CSX Fundamentals - Mock Exam

Exam notes:
- This is a close book exam
- 6 sections - (225) Questions, covering all study guide sections
- Make sure you answer all the questions
- Some questions have multiple selections (select all right and it counts for 1 mark)
- Track your time...

Have fun! - You can do it!

Email address *

qc.trevor.shi@gmail.com

Name (First name / Last name) *

trevor shi

Cohort *

5

Section 1- INTRODUCTION TO CYBERSECURITY

✓ 1. The objective of information security is threefold, it involves:

- a) Availability, security, assurance
- b) Confidentiality, integrity, availability ✓
- c) Cyber assurance, integrity, hacking
- d) None of the above

✓ 2. The terms “cybersecurity” and “information security” are often used interchangeably, but in reality, cybersecurity is part of _____.:

- a) Network security
- b) Data security
- c) Information security ✓
- d) Enterprise security

✓ 3. Controls used to protect assets, reduce _____ and _____ and/or reduce risk to an acceptable level.

- a) Security, protection
- b) Threats, weaknesses
- c) Cost, security
- d) Vulnerabilities, impacts ✓

✓ 4. The National Institute of Standards and Technology (NIST) identifies five keys functions necessary for protection of digital assets, they are:

- a) Identify, security, protect, detect, standards
- b) Respond, identify protect, detect, recover ✓
- c) Password, policies, standards, identity, culture
- d) None of the above

✗ 5. Nonrepudiation refers to the concept of:

- a) Delegating security
- b) Removing all responsibility from cyber professionals
- c) Refusing evidence ✗
- d) Ensuring that a message or other piece of information is genuine

Correct answer

- d) Ensuring that a message or other piece of information is genuine

✕ 6. Governance is the responsibility of _____ and _____

- a) Cyber practitioners, network administrators
- b) Government, lawyers
- c) Data owners, system architects ✕
- d) Board of directors, senior management

Correct answer

- d) Board of directors, senior management

✕ 7. An organization's executive management team is responsible for:

- a) Ensuring that needed organizational functions, resources and supporting infrastructures are available and properly utilized to fulfill the directives of the board
- b) Ensuring the IT operations is working in accordance to system specifications
- c) Ensuring the IT departments is well organized and follows a cyber security framework in accordance to the executives and operational standards ✕
- d) None of the above

Correct answer

- a) Ensuring that needed organizational functions, resources and supporting infrastructures are available and properly utilized to fulfill the directives of the board

✗ 8. Some of the responsibilities of a CISO or CSO include:

- a) Developing the security strategy
- b) Ensuring that risk and business impact assessments are conducted
- c) Directing and monitoring security activities
- d) (a),(b),(c)
- e) (a), (b) ✗
- f) None of the above

Correct answer

- d) (a),(b),(c)

✓ 9. In most organizations cyber security is managed by a team, which may include – select the MOST accurate statement:

- a) Subject matter experts, cybersecurity practitioners, security architects, administrators, digit forensics, vulnerability researchers and network specialist ✓
- b) Human resource, compliancy consultants, board of directors, CEO
- c) External consultants
- d) Network administrators and risk authority

10. Read the description and match column with correct word: (3 marks max)

	Compliance	Risk Management	Governance	
The responsibility of the board of directors and senior management of the organization	○	○	◉	✓
The coordination of activities that direct and control	◉	○	○	✗
The act of adhering to, and the ability to demonstrate adherence to,	○	◉	○	✗

Correct answers

	Compliance	Risk Management	Governance
The coordination of activities that direct and control	○	◉	○
The act of adhering to, and the ability to demonstrate adherence to,	◉	○	○

✕ 11. Three common controls used to protect the availability of information are:

- ○ a) Redundancy, backups and access controls.
- ◉ b) Encryption, file permissions and access controls. ✕
- ○ c) Access controls, logging and digital signatures.
- ○ d) Hashes, logging and backups.

Correct answer

- ◉ a) Redundancy, backups and access controls.

✕ 12. Select all that apply. Governance has several goals, including:

- [x] a) Providing strategic direction. ✓
- [x] b) Ensuring that objectives are achieved. ✓
- [x] c) Verifying that organizational resources are being used appropriately. ✓
- [x] d) Directing and monitoring security activities. ✕
- [x] e) Ascertaining whether risk is being managed properly ✓

Correct answer

- [x] a) Providing strategic direction.
- [x] b) Ensuring that objectives are achieved.
- [x] c) Verifying that organizational resources are being used appropriately.
- [x] e) Ascertaining whether risk is being managed properly

✗ 13. Choose three. According to the NIST cybersecurity framework, which of the following are considered keyfunctions necessary for the protection of digital assets?

- [x] a) Encrypt ✗
- [x] b) Protect ✓
- [ ] c) Investigate
- [ ] d) Recover
- [x] e) Identify ✓

Correct answer

- [x] b) Protect
- [x] d) Recover
- [x] e) Identify

✓ 14. Which of the following is the best definition for cybersecurity?

- ○ A. The process by which an organization manages cybersecurity risk to an acceptable level
- ○ B. The protection of information from unauthorized access or disclosure
- ○ C. The protection of paper documents, digital and intellectual property, and verbal or visual communications
- ◉ D. Protecting information assets by addressing threats to information that is processed, stored or transported by ✓
- ○ internetworked information systems

✗ 15. Which of the following cybersecurity roles is charged with the duty of managing incidents and remediation?

- A. Board of directors
- B. Executive committee ✗
- C. Cybersecurity management
- D. Cybersecurity practitioners

Correct answer

- C. Cybersecurity management

✓ 16. Which of the following describes the activities required to identify the occurrence of a cybersecurity incident?

- Data security, awareness/training, access control and processes/procedures
- Communications, analysis and mitigation
- Security continuous monitoring, detection and evaluating anomalies/incidents ✓
- Asset management, risk management and risk assessment

✓ 17. This key function ensures that organizational objectives and stakeholder needs are aligned with desired outcomes through effective decision making and prioritization.

- (●) Governance ✓
- ( ) Risk management
- ( ) Risk mitigation
- ( ) Risk assessment

✓ 18. The primary objective of cybersecurity is:

- ( ) Protection of all company assets
- ( ) Responding to security incidents
- (●) Protecting a company's digital assets ✓
- ( ) Managing risk through countermeasures and controls

✗ 19. Which activity ensures that business processes continue after a security incident?

- ( ) Recovery
- ( ) Detection
- (●) Response ✗
- ( ) Protection

Correct answer

- (●) Recovery

✓ 20. Which of the following activities is associated with identifying digital assets?

- (●) Asset management ✓
- ( ) Awareness and training
- ( ) Recovery management
- ( ) Security continuous monitoring

✓ 21. Which of the following are responsibilities and/or duties of Governance, Risk Management and Compliance (GRC)? Select all that apply.

- [x] Adherence to required laws and regulations ✓
- [x] Implementation of required procedures ✓
- [x] Development of internal controls to mitigate risk ✓
- [x] Adherence to voluntary contractual requirements. ✓

✓ 22. In most information security organizations, which role sets the overall strategic direction?

- ( ) Chief Security Officer (CSO) or Chief Information Security Officer (CISO)
- (●) Board of Directors ✓
- ( ) Individual contributors
- ( ) Chief Information Security Officer (CISO)

✓ 23. Governance involves all of the following except:

- ○ Provide strategic direction
- ○ Ensure responsible use of company resources
- ○ Evaluate whether risk is managed appropriately
- ◉ Implement contractual obligations ✓

✗ 24. Which role is generally responsible for the design, implementation, management processes and technical controls within a security organization?

- ○ Cybersecurity practitioners
- ○ Board of Directors
- ◉ Executive management ✗
- ○ Senior information security management

Correct answer

- ◉ Cybersecurity practitioners

✓ 25. Which of the following falls within the scope of risk management? Investment risk and cyber risk

- ◉ Cyber risk, investment risk and financial risk ✓
- ○ Cyber risk and financial risk
- ○ Only cyber risk

✓ 26. Which term describes the overall structure designed to protect an organization from disclosure of information to unauthorized users, improper modification of data, and non-access to systems?

- ○ Cybersecurity
- ◉ Information security ✓
- ○ Information risk management

✓ 27. All of the following statements are true except:

- ○ Cybersecurity is a component of information security
- ○ Cybersecurity deals with the protection of digital assets
- ◉ Cybersecurity includes protection of paper documents ✓
- ○ Cybersecurity should align with enterprise information security objectives

✓ 28. Risk management involves which of the following activities? Select all that apply.

- ☑ Recognizing risk ✓
- ☑ Assessing impact and likelihood of risk ✓
- ☐ Ensuring information security objectives are achieved
- ☑ Developing strategies to mitigate risk ✓

✓ 29. Cybersecurity involves the protection of the following digital assets:

- ○ Networks, hardware and paper documents
- ○ Digital or intellectual property stored in someone's mind, verbal and visual communications
- ◉ Information that is processed, stored or transported within internetworked information systems ✓
- ○ Only digital intellectual property, verbal or visual communications

✗ 30. Which terms describe the overall concept of information security? Select all that apply.

- ☑ Linear ✗
- ☑ Ongoing ✓
- ☑ Evolving ✓
- ☑ Systemic ✓

Correct answer

- ☑ Ongoing
- ☑ Evolving
- ☑ Systemic

Section 2 - CYBERSECURITY CONCEPTS

1. Read the description and match the correct column word to describe it (6 marks):

	Residual risk	Vulnerability	Inherent risk	Asset	Risk	Threat	
The combination of the probability of an event and its consequence (ISO/IEC 73). Risk is mitigated through the use of controls or safeguards	○	○	○	○	◉	○	✓
Even after safeguards are in place, there will always be residual risk, defined as the remaining risk after management has implemented a risk response	◉	○	○	○	○	○	✓
The risk level or exposure without taking into account the actions that management has taken or might take (e.g., implementing controls)	○	○	◉	○	○	○	✓
Something of either tangible or intangible value that is worth protecting, including people, information, infrastructure, finances and reputation	○	○	○	◉	○	○	✓
A weakness in the design, implementation, operation or internal control of a process that could expose the	○	◉	○	○	○	○	✓

system to adverse threats from threat events						
Anything (e.g., object, substance, human) that is capable of acting against an asset that can result in harm	○	○	○	○	○	◉ ✓

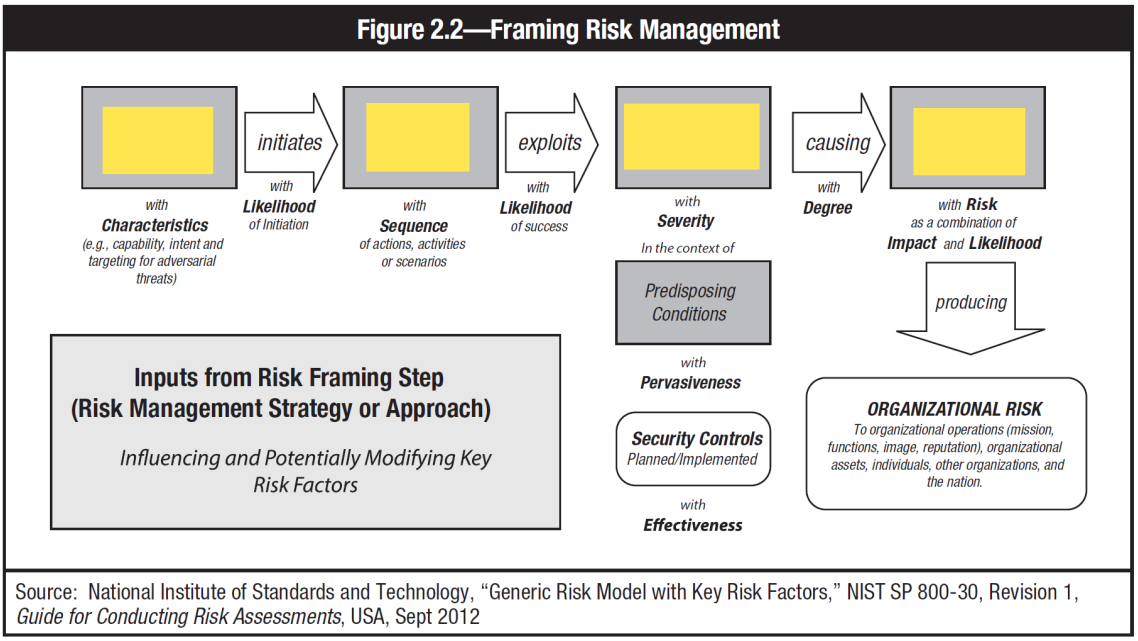
✓ 2. COBIT 5 for Risk, ISO31000:2009, IEC 31010:2009, ISO/IEC 27001:2013, are examples of :

- ○ a) Rules and regulations
- ◉ b) Frameworks and standards ✓
- ○ c) Software to asses risk
- ○ d) Policy templates for organizations

✓ 3. Review the NIST diagram, select the correct workflow order:

- ○ a) Adverse impact, Vulnerability, Threat event, Threat source
- ○ b) Threat event, Adverse impact, Threat source, Vulnerability
- ○ c) Vulnerability, Threat source, Threat event, Adverse impact
- ◉ d) Threat source, Threat event, Vulnerability, Adverse impact ✓

NIST Diagram (Question 3)



Source: National Institute of Standards and Technology, "Generic Risk Model with Key Risk Factors," NIST SP 800-30, Revision 1, *Guide for Conducting Risk Assessments*, USA, Sept 2012

✕ 4. Risk scenario structure includes the following components:

- ○ e) Actor, threat type, policies
- ◉ f) Threat type, Asset/Resources, frameworks ✕
- ○ g) Event, logs, story lines, platform
- ○ h) Actor, threat type, event, asset/resources, time

Correct answer

- ◉ h) Actor, threat type, event, asset/resources, time

✗ 5. A _____ approach to scenario development is based on understanding business goals and how a risk event could affect the achievement of those goals.

- a) Management
- b) Bottom-up ✗
- c) Top-down
- d) Cybersecurity

Correct answer

- c) Top-down

✓ 6. The measure of frequency of which an event may occur is known as:

- a) Likelihood (also called probability) ✓
- b) Criticality
- c) Time
- d) Chance

✓ 7. Three different approaches to implementing cybersecurity, include:

- (●) a) Ad-hoc, risk-based, compliance-based ✓
- ( ) b) Penetration test, hackathon, port scanning
- ( ) c) Contracts, regulations, bi-laws
- ( ) d) Employee monitoring, compliance, policies

✓ 8. While risk is measured by potential activity, an _____ is the actual occurrence of a threat.

- ( ) a) Scam
- (●) b) Attack ✓
- ( ) c) Virus
- ( ) d) Revenue loss

✕ 9. Place the attributes of an attack in order, from left to right:

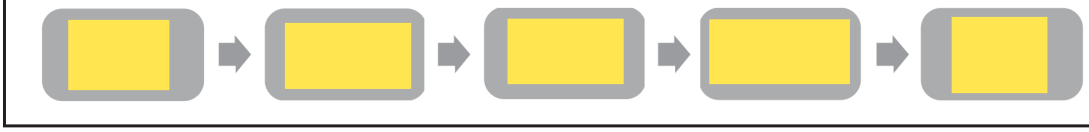
- (●) a) Target (asset), Payload, Exploit, Attack vector, Vulnerability ✕
- ( ) b) Payload, Target (asset), Exploit, Attack vector, Vulnerability
- ( ) c) Exploit, Vulnerability, Attack vector, Payload, Target (asset)
- ( ) d) Attack vector, Exploit, Payload, Vulnerability, Target (asset)
- ( ) e) Vulnerability

Correct answer

- (●) d) Attack vector, Exploit, Payload, Vulnerability, Target (asset)

Attack Attributes (Question 9)

Figure 2.6—Attack Attributes



✓ 10. An _____ is made by human threat agent (or adversary), while a _____ is usually the result of an error, malfunction or mishap of some sort.

- ( ) a) Security threat event, emergency event
- (●) b) Adversarial threat event, nonadversarial threat event ✓
- ( ) c) Nonadversarial threat event, adversarial
- ( ) d) None of the above

11. Match the correct description with the column word (7 Marks)

	Asset	Attack vector	Payload	Policies	Threat	Vulnerability	Cyberrisk
The core duty of cybersecurity is to identify, mitigate and manage _____ to an organization's digital assets.	○	○	○	○	○	○	◉
2. A(n) _____ is anything capable of acting against an asset in a manner that can cause harm.	○	○	○	○	◉	○	○
3. A(n) _____ is something of value worth protecting.	◉	○	○	○	○	○	○
4. A(n) _____ is a weakness in the design, implementation, operation or internal controls in a process that could be exploited to violate the system security.	○	○	○	○	○	◉	○
The path or route used to gain access to the target asset is known as a(n) _____ .	○	◉	○	○	○	○	○
In an attack, the container that delivers the exploit to the target is called a(n) _____ .	○	○	◉	○	○	○	○
_____ communicate required and	○	○	○	◉	○	○	○

prohibited activities and behaviors.

12. Match the correct description with the column word (7 Marks)

	Patches	Rootkit	Standards	Guidelines	Policies	Identity management	Procedu
_____ is a class of malware that hides the existence of other malware by modifying the underlying operating system.	○	○	○	○	○	○	○
_____ provide details on how to comply with policies and standards.	○	○	○	○	○	○	○
_____ provide general guidance and recommendations on what to do in particular circumstances.	○	○	○	○	○	○	○
_____, also called malicious code, is software designed to gain access to targeted computer systems, steal information or disrupt computer operations.	○	○	○	○	○	○	○
_____ are used to interpret policies in specific situations.	○	○	○	○	○	○	○
_____ are solutions to software programming and coding errors.	○	○	○	○	○	○	○
_____ includes many components such as directory services, authentication and authorization services, and user management capabilities such as provisioning	○	○	○	○	○	○	○

and
deprovisioning.

✕ 13. The following are all potential consequences of lack of confidentiality except:

- ○ Disclosure of information protected by privacy laws
- ○ Legal action against the enterprise
- ◉ Interference with national security ✕
- ○ Fraud

Correct answer

◉ Fraud

✕ 14. The degree to which a user or program can create, modify, read, or write to a file is called:

- ◉ Access control ✕
- ○ File permission
- ○ Redundancy
- ○ Certification

Correct answer

◉ File permission

✓ 15. Which information security component considers the level of sensitivity and legal requirements and is subject to change over time?

- ○ Integrity
- ◉ Confidentiality ✓
- ○ Availability
- ○ Authentication

✗ 16. Authentication is defined as which of the following? Select all that apply.

- ☑ A system's ability to identify and differentiate between users ✗
- ☑ Users within an organization authorized to maintain and protect systems and networks ✗
- ☐ The act of verifying identity
- ☑ The act of verifying a user's eligibility to access computerized information ✓

Correct answer

- ☑ The act of verifying identity
- ☑ The act of verifying a user's eligibility to access computerized information

✓ 17. Establishment and maintenance of user profiles that define the authentication, authorization and access controls for each user is called:

- ○ Privileged user management
- ○ Access rights
- ◉ Identity management ✓
- ○ Authentication

✓ 18. Which term describes a cryptology tool used to prove message integrity using algorithms to create unique numeric values?

- ○ Digital signatures
- ◉ Hashes ✓
- ○ Encryption
- ○ Access controls

✕ 19. The following are all potential consequences of lack of integrity except:

- ○ Inaccuracy
- ◉ Erroneous decisions ✕
- ○ Loss of productive time
- ○ Fraud

Correct answer

- ◉ Loss of productive time

✕ 20. Integrity is described as:

- ○ Protection of information from unauthorized modification
- ○ Protection of information from unauthorized access or disclosure
- ○ Timely and reliable access to and use of information and systems
- ◉ All of the above ✕

Correct answer

- ◉ Protection of information from unauthorized modification

✗ 21. Which of the following methods of control can help protect integrity? Select all that apply.

- [x] Logging ✓
- [x] Digital Signatures ✓
- [x] Hashes ✓
- [ ] Encryption

Correct answer

- [x] Logging
- [x] Digital Signatures
- [x] Hashes
- [x] Encryption

✓ 22. Which type of documentation records details of information or events in an organized record-keeping system, usually sequenced in the order in which they occurred?

- ○ Digital certificate
- ○ Digital signature
- ◉ Log ✓
- ○ Backup

✓ 23. A week of severe rainstorms has flooded your company's building. All servers have been ruined. It is estimated that business will be down for 3 weeks. This is an example of:

- ○ Lack of confidentiality
- ◉ Lack of availability ✓
- ○ Lack of integrity
- ○ All of the above

✓ 24. When two or more controls work in parallel to protect an asset, it is called:

- ○ Access control
- ○ Backup
- ◉ Redundancy ✓
- ○ Logging

✗ 25. Which of the following are types of backups?

- ○ Full, incremental and differential
- ○ Full, partial and differential
- ◉ Full, incremental and variable ✗
- ○ Full and differential

Correct answer

- ◉ Full, incremental and differential

✕ 26. Which of the following describes a differential backup?

- ○ Only copies files that have changed since last full backup
- ◉ Copies all files that have changed, regardless of last backup type ✕
- ○ Copies every file in the system, regardless of last backup
- ○ None of the above

Correct answer

- ◉ Only copies files that have changed since last full backup

✕ 27. Potential consequences resulting from lack of availability include which of the following? Select all that apply.

- ☑ Loss of functionality and operational effectiveness ✓
- ☑ Loss of productive time ✓
- ☐ Interference with enterprise's objectives
- ☐ Erroneous decisions

Correct answer

- ☑ Loss of functionality and operational effectiveness
- ☑ Loss of productive time
- ☑ Interference with enterprise's objectives

✕ 28. The concept that a message or other piece of information is genuine is called:

- ○ Integrity
- ○ Nonrepudiation
- ◉ Confidentiality ✕
- ○ Authentication

Correct answer

◉ Nonrepudiation

✕ 29. Which of the following describe authentication? Select all that apply.

- ☑ The act of verifying identity ✓
- ☐ Verification of the correctness of a piece of data
- ☐ A system's ability to identify and differentiate between users
- ☐ Designed to protect against fraudulent logon activity
- ☑ Verifying a user's eligibility to access computerized information ✓

Correct answer

- ☑ The act of verifying identity
- ☑ Verification of the correctness of a piece of data
- ☑ Designed to protect against fraudulent logon activity
- ☑ Verifying a user's eligibility to access computerized information

✗ 30. Nonrepudiation is implemented through which of the following methods? Select all that apply.

- [ ] Backups
- [ ] Transactional logs
- [x] Digital signatures ✓
- [ ] Encryption

Correct answer

- [x] Transactional logs
- [x] Digital signatures

✓ 31. The process of converting plaintext messages, applying a mathematical function to them and producing ciphertext messages is called:

- (•) Encryption ✓
- ( ) Two factor authentication
- ( ) Nonrepudiation
- ( ) Cryptology

✓ 32. Which control mechanism defines authentication and authorization protocols for users?

- ○ Digital signature
- ○ Hashes
- ◉ Access controls ✓
- ○ File permissions

Section 3 - SECURITY ARCHITECTURE PRINCIPLES

✗ 1. Defense in depth can be defined as:

- ◉ a) The depth of security in a security system model ✗
- ○ b) Maturity of the organization cybersecurity program
- ○ c) The knowledge of security in the organization
- ○ d) The practice of layering defense to provide added protection

Correct answer

- ◉ d) The practice of layering defense to provide added protection

✓ 2. The protection of data regardless of its location is a _____ model.

- (●) a) Data-centric ✓
- ( ) b) Network or system-centric
- ( ) c) Well known
- ( ) d) None of the above

✗ 3. SABSA, ZACHMAN, TOGAF are examples of:

- ( ) a) Frameworks
- (●) b) Standards ✗
- ( ) c) Policies
- ( ) d) Procedure models

Correct answer

- (●) a) Frameworks

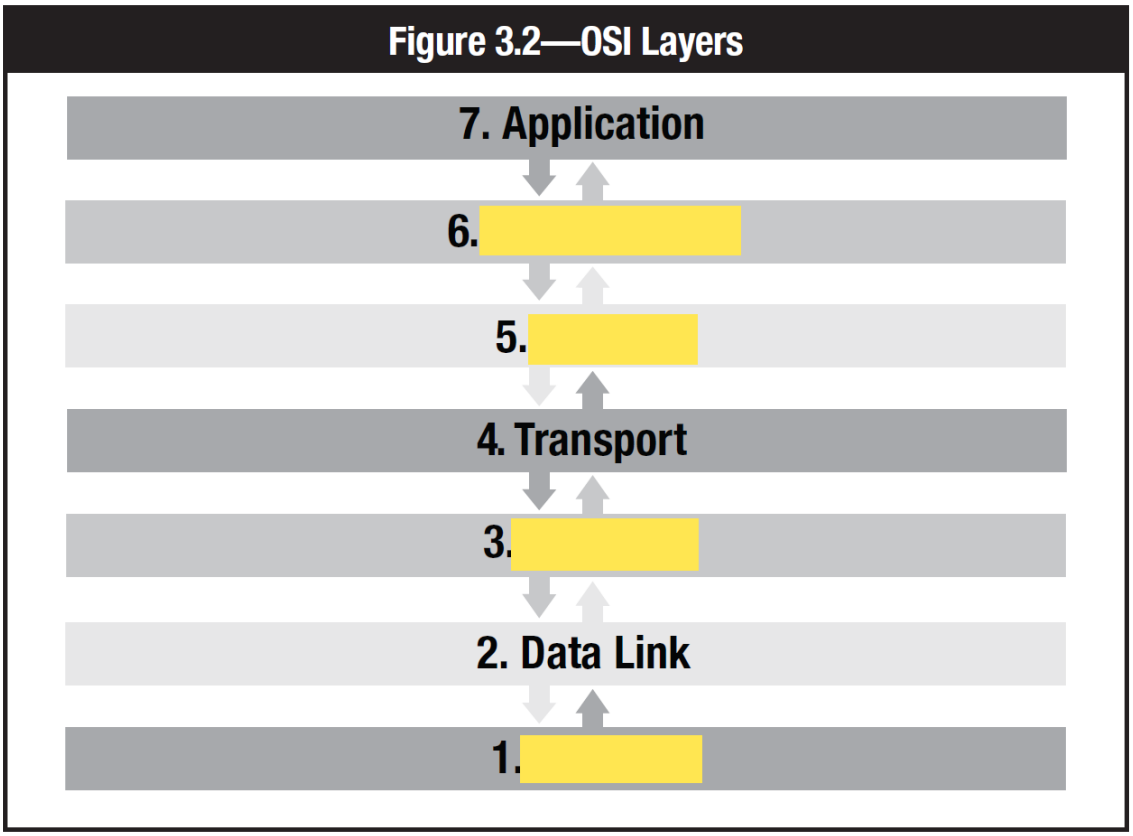
✓ 4. Encapsulation is the process of _____ to data as they are transmitted down the OSI stack:

- ( ) a) Security information
- ( ) b) Database code
- (●) c) Addressing information ✓
- ( ) d) None of the above

✓ 5. Organise the OSI model in the diagram below (place the letter in the box):

- (●) a) 1. Physical, 3. Network, 5. Session, 6. Presentation ✓
- ( ) b) 1.Presentation, a) 3. Physical, 5. Network, 6. Session
- ( ) c) 1. Network, 3. Session, 5. Presentation, 6. Physical
- ( ) d) 1. Session, 4. Physical, 5. Presentation, 6. Network

OSI Model (Question 5)



✓ 7. A _____ is defined as a system or combination of systems that enforces a boundary between two or more networks.

- a) Software filter
- b) Firewall ✓
- c) Network adaptor
- d) None of the above

✓ 8. This type of firewall brings in the functionality of an intrusion prevention system (IPS) and will often inspect Secure Socket Layer (SSL) or Secure Shell (SSH) connections

- a) First generation
- b) Second generation
- c) Third generation
- d) Next generation ✓

✓ 9. In this type of attack, the attacker fakes the IP address of either an internal network host or trusted network host:

- a) Miniature fragment attack
- b) IP spoofing ✓
- c) Source routing specification
- d) Fake attack

✕ 10. This type of filter does not keep the state of ongoing TCP connection sessions:

- a) State filtering
- b) Stateful filtering ✕
- c) TCP filtering
- d) Stateless filtering

Correct answer

- d) Stateless filtering

✕ 11. This type of firewall implementation has two or more networks interfaces, each of which is connected to a different network

- a) Dual-homed firewall
- b) Demilitarized zone or screened-subnet firewall ✕
- c) Screen-host firewall
- d) Multi-firewall

Correct answer

- a) Dual-homed firewall

✓ 12. A common technique for implementing network security is to segment an organization's network so that each segment can be separately controlled, monitored and protected. A network administrator therefore will:

- a) Design a security hot site
- b) Implement various operating system
- c) Purchase more servers
- d) Implement virtual local networks (VLANs) ✓

✓ 13. _____ reviews can identify risk-relevant events such as compliance violations, suspicious behaviour, errors, probes or scans and abnormal activity.

- a) Log ✓
- b) Personnel
- c) Server
- d) Firewall

✓ 14. This attack vector refers to network communications coming in:

- a) Ingress ✓
- b) Direct
- c) Egress
- d) Perpetrator

✕ 15. _____ works in conjunction with routers and firewalls by monitoring network usage anomalies. It protects a company's IS resources from external as well as internal misuse.

- a) Intrusion detection systems (IDS)
- b) Packet sniffers ✕
- c) Wireshark
- d) Intrusion prevention systems (IPS)

Correct answer

- a) Intrusion detection systems (IDS)

✗ 16. Select all that apply. The Internet perimeter should:

- [x] A. detect and block traffic from infected internal end points. ✓
- [x] B. eliminate threats such as email spam, viruses and worms. ✓
- [x] C. format, encrypt and compress data. ✗
- [x] D. control user traffic bound toward the Internet. ✓
- [x] E. monitor internal and external network ports for rogue activity. ✓

Correct answer

- [x] A. detect and block traffic from infected internal end points.
- [x] B. eliminate threats such as email spam, viruses and worms.
- [x] D. control user traffic bound toward the Internet.
- [x] E. monitor internal and external network ports for rogue activity.

✓ 17. The _____ layer of the OSI model ensures that data are transferred reliably in the correct sequence, and the _____ layer coordinates and manages user connections.

- ○ A. Presentation, data link
- ◉ B. Transport, session ✓
- ○ C. Physical, application
- ○ D. Data link, network

✕ 18. Choose three. The key benefits of the DMZ system are:

- [x] A. DMZs are based on logical rather than physical connections. ✕
- [ ] B. an intruder must penetrate three separate devices.
- [x] C. private network addresses are not disclosed to the Internet. ✓
- [x] D. excellent performance and scalability as Internet usage grows. ✕
- [ ] E. internal systems do not have direct access to the Internet.

Correct answer

- [x] B. an intruder must penetrate three separate devices.
- [x] C. private network addresses are not disclosed to the Internet.
- [x] E. internal systems do not have direct access to the Internet.

✕ 19. Which of the following best states the role of encryption within an overall cybersecurity program?

- (●) A. Encryption is the primary means of securing digital assets. ✕
- ( ) B. Encryption depends upon shared secrets and is therefore an unreliable means of control.
- ( ) C. A program's encryption elements should be handled by a third-party cryptologist.
- ( ) D. Encryption is an essential but incomplete form of access control.

Correct answer

- (●) D. Encryption is an essential but incomplete form of access control.

✕ 20. The number and types of layers needed for defense in depth are a function of:

- A. asset value, criticality, reliability of each control and degree of exposure.
- B. threat agents, governance, compliance and mobile device policy.
- C. network configuration, navigation controls, user interface and VPN traffic.
- D. isolation, segmentation, internal controls and external controls. ✕

Correct answer

- A. asset value, criticality, reliability of each control and degree of exposure.

✕ 21. Which activity is NOT part of the systems development lifecycle (SDLC)?

- Service delivery
- Feasibility study
- Requirements study
- Requirements definition
- Post-implementation review ✕

Correct answer

- Service delivery

✕ 22. The design and coding specifications describing how the system will interact, conditions under which the system will operate and the information criteria that the system should meet are called:

- Technical requirements
- Functional requirements ✕
- Business requirements
- Control requirements

Correct answer

- Technical requirements

✕ 23. The testing phase of the systems development lifecycle (SDLC) includes all of the following except:

- Verification and validation that functions perform as designed
- Confirmation that test units operate without adverse effect on other system components ✕
- Development methodologies and organizational requirements for testing
- Deliverables for the next phase in the implementation process

Correct answer

- Deliverables for the next phase in the implementation process

✕ 24. The system development lifecycle (SDLC) process guides all phases of software development including which of the following? Select all that apply.

- [x] Acquisition ✓
- [ ] Retirement
- [x] Governance ✕
- [x] Cost ✕

Correct answer

- [x] Acquisition
- [x] Retirement

✕ 25. The process by which changes to processes, systems, software, applications, platforms and configuration are introduced in an orderly, controlled manner is called:

- ( ) Change management
- (•) System development lifecycle (SDLC) ✕
- ( ) Risk management
- ( ) Compliance

Correct answer

- (•) Change management

✓ 26. The practice of layering defenses to provide added protection is called:

- (●) Defense in depth ✓
- ( ) Risk mitigation
- ( ) Edge protection
- ( ) Network foundation protection

✓ 27. The type of defense in which a series of nested layers must be bypassed in order to execute an attack is called:

- (●) Concentric rings ✓
- ( ) Overlapping redundancy
- ( ) Segregation
- ( ) Compartmentalization

✓ 28. Two or more controls that work in parallel to protect an asset is called:

- (●) Overlapping redundancy ✓
- ( ) Concentric rings
- ( ) Segregation
- ( ) Compartmentalization

✗ 29. The type of defense in which two or more processes, controls or individuals are required for access is called:

- ○ Overlapping redundancy
- ○ Concentric rings
- ○ Segregation/Compartmentalization
- ◉ Horizontal defense ✗

Correct answer

- ◉ Segregation/Compartmentalization

✓ 30. Ingress and egress are types of:

- ○ Horizontal defense
- ◉ Attack vector ✓
- ○ Vertical defense
- ○ Data

✓ 31. A virtual boundary which protects an organization from threats that come from the outside world is called a(n):

- ◉ Security perimeter ✓
- ○ Defense in depth
- ○ Virtual private network
- ○ Content filter

✓ 32. A system or combination of systems that enforces a boundary between two or more networks is called a(n):

- (●) Firewall ✓
- ( ) Application-level gateway
- ( ) Circuit-level gateway
- ( ) Demilitarized zone

✓ 33. A small, isolated network for an organization's public servers, bastion host information servers and modem pools is called a(n):

- (●) Demilitarized zone (DMZ) ✓
- ( ) Virtual local area network (VLAN)
- ( ) Dual-homed firewall
- ( ) Screened-host firewall

✓ 34. The process of eliminating as many security risks as possible by removing all nonessential components is called:

- (●) System hardening ✓
- ( ) Stateless filtering
- ( ) Stateful inspection
- ( ) Isolation

✕ 35. Network segmentation does which one of the following?

- ○ Allows an organization's network to be controlled, monitored and protected in separate zones
- ◉ Blocks some or all of the traffic trying to pass between the networks ✕
- ○ Protects the entire network by limiting break-ins to firewalls
- ○ Maps the source of an IP address of an incoming packet with the list of destination IP addresses

Correct answer

- ◉ Allows an organization's network to be controlled, monitored and protected in separate zones

✕ 36. Advantages of application firewalls include which of the following? Select all that apply.

- ☑ Provide security for commonly used protocols ✓
- ☐ Hide the network from untrusted networks
- ☑ Easy scalability as internet usage grows ✕
- ☑ Protect the network by limiting firewall break-ins ✓

Correct answer

- ☑ Provide security for commonly used protocols
- ☑ Hide the network from untrusted networks
- ☑ Protect the network by limiting firewall break-ins

✓ 37. A stateful inspection firewall is also known as:

- (●) Dynamic packet filtering ✓
- ( ) Screened-host firewall
- ( ) Dual-homed firewall
- ( ) Demilitarized zone (DMZ)

✓ 38. A key limitation of anti-malware is that it:

- (●) Is generally not effective in identifying malicious code that has yet to be identified ✓
- ( ) Is complex to administer
- ( ) Is not scalable as internet usage grows
- ( ) Is generally not effective for known threats

✓ 39. The art of designing, analyzing and attacking cryptographic schemes is called:

- ( ) Encryption
- (●) Cryptography ✓
- ( ) Symmetric Key Encryption
- ( ) Quantum Cryptography

✕ 40. Symmetric and asymmetric are types of:

- ○ Cryptographic systems
- ○ Nonrepudiation
- ○ Public key infrastructure
- ◉ Encryption standards ✕

Correct answer

- ◉ Cryptographic systems

✓ 41. All of the following are encryption techniques except:

- ○ Elliptical curve cryptography
- ○ Quantum cryptography
- ○ Advanced encryption standard
- ◉ Key length ✓

✗ 42. Which of the following are considered applied cryptographic techniques? Select all that apply.

- [ ] Digital signature
- [ ] Virtual private network (VPN)
- [x] Digital certificate ✓
- [x] Registration authority ✓

Correct answer

- [x] Digital signature
- [x] Virtual private network (VPN)
- [x] Digital certificate
- [x] Registration authority

✓ 43. An authority in a network that verifies user requests for a digital certificate and tells the certificate authority (CA) to issue it is called:

- (•) Registration authority ✓
- ( ) Certificate authority
- ( ) Digital certificate
- ( ) Digital signature

✓ 44. Keys and hashes are used to:

- (●) Transform a string of characters into a shorter or fixed-length value ✓
- ( ) Decrypt parts of a ciphertext message
- ( ) Compute the digital signature inside a certificate
- ( ) Initiating the key recovery process

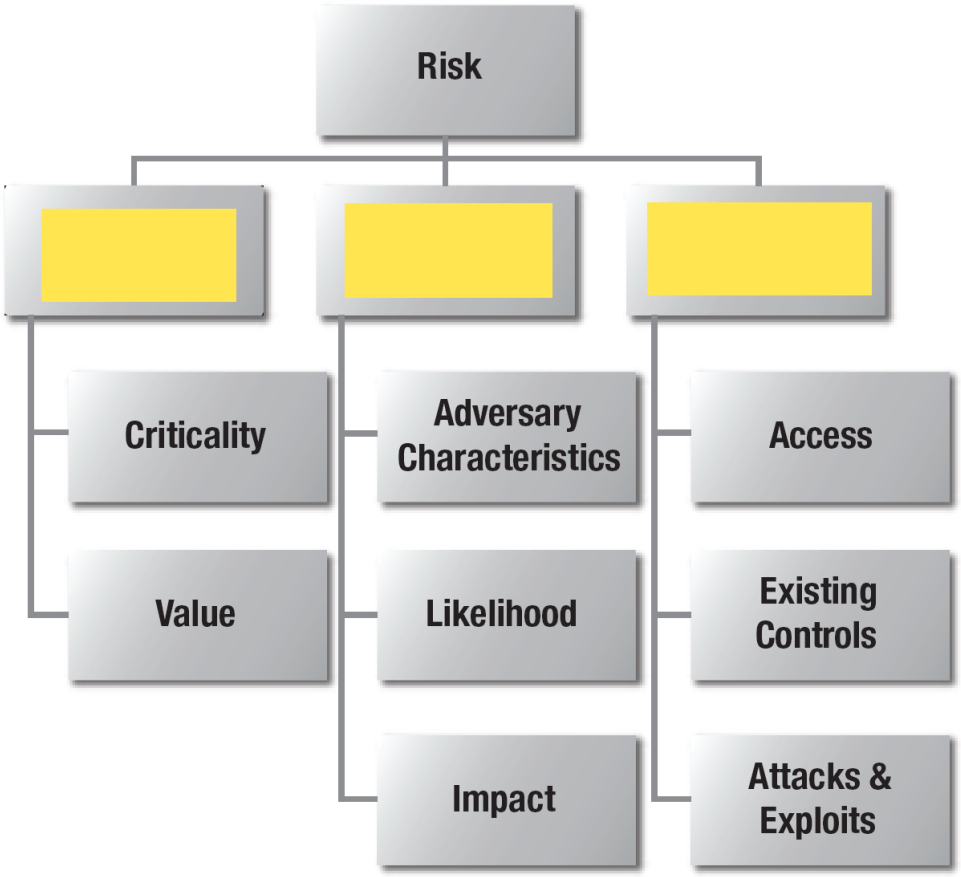
Section 4 - SECURITY OF NETWORKS, SYSTEMS, APPLICATIONS AND DATA

✓ 1. Place the correct term (left to right) in risk assessment methodology below:

- (●) a) Assets, Threats, Vulnerabilities ✓
- ( ) b) Logs, Threats, Vulnerabiities, Assets
- ( ) c) Threats, Logs, Vulnerabilites, Assests
- ( ) d) Vulnerabilities, Assests, Logs, Threats

Attribute of Risk (Question 1)

Figure 4.1—Attributes of Risk



Source: Encurve, LLC.

✗ 2. These two inputs are used to collect data on assets, threats and vulnerabilities together and analyze them together to determine risk, _____ and _____.

- a) Likelihoods, impacts
- b) Logs, access-lists ✗
- c) Likes, dislikes
- d) Employee experience, industry standards

Correct answer

- a) Likelihoods, impacts

✓ 3. Remediation means to:

- a) Provide security solutions
- b) Work with management
- c) To protect digital asset
- d) Mitigate or eliminate the vulnerability (such as patching) ✓

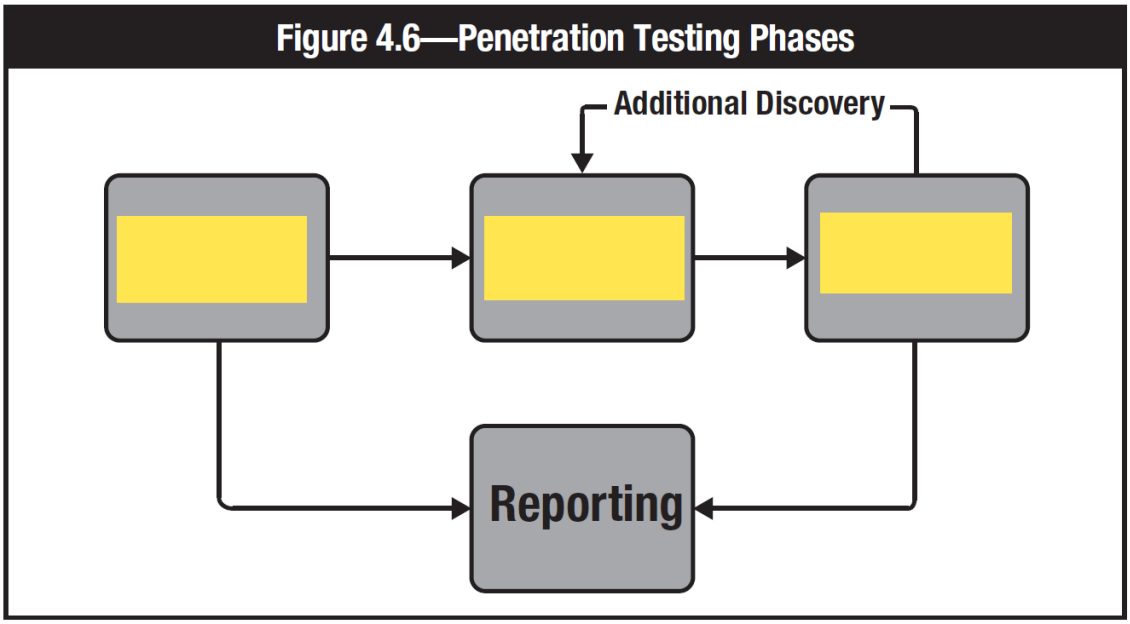
✕ 4. Penetration testing common phases. Place the correct letter in blank spaces in the diagram.

- a) Planning, Discover, Attacks
- b) Discovery, Planning, Logs ✕
- c) Attacks, Planning, Discovery
- d) Logs, Planning, Attacks

Correct answer

- a) Planning, Discover, Attacks

Penetration Test Phase (Question 4)



✓ 5. Repeaters, hubs, Layer 2 switches, routers, Layer 3 & 4 switches are on premises _____ components in an organization.

- (●) a) LAN ✓
- ( ) b) WAN
- ( ) c) MPLS
- ( ) d) NAC

✓ 6. The aim of a NAC device is to:

- ( ) a) Scan for unused ports
- ( ) b) Monitor network traffic
- ( ) c) Report security breaches
- (●) d) Control the access to a network using policies that describe how devices can secure access to network nodes when they first try to access the network. ✓

✓ 7. Allowable ports numbers range from:

- (●) a) 0 to 65535 ✓
- ( ) b) 0 to 1024
- ( ) c) 0 to 2058
- ( ) d) 0 to 85535

✓ 8. Ports reserved for certain privileged services:

- (●) a) 0 to 1023 ✓
- ( ) b) 200 to 400
- ( ) c) 0 to 10
- ( ) d) 500 to 1000

✓ 9. This is an example of a Virtual Private Network (VPN):

- ( ) a) Stealth network
- ( ) b) Layer 10 tunneling
- ( ) c) B2B
- (●) d) Point-to-point tunneling protocol (PPTP) ✓

✗ 10. System hardening is the process of implementing:

- ( ) a) A solid network
- ( ) b) Cable assurance and connectivity
- (●) c) Ensuring the servers are well protected with a hard case ✗
- ( ) d) Security controls on a computer system

Correct answer

- (●) d) Security controls on a computer system

✓ 11. Graphic below is an example of what type of filesystem system:

- (●) a) UNIX ✓
- ( ) b) DOS
- ( ) c) Windows
- ( ) d) None of the above

Graphic for Question 11

- /etc/passwd—Maintains user account and password information
- /etc/shadow—Retains the encrypted password of the corresponding account
- /etc/group—Contains group information for each account
- /etc/gshadow—Contains secure group account information
- /bin—Location of executable files
- /boot—Contains files for booting system
- /kernel—Kernel files
- /sbin—Contains executables, often for administration
- /usr—Include administrative commands

✓ 12. Below is an example of _____ commands:

- (●) a) UNIX ✓
- ( ) b) DOS
- ( ) c) Windows
- ( ) d) None of the above

Graphic for Question 12

Figure 4.10—[redacted] Commands	
Command	**Description**
finger {userid}	Display information about a user
cat	Display or concatenate file
cd	Change directory
chmod	Change file permissions Note: UNIX permissions are managed using octal notation by user, group, and others. Manipulating permissions is above the purpose of this material but is critical as you further your cybersecurity career.
cp	Copy
date	Display current date and time
diff	Display differences between text files
grep	Find string in file

✓ 13. This technology allows multiple OSs (guests), to coexist on the same physical server (host), in isolation of one another:

- a) Cohabit servers technology
- b) Virtualization technology ✓
- c) Server integration technology
- d) None of the above

✓ 14. Below is an example of what type of registry system:

- a) UNIX
- b) DOS
- c) Windows ✓
- d) None of the above

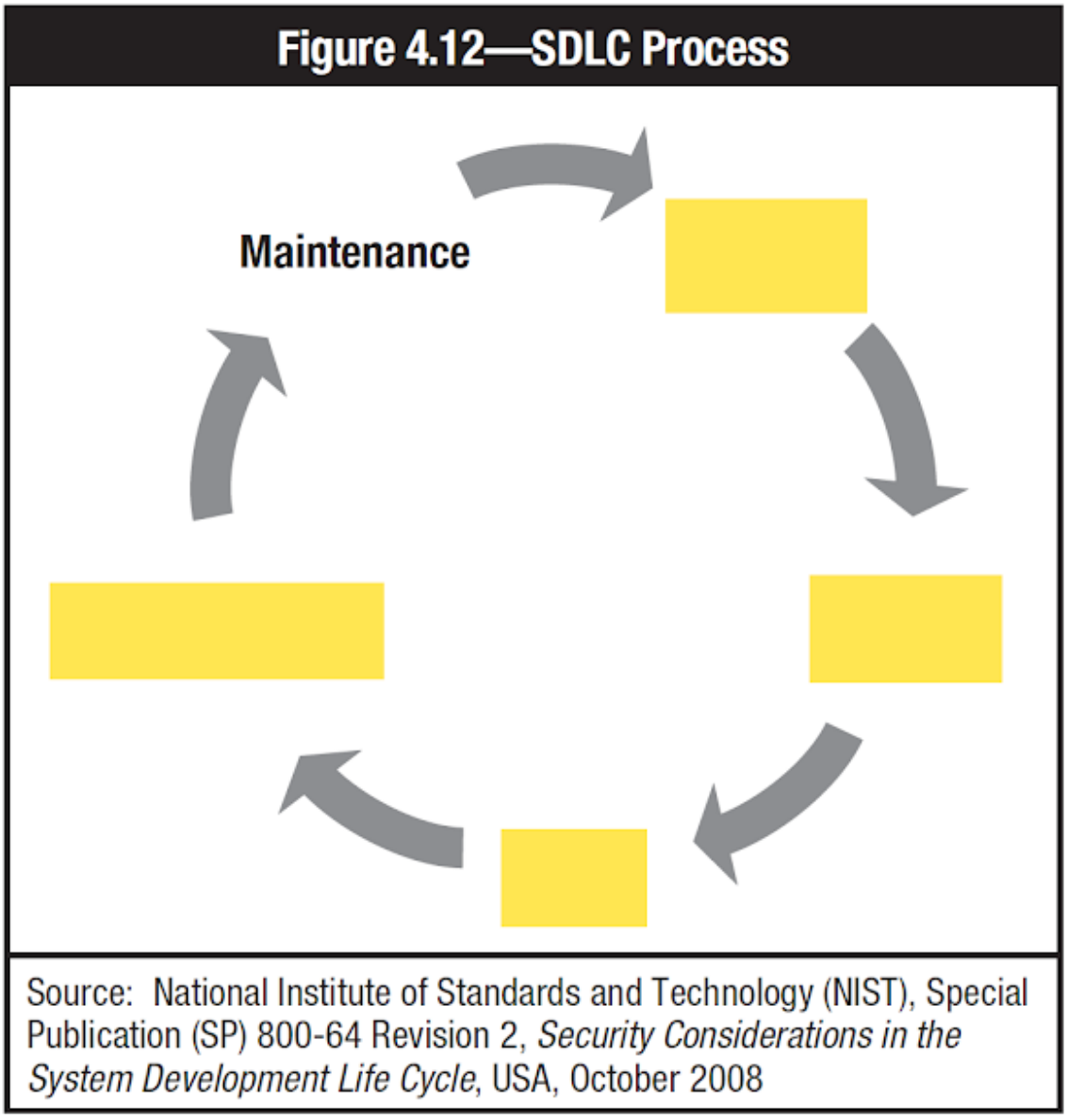
Graphic for Question 14

- HKEY_CURRENT_CONFIG—Contains volatile information generated at boot
- HKEY_CURRENT_USER—Settings specific to current user
- HKEY_LOCAL_MACHINE\SAM—Holds local and domain account information
- HKEY_LOCAL_MACHINE\Security—Contains security policy referenced and enforced by kernel
- HKEY_LOCAL_MACHINE\Software—Contains software and Windows settings
- HKEY_LOCAL_MACHINE\System—Contains information about Windows system setup
- HKEY_USERS\.DEFAULT—Profile for Local System account

✓ 15. The system development life cycle includes these process, place them in the correct order:

- a) Design -> Implementation ->Troubleshooting -> Planning
- b) Implementation -> Troubleshooting -> Analysis -> Design
- c) Troubleshooting -> Planning -> Analysis -> Design
- d) Planning -> Analysis -> Design -> Implementation ✓
- e) Design ->Analysis -> Planning -> Implementation

Graphic for Question 15



✓ 17. Why is it important for an organization to classify its data

- a) To keep it neat and tidy meeting LEED building certification and standards
- b) It will quicken inspection from the CRA by allowing appropriate classification for indexing
- c) Make the documentation managers happy
- (●) d) Allow the organization the capability to understand the sensitivity of information and classify data based on sensitivity and the impact of release or loss. ✓

✓ 18. When classifying data, the following should be considered:

- (●) a) Confidentiality, privacy, access and authentication data retention, auditability, integrity ✓
- b) Confidentiality, process, access and authentication data retention, auditability, integrity
- c) Classification, process, access and authentication data retention, auditability, integrity
- d) The amount of data

✓ 19. After data classification has been assigned, security controls can be established such as:

- a) Not needed
- b) Backup, replication
- c) Deduplication, offsite storage
- (●) d) Encryption, authentication and logging ✓

✓ 20. Another important consideration for data security is to define:

- a) The storage capacity
- b) The database replication
- c) The data owner ✓
- d) Cloud security

✗ 21. Put the steps of the penetration testing phase into the correct order.

- A. Attack, Planning, Reporting, Discovey ✗
- B. Discovery, Reporting, Attack, Planning
- C. Reporting, Attack, Discovery, Planning
- D. Planning, Discovery, Attack, Reporting

Correct answer

- D. Planning, Discovery, Attack, Reporting

✓ 22. System hardening should implement the principle of _____ or _____ .

- A. Governance, compliance
- B. Least privilege, access control ✓
- C. Stateful inspection, remote access
- D. Vulnerability assessment, risk mitigation

✗ 23. Select all that apply. Which of the following are considered functional areas of network management as defined by ISO?

- [ ] A. Accounting management
- [ ] B. Fault management
- [x] C. Firewall management ✗
- [x] D. Performance management ✓
- [ ] E. Security management

Correct answer

- [x] A. Accounting management
- [x] B. Fault management
- [x] D. Performance management
- [x] E. Security management

✓ 24. Virtualization involves:

- ○ A. the creation of a layer between physical and logical access controls.
- ◉ B. multiple guests coexisting on the same server in isolation of one another. ✓
- ○ C. simultaneous use of kernel mode and user mode.
- ○ D. DNS interrogation, WHOIS queries and network sniffing.

✓ 25. Vulnerability management begins with an understanding of cybersecurity assets and their locations, which can be accomplished by:

- ○ A. vulnerability scanning.
- ○ B. penetration testing.
- ◉ C. maintaining an asset inventory. ✓
- ○ D. using command line tools.

✓ 26. What is the main difference between a risk and a threat?

- ◉ Risk involves the probability of an event and its consequence, a threat is anything that can cause harm ✓
- ○ Risk involves determining weakness in design, a threat is anything that can cause harm
- ○ Risk is the combined action of a threat source with a threat event, a threat is the result of malicious activity
- ○ Risk is determined first, then potential threats are assessed

✓ 27. Risk assessment involves the analysis of:

- (●) Assets, threats and vulnerabilities ✓
- ( ) Risk tolerance, amount of data and scope of environment
- ( ) Assets, threats and response
- ( ) Risk response options, parameters and prioritization

✓ 28. People, information, infrastructure, finances and reputation are all considered:

- (●) Assets ✓
- ( ) Risks
- ( ) Vulnerabilities
- ( ) Threats

✓ 29. A weakness in the design, implementation, operation or internal control of a process that could expose the system to adverse threats is called a(n):

- ( ) Asset
- (●) Vulnerability ✓
- ( ) Threat
- ( ) Risk

✓ 30. All of the following are approaches to cybersecurity except:

- Compliance-based
- Ad hoc
- Risk-based
- Threat-based ✓

✓ 31. After assets, threats and vulnerabilities have been assessed, risk can be rated based on:

- Likelihood and impact ✓
- Threat events and threat source
- Threat source and likelihood
- Risk tolerance

✗ 32. The actual occurrence of a threat is called a(n):

- Attack
- Incident ✗
- Target
- Event

Correct answer

- Attack

✗ 33. Attack attributes include which of the following? Select all that apply.

- [x] Attack vector ✓
- [x] Payload ✓
- [x] Exploit ✓
- [x] Vulnerability ✓
- [ ] Asset

Correct answer

- [x] Attack vector
- [x] Payload
- [x] Exploit
- [x] Vulnerability
- [x] Asset

✓ 34. Scanning the network perimeter, using open source discovery of organizational information and running malware to identify potential targets are activities that may be performed during which phase of the attack process?

- ( ) Creating attack tools
- (•) Performing reconnaissance ✓
- ( ) Exploiting and compromising
- ( ) Conducting an attack

✓ 35. Problems caused by aging equipment, natural disasters and mishandling of information by authorized users are all examples of:

- (●) Nonadversarial threats ✓
- ( ) Attack types
- ( ) Risk attributes
- ( ) Adversarial threats

✗ 36. The path or route used to gain access to a target (asset) is called a(n):

- ( ) Attack vector
- (●) Exploit ✗
- ( ) Attack mechanism
- ( ) Payload

Correct answer

- (●) Attack vector

✗ 37. Any method that is used to deliver an exploit is called a(n):

- ○ Attack mechanism
- ○ Attack vector
- ◉ Payload ✗
- ○ Vulnerability

Correct answer

- ◉ Attack mechanism

✓ 38. All of the following are considered hostile threat agents except:

- ○ Script kiddies
- ○ Online social hackers
- ○ Hacktivists
- ◉ Ethical hackers ✓

✓ 39. Software designed to gain access to targeted computer systems, steal information or disrupt computer operations is called:

- ◉ Malware ✓
- ○ Botnet
- ○ Social engineering
- ○ Zero-day exploit

✓ 40. A piece of code that can replicate itself and spread from one computer to another is called a(n):

- (●) Virus ✓
- ( ) Trojan horse
- ( ) Exploit
- ( ) Rootkit

✓ 41. Spyware is a type of malware which:

- (●) Gathers information about a person or organization without the person's or the organization's knowledge ✓
- ( ) Locks or encrypts data or functions and demands a payment to unlock them
- ( ) Secretly records user keystrokes and, in some cases, screen content
- ( ) Hides the existence of other malware by modifying the underlying operating system

✓ 42. An attack made by trying all possible combinations of passwords or encryption keys until the correct one is found is called a(n):

- (●) Brute force attack ✓
- ( ) Botnet
- ( ) SQL injection
- ( ) Zero-day exploit

✗ 43. This variant of computer virus is a piece of self-replicating code designed to spread itself across computer networks:

- ○ Network worm
- ◉ Trojan horse ✗
- ○ Malware
- ○ Backdoor

Correct answer

- ◉ Network worm

Section 5 - INCIDENT RESPONSE

✓ 1. An _____ is any change, error or interruption within an IT infrastructure, such as a crash, disk error or a user forgetting their password.

- ○ a) Incident
- ◉ b) Event ✓
- ○ c) None of the above

✓ 2. A _____ violation or imminent threat of violation of computer polices, acceptable use policies or standard practices.

- (●) a) Incident ✓
- ( ) b) Event
- ( ) c) None of the above

✓ 3. A cybersecurity incident is an adverse event that negatively impacts the:

- ( ) a) Accessibility, availability, agility
- ( ) b) Moral, profit, business department
- (●) c) Confidentiality, integrity, availability ✓
- ( ) d) None of the above

✓ 4. Why do we need incident response?

- (●) a) Adequate incident response planning and implementation allows organization to respond to an incident in a systematic manner that is more effective ✓
- ( ) b) Guarantees security for the organization
- ( ) c) Doesn't do anything
- ( ) d) Responds to management concerns

✓ 5. Elements of an Incident Response Plan (IRP) include:

- a) Preparation, indemnity, containment, eradication, recovery, lessons learned
- b) Preparation, identification, containment, eradication, restoration, lessons learned
- c) Preparation, identification, consent, eradication, recovery, lessons learned
- (●) d) Preparation, identification, containment, eradication, recovery, lessons learned ✓

✓ 6. RTO, BCP, SDO are part of what element of the Incident Response Plan (IRP):

- a) Identification
- b) Containment
- (●) c) Recovery ✓
- d) Lessons learned

✓ 7. This element of the Incident Response Plan (IRP) deals with the next step after the root cause of the incident has be determined:

- a) Identification
- (●) b) Eradication ✓
- c) Recovery
- d) Lessons learned

✓ 8. This element in the Incident Response Plan (IRP) aims to verify if an incident has happened and to find out more details about an incident:

- (●) a) Identification ✓
- ( ) b) Containment
- ( ) c) Recovery
- ( ) d) Lessons learned

✓ 9. When trying to preserve evidence, why is rebooting a system a bad idea?

- ( ) a) Wrong, it is a good idea, it speeds things up
- (●) b) Rebooting the system or accessing files could result in evidence being lost ✓
- ( ) c) The boot up sequence can delay the investigation
- ( ) d) The administrator might not be around if something goes wrong

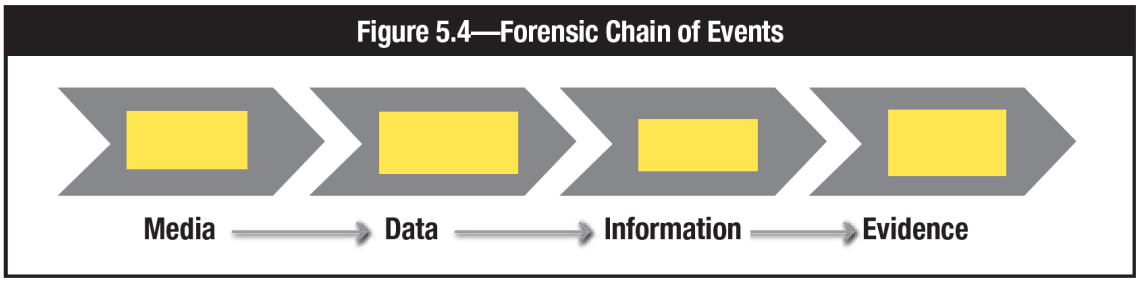
✓ 10. For evidence to be admissible in a court of law, the chain of custody needs this information?

- ( ) a) All the employees name and email addresses to contact
- ( ) b) The serial numbers of all servers involved
- ( ) c) The names of all IT security managers
- (●) d) Who had access to the evidence (chronological manner) ✓

✓ 11. Label the diagram (left to right) - select the right term for the four major considerations in the chain of events in regards to evidence in digital forensics:

- a) Preserve, Present, Identify, Analyze
- b) Present, Perserve, Analyze, Identify
- c) Analyze, Perserve, Present, Identify
- ◉ d) Identify, Perserve, Analyze, Present ✓

Graphic for Question 11



✓ 12. Imaging is a process in forensics, it involves:

- a) Imaging involves taking an image of the servers for evidence
- b) Imaging is imitating the processing server through a software image
- c) Imaging process makes a copy of the serial numbers of the entire server's hardware
- ◉ d) Is a process that allows one to obtain a bit-for-bit copy of data to avoid damage of original data or information when multiple analyses may be preformed. ✓

✗ 13. Digital forensic tools can be sorted into four categories:

- a) Computer, Memory, Mobile devices, Network
- b) Computer, Servers, Software, Hardware
- c) Memory, Hard drives, CDs, USB drives ✗
- d) Finger print powder, video evidence, witness statements

Correct answer

- a) Computer, Memory, Mobile devices, Network

✓ 14. The purpose of anti-forensic tools to:

- a) Harden evidence in a forensic operation
- b) To make it easier to find evidence information
- c) To provide a better lab environment to investigate evidence
- d) Make it difficult or impossible for investigators retrieve information ✓

✓ 15. The purpose of a Business Continuity Plan (BCP)and Disaster Recovery Plan (DRP) is to:

- a) Improve profits in times of business crisis
- b) Continue to operate in times of problems in the organization
- c) Continue to offer critical services in the event of disruption and to survive a disastrous interruption to activities ✓
- d) Continue to offer revenue to shareholders in the event of disruption and to survive a disastrous interruption to activities

✗ 16. Arrange the steps of the incident response process into the correct order.

- A. Mitigation and recovery, Investigation, Postincident analysis, Preparation, Detection and analysis
- B. Investigation, Detection and analysis, Postincident analysis, Preparation, Mitigation and recovery ✗
- C. Postincident analysis, Postincident analysis, Detection and analysis, Mitigation and recovery
- D. Preparation, Detection and analysis, Investigation, Mitigation and recovery, Postincident analysis
- E. Detection and analysis, Postincident analysis, Preparation, Mitigation and recovery, Preparation

Correct answer

- D. Preparation, Detection and analysis, Investigation, Mitigation and recovery, Postincident analysis

✓ 17. Which element of an incident response plan involves obtaining and preserving evidence?

- A. Preparation
- B. Identification
- C. Containment ✓
- D. Eradication

✗ 18. Select three. The chain of custody contains information regarding:

- [x] A. disaster recovery objectives, resources and personnel. ✗
- [x] B. who had access to the evidence, in chronological order. ✓
- [ ] C. labor, union and privacy regulations.
- [x] D. proof that the analysis is based on copies identical to the original evidence. ✓
- [ ] E. the procedures followed in working with the evidence.

Correct answer

- [x] B. who had access to the evidence, in chronological order.
- [x] D. proof that the analysis is based on copies identical to the original evidence.
- [x] E. the procedures followed in working with the evidence.

✓ 19. NIST defines a(n) _____ as a “violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices.”

- ( ) A. Disaster
- ( ) B. Event
- ( ) C. Threat
- (•) D. Incident ✓

✗ 20. Select all that apply. A business impact analysis (BIA) should identify:

- [ ] A. the circumstances under which a disaster should be declared.
- [ ] B. the estimated probability of the identified threats actually occurring.
- [x] C. the efficiency and effectiveness of existing risk mitigation controls. ✓
- [x] D. a list of potential vulnerabilities, dangers and/or threats. ✓
- [ ] E. which types of data backups (full, incremental and differential) will be used.

Correct answer

- [x] C. the efficiency and effectiveness of existing risk mitigation controls.
- [x] D. a list of potential vulnerabilities, dangers and/or threats.
- [x] E. which types of data backups (full, incremental and differential) will be used.

✓ 21. A major incident which has grown out of control and increased in severity is called a(n):

- (●) Crisis ✓
- ( ) Event
- ( ) Incident
- ( ) Emergency

✓ 22. What is a key difference between an incident and an event?

- (●) An incident implies a violation or imminent threat, an event does not ✓
- ( ) An event implies a violation or imminent threat, an incident does not
- ( ) Events negatively impacts the confidentiality, integrity and availability, incidents do not
- ( ) Incident and event means the same thing

✓ 23. Which of the following is an example of a security incident?

- ( ) System crash
- ( ) Disk error
- ( ) User forgetting their password
- (●) Denial of service ✓

✓ 24. An individual gains logical or physical access without permission to a network, system, application, data or other resource. This describes which incident category?

- (●) Category 1: Unauthorized access ✓
- ( ) Category 2: Denial of service
- ( ) Category 4: Improper usage
- ( ) Category 5: Scans/probes/improper access

✓ 25. Fallback plans may be invoked in the event of a(n):

- ○ Emergency
- ◉ Disaster ✓
- ○ Crisis
- ○ Incident

✓ 26. Technical information security incidents may involve:

- ◉ Viruses, malware or denial-of-service (DoS) ✓
- ○ System failure, social engineering or viruses
- ○ Viruses, denial-of-service or system failure
- ○ Malware, system failure or social engineering

✓ 27. The strategy used by an enterprise to respond to disruption of critical business processes is called a:

- ◉ Business continuity plan (BCP) ✓
- ○ Service delivery objective (SDO)
- ○ Computer emergency response team (CERT)
- ○ Disaster response plan (DRP)

✓ 28. Incident response includes which of the following activities?

- (●) Preparation, detection, recovery and post incident activity ✓
- ( ) Preparation, alignment and response
- ( ) Preparation, detection, and post incident activity
- ( ) Preparation, analysis, alignment and post incident activity

✓ 29. Obtaining and preserving evidence, documenting action and managing public communications are actions associated with:

- (●) Incident containment ✓
- ( ) Incident response
- ( ) Incident eradication
- ( ) Incident preparation

✗ 30. Log data overload can be mitigated by employing:

- ( ) Security event management (SEM)
- ( ) Security response plans
- ( ) Computer security incident response teams (CSIRT)
- (●) Business continuity plans (BCP) ✗

Correct answer

- (●) Security event management (SEM)

✕ 31. Incident preparation includes all of the following except:

- (●) Establish approach to handling incidents ✕
- ( ) Establish communication plan with stakeholders
- ( ) Develop incident reporting criteria
- ( ) Establish chain of custody

Correct answer

- (●) Establish chain of custody

✕ 32. Post-incident activities typically include which of the following? Select all that apply.

- [x] Writing an incident report ✕
- [x] Proposing improvements ✓
- [x] Communicating findings to key stakeholders ✓
- [ ] Declaring normal operation

Correct answer

- [x] Proposing improvements
- [x] Communicating findings to key stakeholders
- [x] Declaring normal operation

✗ 33. Assigning ownership and establishing chain of custody are part of which incident response plan activity?

- (●) Preparation ✗
- ( ) Identification
- ( ) Containment
- ( ) Eradication

Correct answer

- (●) Identification

✓ 34. A business impact analysis (BIA) provides the basis for which of the following? Select all that apply.

- [x] Recovery time objectives ✓
- [x] Recovery point objectives ✓
- [x] Maximum tolerable outages ✓
- [x] Service delivery objectives ✓

✗ 35. The most important objective of a business continuity plan (BCP) is:

- ○ Ensuring safety and security of human life
- ◉ Maintaining operations critical to survival of the organization ✗
- ○ Defining evacuation procedures
- ○ Outlining a step-by-step explanation of the recovery plan

Correct answer

- ◉ Ensuring safety and security of human life

✓ 36. The process of restoring data that has been lost, accidentally deleted, corrupted or made inaccessible for any reason is called:

- ◉ Data recovery ✓
- ○ Backup
- ○ Business continuity
- ○ Incident recovery

✕ 37. In order for a business continuity plan (BCP) to be effective, it must:

- ○ Be documented on paper
- ○ Be aligned with the strategy of the organization
- ◉ Be tested regularly ✕
- ○ Be approved by senior management

Correct answer

- ◉ Be aligned with the strategy of the organization

✕ 38. The business impact analysis (BIA) should consider which of the following critical resources? Select all that apply.

- ☐ Potential vulnerabilities
- ☑ Probability of occurrence of threats ✓
- ☑ Human, data and infrastructure resources ✓
- ☐ Efficiency and effectiveness of risk countermeasures

Correct answer

- ☑ Potential vulnerabilities
- ☑ Probability of occurrence of threats
- ☑ Human, data and infrastructure resources
- ☑ Efficiency and effectiveness of risk countermeasures

✕ 39. In a disaster recovery plan (DRP), the last known point of good data is identified as:

- ○ Recovery point objective
- ○ Recovery time objective
- ○ Full backup
- ◉ Data recovery ✕

Correct answer

- ◉ Recovery point objective

✕ 40. The amount of time allowed for the recovery of a business function or resource after a disaster occurs is called:

- ○ Recovery point objective
- ○ Recovery time objective
- ○ Service delivery objective
- ◉ Maximum tolerable outages ✕

Correct answer

- ◉ Recovery time objective

Section 6 - Security Implications and Adoption of Evolving Technologies

✓ 1. _____is defined as “a model for enabling convenient, on-demand network access to a shared pool of configurable resources (e.g., networks, servers, storage, applications and services) that can be rapidly provisioned and released with minimal management or service provider interaction.”

- A. Software as a Service (SaaS)
- B. Cloud computing ✓
- C. Big data
- D. Platform as a Service (PaaS)

✕ 2. Select all that apply. Which of the following statements about advanced persistent threats (APTs) are true?

- [x] A. APTs typically originate from sources such as organized crime groups, activists or governments. ✓
- [x] B. APTs use obfuscation techniques that help them remain undiscovered for months or even years. ✓
- [x] C. APTs are often long-term, multi-phase projects with a focus on reconnaissance. ✓
- [x] D. The APT attack cycle begins with target penetration and collection of sensitive information. ✕
- [ ] E. Although they are often associated with APTs, intelligence agencies are rarely the perpetrators of APT attacks.

Correct answer

- [x] A. APTs typically originate from sources such as organized crime groups, activists or governments.
- [x] B. APTs use obfuscation techniques that help them remain undiscovered for months or even years.
- [x] C. APTs are often long-term, multi-phase projects with a focus on reconnaissance.

✕ 3. Which of the following are benefits to BYOD? (more than one)

- [x] A. Acceptable Use Policy is easier to implement. ✕
- [x] B. Costs shift to the user. ✓
- [ ] C. Worker satisfaction increases.
- [ ] D. Security risk is known to the user.

Correct answer

- [x] B. Costs shift to the user.
- [x] C. Worker satisfaction increases.

✕ 4. Choose three. Which types of risk are typically associated with mobile devices?

- [ ] A. Organizational risk
- [x] B. Compliance risk ✕
- [x] C. Technical risk ✓
- [ ] D. Physical risk
- [x] E. Transactional risk ✕

Correct answer

- [x] A. Organizational risk
- [x] C. Technical risk
- [x] D. Physical risk

✓ 5. Which three elements of the current threat landscape have provided increased levels of access and connectivity, and, therefore, increased opportunities for cybercrime?

- A. Text messaging, Bluetooth technology and SIM cards
- B. Web applications, botnets and primary malware
- C. Financial gains, intellectual property and politics
- D. Cloud computing, social media and mobile computing ✓

✗ 6. A collection of threats is generally referred to as a(n):

- Threat environment
- Advanced persistent threat (APT)
- Cyberwarfare ✗
- Hacktivism

Correct answer

- Threat environment

✗ 7. An adversary which leverages sophisticated expertise, significant resources and multiple attack vectors is known as a(n):

- ○ Advanced persistent threat (APT)
- ○ Hacktivist
- ◉ Cyberwarrior ✗
- ○ Terrorist group

Correct answer

- ◉ Advanced persistent threat (APT)

✓ 8. Most advanced persistent threat (APT) attacks are aimed at:

- ◉ Stealing or manipulating data ✓
- ○ Causing physical harm to employees
- ○ Causing damage to facilities
- ○ Disrupting organizational operations

✓ 9. When an attacker seeks to gain an initial entry to the enterprise infrastructure through a simple social engineering attack, it is called:

- (●) Spear phishing ✓
- ( ) Code injection
- ( ) Target discovery
- ( ) Data exfiltration

✓ 10. The key attributes of an advanced persistent threat (APT) include which of the following? Select all that apply.

- [x] Well-researched ✓
- [x] Stealthy ✓
- [x] Sophisticated ✓
- [x] Persistent ✓

✓ 11. At this stage of an attack, the adversary explores networked platforms within reach, maps out the network and harvests user credentials:

- ( ) Command and control
- (●) Target discovery ✓
- ( ) Target penetration
- ( ) Target research

✓ 12. Major physical risks of mobile devices include which of the following? Select all that apply.

- [x] Data breaches ✓
- [x] Identity theft ✓
- [x] Work disruptions ✓
- [ ] Data retrieval

✓ 13. The lack of formal training for employees on the use of mobile devices is considered a(n):

- (•) Organizational risk ✓
- ( ) Physical risk
- ( ) Technical risk
- ( ) Informational risk

✓ 14. Physical risk involving mobile devices can be mitigated through the use of which of the following? Select all that apply.

- [x] Cell-based tracking and locating the device ✓
- [x] Remote shutdown/wipe capabilities ✓
- [x] Remote SIM card lock capabilities ✓
- [ ] Employee training programs

✗ 15. Messaging, audio and Bluetooth are all examples of:

- (●) Physical risk ✗
- ( ) Technical risk
- ( ) Informational risk
- ( ) Organizational risk

Correct answer

- (●) Technical risk

✓ 16. Proxy level and presentation level are common attacks to:

- (●) Web view applications ✓
- ( ) Outdated hardware
- ( ) Static data
- ( ) History files

✓ 17. A fake web site presented through a mobile view is known as a(n):

- (●) Presentation level attack ✓
- ( ) Proxy level attack
- ( ) Code injection
- ( ) Script kiddie

✓ 18. Major benefits of cloud computing include which of the following? Select all that apply.

- [x] Scalability ✓
- [x] Cost-effectiveness ✓
- [ ] Data protection
- [x] Timeliness of updates ✓

✓ 19. Major risks of cloud computing include which of the following? Select all that apply.

- [ ] Lack of scalability
- [x] Difficult to protect data ✓
- [x] Provider non-compliance with requirements ✓
- [x] Loss of governance ✓

✕ 20. When vetting or auditing a cloud provider, organizations should assess the provider's:

- ○ Facilities, networks, hardware and operating systems
- ○ Facilities, networks, hardware and financial documents
- ○ Human resources, financial documents, hardware and operating systems
- ◉ Networks, operating systems, human resources and references ✕

Correct answer

- ◉ Facilities, networks, hardware and operating systems