Workshop Questions for Week 13

1. **Quick Quiz:**

1.____ of information exists when a control provides assurance that every activity undertaken can be attributed to a named person or automated process.

a. Privacy
b. Authentication
c. Authorization
d. Accountability

2.What are the four principles of popular management theory?

3.____ planning focuses on the day-to-day operations of local resources, and occurs in the present or short term.

a. Operational
b. Tactical
c. Strategic
d. Business

4. Which statement describes what an organization wants to become?

a. Values statement
b. Vision statement
c. Mission statement
d. Aspiration statement

5.What are the major components of contingency planning?

a. Business impact analysis
b. Incident response plan
c. Disaster recovery plan
d. Business continuity plan

6. In the bull's-eye model, the outer layer in the diagram represents _____.

a. networks
b. applications
c. policies
d. systems

7.What is one of the three types of an information security policy?

a. Enterprise information security policy
b. Network information security policy
c. Threat assessment information security policy
d. Privacy information security policy

2. Describe the CNSS security model. What are its three dimensions?

John McCumber has developed the CNSS security model. It is a three-dimension model and known as the McCumber Cube. It is becoming standard for many aspects of security of information systems. It has 27 cells in a cube. Each cell in the cube represented an area of intersection among these three dimensions that must be addressed to secure information systems. Organization must make sure that each of the three communities of interest properly addresses each of the 27 cells. The three dimension of the CNSS model are Confidentiality, Integrity, Availability, Policy, Education, Technology Storage, Processing, and Transmission

3. What is InfoSec governance?
What are the five basic outcomes that should be achieved through InfoSec governance?

InfoSec Governance ensures that the strategic direction of information security aligns with business objectives, risks are managed, resources are utilized effectively, performance is measured, and value is delivered optimally.

1. Strategic alignment of InfoSec with business strategy to support organizational objectives
2. Risk management by executing appropriate measures to manage and mitigate threats to information resources
3. Resource management by utilizing InfoSec knowledge and infrastructure efficiently and effectively
4. Performance measurement by measuring, monitoring, and reporting InfoSec governance metrics to ensure that organizational objectives are achieved
5. Value delivery by optimizing InfoSec investments in support of organizational objectives.

4. What are the three major benefits of a SETA (security education, training and awareness) program?

A SETA program improves an organization's security posture, ensures regulatory compliance, mitigates insider threats, enhances incident response, and fosters a security-conscious culture among employees.

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

The TVA worksheet combines a prioritized list of assets and their vulnerabilities and a list that prioritizes threats facing the organization. The resulting grid provides a convenient method of examining the "exposure" of assets, allowing a simple vulnerability assessment.

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

Risk appetite is the amount and type of risk an organization is willing to accept in pursuit of its objectives. It varies from organization to organization due to factors such as industry and regulatory environment, organizational goals and strategy, financial stability and resources, stakeholder expectations, and the leadership and culture of the organization. These factors collectively shape how much risk an organization is prepared to tolerate, influencing decisions and actions across different sectors and contexts.

7. What are the main components of cryptology?

The main components of cryptology include cryptography and cryptanalysis.