# IC32 - Pre-Instructional Survey

1. What is the primary function of a firewall?

    a. Block all internet traffic
    b. Detect network intrusions
    c. Filters network traffic
    d. Authenticate users

2. Inter-network connection device that restricts data communication traffic between two connected networks is called a(n) ________________.

    a. IDS
    b. Firewall
    c. Router
    d. Anti-virus software

3. The process of securing a system by reducing its attack surface is known as

    a. Threat Modeling
    b. System Hardening
    c. Intrusion Detection
    d. Whitelisting

4. Policies, procedures and technical controls that govern the use of system resources are known as

    a. Data Flow Controls
    b. System Integrity Controls
    c. Access Controls
    d. System Hardening Controls

5. Which of the following is an objective of cybersecurity acceptance testing?

    a. Verification of cybersecurity specifications
    b. Root cause analysis
    c. Cyber risk determination
    d. Verification of system functionality

6. What are the three main phases of the IACS Cybersecurity Lifecycle?

   a. Assess, Develop & Mitigate, Maintain
   b. Design, Implement, Maintain
   c. Assess, Develop & Implement, Maintain
   d. Design, Mitigate, Maintain

7. Which of the following is the correct risk equation?

   a. Risk = Threat x Asset x Consequence
   b. Risk = Threat x Vulnerability x Cost
   c. Risk = Threat Agent x Threat x Vulnerability
   d. Risk = Threat x Vulnerability x Consequence

8. The desired level of security for a system is known as?

   a. Target Security Level
   b. Achieved Security Level
   c. Capability Security Level
   d. Protection Level

9. Which of the following is the correct formula for Cyber Risk Reduction Factor (CRRF)?

   a. CRRF = Unmitigated Risk / Tolerable Risk
   b. CRRF = Mitigated Risk / Tolerable Risk
   c. CRRF = Tolerable Risk / Unmitigated Risk
   d. CRRF = Tolerable Risk / Mitigated Risk

10. An Intrusion Detection System (IDS) is an example of what method of treating risk?

    a. Detect
    b. Deter
    c. Defend
    d. Defeat

11. Security service system that monitors and analyzes system events for the purpose of finding, and providing real-time or near real-time warning of attempts to access system resources in an unauthorized manner is called a(n) _______________.

   a. IDS
   b. Firewall
   c. Router
   d. Anti-virus software

12. What is the name of the firewall feature that analyzes protocols at the application layer to identify malicious or malformed packets?

   a. Stateful inspection
   b. Deep packet inspection
   c. Packet filter
   d. Layer 3 check

13. A three-tier network segmentation design that prevents direct communication between the enterprise network and the process control network by creating a buffer is also known as a(n) _____________.

   a. Zones and conduits
   b. Perimeter firewall
   c. ICS firewall
   d. DMZ

14. Which of the following represents the recommended process of firewall planning and implementation?

   a. Plan, Configure, Test, Deploy, Manage
   b. Plan, Configure, Deploy, Test, Manage
   c. Plan, Deploy, Manage, Test, Configure
   d. Design, Configure, Test, Deploy, Document

15. What are the main types of intrusion detection systems?

   a. Perimeter Intrusion Detection & Network Intrusion Detection
   b. Host Intrusion Detection & Network Intrusion Detection
   c. Host Intrusion Detection & Intrusion Prevention Systems
   d. Intrusion Prevention & Network Intrusion Detection

16. What is the desired outcome of the Initiate a CSMS program activity?

   a. Conceptual diagrams that show how an AD forest can be attacked
   b. Obtain leadership commitment, support, and funding
   c. Identify software agents used by threat agents to propagate attacks
   d. Conduct periodic IACS conformance audits

17. Which of the following is NOT a network device hardening best practice?

   a. Install latest firmware updates
   b. Shut down unused physical interfaces
   c. Enable logging, collect logs (e.g. Syslog) and review regularly
   d. Use Telnet for remote management

18. Which of the following is an example of dual-factor authentication?

   a. Username and password
   b. Digital certificate and smart card
   c. Fingerprint and retinal signature
   d. Fingerprint and smart card

19. A network that uses a public telecommunication infrastructure such as the Internet to provide remote networks or computers with secure access to another network is known as a ________.

   a. VLAN
   b. VSAT
   c. VPN
   d. VNC

20. If a virus shuts down an industrial network by overloading the Ethernet switches which basic information security property is affected?

   a. Integrity
   b. Confidentiality
   c. Availability
   d. Reliability

# IC32 - Pre-Instructional Survey

## Answer Key

1. c
2. b
3. b
4. c
5. a
6. c
7. d
8. a
9. a
10. a
11. a
12. b
13. d
14. a
15. b
16. b
17. d
18. d
19. c
20. c