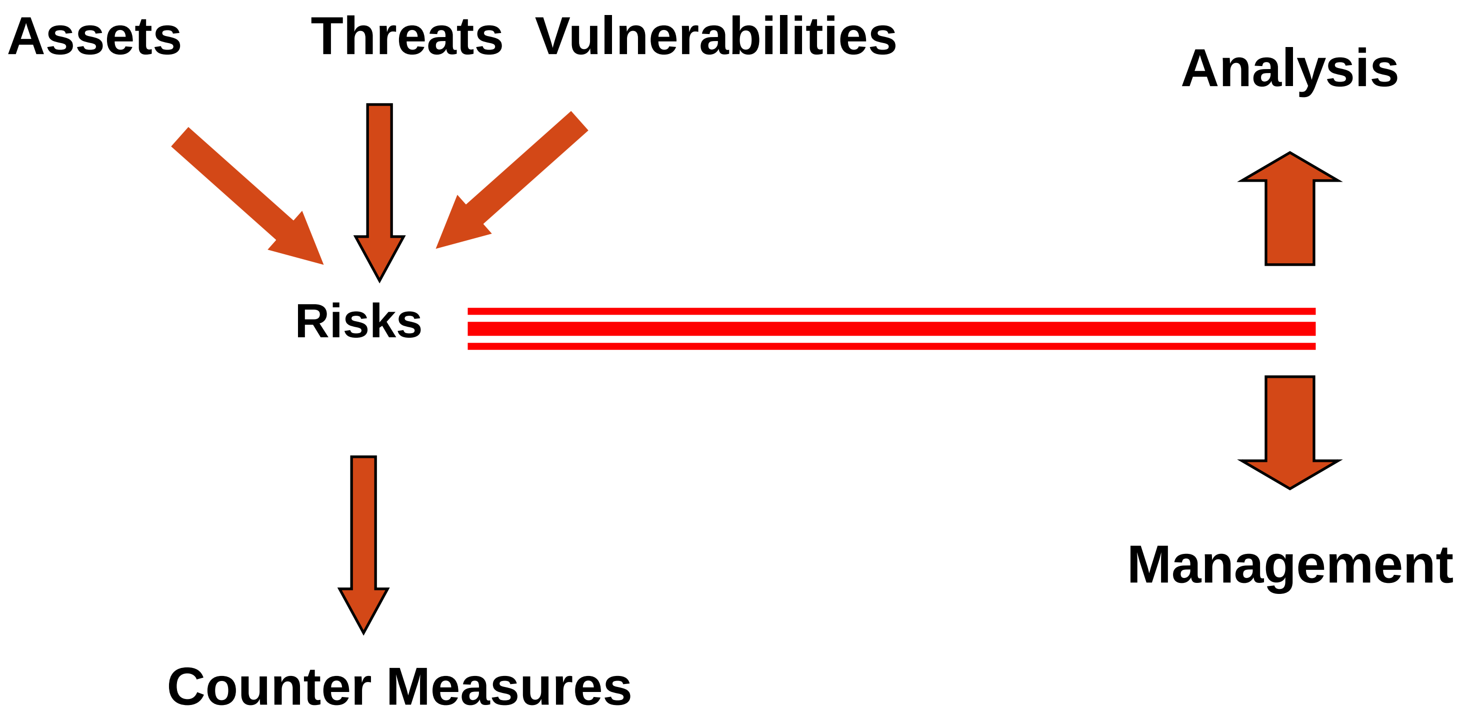
Government and private intelligence communities

Organization's computer systems

Business partners (customers, competitors, suppliers, etc.)

Hackers, investigator, reporters etc.

RISK ANALYSIS / ASSESSMENT



Assets Threats Vulnerabilities

Risks

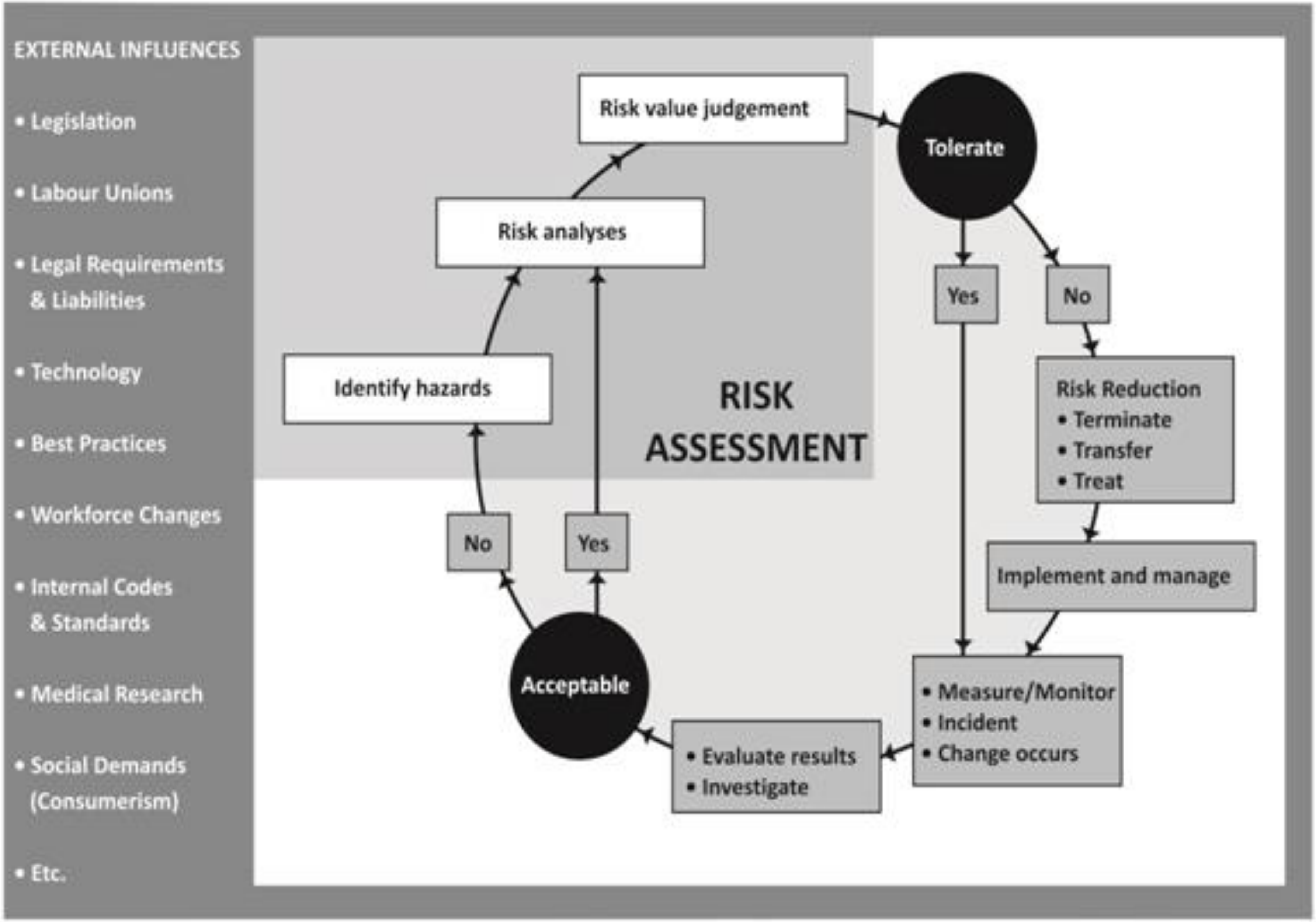
Counter Measures

Analysis

Management

RISK ASSESSMENT PROCESS

The Risk Management Process



EXTERNAL INFLUENCES

- Legislation
- Labour Unions
- Legal Requirements & Liabilities
- Technology
- Best Practices
- Workforce Changes
- Internal Codes & Standards
- Medical Research
- Social Demands (Consumerism)
- Etc.

RISK ASSESSMENT

Identify hazards

Risk analyses

Risk value judgement

Tolerate

Yes

No

Risk Reduction
- Terminate
- Transfer
- Treat

Implement and manage

- Measure/Monitor
- Incident
- Change occurs

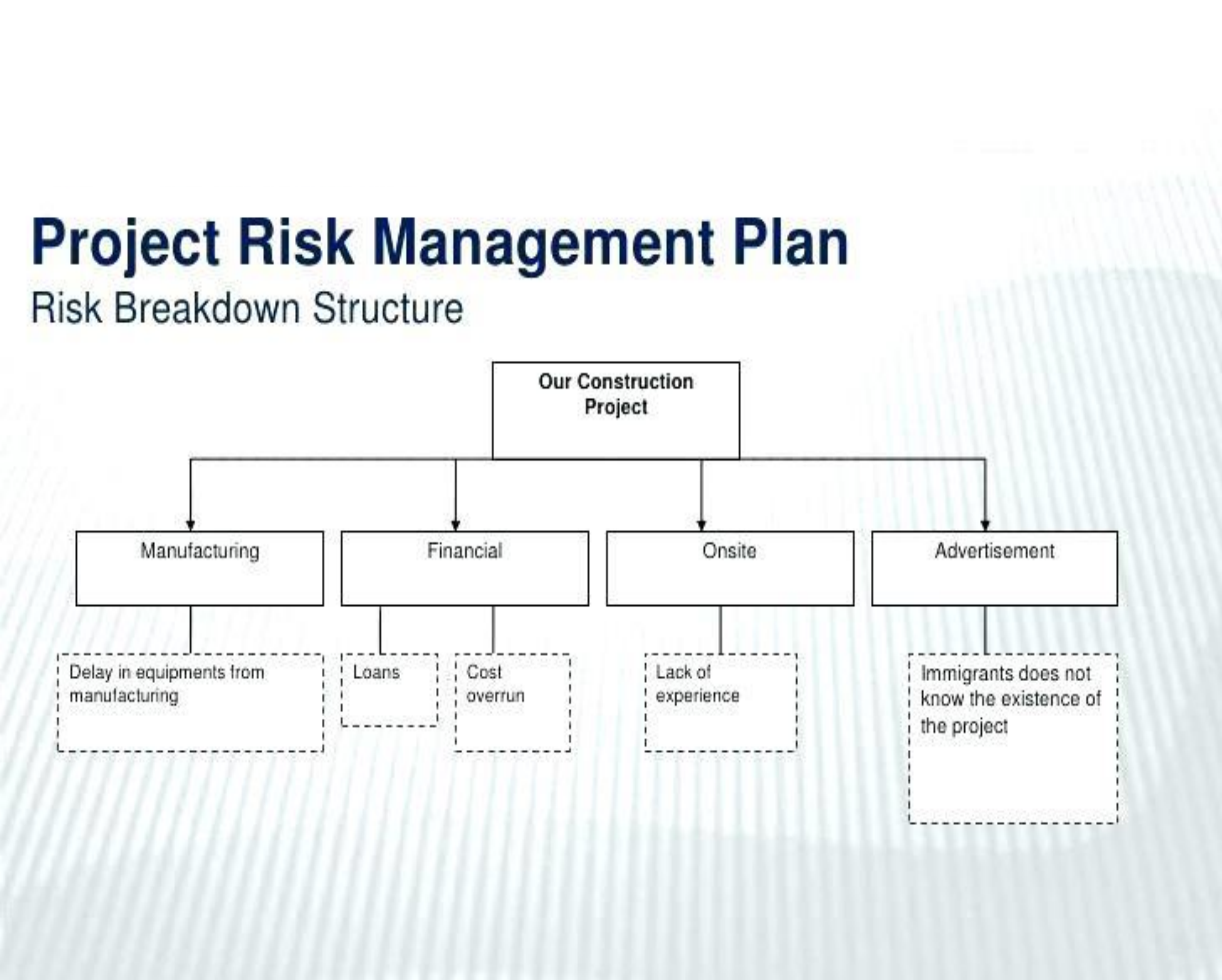
- Evaluate results
- Investigate

Acceptable

No

Yes

EXAMPLE OF RISK BREAKDOWN STRUCTURE



Project Risk Management Plan

Risk Breakdown Structure

Our Construction Project

Manufacturing

- Delay in equipments from manufacturing

Financial

- Loans
- Cost overrun

Onsite

- Lack of experience

Advertisement

- Immigrants does not know the existence of the project

RISK ASSESSMENT / RISK ANALYSIS

- Security risk analysis, otherwise known as risk assessment, is fundamental to the security of any organization. It is essential in ensuring that controls and expenditure are fully commensurate with the risks to which the organization is exposed.
- It is a process of evaluating risks to assess the range of possible project outcomes. Also, it helps to determine which opportunities and risks to respond to which to accept and which to ignore.
- Techniques for quantifying risks include expected monetary value (EMV) analysis, calculation of risks factor, PERT estimations, simulations and expert judgment.

RISK ANALYSIS

- Suppose an event is associated with a loss - this loss is the **risk impact** (sometime simply called **risk**), measured in RM's
- There is a probability (**risk probability**) of occurrence, a number in the range 0 (if not possible) to 1 (if certain)
- Risk exposure is the RM amount

  Risk-exposure = Risk-impact *x* Risk-probability
- For risk analysis:

  RISK = LOSS (RM) *x* PROBABILITY

  Usually measured as RM per annum.
- Expressed as **Annual Loss Expectancy** (ALE) expressed as: RM per annum
- By *quantifying* the risk, we can justify the *benefit* of spending money to implement *controls*

EXAMPLE 1

- Hard Disk Failure on your PC
  - Hard Disks fail about every three years;
    Probability of failure is 1/3 per year
  - Intrinsic cost say RM600 – to buy a new disk
  - But also, say 10 hours of your effort to reload O/sys and software *and*
  - Say 4 hours to re-key assignments from last backup.
  - Assume RM10.00 per hour for your effort
  - *Total loss = RM600 + 10 x(10 + 4) = RM740*
- Annual loss expectancy = (740 x 1/3) RM pa = RM246.66 pa

EXAMPLE 2

- What about a virus attack on the same system?
  - You frequently swap stuff with other people, but have no ant-viral software running.
  - Assume an attack every 6 months; *Probability is 2 per annum*
  - No need to buy a new disk
  - *Assume the same r*ebuild effort = (10 + 4)hours,
    Total loss = 10 x(10+4) = RM140
  - ALE = (140 x 2) RM pa = RM280 pa

EXAMPLE TO CALCULATE ASSET

- Asset Valuation Worksheet
  - Asset: *(name, serial number)*
  - Asset Intrinsic value: $
  - Which value is the intrinsic value ?
    - physical, insured, depreciated, replacement, value or
  - Asset Acquired value:
    which includes the cost of the loss of:
    - Integrity $
    - Availability $
    - Confidentiality $

COMPUTE THE EXPECTED LOSS

- For each asset,
  (total) risk = Σ (risks) = Sum(risks)
  =Sum(Loss *x* Probability per annum) RM pa

- *For ALL assets* we can derive a *total* sum,
  the *Annual Loss Expectancy, RM per annum*

- Price-Waterhouse study: For Australian organizations with no security plan in place,
  <u>8% of turnover is lost each year</u> (!)

MAKING SENSE?

- *REALITY CHECK:*
- If a company is still in business, the **Annual Loss Expectancy** (ALE) has to be a *lot* less than the annual turnover

COST OF APPLYING CONTROLS

- Actual cost of control include
  - software purchase price
  - Installation cost
  - training cost
- Effective cost of a control = actual cost – any expected loss from using the control (such as admin or maintenance costs)
- e.g: Cost to reconstruct data: $1M at 10% probability of loss = RM100K
  Effectiveness of access control software: (say) 60% = RM60K
  Cost of the access control software = RM25K
  Expected annual cost due to loss and controls = (40+25) = RM65K
  Effective cost the control (100-65) = -RM35K
- Note that the effective cost of a control can be positive (when the control is expensive to administer or introduces new risks in another area) or negative (when the reduction in risk is greater than the cost of the control)

SOME CRITICISMS OF RISK ANALYSIS

- Although many large organizations use RA, there are some criticisms of both the idea and the methods of RA
- It may not appear sensible to talk of a *probable* loss of a specific number of dollars,
  - only when the loss occurs will we know how much it costs to fix, and bringing that cost to a one-year base is artificial.
- There is so much uncertainty in the method of calculation, that any numerical figure is meaningless
- However, Risk Management is seen as a valid undertaking, and using figures to attempt to quantify risk does give us an accountable basis for spending resources on controls

VULNERABILITY IDENTIFICATION

VULNERABILITY

- Vulnerability means a flaw or weakness in system security procedures, design, implementation or internal controls which accidentally or intentionally exploited and caused security breaches.
- Vulnerabilities occur in hardware / networks / OS / dB systems / Applications
- Examples of vulnerability in incident metabases (CVE (Mitre), ICAT (NIST), OSVDB (osvdb.com))
- Example of vulnerability at notification systems such as CERT (SEI_CMU) and Cassandra (CERIAS-Purdue)
- Deal with through threat detection / threat avoidance / threat tolerance

VULNERABILITY ASSESSMENT

- Assess and secure all parts individually

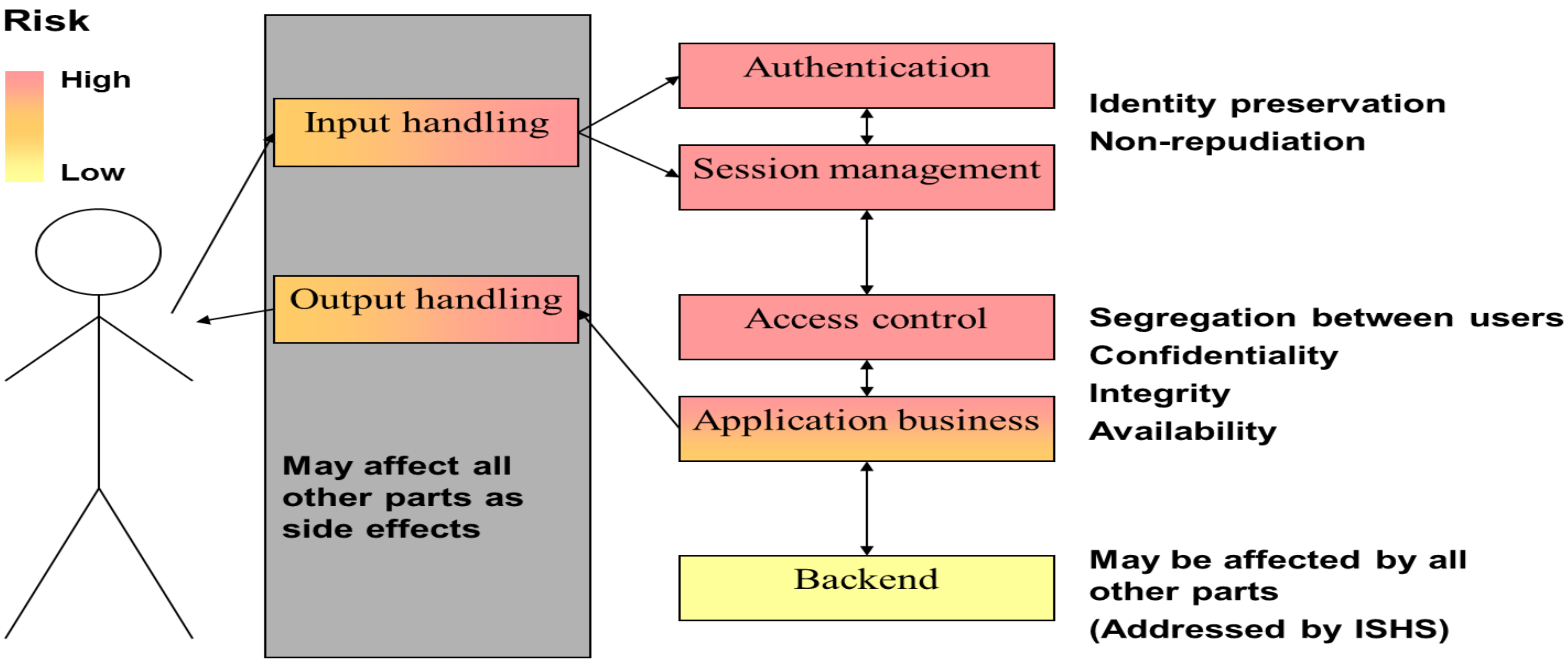
- The idea is to force an attacker to penetrate several defence layers

- As a general rule, data stored in databases are considered as "untrusted"

"In God we trust,

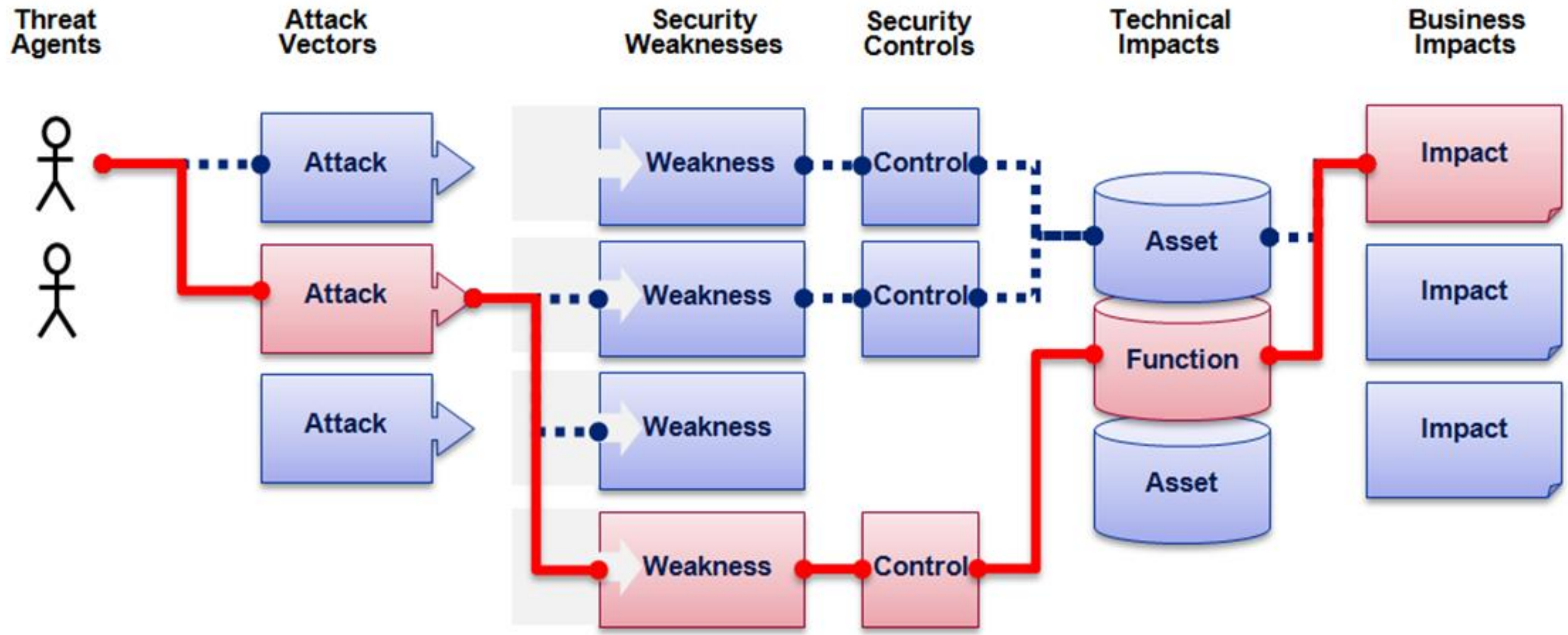
for the rest, we test"

VULNERABILITY RISK AREAS



(Gabriel BABIANO, 2012)

ENGINEERING OF ATTACKS



(Gabriel BABIANO, 2012)

RISK RESPONSE DEVELOPMENT

Risk avoidance

Risk acceptance

Risk mitigation

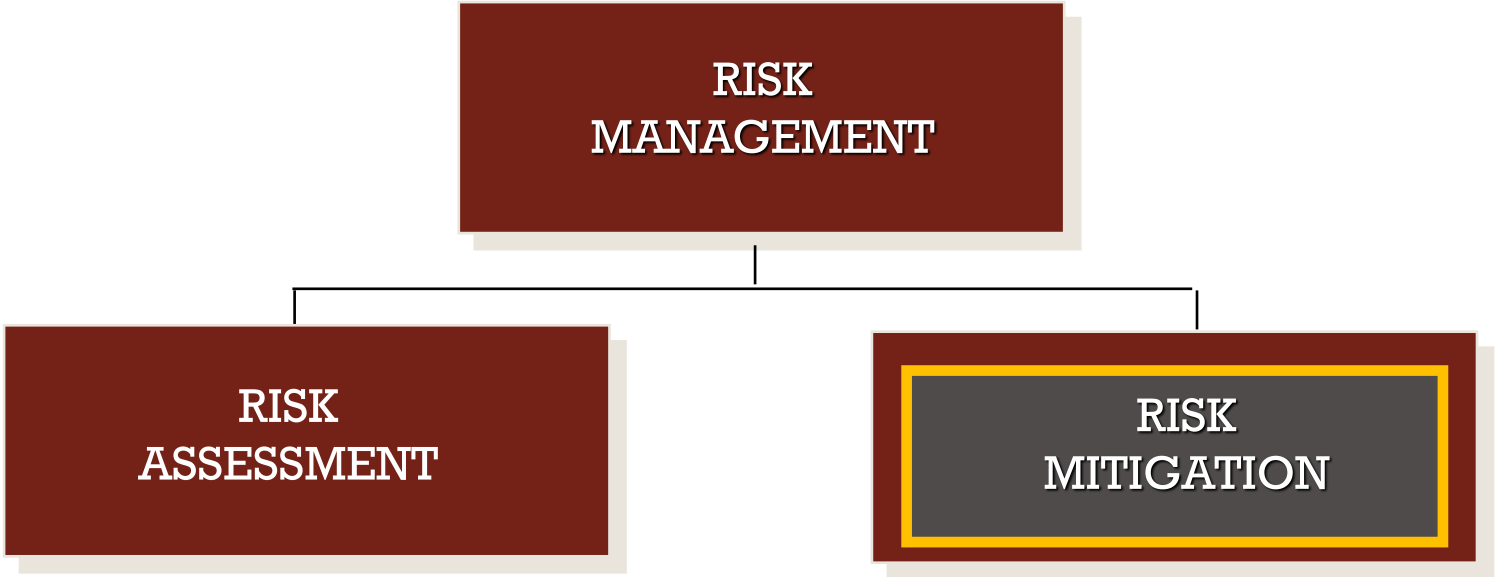
RISK RESPONSE DEVELOPMENT

- **Risk avoidance** involves eliminating specific threat or risk, usually by eliminating its causes. For example, the project team may decide to continue using specific hardware or software on the project because he /she knows it function well.

- **Risk acceptance** means accepting the consequences should a risk occur. For example, project team has a back-up plan or contingency if the specific tasks are unable to be delivered on time or as schedule.

- **Risk mitigation** reduces the impact of a risk event by reducing the probability of its occurrence. For example, using proven technology and validation techniques for better decision making.

CLASSIFICATION IN RISK MANAGEMENT



RISK MANAGEMENT

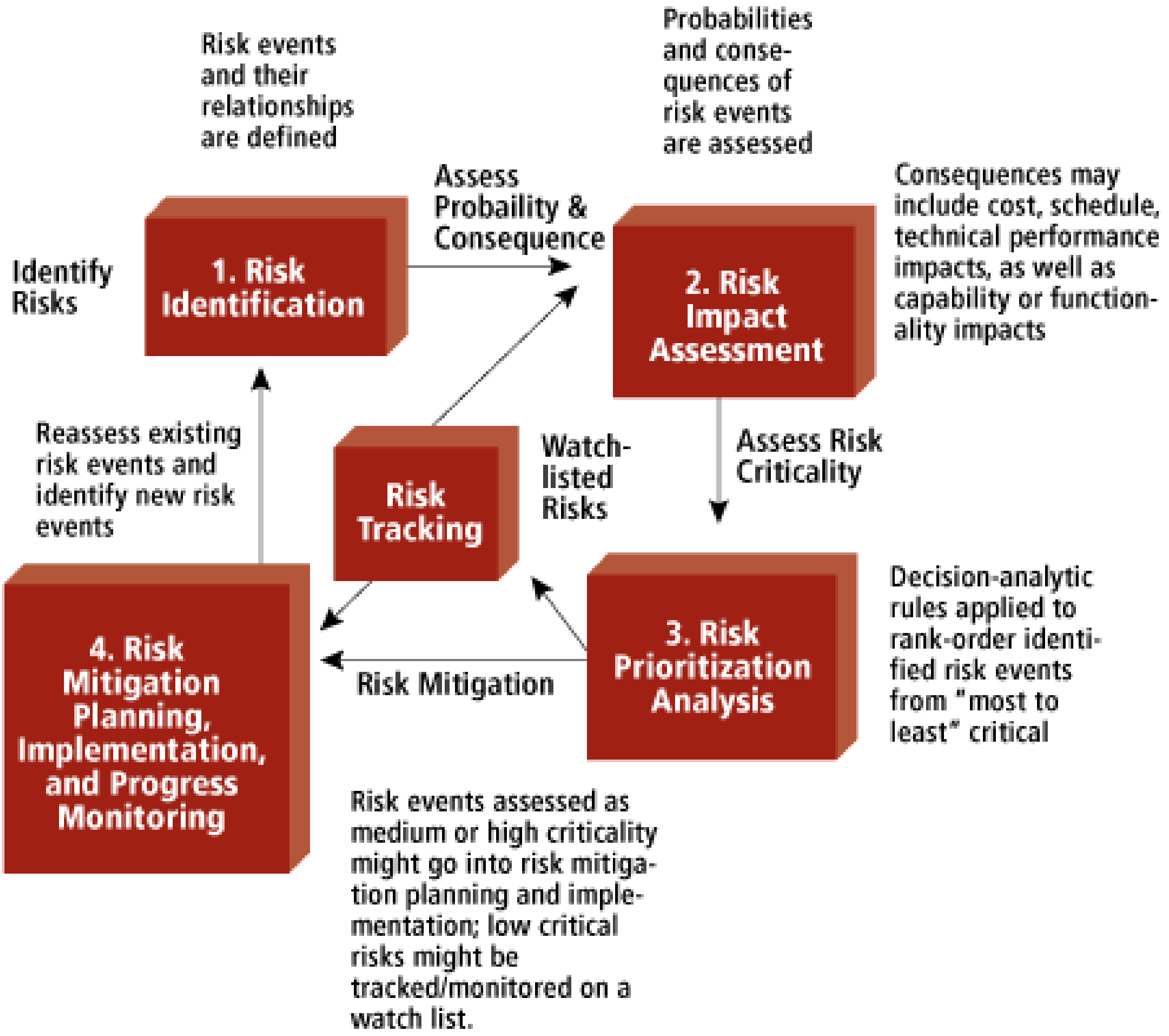
RISK ASSESSMENT

RISK MITIGATION

RISK MITIGATION

RISK MITIGATION

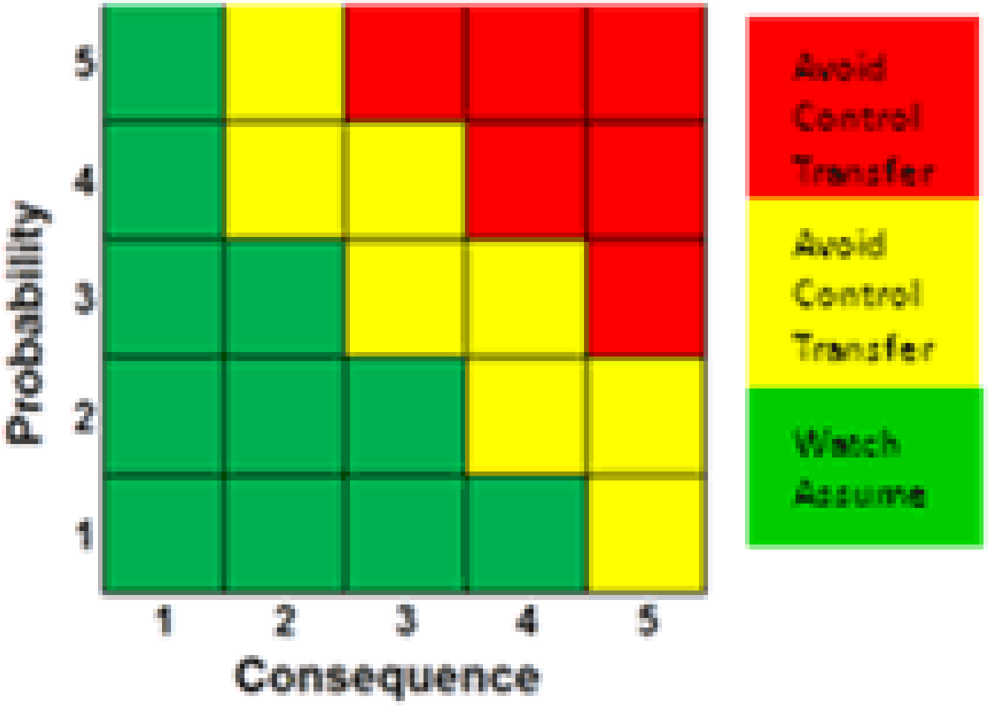
- Risk Mitigation is any step taken or countermeasures to reduce risk.
- A document that describes how an organization will address its security needs.
- As the needs of the organization evolve, ongoing review and revision of the security plan is important.



Risk events and their relationships are defined
Probabilities and consequences of risk events are assessed
Assess Probaility & Consequence
Identify Risks
1. Risk Identification
2. Risk Impact Assessment
Consequences may include cost, schedule, technical performance impacts, as well as capability or functionality impacts
Reassess existing risk events and identify new risk events
Risk Tracking
Watch-listed Risks
Assess Risk Criticality
4. Risk Mitigation Planning, Implementation, and Progress Monitoring
Risk Mitigation
3. Risk Prioritization Analysis
Decision-analytic rules applied to rank-order identified risk events from "most to least" critical
Risk events assessed as medium or high criticality might go into risk mitigation planning and implementation; low critical risks might be tracked/monitored on a watch list.

Garvey, P.R., 2008, *Analytical Methods for Risk Management: A Systems Engineering Perspective*, Chapman-Hall/CRC-Press, Taylor & Francis Group (UK), Boca Raton, London, New York, ISBN: 1584886374

GENERAL GUIDELINE FOR RISK HANDLING MITIGATION



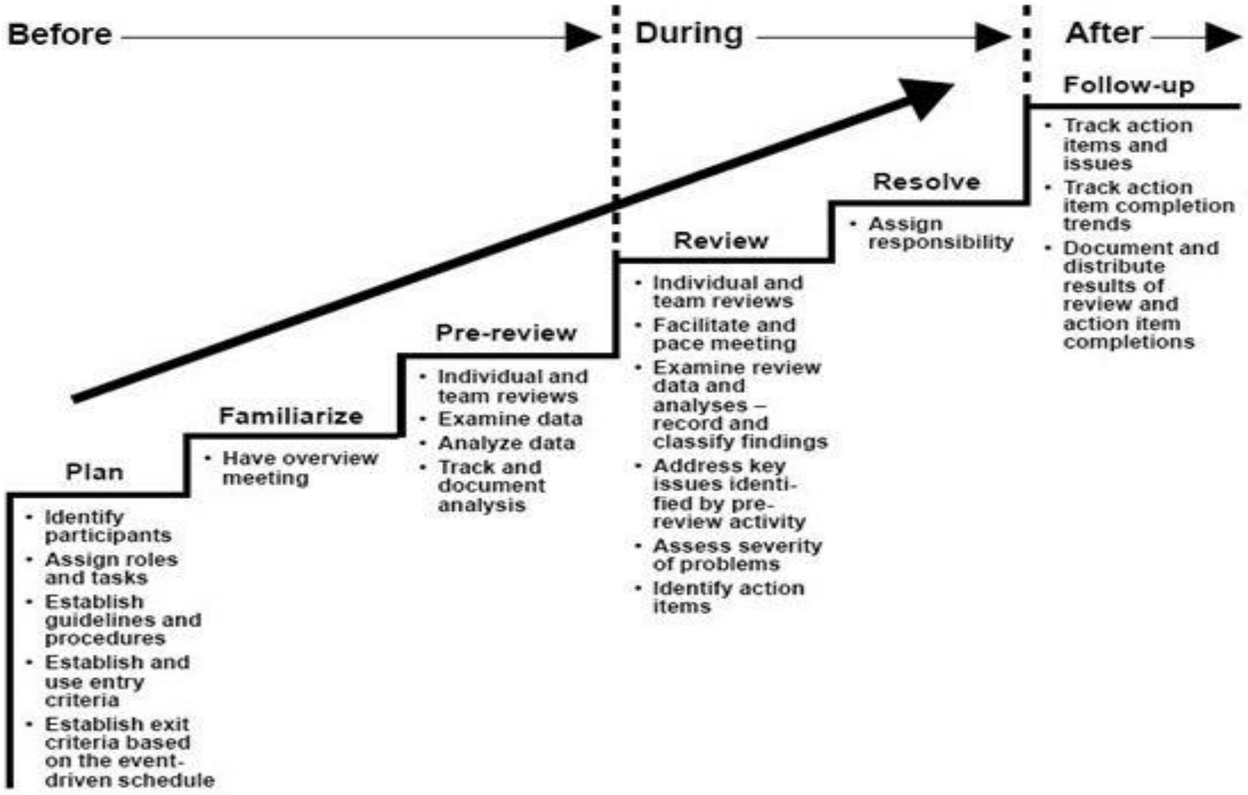
Probability	1	2	3	4	5
5	🟩	🟨	🟥	🟥	🟥
4	🟩	🟨	🟨	🟥	🟥
3	🟩	🟩	🟨	🟨	🟥
2	🟩	🟩	🟩	🟨	🟨
1	🟩	🟩	🟩	🟩	🟨

(Garvey, 2008)

- Risk mitigation handling options include:
- Assume/Accept: Acknowledge the existence of a particular risk, and make a deliberate decision to accept it without engaging in special efforts to control it. Approval of project or program leaders is required.
- Avoid: Adjust program requirements or constraints to eliminate or reduce the risk. This adjustment could be accommodated by a change in funding, schedule, or technical requirements.
- Control: Implement actions to minimize the impact or likelihood of the risk.
- Transfer: Reassign organizational accountability, responsibility, and authority to another stakeholder willing to accept the risk.
- Watch/Monitor: Monitor the environment for changes that affect the nature and/or the impact of the risk.

RISK MITIGATION PLAN

- A risk mitigation plan shall serve as the checklist of the anticipated risks, listed in accordance with the degree of their probability, as High, Medium or Low. Some project managers, however, deem it more appropriate to categorize the risks as Most Likely, Likely or Unlikely.


Before
During
After
Plan
• Identify participants
• Assign roles and tasks
• Establish guidelines and procedures
• Establish and use entry criteria
• Establish exit criteria based on the event-driven schedule
Familiarize
• Have overview meeting
Pre-review
• Individual and team reviews
• Examine data
• Analyze data
• Track and document analysis
Review
• Individual and team reviews
• Facilitate and pace meeting
• Examine review data and analyses – record and classify findings
• Address key issues identified by pre-review activity
• Assess severity of problems
• Identify action items
Resolve
• Assign responsibility
Follow-up
• Track action items and issues
• Track action item completion trends
• Document and distribute results of review and action item completions

EXAMPLE

- Imagine you are the marketing manager for a firm that is planning to introduce a new product. You need to estimate the first year net profit from this product, which will depend on:
- Sales volume in units
- Price per unit
- Unit cost
- Fixed costs
- Net profit will be calculated as Net Profit = Sales Volume* (Selling Price - Unit cost) - Fixed costs. Fixed costs (for overhead, advertising, etc.) are known to be $120,000. But the other factors all involve some *uncertainty*. Sales volume (in units) can cover quite a range, and the selling price per unit will depend on competitor actions. Unit costs will also vary depending on vendor prices and production experience.

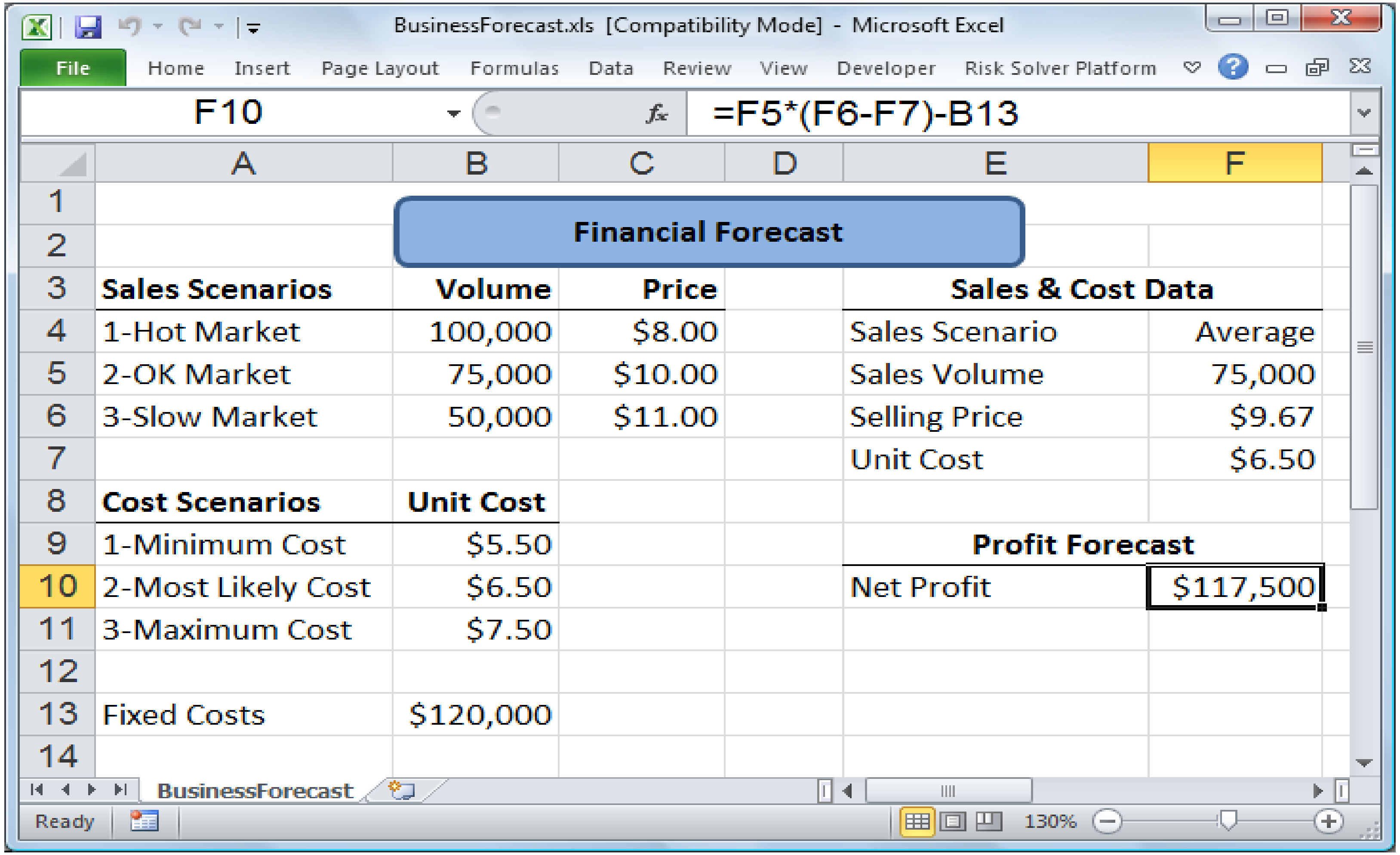
EXAMPLE

- ***<u>Uncertain Variables</u>***
- To build a risk analysis model, we must first identify the uncertain variables -- also called *random variables*. While there's *some* uncertainty in almost *all* variables in a business model, we want to focus on variables where the range of values is significant.
- ***<u>Sales and Price</u>***
- Based on your market research, you believe that there are equal chances that the market will be Slow, OK, or Hot.
- In the "Slow market" scenario, you expect to sell 50,000 units at an average selling price of $11.00 per unit.
- In the "OK market" scenario, you expect to sell 75,000 units, but you'll likely realize a lower average selling price of $10.00 per unit.
- In the "Hot market" scenario, you expect to sell 100,000 units, but this will bring in competitors who will drive down the average selling price to $8.00 per unit.
- As a result, you *expect* to sell 75,000 units (*i.e.*, (50,000+75,000+100,000)/3 = 75,000) at an average selling price of $9.67 per unit (*i.e.*, ($11+$10+$8)/3 = $9.67).

EXAMPLE

- *Unit Cost*
- Another uncertain variable is Unit Cost. Your firm's production manager advises you that unit costs may be anywhere from $5.50 to $7.50, with a most likely cost of $6.50. In this case, the most likely cost is also the average cost.
- Uncertain Functions
- *Net Profit*
- Our next step is to identify uncertain functions -- also called *functions of a random variable*. Recall that Net Profit is calculated as Net Profit = Sales Volume * (Selling Price - Unit cost) - Fixed costs. However, Sales Volume, Selling Price and Unit Cost are all uncertain variables, so Net Profit is an uncertain function.
- The Flawed Average Model
- Before we explore how to use simulation to analyze this problem, consider the Excel model pictured below, which calculates Net Profit based on average sales volume, average selling price, and average unit cost.

EXAMPLE



F10 =F5*(F6-F7)-B13

	A	B	C	D	E	F
1						
2		Financial Forecast				
3	**Sales Scenarios**	**Volume**	**Price**		**Sales & Cost Data**	
4	1-Hot Market	100,000	$8.00		Sales Scenario	Average
5	2-OK Market	75,000	$10.00		Sales Volume	75,000
6	3-Slow Market	50,000	$11.00		Selling Price	$9.67
7					Unit Cost	$6.50
8	**Cost Scenarios**	**Unit Cost**				
9	1-Minimum Cost	$5.50			**Profit Forecast**	
10	2-Most Likely Cost	$6.50			Net Profit	$117,500
11	3-Maximum Cost	$7.50				
12						
13	Fixed Costs	$120,000				
14						

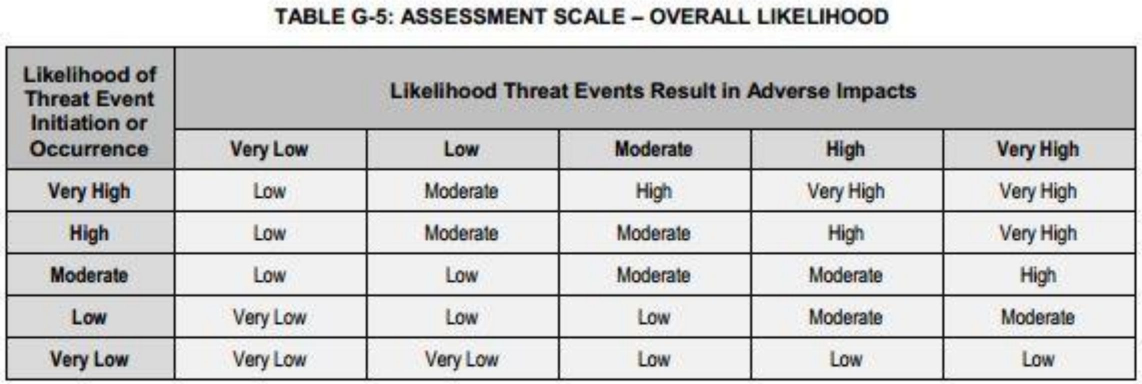


TABLE G-5: ASSESSMENT SCALE – OVERALL LIKELIHOOD

Likelihood of Threat Event Initiation or Occurrence	Likelihood Threat Events Result in Adverse Impacts				
	Very Low	Low	Moderate	High	Very High
Very High	Low	Moderate	High	Very High	Very High
High	Low	Moderate	Moderate	High	Very High
Moderate	Low	Low	Moderate	Moderate	High
Low	Very Low	Low	Low	Moderate	Moderate
Very Low	Very Low	Very Low	Low	Low	Low

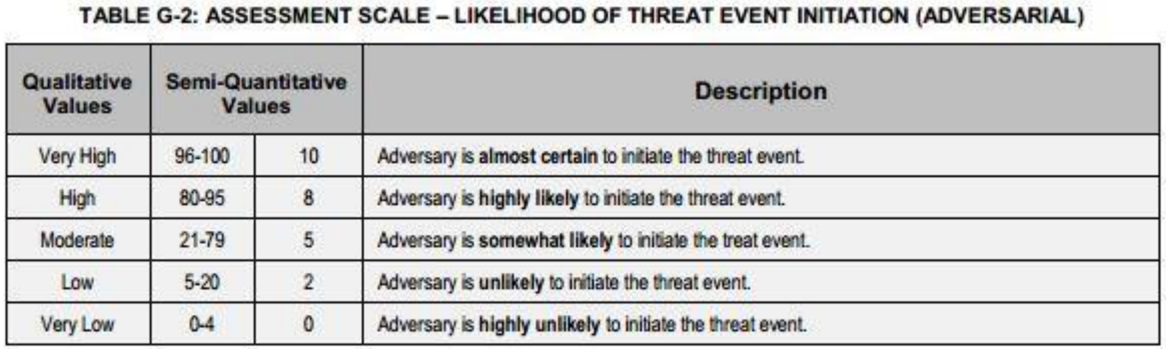


TABLE G-2: ASSESSMENT SCALE – LIKELIHOOD OF THREAT EVENT INITIATION (ADVERSARIAL)

Qualitative Values	Semi-Quantitative Values		Description
Very High	96-100	10	Adversary is **almost certain** to initiate the threat event.
High	80-95	8	Adversary is **highly likely** to initiate the threat event.
Moderate	21-79	5	Adversary is **somewhat likely** to initiate the treat event.
Low	5-20	2	Adversary is **unlikely** to initiate the threat event.
Very Low	0-4	0	Adversary is **highly unlikely** to initiate the threat event.

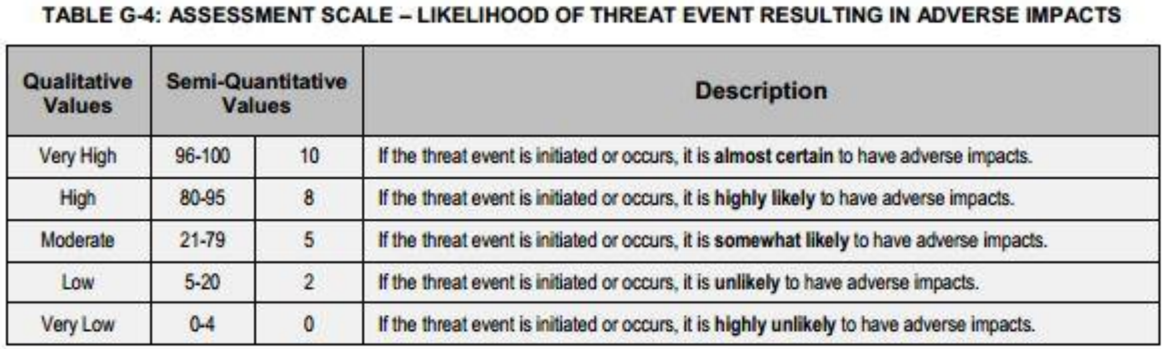
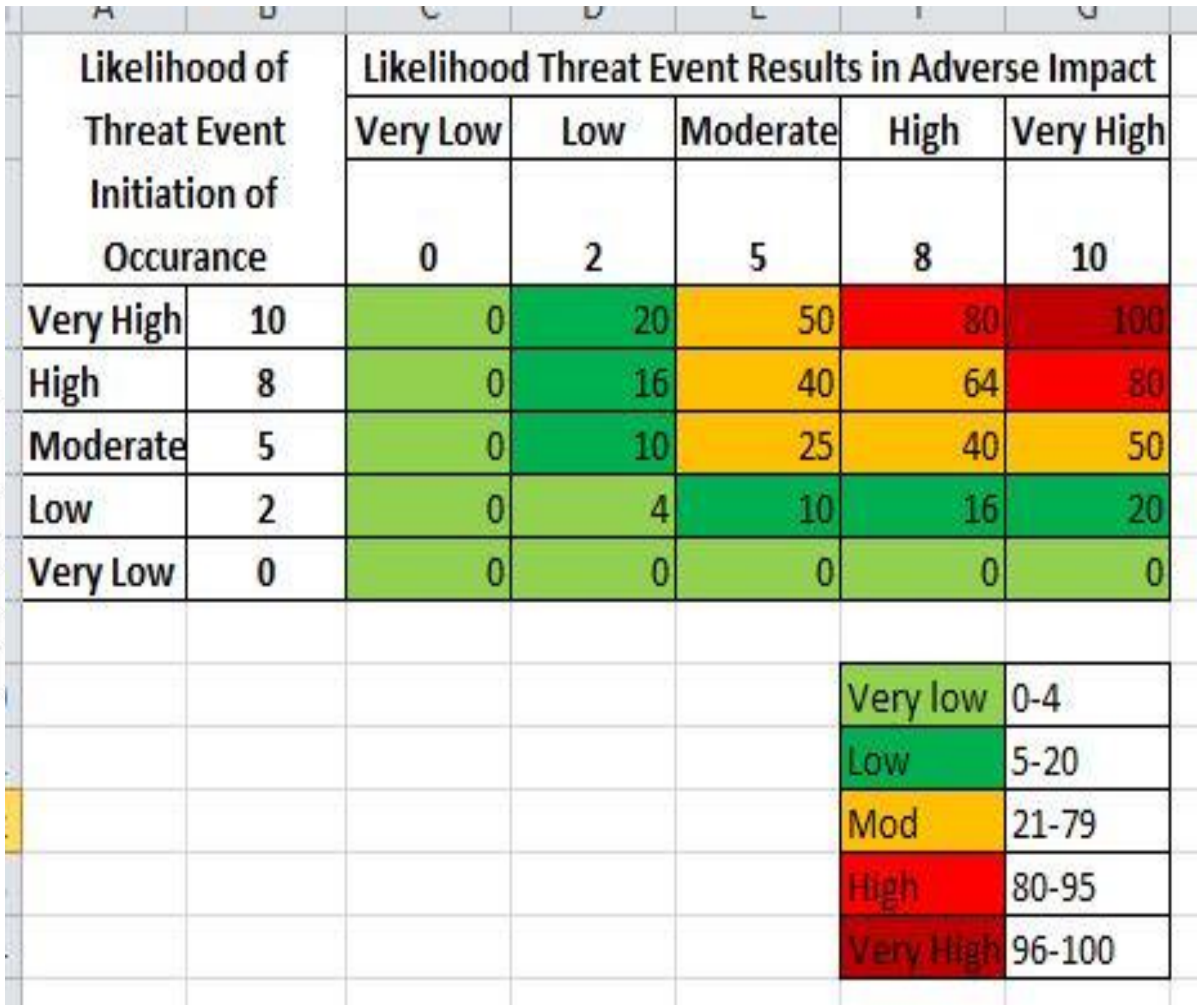


TABLE G-4: ASSESSMENT SCALE – LIKELIHOOD OF THREAT EVENT RESULTING IN ADVERSE IMPACTS

Qualitative Values	Semi-Quantitative Values		Description
Very High	96-100	10	If the threat event is initiated or occurs, it is **almost certain** to have adverse impacts.
High	80-95	8	If the threat event is initiated or occurs, it is **highly likely** to have adverse impacts.
Moderate	21-79	5	If the threat event is initiated or occurs, it is **somewhat likely** to have adverse impacts.
Low	5-20	2	If the threat event is initiated or occurs, it is **unlikely** to have adverse impacts.
Very Low	0-4	0	If the threat event is initiated or occurs, it is **highly unlikely** to have adverse impacts.



Likelihood of Threat Event Initiation of Occurance		Likelihood Threat Event Results in Adverse Impact				
		Very Low	Low	Moderate	High	Very High
		0	2	5	8	10
Very High	10	0	20	50	80	100
High	8	0	16	40	64	80
Moderate	5	0	10	25	40	50
Low	2	0	4	10	16	20
Very Low	0	0	0	0	0	0

Very low	0-4
Low	5-20
Mod	21-79
High	80-95
Very High	96-100

WHAT IS A SECURITY METRIC? – 1

- As defined by the National Institute of Standards and Technology (NIST), metrics are tools that are designed to facilitate decision-making and improve performance and accountability through collection, analysis, and reporting of relevant performance-related data. Security metrics can be naturally interpreted as a standard (or system) used for quantitatively measuring an organization’s security posture. Security metrics are essential to comprehensive network security and CSA management. Without good metrics, analysts cannot answer many security related questions. Some examples of such questions include “Is our network more secure today than it was before?” or “Have the changes of network configurations improved our security posture?”

WHAT IS A SECURITY METRIC? – 2

- The ultimate aim of security metrics is to ensure business continuity (or mission success) and minimize business damage by preventing or minimizing the potential impact of cyber incidents. To achieve this goal, organizations need to take into consideration all information security dimensions, and provide stakeholders detailed information about their network security management and risk treatment processes.

METRICS TO PROTECT THE NETWORK

- NIST provided an overview of existing metrics for network security measurement in (Jansen, 2009). Hecker (2008) distinguished the lower level metrics (based on well-ordered low-level quantitative system parameters) from the higher level metrics (e.g., conformity distance, attack graph or attack surface based estimations). Meland and Jensen (2008) presented a Security-Oriented Software Development Framework (SODA) to adapt security techniques and filter information. Heyman et al. (2008) also presented their work on using security patterns to combine security metrics.

LINDSTROM (2005)

- Lindstrom (2005) further introduced a number of underlying elements required for general security (risk) analysis. Although they may not completely solve all the problems, these underlying elements still provide security analysts a better understanding and insight to develop meaningful metrics and practical solutions for general network security measurements.
- List useful elements introduced are:
  - Calculate the asset value
  - Calculate potential loss
  - Measurement of security spending
  - Attack risk analysis

SUMMARY

- Risk Management is an investment which costs associated with identifying risks, analysing those risks, and establishing plans to mitigate those risks.
- In risk management, consists of risk assessment and risk mitigation.
- Tools and techniques for quantifying risks include EMV, calculate risk factor, PERT estimation, simulations, expert judgment (interviews) and Monte Carlo.
- Three basic responses to risk and there are:
  - Risk avoidance
  - Risk acceptance
  - Risk mitigation

Q & A