MIS607 Cybersecurity – Assessment 3 Related Notes

TORRENS UNIVERSITY AUSTRALIA

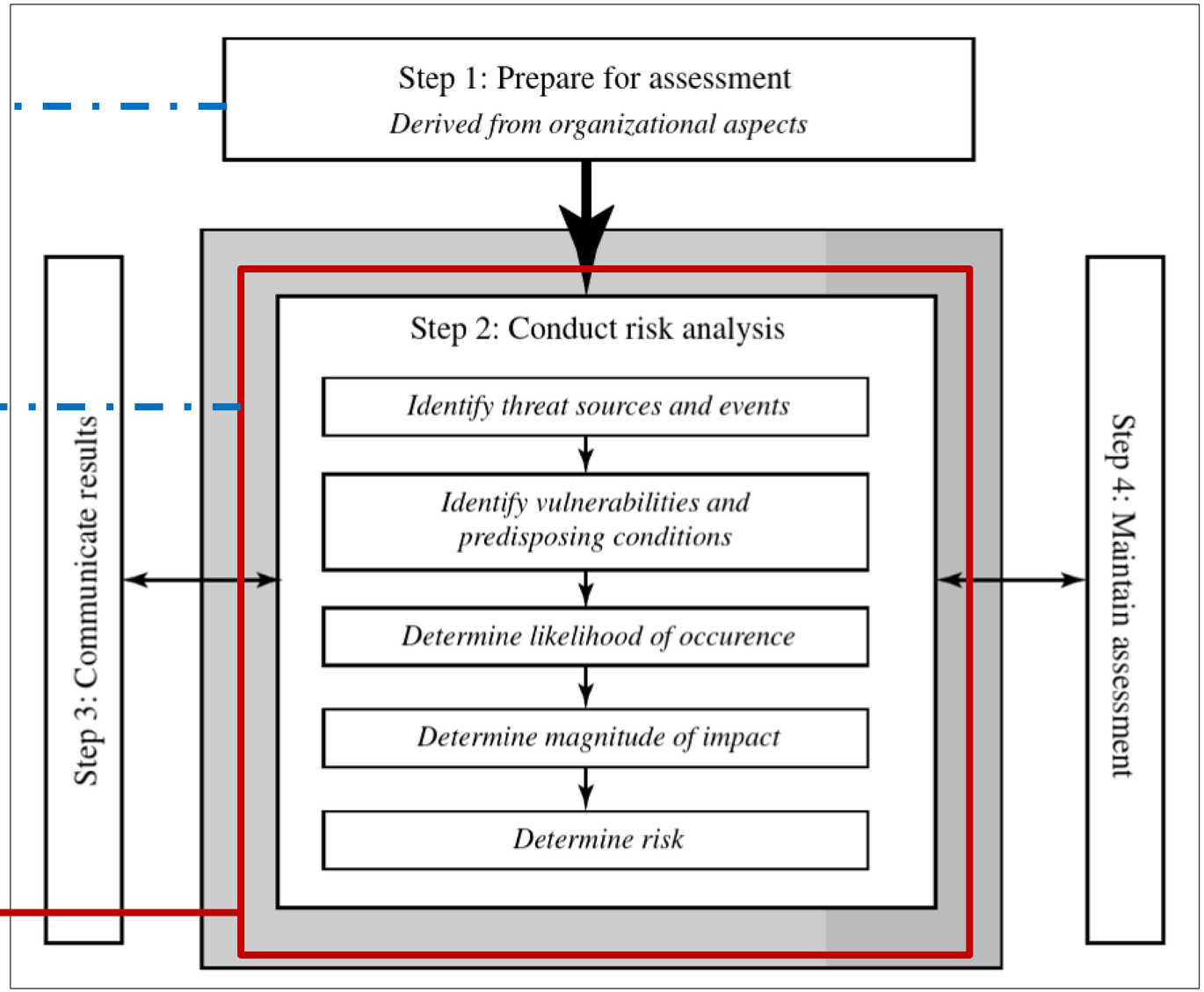
Risk Analysis Steps

TORRENS UNIVERSITY AUSTRALIA

1st Question: *What assets do we need to protect? (Asset identification)*

2nd Question: *How are those assets threatened?*

- ✓ *Who or what could cause it harm?*
- ✓ *How could this occur?*



Risk Analysis Steps

Stallings and Brown (2017, p.491)

TORRENS UNIVERSITY AUSTRALIA

Step 1. Identify threats or risks to which the assets are exposed

- ✓ Threat is anything that might hinder or prevent an asset from providing appropriate levels of the key security services: confidentiality, integrity, availability, accountability, authenticity and reliability.
- ✓ The goal of this stage is to identify potentially significant risks to the assets listed.
- ✓ This requires answering *"Who or what could cause it harm?"*
- ✓ **Note:** one asset may have multiple threats, and a single threat may target multiple assets.
- ✓ A threat may be either natural or human-made and may be accidental or deliberate. This is known as the threat source or threat agent.

Stallings and Brown (2017, p.494)

TORRENS UNIVERSITY AUSTRALIA

Step 2. Identify vulnerability and predispose conditions

- ✓ Involves identifying flaws or weaknesses in the organization's IT systems or processes that could be exploited by a threat source.
- ✓ This requires answering *"How could this threat occur?"*
- ✓ **Note:** that the mere existence of some vulnerability does not mean harm will be caused to an asset.
- ✓ It is the combination of a threat and a vulnerability that creates a risk to an asset.
- ✓ The outcome of this step should be a list of threats and vulnerabilities, with brief descriptions of how and why they might occur.

Stallings and Brown (2017, p.495)

TORRENS UNIVERSITY AUSTRALIA

- **Step 3. Determine likelihood of occurrence of each identified threat to an asset, in the context of any existing controls**

✓ The ideal would be to specify the "likelihood" as a probability value to the organization should it occur

✓ Security controls include management, operational, and technical processes and procedures that act to reduce the exposure of the origination to risks

✓ Security controls can be identified by using checklists and by interviewing key organizational staff.

✓ Then the likelihood that each identified threat could occur and cause harm to some asset needs to be specified. The "likelihood" is typically described "qualitatively".

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.

Stallings and Brown (2017, p.497)

TORRENS UNIVERSITY AUSTRALIA

- **Step 4. Determine magnitude/consequence of impact of the risk on the organization**

  - ✓ The ideal would be to specify the “consequence/magnitude” as a monetary cost to the organization should it occur
  - ✓ A qualitative descriptive value is used to describe the consequences
  - ✓ This determination should be based upon the judgement of the asset’s owners and the organization’s management, rather than the opinion of the risk analyst.
  - ✓ Specified consequences needs to be realistic and must relate to the impact on the organization as a whole should this specific threat eventuate.

Stallings and Brown (2017, p.498)

TORRENS UNIVERSITY AUSTRALIA

Risk Consequences

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.

Stallings and Brown (2017, p.498-499)

TORRENS UNIVERSITY AUSTRALIA

Risk = (Probability that threat occurs) X (Cost to Organization)

IMPORTANT

Many risk analyses use "**qualitative**", rather than "**quantitative**" ratings for both items. The goal is to order the resulting risks to help determine which need to be most urgently treated, rather than to give them an absolute value.

Stallings and Brown (2017, p.496)

TORRENS UNIVERSITY AUSTRALIA

Step 5. Determine resulting level of Risk

- ✓ Once the “likelihood” and “consequence” of each specific threat have been identified, a final level of risk can be assigned.
- ✓ Determined by using a Table that maps these values to a risk level. This table details the risk level assigned to each commination.
- ✓ This Table provides the qualitative equivalent of performing the ideal risk calculation using quantitative values. It also indicates the interpretation of these assigned levels.

Stallings and Brown (2017, p.499)

TORRENS UNIVERSITY AUSTRALIA

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 is 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 is 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.

Stallings and Brown (2017, p.500)

TORRENS
UNIVERSITY
AUSTRALIA