VU21995 – Manage the security infrastructure for the organisation

Risk Assessment – Generic Model

- A risk assessment is a document that will allow you to identify events that could adversely impact an organization.

- This document should include:
  - Events and potential damage they could cause
  - Time required to recover/restore operations
  - Mitigation techniques
  - Probability of an event occurring

- A risk assessment could help you identify what steps, could be put in place to reduce the severity of an event.

Factors of Basic RA

- Basic risk assessment involves only three factors:
  - The importance of the assets at risk,
  - How critical the threat is, and
  - How vulnerable the system is to that threat.

- Usinng the above, the organisation can assess the risk/likelihood of loss to the organisation.

- Although risk assessment is about logical constructs, not numbers, it is useful to represent it as a formula:

  - *Risk = Asset X Threat X Vulnerability*

Risk Assessment – Beginning Steps

Find all valuable assets across the organization that could be harmed by threats in a way that results in a monetary loss. Some examples are:

- Servers
- Website
- Client contact information
- Partner documents
- Trade secrets
- Customer credit card data

Identify potential consequences.

- Determine what financial losses the organization would suffer if a given asset were damaged. Here are some of the consequences you should care about:
  - Data loss
  - System or application downtime
  - Legal consequences

Risk Assessment – Beginning Steps

Identify threats and their level.

- A threat is anything that might exploit a vulnerability to breach your security and cause harm to your assets. Here are some common threats:
- Natural disasters
- System failure
- Accidental human interference
- Malicious human actions (interference, interception or impersonation)

Risk Assessment – Beginning Steps

Identify vulnerabilities and assess the likelihood of their exploitation.

What is a vulnerability?

- Weakness that allows some threat to breach your security and cause harm to an asset.
- Think about what protects your systems from a given threat — if the threat actually occurs, what are the chances that it will actually damage your assets?
- Vulnerabilities can be physical (such as old equipment), problems with software design or configuration (such as excessive access permissions or unpatched workstations), or human factors (such as untrained or careless staff members).

Risk Assessment – Beginning Steps

Assess risk.

- Risk is the potential that a given threat will exploit the vulnerabilities of the environment and cause harm to one or more assets, leading to monetary loss.
- Assess the risk according to the logical formula stated above and assign it a value of high, moderate or low.
- Then develop a solution for every high and moderate risk, along with an estimate of its cost.

Risk Assessment – Beginning Steps

- **Create a risk management plan** using the data collected.

Threat	Vulnerability	Asset and consequences	Risk	Solution
System failure — overheating in server room **High**	Air conditioning system is ten years old. **High**	Servers. All services (website, email, etc.) will be unavailable for at least 3 hours. **Critical**	**High** (potential loss of $50,000 per occurrence)	Buy a new air conditioner (cost: $3,000)
Malicious human (interference) — distributed denial-of-service (DDoS) attack **High**	Firewall configured properly and has good DDOS mitigation. **Low**	Website. Website will be unavailable. **Critical**	**Moderate** (potential loss of $5000 per hour of downtime)	Monitor firewall
Natural disaster — flooding **Moderate**	Server room is on the 3rd floor. **Very low**	Servers. All services will be unavailable. **Critical**	**Very low**	No action needed
Accidental human interference — accidental file deletions **High**	Permissions are configured properly; IT auditing software is in place; backups are taken regularly. **Low**	All files on a file share. Critical data could be lost, but almost certainly could be restored from backup. **Moderate**	**Low**	Continue monitoring permissions changes, privileged users, and backups

Risk Assessment Matrix

- A risk assessment matrix is a visual representation (like a chart) that presents the severity of an event occurring versus the probability of this event occurring

- By visualizing existing and potential risks one can assess their impact, and quickly identify which ones are highest-priority.

- This will allow you to create a plan for responding to the risks that need the most attention and perhaps create mitigation plans to avoid them altogether.

Possible elements in a Risk assessment Matrix:

- Main Aspects:
  - Severity: defines the impact and consequences resulting from an event
  - Likelihood: defines the probability of an event occurring
  - Ranking: quantifies or qualifies, in a broad manner, the result, allowing for quick recognition of the risks and their level of impact.

Severity: Possible classifications

- Insignificant: Risks pose no significant threat to the organisation.
- Minor: Risks that have a small potential for negative consequences, but will not have a significant impact to the organisation.
- Moderate: Risks that could potentially have negative consequences, posing a moderate threat to the organization.
- Critical: Risks with substantial negative consequences that will seriously impact the success of the organization.
- Catastrophic: Risks with extreme negative consequences that could cause the organisation to collapse its business or severely impact daily operations of the organization.

Ranking: Possible classifications

- Low: Risks with minor consequences of the risk ,unlikely to occur, generally ignored, and often colour-coded green.

- Medium: Somewhat likely to occur, slightly more serious consequences, take steps to prevent medium risks from occurring, they are not high-priority and should not significantly affect organization. These risks are often colour-coded yellow.

- High: These are serious risks that both have significant consequences, and are likely to occur. Prioritize and respond to these risks in the near term. They are often colour-coded orange.

- Extreme: Catastrophic risks that have severe consequences and are highly likely to occur. Extreme risks are the highest priority. You should respond to them immediately, as they can threaten the success of the organization or project. They are often colour-coded red.

Risk Assessment Levels

Likelihood scale	Criteria	Description
Rare	0 - 5%	Extremely unlikely or virtually impossible
Unlikely	6 - 25%	Unlikely to occur
Possible	26 - 50%	Fairly likely to occur
Likely	51 - 75%	More likely to occur
Almost certain	>75%	Almost certain will occur

Risk Assessment Matrix - Example

	Consequence				
Likelihood	Insignificant	Minor	Moderate	Major	Critical
Rare	LOW Accept the risk Routine management	LOW Accept the risk Routine management	LOW Accept the risk Routine management	MEDIUM Specific responsibility and treatment	HIGH Quarterly senior management review
Unlikely	LOW Accept the risk Routine management	LOW Accept the risk Routine management	MEDIUM Specific responsibility and treatment	MEDIUM Specific responsibility and treatment	HIGH Quarterly senior management review
Possible	LOW Accept the risk Routine management	MEDIUM Specific responsibility and treatment	MEDIUM Specific responsibility and treatment	HIGH Quartely senior management review	HIGH Quarterly senior management review
Likely	MEDIUM Specific responsibility and treatment	MEDIUM Specific responsibility and treatment	HIGH Quarterly senior management review	HIGH Quarterly senior management review	EXTREME Monthly senior management review
Almost certain	MEDIUM Specific responsibility and treatment	MEDIUM Specific responsibility and treatment	HIGH Quarterly senior management review	EXTREME Monthly senior management review	EXTREME Monthly senior management review

RISK MODELS

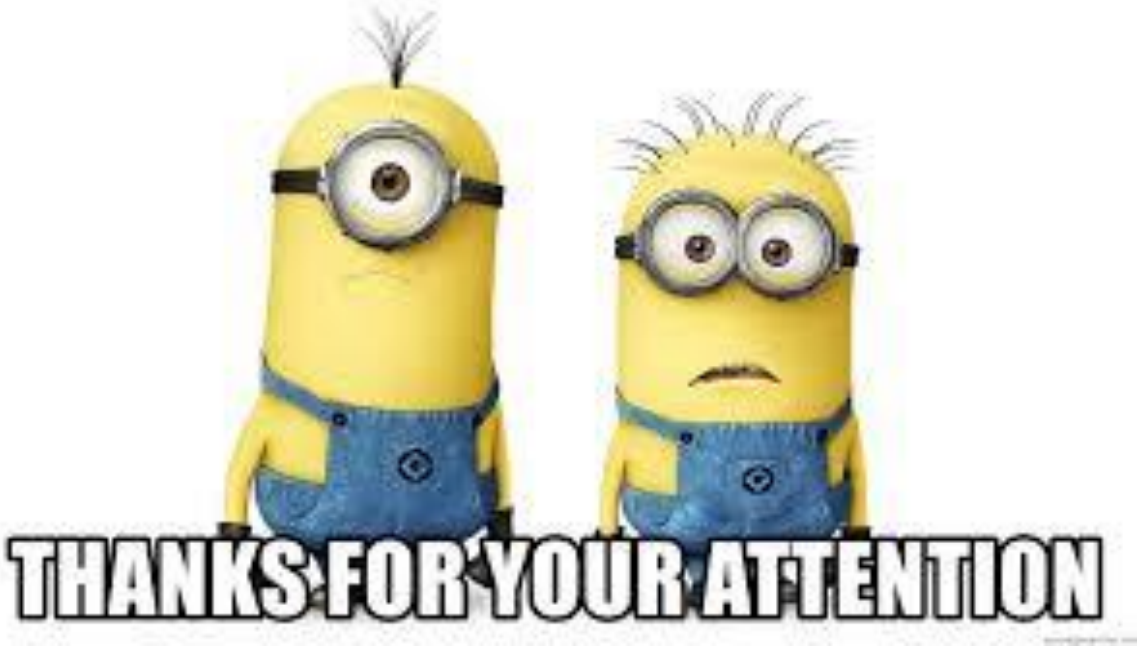
- Different organisations may have dissimilar approaches with respect to modelling their Risk Assessment.

- For example Organisation “A” may decide that the important factors for their Risk Assessment Matrix should contain a fixed set of elements that emphasize external threats. Organisation “B” could have chosen to focus on internal threats and business mission critical elements.

- NIST Special Publication 800-39 defines an organization’s risk frame as the set of assumptions, constraints, risk tolerances, priorities, and trade-offs that underpin the organization’s risk management strategy.

Steps for Risk Assessment

- Preparing : Identification phase
  - purpose, scope, constraints, source of information and analysis approach
- Conducting the Risk Assessment: Create a list of the Risks
  - Threat sources, events, vulnerabilities, exploits, impacts, likelihoods
- Communicate and Share the Assessment Results: Reporting phase
  - Appropriate method, risk assessment results, evidence and mapping against the organisational policies and guides
- Maintenance of the Risk Assessment: keep the document current and relevant
  - Ongoing update, monitoring risk factors, what changed?


THANKS FOR YOUR ATTENTION