Workshop 8 for Week 9

These tutorial questions will not be discussed in the class. They are designed to help you understand the topics discussed in the relevant week.

1. What are the four risk control strategies presented in this week?

Avoidance: Applying safeguards that eliminate or reduce the remaining uncontrolled risks for the vulnerability
Transference: Shifting the risk to other areas or to outside entities
Mitigation: Reducing the impact if the vulnerability is exploited
Acceptance: Understanding the consequences and accepting the risk without control or mitigation

2. Describe how outsourcing can be used for risk transference.

Outsourcing can be used for risk transference when an organization chooses to hire an ISP or a consulting organization for products and services such as server acquisition and configuration, Web development, maintenance, administration, and even InfoSec functions. This allows the organization to transfer the risks associated with managing these complex systems to an organization that has experience with those risks. Outsourcing can shift responsibility for disaster recovery through service level arrangements

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

Risk acceptance has been used properly if the level of risk posed to the asset has been determined, the probability of attack and the likelihood of a successful exploitation of a vulnerability has been assessed, the annual rate of occurrence of such an attack has been approximated, the potential loss that could result from attacks has been estimated, a thorough cost-benefit analysis has been performed, controls using each appropriate type of feasibility have been evaluated, or it has been decided that the particular function, service, information, or asset did not justify the cost of protection

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

Risk appetite is the amount of risk an organization is willing to accept as it evaluates the trade-off between perfect security and unlimited accessibility. Risk appetite varies from organization to organization because of differences in their size, budget, culture, and the value placed on certain assets.

5. What is single loss expectancy? What is annual loss expectancy?

Single loss expectancy (SLE) is the calculated value associated with a sole occurrence of the most likely loss from an attack. Annualized loss expectancy (ALE) is the calculated value associated with the most likely annual loss from an attack. ALE is often expressed as the SLE multiplied by the number of expected occurrences per year.