CSIT988/CSIT488 – "Security, Ethics and Professionalism"

Autumn 2025

Workshop 5

I. Multiple-Choice Questions

1. Which of the following statements are false?
   Select one or more:

   A. Managing risk is one of the key responsibilities of every manager within the organisation.
   B. Risk management is a major component of risk analysis.
   C. The InfoSec community of interest often take a leadership role in addressing risk.
   D. Risk control is the first operational phase of risk management.
   E. During risk management, classification categories for information assets must be mutually exclusive.

2. Which of the following statements are true?
   Select one or more:

   A. When classifying and categorising information assets, inventory should not reflect assets' security priority.
   B. When assessing the values of information assets, one should not care which asset is the most critical to the success of the organisation.
   C. Technological obsolescence is among the threats to InfoSec.
   D. The amount of danger posed by all threats are always easy to assess.
   E. Vulnerabilities are specific avenues where successful attacks to the information assets of the organisations have been known.

3. Which of the following statements are false?
   Select one or more:

   A. At the end of the risk identification process, an organisation should have a working knowledge of the vulnerabilities existing between each threat and each asset.
   B. Risk assessment assigns a risk rating or score to each specific vulnerability.

C. The likelihood of vulnerability occurrence must always be the same for all vulnerabilities
D. The uncertainty of current knowledge about a given vulnerability is always smaller than the percentage of risk mitigated by current controls.
E. The Australian and New Zealand Risk Management Standard 4360 uses quantitative methods to determine risk.

4. Which of the following statements are true?

   Select one or more:

   A. Risk defence is one of the five basic strategies to control risks.
   B. Risk mitigation aims to shift the risk to other areas or to outside entities.
   C. Risk acceptance aims to remove or discontinue the information asset.
   D. Risk transference aims to accept the risk without control or mitigation.
   E. Risk termination aims to apply safeguards that eliminate or reduce the remaining uncontrolled risks.

5. Which of the following statements are false?
   Select one or more:

   A. Residual risk is the risk that has not been covered by one of the safeguards.
   B. The goal of InfoSec is to bring residual risk to zero.
   C. Risk controls should be monitored and measured on an ongoing basis.
   D. Before using the risk acceptance strategy, one must perform a through cost-benefit analysis
   E. Risk transference may be accomplished by purchasing insurance.

6. Which of the following statements are true?
   Select one or more:

   A. Asset valuation is the process of evaluating the loss in value if the given information asset is compromised.
   B. Annualised loss expectancy (ALE) is the expected amount of loss that would occur from a single attack.
   C. Cost-Benefit Analyses may be calculated before a control or safeguard is implemented.
   D. To calculate CBA, one should consider the annual cost of the safeguards.
   E. Political feasibility aims to examine whether the organisation has or can acquire the technology to implement and support the InfoSec alternatives.

II. Short-Answer Questions and Case Studies

1. What is risk management? What is risk analysis?

2. Who is responsible for risk management in an organization? Which community of interest usually takes the lead and which community of interests usually provides the resources used when undertaking information asset risk management?

3. Describe the TVA worksheet. What is it used for?

4. Examine the risk formula presented in Lecture 09. What are its primary elements?

5. If an organization has three information assets to evaluate for risk management, as shown in the accompanying data, which vulnerability should be evaluated for additional controls first? Which one should be evaluated last?

   Asset A:

   Switch L47 connects a network to the Internet. It has two vulnerabilities: it is susceptible to hardware failure at a likelihood of 0.2, and it is subject to an SNMP buffer overflow attack at a likelihood of 0.1. This switch has an impact rating of 90 and has no current controls in place. You are 75 percent certain of the assumptions and data.

   Asset B:

   Server WebSrv6 hosts a company Web site and performs e-commerce transactions. It has a Web server version that can be attacked by sending it invalid Unicode values. The likelihood of that attack is estimated at 0.1. The server has been assigned an impact value of 100, and a control has been implanted that reduces the impact of the vulnerability by 75 percent. You are 80 percent certain of the assumptions and data.

   Asset C:

   Operators use an MGMT45 control console to monitor operations in the server room. It has no passwords and is susceptible to unlogged misuse by the operators. Estimates show the likelihood of misuse is 0.1. There are no controls in place on this asset; it has an impact rating of 5. You are 90 percent certain of the assumptions and data.

6. What are the five risk control strategies described in Lecture 10?

7. What conditions must be met to ensure that risk acceptance has been used properly?

8. What is risk appetite? Explain why risk appetite varies from organization to organization.

9. What is a cost-benefit analysis?

10. Using the following table, calculate the SLE, ARO and ALE for each threat category listed.

\

XYZ Software Company (Asset value: $1,200,000 in projected revenues)		
Threat Category	**Cost per Incident**	**Frequency of Occurrence**
Programmer mistakes	$5,000	1 per week
Loss of intellectual property	$75,000	1 per year
Software piracy	$500	1 per week
Theft of information (hacker)	$2,500	1 per quarter
Theft of information (employee)	$5,000	1 per 6 months
Web defacement	$500	1 per month
Theft of equipment	$5,000	1 per year
Viruses, worms, Trojan horses	$1,500	1 per week
Denial-of-service attack	$2,500	1 per quarter
Earthquake	$250,000	1 per 20 years
Flood	$250,000	1 per 10 years
Fire	$500,000	1 per 10 years

11. Assume a year has passed and XYZ has improved its security. Using the following table, calculate the SLE, ARO, and ALE for each threat category listed.

XYZ Software Company (Asset value: $1,200,000 in projected revenues)				
Threat Category	**Cost per Incident**	**Frequency of Occurrence**	**Cost of Controls**	**Type of Control**
Programmer mistakes	$5,000	1 per month	$20,000	Training
Loss of intellectual property	$75,000	1 per 2 years	$15,000	Firewall/IDS
Software piracy	$500	1 per month	$30,000	Firewall/IDS
Theft of information (hacker)	$2,500	1 per 6 months	$15,000	Firewall/IDS
Theft of information (employee)	$5,000	1 per year	$15,000	Physical security
Web defacement	$500	1 per quarter	$10,000	Firewall
Theft of equipment	$5,000	1 per 2 year	$15,000	Physical security
Viruses, worms, Trojan horses	$1,500	1 per month	$15,000	Antivirus
Denial-of-service attack	$2,500	1 per 6 months	$10,000	Firewall
Earthquake	$250,000	1 per 20 years	$5,000	Insurance/backups
Flood	$50,000	1 per 10 years	$10,000	Insurance/backups
Fire	$100,000	1 per 10 years	$10,000	Insurance/backups

12. Assume that the costs of controls presented in the table for Question 8 were unique costs directly associated with protecting against that threat. In other words, do not worry about overlapping costs between threats. Calculate the CBA for each control. Are they worth the costs listed?