NPTEL ASSIGNMENT
WEEK-3

1. The process of defining and specifying the long-term direction to be taken by an organization, and the allocation and acquisition of resources needed to pursue this effort is known as:
   a. Governance
   b. Security Management
   c. Strategic Planning
   d. Objectives

2. Which of the following statements best describes the relationship between GRC (Governance, Risk, and Compliance) and cybersecurity ?
   a. GRC focuses solely on cybersecurity management and overlooks other risk management initiatives.
   b. Cybersecurity is the primary focus of GRC, with minimal consideration for other risks.
   c. GRC integrates cybersecurity as one component within the broader framework of enterprise risk management (ERM).
   d. GRC is a standalone framework independent of cybersecurity and risk management.

3. A written document provided by management that inform employees and others in the workplace about proper behavior regarding the use of information and information assets are known as:
   a. Guidelines
   b. Information Security Policy
   c. De facto standard
   d. Practices

4. Which approach to cybersecurity management treats cybersecurity as a separate category distinct from other risks an organization may face, and focuses solely on cybersecurity, depending on the size and nature of the organization?
   a. Standard Driven Approach
   b. Organization Planning Approach
   c. GRC Framework
   d. Risk Management Framework

5. Benefits of implementing a GRC in an organization include:
   a. Responsible operations
   b. Data-driven decision-making
   c. Improved cybersecurity
   d. All the above

6. What is the purpose of the COBIT maturity model?
   a. To assess an organization's maturity in IT governance processes
   b. To rank organizations based on their financial performance
   c. To determine the efficiency of network infrastructure
   d. To evaluate employee satisfaction levels in the IT department

7. COSO's ERM framework emphasizes:

a. Operational efficiency
b. Risk identification and assessment
c. Regulatory compliance
d. Human resource management

8. Which characteristic distinguishes the approaches of COBIT, COSO, and COSO-ERM from specific standards like ISO or NIST?

a. They prioritize cybersecurity over other risk management aspects.
b. They focus exclusively on small to medium-sized enterprises (SMEs).
c. They operate at the enterprise level rather than focusing on specific standards.
d. They are primarily developed by governmental regulatory bodies.

9. Why might some countries be hesitant to adopt the ISO 27001 model?

a. It is a mandatory standard with strict compliance requirements.
b. It is not recognized as a valid security framework by international organizations.
c. There are concerns about the model's overall effectiveness compared to existing approaches.
d. It prioritizes specific security vendors or technologies.

10. Which of the following is not considered a principle or practice for securing IT systems?

a. Implement layered security to ensure there is no single point of vulnerability.
b. Do not implement unnecessary security mechanisms.
c. Maximize the system elements to be trusted.
d. Assume that external systems are insecure.