INTRODUCTION TO RISK MANAGEMENT &RISK ANALYSIS

BY : SAMI AL-MASHAQBEH

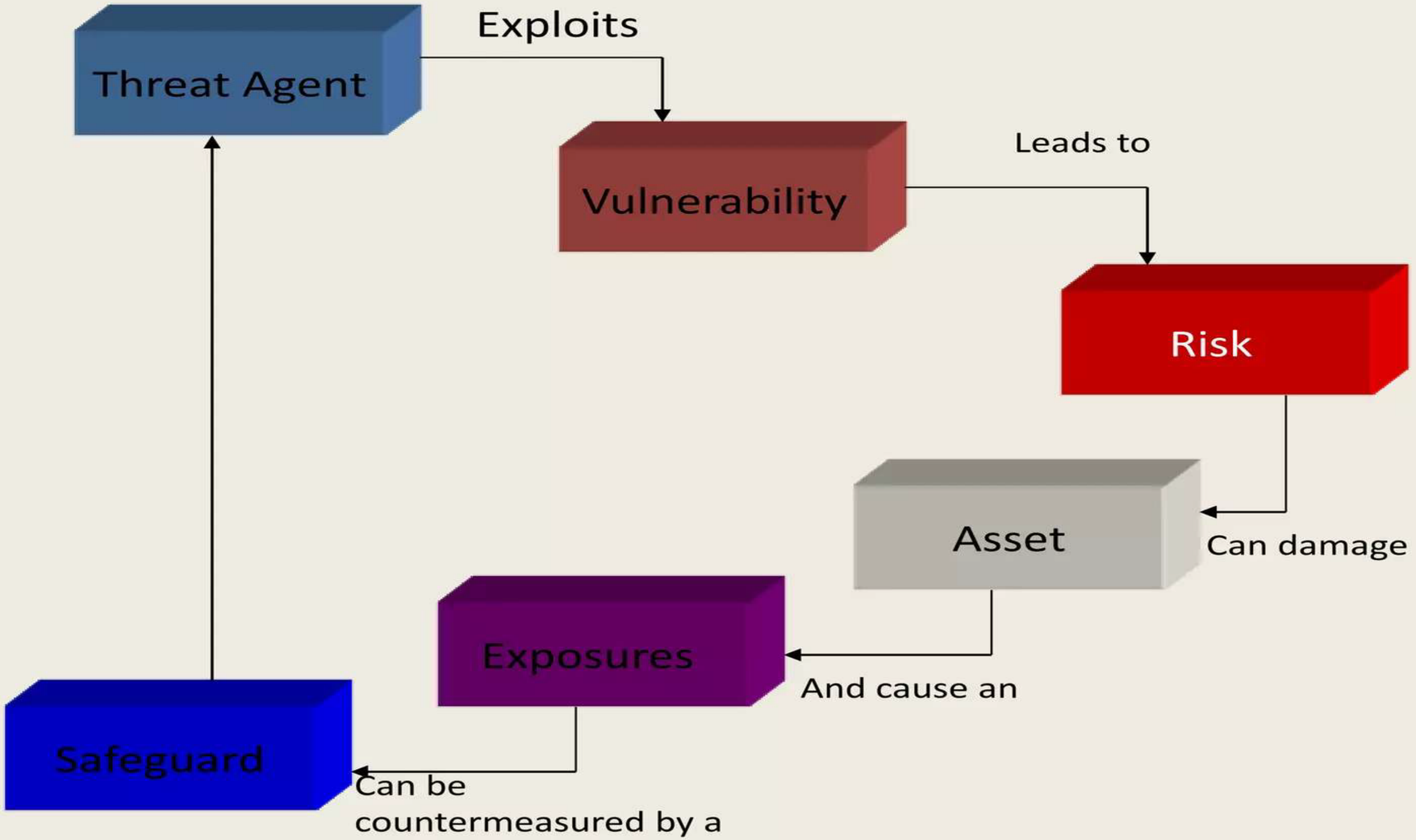
WHAT IS RISK

- A Risk is a potential or future event that, should it occur, will have a (negative) impact on the Business Objectives of an Organization

That is, Asset + Threat + Vulnerability = Risk.

- Risk is a function of threats exploiting vulnerabilities to obtain, damage or destroy assets. Thus, threats (actual, conceptual, or inherent) may exist, but if there are no vulnerabilities then there is little/no risk. Similarly, you can have a vulnerability, but if you have no threat, then you have little/no risk.

Risk Life Cycle

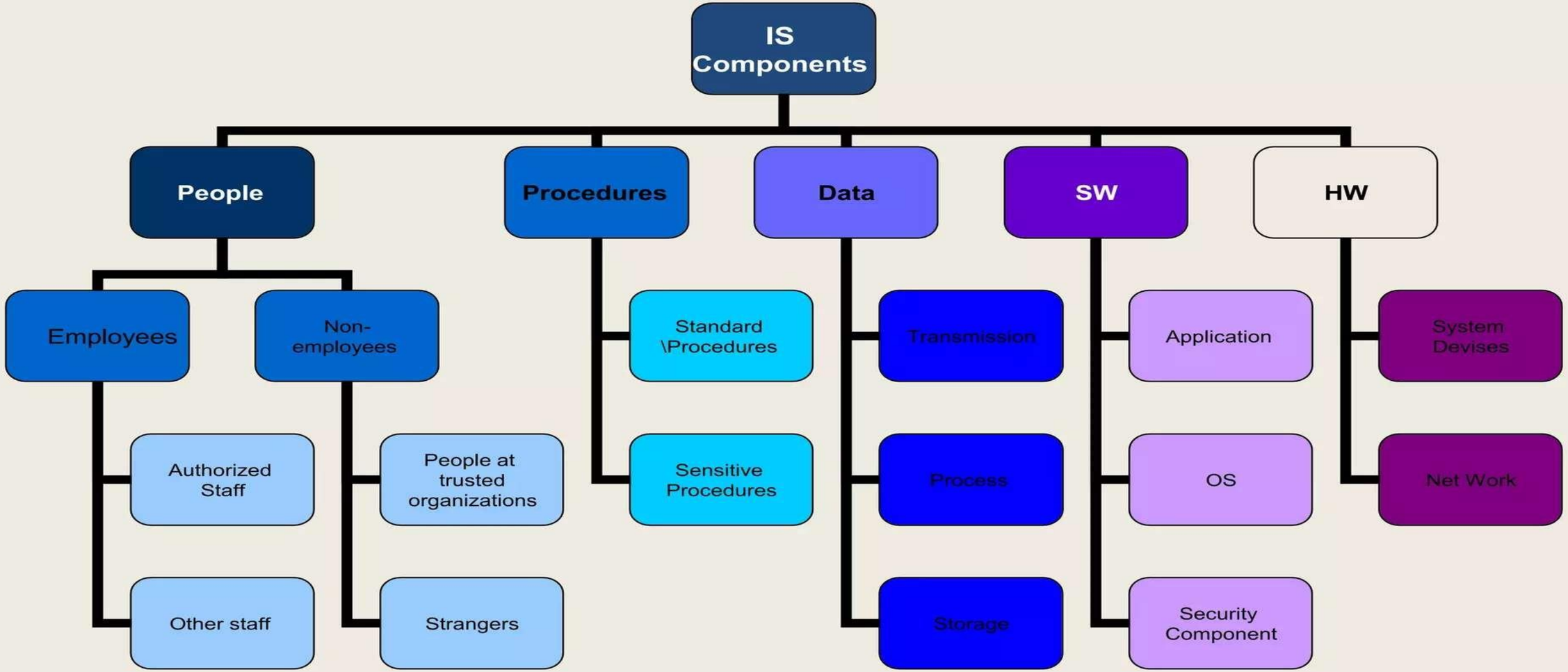


GENERAL TERMS

- Asset —People, property, and information. People may include employees and customers along with other invited persons such as contractors or guests.
- Property assets consist of both tangible and intangible items that can be assigned a value. intangible assets include reputation and proprietary information.
- information may include databases, software code, critical company records, and many other intangibie items.

An asset is what we're trying to protect.

Information Assets



GENERAL TERMS

- Threat —Anything that can exploit a vulnerability, intentionally or accidentally, and obtain, damage, or destroy an asset.

A threat is what we're trying to protect against.

- Vulnerability - Weaknesses or gaps in a security program that can be exploited by threats to gain unauthorized access to an asset.

A vulnerability is a weakness or gap in our protection efforts.

GENERAL TERMS

- Risk —The potential for loss, damage or destruction of an asset as a result of a threat exploiting a vulnerability.

Risk is the intersection of assets, threats, and vulnerabilities.

Risk management vs. risk assessment vs. risk analysis

- **Risk management, risk assessment and risk analysis :** are often used interchangeably, leading some to believe they are synonyms. In reality, each is its own unique process that IT and business leaders need to understand.

- At their most basic, a risk assessment is the information, a risk analysis is the processing and risk management is the plan.

Risk management vs. risk assessment vs. risk analysis

- **What is a risk assessment?**
- A risk assessment involves evaluating existing security controls and assessing their adequacy relative to the potential threats of the organization. It also covers potential consequences of the risks if they go unmitigated.
- The goal of a risk assessment will depend on the specific organization and its industry, as well as its compliance regulations. Common goals include developing a risk profile, inventorying IT and data assets, or supporting the costs of security countermeasures.
- To conduct a risk assessment, companies should use a risk assessment framework (RAF), which helps prioritize and share information gleaned during an assessment about the security risks to IT infrastructure in particular. Ideally, the RAF includes language that is usable to people with technical and nontechnical backgrounds.

Risk management vs. risk assessment vs. risk analysis

- **What is a risk analysis?**

- A risk analysis involves identifying the most probable threats to an organization and analyzing the related vulnerabilities of the organization to these threats. Risk analysis is used to estimate and manage the cost of potential threats, which influences company decision-making. To properly analyze risk, organizations must calculate the probability potential negative events could impact their risk profile. These events range from natural disasters to public health issues to events caused by humans, including malicious or accidental insider threats.

Risk management vs. risk assessment vs. risk analysis

- **What is a risk analysis?**

- The first step in a risk analysis is to conduct a risk assessment.
- Second, organizations identify and analyze the results.
- Third, they develop and subsequently enact a risk management plan. Finally, they must continually monitor the risks and update their plans accordingly.
- **There are two main schools of risk analysis:** qualitative and quantitative. *Qualitative risk analyses attempt to predict the likelihood of a risk occurring against its potential effects.* The predicted effects are ranked low, medium or high. Quantitative analyses seek to put *an estimated price tag on each risk's monetary impact.*

Risk management vs. risk assessment vs. risk analysis

Quantitative risk analysis example

EVENT	LIKELIHOOD (A)	IMPACT (B)	RISK FACTOR (A x B)
Fire in data center	0.7	0.9	0.63
Loss of power	0.5	0.8	0.40
Staff illness	0.6	0.5	0.30
Hurricane	0.4	0.9	0.36
Water leak	0.3	0.5	0.15
Employee forgot to log off	0.8	0.3	0.24

Risk management vs. risk assessment vs. risk analysis

- **What is risk management?**
- Risk management is the systematic application of management policies, procedures and practices to manage risk. Managing risk requires an organization to contextualize, identify, evaluate, treat, monitor and communicate risk.

- To carry out these requirements, organizations can implement a few different strategies. Commonly used risk management strategies include risk avoidance, risk reduction, risk sharing and risk retaining. The risk management plan must address a few critical elements of the organization's risk profile, specifically what steps need to be taken to manage risk and how to budget for those steps.

Risk management vs. risk assessment vs. risk analysis

- **What is risk management?**

- During the process of orchestrating a risk management strategy, organizations should identify their most critical threats and where surprise costs may turn up. What is learned during this planning process can be used to shore up defenses against newly discovered risks or to request additional budget to better address those risks.

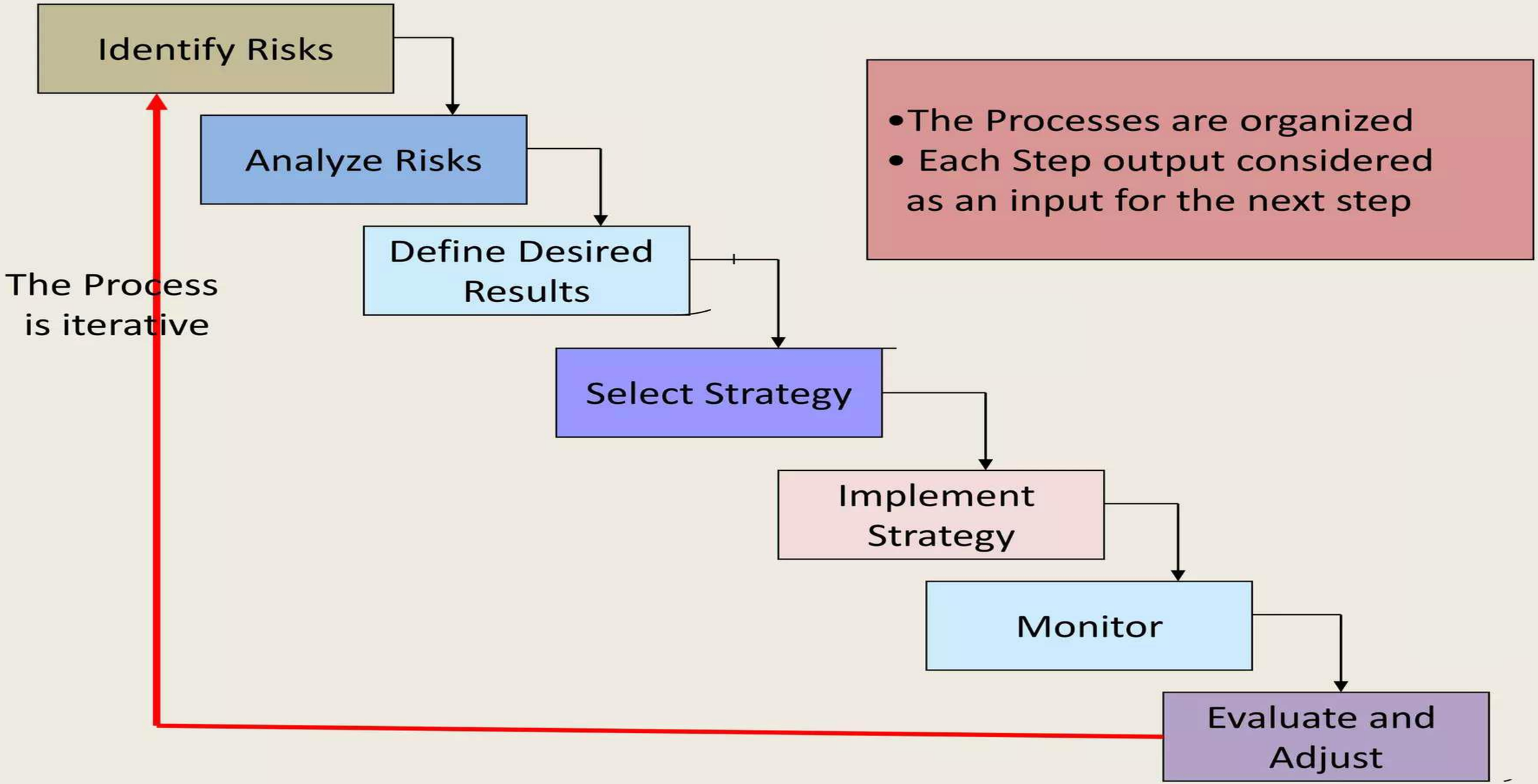
Risk management vs. risk assessment vs. risk analysis

- **How do they relate?**

- Though risk assessment, analysis and management all have different functions, they work best when they inform each other. Without the information from risk assessments and investigation of that information during risk analysis, a risk management plan is nearly obsolete.

- This is important for infosec professionals to understand, especially if they have their hands in only one or two of the tasks. To best mitigate risk, the teams conducting risk assessments, analyses and management should know how their efforts affect the others and the organization's defenses as a whole.

Risk Management Process



RISK IDENTIFICATION

- First step in the process of managing risk is to identify potential risks. Risks are about events that, when triggered, will cause problems.
- This is a crucial phase. If a risk is not identified it cannot be evaluated and managed
- Any failure at this stage to identify risk may cause a major loss for the organization.
- Risk identification provides the foundation of risk management.

RISK IDENTIFICATION

- Risk identification requires knowledge of the organization, the market in which it operates, the legal, social, economic, political, and climatic environment in which it has its impact.

RISK ANALYSIS

- Assessing risk is the process of determining the likelihood of the threat being exercised against the vulnerability and the resulting impact from a successful compromise.

- The risk analyzing step assist in determining which risks have a greater consequence or impact than others.

RISK ANALYSIS METHODS

Risk analysis is generally lumped into two main categories: **Qualitative and Quantitative.**

- ***Qualitative Risk Analysis:***

  The root word of qualitative is “quality” and that is what these techniques focus on. Qualifying risks under this method involves making a simple list of the risks themselves, along with ranking them and mapping them out.

–

QUALITATIVE RISK ANALYSIS

The following are some common tricks used for assessing risks from a qualitative aspect:

- **Probability And Impact Assessment And Matrix:** Analyzing and rating risks using probability and impact on things like cost, schedule and performance.
- **Risk Categorization:** Grouping risks by common root causes to develop effective responses.
- **Risk Urgency:** The risk ranking from your probability matrix combined with urgency can help place risks priorities.
- **Expert Judgment:** Professional opinions from people in the industry or with similar project

QUANTITATIVE RISK ANALYSIS

Quantitative Risk Analysis:

These methods are more about definitive measuring and probabilistic techniques. The greatest risk of all is the risk of losing money and you cannot use qualitative systems to count your cost.

QUANTITATIVE RISK ANALYSIS

The following are a few simple ways in which organizations are counting their risks:

- **Probability distributions:** Used in modeling and simulation to represent the uncertainty of values in things like task costs and labor.
- **Cost and Schedule Risk Analysis:** Cost estimates and scheduling are used as input values that are chosen randomly for each iteration.
- **Sensitivity Analysis:** This is a simple technique to determine how much impact a risk poses to a project.
- **Expected Monetary Value analysis (EMV):** Calculating the average outcome of scenarios that may or may not happen

QUALITATIVE VS. QUANTITATIVE ANALYSIS

- **Qualitative Risk Analysis** – **scenario based approach - uses <u>labels & relative values</u>** (high/low) **rather than numbers; blends in experience & personal judgment**

- **Quantitative Risk Analysis** – **predicts level of <u>monetary loss</u> for each threat, and <u>monetary benefit</u> of controlling the treat**

  - **each element is quantified and entered into equations, e.g.:**
    - asset value
    - threat frequency
    - severity of vulnerability
    - damage impact
    - safeguard cost …

QUALITATIVE VS. QUANTITATIVE ANALYSIS

	Qualitative Analysis	Quantitative Analysis
pros	• Requires simple (or no) calculations.	• Easier to automate and evaluate.
pros	• Considers hands-on opinions of individuals who know the process best.	• Very useful in performance tracking - provide credible **cost/benefit analysis**.
cons	• Assessment and results are subjective.	• Complex calculations – may not be understood by all.
cons	• Does not enable dollar cost/benefit discussion. • Difficult to track performance.	• Very detailed information about environment need to be gathered.

QUALITATIVE VS. QUANTITATIVE ANALYSIS

Quantitative risk measurement is the standard way of measuring risk in many fields, such as finance and insurance, but it is not commonly used to measure risk in information systems.

Two of the reasons claimed for this are:

- the difficulties in identifying and assigning a value to assets.
- the lack of statistical information that would make it possible to determine frequency.

Thus, most of the risk assessment tools that are used today for information systems are measurements of qualitative risk.”

QUALITATIVE ANALYSIS

- **Challenges of Qualitative Analysis** – **define likelihood and impact values in a manner that would allow the same scale to be used across multiple risk assessments**

Example: Sample '**likelihood of threat**' definitions

Figure 2 – Sample Likelihood Definitions

	Definition
Low	0-25% chance of successful exercise of threat during a one-year period
Moderate	26-75% chance of successful exercise of threat during a one-year period
High	76-100% chance of successful exercise of threat during a one-year period

QUALITATIVE ANALYSIS (CONT.)

Example: Sample '**impact**' definitions

Figure 3 – Sample Impact Definitions

	Confidentiality	Integrity	Availability
Low	Loss of confidentiality leads to a **limited effect** on the organization.	Loss of integrity leads to a **limited effect** on the organization.	Loss of availability leads to a **limited effect** on the organization.
Moderate	Loss of confidentiality leads to a **serious effect** on the organization.	Loss of integrity leads to a **serious effect** on the organization.	Loss of availability leads to a **serious effect** on the organization.
High	Loss of confidentiality leads to a **severe effect** on the organization.	Loss of integrity leads to a **severe effect** on the organization.	Loss of availability leads to a **severe effect** on the organization.

Example: Sample 'risk determination' matrix

Figure 5 – Sample Risk Determination Matrix

		Impact		
		High	**Moderate**	**Low**
Likelihood	**High**	High	High	Moderate
	Moderate	High	Moderate	Low
	Low	Moderate	Low	Low

QUALITATIVE ANALYSIS (CONT.)

risk = likelihood x impact

Impact

How severe would the outcomes be if the risk occurred?

Probability

What is the probability the risk will happen?

	Insignificant 1	Minor 2	Significant 3	Major 4	Severe 5
5 Almost Certain	Medium 5	High 10	Very high 15	Extreme 20	Extreme 25
4 Likely	Medium 4	Medium 8	High 12	Very high 16	Extreme 20
3 Moderate	Low 3	Medium 6	Medium 9	High 12	Very high 15
2 Unlikely	Very low 2	Low 4	Medium 6	Medium 8	High 10
1 Rare	Very low 1	Very low 2	Low 3	Medium 4	Medium 5

Table 14.2
Risk Likelihood

Rating	Likelihood Description	Expanded Definition
1	**Rare**	May occur only in exceptional circumstances and may be deemed as “unlucky” or very unlikely.
2	**Unlikely**	Could occur at some time but not expected given current controls, circumstances, and recent events.
3	**Possible**	Might occur at some time, but just as likely as not. It may be difficult to control its occurrence due to external influences.
4	**Likely**	Will probably occur in some circumstance and one should not be surprised if it occurred.
5	**Almost Certain**	Is expected to occur in most circumstances and certainly sooner or later.

TABLE 14.3

RISK CONSEQUENCES (IMPACT)

Rating	Consequence	Expanded Definition
1	**Insignificant**	Generally a result of a minor security breach in a single area. Impact is likely to last less than several days and requires only minor expenditure to rectify. Usually does not result in any tangible detriment to the organization.
2	**Minor**	Result of a security breach in one or two areas. Impact is likely to last less than a week but can be dealt with at the segment or project level without management intervention. Can generally be rectified within project or team resources. Again, does not result in any tangible detriment to the organization, but may, in hindsight, show previous lost opportunities or lack of efficiency.
3	**Moderate**	Limited systemic (and possibly ongoing) security breaches. Impact is likely to last up to 2 weeks and will generally require management intervention, though should still be able to be dealt with at the project or team level. Will require some ongoing compliance costs to overcome. Customers or the public may be indirectly aware or have limited information about this event.
4	**Major**	Ongoing systemic security breach. Impact will likely last 4-8 weeks and require significant management intervention and resources to overcome. Senior management will be required to sustain ongoing direct management for the duration of the incident and compliance costs are expected to be substantial. Customers or the public will be aware of the occurrence of such an event and will be in possession of a range of important facts. Loss of business or organizational outcomes is possible, but not expected, especially if this is a once off.
5	**Catastrophic**	Major systemic security breach. Impact will last for 3 months or more and senior management will be required to intervene for the duration of the event to overcome shortcomings. Compliance costs are expected to be very substantial. A loss of customer business or other significant harm to the organization is expected. Substantial public or political debate about, and loss of confidence in, the organization is likely. Possible criminal or disciplinary action against personnel involved is likely.
6	**Doomsday**	Multiple instances of major systemic security breaches. Impact duration cannot be determined and senior management will be required to place the company under voluntary administration or other form of major restructuring. Criminal proceedings against senior management is expected, and substantial loss of business and failure to meet organizational objectives is unavoidable. Compliance costs are likely to result in annual losses for some years, with liquidation of the organization likely.

(Table can be found on pages 503-504 in textbook)

RISK LEVEL DETERMINATION AND MEANING

	Consequences					
Likelihood	**Doomsday**	**Catastrophic**	**Major**	**Moderate**	**Minor**	**Insignificant**
Almost Certain	E	E	E	E	H	H
Likely	E	E	E	H	H	M
Possible	E	E	E	H	M	L
Unlikely	E	E	H	M	L	L
Rare	E	H	H	M	L	L

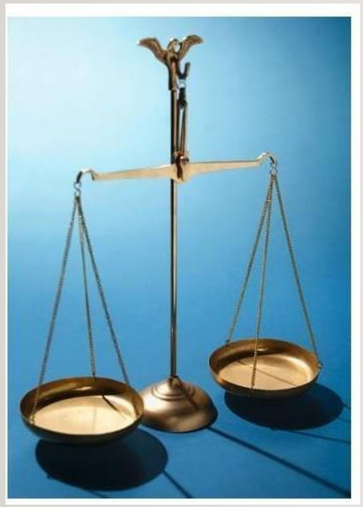
Risk Level	Description
Extreme (E)	Will require detailed research and management planning at an executive/director level. Ongoing planning and monitoring will be required with regular reviews. Substantial adjustment of controls to manage the risk are expected, with costs possibly exceeding original forecasts.
High (H)	Requires management attention, but management and planning can be left to senior project or team leaders. Ongoing planning and monitoring with regular reviews are likely, though adjustment of controls are likely to be met from within existing resources.
Medium (M)	Can be managed by existing specific monitoring and response procedures. Management by employees is suitable with appropriate monitoring and reviews.
Low (L)	Can be managed through routine procedures.

TABLE 14.6
SILVER STAR MINES RISK REGISTER

Asset	Threat/ Vulnerability	Existing Controls	Likelihood	Consequence	Level of Risk	Risk Priority
Reliability and integrity of the SCADA nodes and network	Unauthorized modification of control system	Layered firewalls and servers	Rare	Major	High	1
Integrity of stored file and database information	Corruption, theft, loss of info	Firewall, policies	Possible	Major	Extreme	2
Availability and integrity of financial system	Attacks/errors affecting system	Firewall, policies	Possible	Moderate	High	3
Availability and integrity of procurement system	Attacks/errors affecting system	Firewall, policies	Possible	Moderate	High	4
Availability and integrity of maintenance/ production system	Attacks/errors affecting system	Firewall, policies	Possible	Minor	Medium	5
Availability, integrity and confidentiality of mail services	Attacks/errors affecting system	Firewall, ext mail gateway	Almost Certain	Minor	High	6

QUANTITATIVE ANALYSIS

- **Cost-Benefit Analysis** – **aka economic feasibility study - <u>quantitative</u> decision-making process that:**



  - **determines the loss in value if the asset remained unprotected**
  - **determines the cost of protecting an asset**
  - **helps prioritize actions and spending on security …**

Company should not spend more to protect an asset than the asset is worth!

QUANTITATIVE ANALYSIS (CONT.)

- **Asset Value (AV) – includes the following:**

- **cost of buying/developing hardware, software, service**
- **cost of installing, maintaining, upgrading hardware, software, service**
- **cost to train and re-train personnel**

- **Exposure Factor (EF) – percentage loss that would occur from a given vulnerability being exploited by a given threat**

QUANTITATIVE ANALYSIS (CONT.)

- **Single Loss Expectancy (SLE)** – **most likely loss (in value) from an attack**

SLE = AV * EF

Example: A Web-site's SLE due to a DDoS Attack

Estimated value of a Web-site: AV = $ 1,000,000.

A DDoS on the site would result in 10% losses of the site value (EF=0.1).

SLE for the site: AV * EF = $ 100,000.

Would it be worth investing in anti-DDoS system that costs $100,000 a year?

QUANTITATIVE ANALYSIS (CONT.)

- **Annualized Rate of Occurrence (ARO)** – **indicates how often an attack is expected to successfully occur in a year**
  - **if an attack occurs once every 2 years ⇒ ARO = 0.5**

- **Annualized Loss Expectancy (ALE)** – **overall loss incurred by an attack (i.e. by exploiting a vulnerability) in each year**

ALE = ARO * SLE

Quantitative Analysis (cont.)

Example: Determining ARO, SLE, ALE

Table 3.2 How SLE, ARO, and ALE Are Used

Asset	Risk	Asset Value	Exposure Factor	SLE	Annualized Frequency	ALE
Customer database	Hacked	$432,000	.74	$320,000	.25	$80,000
Word documents and data files	Virus	$9,450	.17	$ 1,650	.9	$1,485
Domain controller	Server failure	$82,500	.88	$ 72,500	.25	$18,125
E-commerce website	DDoS	$250,000	.44	$110,000	.45	$49,500

QUANTITATIVE ANALYSIS EXAMPLES

- **Example 1: Ransomware Attack on a Financial Services Firm**

- **A financial services firm stores sensitive customer financial data. The company is concerned about ransomware attacks that could encrypt critical data and demand payment for decryption.**

- **Asset Value (AV):** The firm's database containing customer financial records is valued at $2,000,000.

- **Exposure Factor (EF):** A ransomware attack is estimated to cause **a 30%** loss of the asset's value due to business disruption, data recovery costs, and reputational damage.

- **Based on historical data**, industry reports, and security assessments, the company determines that ransomware attacks are likely to occur once every 5 years.

QUANTITATIVE ANALYSIS EXAMPLES

- **Solution: Ransomware Attack on a Financial Services Firm**

- Step 1: Determine the Single Loss Expectancy (SLE)

$$SLE = Asset\ Value \times Exposure\ Factor\ (EF)$$

$$SLE = 2,000,000 \times 0.30 = 600,000$$

- Step 2: Determine the Annualized Rate of Occurrence (ARO)

ARO is the estimated frequency of the threat occurring within a year

$$ARO = \frac{1}{5} = 0.2$$

- Step 3: Calculate the Annualized Loss Expectancy (ALE)

$$ALE = SLE \times ARO$$

$$ALE = 600,000 \times 0.2 = 120,000$$

QUANTITATIVE ANALYSIS EXAMPLES

- **Solution: Ransomware Attack on a Financial Services Firm**

- **Risk Management Implications:**

- If the company implements cybersecurity controls (e.g., endpoint detection, network segmentation, employee training), the ARO may decrease to once every 10 years (ARO = 0.1).

- If the company adopts data backup and recovery strategies, the Exposure Factor (EF) may decrease from 30% to 10%, reducing the SLE.

- **Re-evaluating with these mitigations:**

- New SLE = $2,000,000 × 0.10 = $200,000
- New ARO = 0.1
- New ALE = $200,000 × 0.1 = $20,000 per year
- By implementing controls, the company reduces ALE from $120,000 to $20,000, showing a significant risk reduction.

QUANTITATIVE ANALYSIS EXAMPLES

- **Example 2: Data Breach Due to Phishing Attack**

- **A healthcare organization stores electronic health records (EHRs) of patients. Cybercriminals often target such organizations through phishing attacks to steal login credentials and access sensitive patient data.**

- **Asset Value (AV):** The estimated value of the patient database, including regulatory fines, legal fees, notification costs, and reputational damage, is $5,000,000.

- **Exposure Factor (EF):** A successful phishing attack is estimated to compromise 25% of the database.

- **Based on historical data**, and past incidents, the organization determines that successful phishing attacks leading to data breaches occur once every 3 years.

QUANTITATIVE ANALYSIS EXAMPLES

- **Solution: Ransomware Attack on a Financial Services Firm**

- Step 1: Determine the Single Loss Expectancy (SLE)

$$SLE = Asset\ Value \times Exposure\ Factor\ (EF)$$

$$SLE = 5,000,000 \times 0.25 = 1,250,000$$

- Step 2: Determine the Annualized Rate of Occurrence (ARO)

ARO is the estimated frequency of the threat occurring within a year

$$ARO = \frac{1}{3} = 0.33$$

- Step 3: Calculate the Annualized Loss Expectancy (ALE)

$$ALE = SLE \times ARO$$

$$ALE = 1,250,000 \times 0.33 = 412,500$$

QUANTITATIVE ANALYSIS EXAMPLES

- **Solution: Ransomware Attack on a Financial Services Firm**

- **Risk Management Implications:**

- **To reduce risk, the healthcare organization can:**
- **Implement Multi-Factor Authentication (MFA):** Reduces the EF by ensuring stolen credentials alone don't grant access.
- **Security Awareness Training:** Lowers the ARO by reducing employee susceptibility to phishing.
- **Deploy Advanced Email Filtering & AI-based Detection:** Further reduces ARO by blocking phishing attempts.

Re-evaluating with Mitigation Controls:

- **New EF** = **15%** instead of 25% (due to stronger security measures).
- **New ARO** = **0.2** (1 attack every 5 years instead of 3 years).
- **New SLE** = $5,000,000 × 0.15 = **$750,000**.
- **New ALE** = $750,000 × 0.2 = **$150,000 per year**.

By implementing these controls, the organization reduces **ALE from $412,500 to $150,000**, demonstrating effective risk mitigation.

STRATEGIES: SELECTION & IMPLEMENTATION

- Risk treatment is about considering options for treating risks that were not considered acceptable or tolerable.

- Risk treatment involves identifying options for treating or controlling risk, in order to either reduce or eliminate negative consequences, or to reduce the likelihood of an adverse occurrence.

STRATEGIES: SELECTION & IMPLEMENTATION

- Risk control should also aim to enhance positive outcomes.
- Organizations can respond to risk in a variety of ways. These include:
  - (i) risk acceptance
  - (ii) risk avoidance
  - (iii) risk mitigation
  - (iv) risk sharing
  - (v) risk transfer
  - (vi) a combination of the above.

STRATEGIES: SELECTION & IMPLEMENTATION

- ***Risk Acceptance:*** Risk acceptance is the appropriate risk response when the identified risk is within the organizational risk tolerance. Organizations can accept risk deemed to be low, moderate, or high depending on particular situations or conditions.

STRATEGIES: SELECTION & IMPLEMENTATION

- ***Risk Avoidance:*** Risk avoidance may be the appropriate risk response when the identified risk exceeds the organizational risk tolerance. Organizations may conduct certain types of activities or employ certain types of information technologies that result in risk that is unacceptable. In such situations, risk avoidance involves taking specific actions to eliminate the activities or technologies that are the basis for the risk or to revise or reposition these activities or technologies in the organizational mission/business processes to avoid the potential for unacceptable risk

STRATEGIES: SELECTION & IMPLEMENTATION

- **Risk Mitigation :** Risk mitigation, or risk reduction, is the appropriate risk response for that portion of risk that cannot be accepted, avoided, shared, or transferred.
- Risk mitigation involves taking action to reduce an organization's exposure to potential risks and reduce the likelihood that those risks will happen again.

STRATEGIES: SELECTION & IMPLEMENTATION

- *Risk Sharing or Transfer:* Risk sharing or risk transfer is the appropriate risk response when organizations desire and have the means to shift risk liability and responsibility to other organizations.

- Risk transfer shifts the entire risk responsibility or liability from one organization to another organization (e.g., using insurance to transfer risk from particular organizations to insurance companies).

STRATEGIES: SELECTION & IMPLEMENTATION

- It is important to note that risk transfer reduces neither the likelihood of harmful events occurring nor the consequences in terms of harm to organizational operations and assets, individuals, other organizations, or the Nation.

MONITOR AND REVIEW

- Monitor and review is an essential and integral step in the risk management process.
- An owner of the organization must monitor risks and review the effectiveness of the treatment plan, strategies and management system that have been set up to effectively manage risk.
- Risks need to be monitored periodically to ensure changing circumstances do not alter the risk priorities. Very few risks will remain static, therefore the risk management process needs to be regularly repeated, so that new risks are captured in the process and effectively managed.