|  |  |
| --- | --- |
| 1. When writing a corporate policy that explains the security objectives of confidentiality, integrity, and availability; what is the best definition for integrity?
	1. To protect information asset from modification or destruction of information assets
	2. To prevent unauthorized personnel and/or program from accessing information assets
	3. To protect information assets from unauthorized modification or destruction
	4. To authorize personnel and/or program to access information assets
 | Domain: Information Security & Risk ManagementBest answer: **A**“Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity.” (44 U.S.C. Section 3542) |
| 1. A good and effective information security policy should have the following characteristics, except?
	1. Delegation of roles and responsibilities
	2. Explanation of management objectives that are aligned with business goals
	3. Enumeration of short- and long-term goals
	4. Definition of terms
 | Domain: Information Security & Risk ManagementBest answer: **C**A information security policy should:* **Explain** laws, regulations, business needs, and management’s expectations (goals & objectives)
* **Identify** roles and delineate responsibilities
 |
| 1. “Users should only have access to information that enables them to perform their assigned job functions.” Is a practice of which security implementation principles?
	1. Need to know
	2. Least privilege
	3. Separation of duties
	4. Confidentiality
 | Domain: Information Security & Risk ManagementBest answer: **A**“**Need to know**” is where users should only have access to information that enables them to perform their assigned job functions.“**Least privilege**” is where users should only have sufficient access privilege that allow them to perform their assigned work.“**Separation of duties**” is where no single person should be responsible for carrying out a series of critical tasks from beginning to end; where the tasks requires more than one internal controls to prevent fraud and errors. |
| 1. What type of information security requirement is design to establish confidence that a control will perform as intended?
	1. Functional requirements
	2. Assurance requirements
	3. Performance requirements
	4. Operational requirements
 | Domain: Information Security & Risk ManagementBest answer: **B**Functional requirement describes the functionality or behavior which a system shall perform.Assurance requirement measures level of confidence that the security function will perform as intended. |
| 1. What type of security control is designed to preclude actions that violate policy or increase risks to information assets?
	1. Directive
	2. Preventive
	3. Detective
	4. Corrective
 | Domain: Information Security & Risk ManagementBest answer **B*** **Directive controls** are intended to advise employees of the behavior expected of them during their interfaces with or use the organization’s information systems.
* **Preventive controls** are the physical, administrative, and technical measures intended to preclude actions violating policy or increasing risk to system resources.
* **Detective controls** involve the use of practices, processes, and tools that identify and possibly react to security violations.
* **Corrective controls** involve physical, administrative, and technical measures designed to react to detection of an incident in order to reduce or eliminate the opportunity for the unwanted event to recur.
 |
| 1. As a security professional, how would you explain the definition of a risk?
	1. An entity that may act on a vulnerability
	2. Any potential danger to information (/ system) life cycle
	3. The likelihood of a threat source take advantage of a vulnerability
	4. An instance of being compromised by a threat source.
 | Domain: Information Security & Risk ManagementBest answer: **C**Risk is the likelihood of a threat source exploiting vulnerability.Vulnerability is a weakness or flaw that may provide an opportunity to a threat source to exploit.Threat is any potential danger to information (/ system) life cycle.Risk = Threat X Vulnerability |
| 1. What is the process that determines what security controls are needed to adequately protect the information system that supports the operations and assets of an organization?
	1. Risk management
	2. Threat assessment
	3. Vulnerability assessment
	4. Security audit
 | Domain: Information Security & Risk ManagementBest answer: **A**Threat and vulnerability assessments are a part of risk management process.Security audit determines whether the required controls have been implemented.  |
| 1. In information security management, what is the primary responsibility of an information (/ data) owner?
	1. Ensure accuracy of the data
	2. Authorizes user access and determine privilege
	3. Back up data regularly
	4. Determine the data sensitivity (/ classification) level
 | Domain: Information Security & Risk ManagementBest answer: **D**The owner of information (/ data) that understands the value and potential impact should determine the sensitivity of data. |
| 1. As the information security engineer estimating the annual budget for an information security program, what would be the appropriate amount you would recommend to protect an asset valued at $1 million from a threat that has annualized rate of occurrence (ARO) of once every 5 years and an exposure factor (EF) of 30%?
	1. $1,500
	2. $60,000
	3. $150,000
	4. $300,000
 | Domain: Information Security & Risk ManagementBest answer: **B**SLE = Asset value x EF ($1,000,000 x 30% = $300,000)ALE = ARO x SLE (1/5 x $300,000 = $60,000) |
| 1. In an enterprise, who is primarily responsible for determining the level of protection needed for information assets?
	1. Senior management
	2. Program manager
	3. Auditor
	4. Information systems security engineer
 | Domain: Information Security & Risk ManagementBest answer: **D**Security engineers or analysts determine the level of protection based on the risk assessment results. |
| 1. When using quantitative risk assessment method, which of the following statement is incorrect?
	1. Assessment & results are based substantially on independently objective processes & metrics. Thus, meaningful statistical analysis is supported.
	2. A credible basis for cost/benefit assessment of risk mitigation measures is provided. Thus, information security budget decision-making is supported.
	3. Risk assessment & results are essentially subjective in both process & metrics.
	4. Calculations are complex.
 | Domain: Information Security & Risk ManagementBest answer: **C**Quantitative risk assessment method is not subjective. It requires the value of information be expressed in monetary terms. Hence the calculations are complex and the assessment results are objective. |
| 1. What is the primary rationale for implementing security controls?
	1. To eliminate risk and the potential for loss.
	2. To eliminate risk and reduce the potential for loss.
	3. To mitigate risk and reduce the potential for loss.
	4. To mitigate risk and eliminate the potential for loss.
 | Domain: Information Security & Risk ManagementBest answer: **D**Risk can be accepted, mitigated, or transferred, but cannot be eliminated.Implement security controls can eliminate potential for loss.If a security control cannot fully eliminate the potential for loss, then the risk would have to be accepted. |
| 1. A disciplined approach to evaluate level of conformance to the prescribed security requirements and the implemented security controls is?
	1. Certification
	2. Accreditation
	3. Risk management
	4. Vulnerability assessment
 | Domain: Information Security & Risk ManagementBest answer: **A**Accreditation is the official management decision of operate the certified system. It is also a formal acceptance of the responsibility to the security of the certified system.Risk management is a process for managing risks to an acceptable level. |
| 1. Using the “reasonable and prudent person” concept; performing background investigation, interviewing references, conducting counterintelligence and lifestyle polygraphs are what type of personnel security activities?
	1. Due diligence
	2. Due care
	3. Due process
	4. Management controls
 | Domain: Information Security & Risk ManagementBest answer: **B****Due care** are the actions **taken** to minimize risks.**Due diligence** are the **continual** actions that an organization doing to protect and minimize risks. |
| 1. Why is configuration management a key component of information security management?
	1. Ensures the change does not affect the system accreditation.
	2. Ensures the change is documented.
	3. Ensures the change improves the security posture baseline.
	4. Ensures the change does not adversely affect the security posture baseline.
 | Domain: Information Security & Risk ManagementBest answer: **D**Configuration management ensures the system configuration baseline is recorded and changes are documented, so associated risks maybe assessed and actions can be taken. |
| 1. What is the document that illustrates an integrated view of enterprise system architecture from a perspective of meeting the organizational security policy, standards, and process?
	1. The enterprise security architecture
	2. The security architecture reference model
	3. The trusted facility manual
	4. The security model
 | Domain: Security Architecture & DesignBest answer: **A**Enterprise security architecture is an integrated view of the enterprise system architecture from a perspective of meeting the organizational security policy, standards, and processes. |
| 1. What is the importance of an architecture framework?
	1. It provides an investment alignment between the business and the IT organizations.
	2. It ensures interoperability between systems within an enterprise.
	3. It explains the concept of how a system shall meet the operational needs of an enterprise.
	4. It provides a common standard of terminology, description, and models to facilitate communications amongst the project stakeholders.
 | Domain: Security Architecture & DesignBest answer: **D**An architecture framework provides a common standard of terminology, description, and models to facilitate communications amongst the project stakeholders such as: * Program Managers and System Designers (Contextual).
* System Designers and System Engineers (Conceptual).
* System Engineers and System Developers (Logical).
* System Developers and System Integrators (Physical).
* System Integrators and System Operators (Component).
* System Users to System Engineers, Developers, Integrators, and Operators (Concept of Operations).
 |
| 1. What security model is expressed using access control matrices that explain operations between subjects and objects and it has no rule for state-transitions?
	1. Graham-Denning
	2. Bell-LaPadula
	3. Biba
	4. Clark-Wilson
 | Domain: Security Architecture & DesignBest answer: **A**Graham-Denning is usually expressed using access control matrices that explain how subjects can perform actions on objects. It has no rule for state-transitions.Bell-LaPadula, Biba, and Clark-Wilson are state-machine models. |
| 1. What security model is designed for controlled access to classified national security information and focuses on meeting the confidentiality objective only?
	1. Graham-Denning
	2. Bell-LaPadula
	3. Biba
	4. Clark-Wilson
 | Domain: Security Architecture & DesignBest answer: **B**Bell-LaPadula is a state-machine model has 3 access actions: read-only, write-only, and read & write. It focuses on meeting the confidentiality objective only. |
| 1. In the Bell-LaPadula security model, what does the \* (star) property mean?
	1. Subject cannot read object of higher sensitivity
	2. Subject cannot write to object of lower sensitivity
	3. Subject cannot read/write to object of higher/lower sensitivity
	4. Subject cannot write to object of higher integrity
 | Domain: Security Architecture & DesignBest answer: **B*** **Simple security property**: Subject cannot read object of higher sensitivity (No read up)
* **property**: Subject cannot write to object of lower sensitivity (No write down)
* **Strong \* property**: Subject cannot read/write to object of higher/lower sensitivity (No read up and write down)

 |
| 1. What security model is designed to address the integrity of information and systems that focuses on preventing unauthorized subjects from modifying objects?
	1. Graham-Denning
	2. Bell-LaPadula
	3. Biba
	4. Clark-Wilson
 | Domain: Security Architecture & DesignBest answer: **C**Biba security model focuses on preservation of data and system integrity. |
| 1. In the Biba security model, what does the integrity \* (star) property mean?
	1. Subject cannot read objects of lesser integrity
	2. Subject cannot write to objects of higher integrity
	3. Subject cannot send messages to object of higher integrity
	4. Subject cannot write to objects of lower sensitivity
 | Domain: Security Architecture & DesignBest answer: **B*** **Simple integrity condition**: Subject cannot read objects of lesser integrity (No read down)
* **Integrity \* (star) property**: Subject cannot write to objects of higher integrity (No write up)
* **Invocation property**: Subject cannot send messages (logical service request) to object of higher integrity (No invocation up)

 |
| 1. What security model requires the use of access triple of subject-program-object to ensure well-formed transactions for preserving data integrity, preventing arbitrary modification, and separation of duty?
	1. Graham-Denning
	2. Bell-LaPadula
	3. Biba
	4. Clark-Wilson
 | Domain: Security Architecture & DesignBest answer: **D**Clark-Wilson is a security model address the integrity goals of:* Preventing unauthorized subjects from modifying objects
* Preventing authorized subjects from making improper modification to objects
* Maintaining internal and external consistency

To ensure well-formed transaction, Clark-Wilson security model requires program to certify and enforce policy rules. |
| 1. What security model is often implemented in modern database management systems (DBMS)?
	1. Graham-Denning
	2. Bell-LaPadula
	3. Biba
	4. Clark-Wilson
 | Domain: Security Architecture & DesignBest answer: **D**Most modern DBMS such as Oracle, DB2, or MS SQL, implements Clark-Wilson security model to preserve data/system integrity and ensures separation of duty.**Ref:** *Secure Database Development and the Clark-Wilson Security Model*, X.Ge, F.Polack, R.Laleau, University of York, UK. |
| 1. What security model is designed to prevent conflict of interest?
	1. Brewer-Nash
	2. Bell-LaPadula
	3. Biba
	4. Clark-Wilson
 | Domain: Security Architecture & DesignBest answer: ABrewer-Nash security model is designed to implement dynamically changing access permissions to prevent conflict of interest. |
| 1. What security mode of operation where it assumes all users have the necessary clearance, need-to-know, and can access to the system?
	1. Dedicated security mode
	2. System high-security mode
	3. Multi-level security mode
	4. Compartmented security mode
 | Domain: Security Architecture & DesignBest answer: **A**In dedicated operating mode, all users have the required security clearance, the need-to-know for all, and can access to all. |
| 1. What security mode of operation where the system operates at the highest security classification level, all users have the necessary clearance, access to all system components, but not all users have the need-to-know for all information?
	1. Dedicated security mode
	2. System high-security mode
	3. Multi-level security mode
	4. Compartmented security mode
 | Domain: Security Architecture & DesignBest answer: **B**In system high mode, all users have the required security clearance, can access to all system components, but do not have the need-to-know for all information within the system. |
| 1. What security mode of operation allows system to operate and process information at multiple classification levels?
	1. Dedicated security mode
	2. System high-security mode
	3. Multi-level security mode
	4. Compartmented security mode
 | Domain: Security Architecture & DesignBest answer: **C**In multi-level security (MLS) mode of operation, the system that has implemented Bell-LaPadula security model can operate and process information at multiple classification levels. |
| 1. What is the security architecture concept that describes an abstract machine that mediates all subjects’ accesses to objects?
	1. Trusted computing base (TCB)
	2. Clark-Wilson security model
	3. Reference monitor
	4. Security kernel
 | Domain: Security Architecture & DesignBest answer: **C*** **Reference monitor** is a concept performed by a reference validation mechanism.
* **Trusted computing base (TCB)** is the totality of protection mechanisms that focuses on meeting the security objective of confidentiality and integrity.
* **Security kernel** is a software mechanism that is an implementation of reference monitor and is a part of TCB.
 |
| 1. What is the information security system design concept that consists of hardware, firmware, software, data processes, and transports for meeting the confidentiality and integrity security objectives?
	1. Trusted computing base (TCB)
	2. Reference monitoring mechanism
	3. Security kernel
	4. Rings of protection
 | Domain: Security Architecture & DesignBest answer: **A*** **Trusted computing base (TCB)** is the totality of protection mechanisms that focuses on meeting the security objective of confidentiality and integrity.
* **Reference monitoring mechanism** does not specify the security policy model, or mechanisms. And it does not specify the security objectives.
* **Security kernel** is a software mechanism that is an implementation of reference monitor and is a part of TCB.
 |
| 1. In an operating system, what type of process scheduling is where the operating system schedules computational processes by a series of threads that enables multiple users to request services?
	1. Multi-programming
	2. Multi-tasking
	3. Multi-threading
	4. Multi-processing
 | Domain: Security Architecture & DesignBest answer: **C*** **Multi-programming**: An operating system process scheduling can coordinate multiple sets of programmed instructions.
* **Multi-tasking**: An operating system process scheduling that allows a user to run multiple programs.
* **Multi-threading**: An operating system process scheduling that allows multiple users/ programs to request services and execute them in a series of threads.
* **Multi-processing**: An operating system process scheduling that allows multiple users/ programs to request services and allocate them to multiple CPUs for execution.
 |
| 1. In management of virtual memory in a modern computing system, the act of moving information between primary and secondary memory storages is called?
	1. Paging
	2. Swapping
	3. Relocating
	4. Data input and output
 | Domain: Security Architecture & DesignBest answer: **B*** **Paging** splits memory into equal-sized blocks called page frames.
* **Swapping** is the act of transferring pages between physical memory and the swap space on a disk.
 |
| 1. Which of the following security evaluation standard focuses on meeting the confidentiality objective?
	1. Trusted Computer System Evaluation Criteria (TCSEC)
	2. Information Technology Security Evaluation Criteria (ITSEC)
	3. Common Criteria Evaluation and Validation Scheme (CCEVS)
	4. Security Content Automation Protocol (SCAP)
 | Domain: Security Architecture & DesignBest answer: **A**Trusted Computer System Evaluation Criteria (TCSEC) (a.k.a. Orange Book/ DoD 5200.28-STD) focuses primarily on meeting the confidentiality objective, because the security policy is based on **Bell-LaPadula** security model. |
| 1. In Trusted Computer System Evaluation Criteria (TCSEC), what certification class requires meeting the security policy requirements of discretionary access control (DAC) and object reuse?
	1. C1: Discretionary Security Protection
	2. C2: Controlled Access Protection
	3. B1: Labeled Security Protection
	4. B2: Structured Protection
 | Domain: Security Architecture & DesignBest answer: **B**In TCSEC, Division C is for discretionary access control. Certification class C2 is C1 + object reuse.  |
| 1. In Trusted Computer System Evaluation Criteria (TCSEC), what certification division requires mandatory access control (MAC), objects must carry the sensitivity labels, and the system design document must include a mathematical proof of the security model?
	1. Division D: Minimal Protection
	2. Division C: Discretionary Protection
	3. Division B: Mandatory Protection
	4. Division A: Verified Protection
 | Domain: Security Architecture & DesignBest answer: **D**In TCSEC, certification class A1 is functionally equivalent to B3, the only additional criteria are in the area of **design verification**. |
| 1. In Trusted Computer System Evaluation Criteria (TCSEC), what the lowest certification class that requires covert channel analysis?
	1. C1: Discretionary Security Protection
	2. C2: Controlled Access Protection
	3. B1: Labeled Security Protection
	4. B2: Structured Protection
 | Domain: Security Architecture & DesignBest answer: **D**In TCSEC, certification class **B2: Structured Protection** is the lowest evaluation level that requires covert channel analysis. |
| 1. When comparing the Trusted Computer System Evaluation Criteria (TCSEC) and the Information Technology Security Evaluation Criteria (ITSEC), what ITSEC’s assurance ratings are equivalent to TCSEC’s certification classes?
	1. F1 – F5
	2. F1 – F6
	3. F-C1 – F-B3
	4. E0 – E6
 | Domain: Security Architecture & DesignBest answer: **D**

|  |  |
| --- | --- |
| **ITSEC** | **TCSEC** |
| E0 | D: Minimal Protection |
| F-C1, E1 | C1: Discretionary Security Protection |
| F-C2, E2 | C2: Controlled Access Protection |
| F-B1, E3 | B1: Labeled Security |
| F-B2, E4 | B2: Structured Protection |
| F-B3, E5 | B3: Security Domains |
| F-B3, E6 | A1: Verified Design |

**Reference:** *Information Technology Security Evaluation Criteria (ITSEC)*, version 1.2, June 28, 1991. |
| 1. In the Information Technology Security Evaluation Criteria (ITSEC), what is the assigned assurance rating for semi-formal system and unit tests with source code review?
	1. E6
	2. E5
	3. E4
	4. E3
 | Domain: Security Architecture & DesignBest answer: **B**

|  |  |
| --- | --- |
| **ITSEC Assurance Level** | **Required activities** |
| E0 | Inadequate assurance |
| E1 | System in development |
| E2 | Informal system tests |
| E3 | Informal system and unit tests |
| E4 | Semi-formal system and unit tests |
| E5 | Semi-formal system and unit tests with source code review |
| E6 | Formal end-to-end security tests plus source code reviews |

 |
| 1. In Common Criteria, what is the “solution neutral” specification that explains the security needs?
	1. Security Target (ST)
	2. Target of Evaluation (TOE)
	3. Protection Profile (PP)
	4. Evaluation Assurance Level (EAL)
 | Domain: Security Architecture & DesignBest answer: **C*** **Protection Profile (PP)** is the “solution neutral” specification that explains the security needs.
* **Security Target (ST)** is a “product/solution-oriented” document, usually provided by solution vendors, to support the security evaluation.
* **Target of Evaluation (TOE)** is the product to be evaluated.
 |
| 1. In Common Criteria, what is the assigned Evaluation Assurance Level (EAL) for the Target of Evaluation (TOE) that has been methodically designed, tested, and reviewed?
	1. EAL 7
	2. EAL 6
	3. EAL 5
	4. EAL 4
 | Domain: Security Architecture & DesignBest answer: **D**

|  |  |
| --- | --- |
| **CC EAL** | **Required activities** |
| EAL1 | Functionally tested |
| EAL2 | Structurally tested |
| EAL3 | Methodically tested and chcked |
| EAL4 | Methodically designed, tested, and reviewed |
| EAL5 | Semi-formally designed and tested |
| EAL6 | Semi-formally verified, designed, and tested |
| EAL7 | Formally verified, designed, and tested |

 |
| 1. What type of data communication network structure is designed to support data transmission in a small geographical area or an office building?
	1. Local area network (LAN)
	2. Personal area network (PAN)
	3. Wide area network (WAN)
	4. Metropolitan area network (MAN)
 | Domain: Telecommunications & Network SecurityBest answer: **A*** Local Area Network (LAN). Primarily limited to a small geographical area or a single site (i.e. an office building).
* Personal Area Network (PAN). Data communications network for short distance (e.g. Bluetooth, Infra-Red).
* Wide Area Network (WAN). Data communications network to multiple long range geographic area.
* Metropolitan Area Network (MAN). Data communications network for a large city (e.g. Washington Metropolitan, New York City, or Boston, etc.)
* Campus Area Network. Data communications network for a campus of buildings (e.g. college campus, military base)
 |
| 1. What is the information communications network designed to service internal customers (within a corporation) over diverse range of telecommunication networks?
	1. Internet
	2. Intranet
	3. Extranet
	4. Cloud
 | Domain: Telecommunications & Network SecurityBest answer: **B*** **Internet** is the **worldwide** system of interconnected **public networks**
* **Intranet** is a type of network that services **internal clients** (/users) over diverse range of telecommunication networks
* **Extranet** is a type of network that services to **external clients** (/customers) over diverse range of telecommunication networks
 |
| 1. What mode of data communication relying on a clocking system to determine sender and receiver communication signals?
	1. Analog communications
	2. Digital communications
	3. Synchronous communications
	4. Asynchronous communications
 | Domain: Telecommunications & Network SecurityBest answer: C* **Synchronous communication** is a mode of data communications usually rely on a **clocking** system to determine sender and receiver communication signals.
* **Asynchronous communication** is a mode of data communications usually controlled by a set of start & stop bits at each end of data signals (header & footers) to **encapsulate** the data.
* Analog and digital communications are methods of data communications.
 |
| 1. What type of data network where information is send through a logical circuit created over a packet-switched network?
	1. Circuit-switched network
	2. Packet-switched network
	3. Virtual circuit
	4. Public switched telephone network
 | Domain: Telecommunications & Network SecurityBest answer: **C*** **Circuit-switched network** is where data are communicated through a dedicated circuit is created between two endpoints.
* **Packet-switched network** is where data are segmented into communication packets and sent through a circuit shared by multiple subscribers.
* **Virtual circuit** is a logical data communication circuit created over a packet-switched network.
 |
| 1. What is the data network topology where the end nodes are connected to each other?
	1. Tree topology
	2. Star topology
	3. Ring topology
	4. Mesh topology
 | Domain: Telecommunications & Network SecurityBest answer: **D**Mesh topology has all the network nodes connected to each other to form a full or partial mesh. |
| 1. What Telecommunications Industry Association (TIA) cable standard is best suited for Gigabit and 10-Gigabit Ethernet networks in a local area networking (LAN) environment up to 100 meter (~328 ft.)?
	1. Category 6
	2. Category 5e
	3. Category 5
	4. Category 3
 | Domain: Telecommunications & Network SecurityBest answer: **A**TIA Category 6 cable standard for twisted wire pairs is designed with better insulation and increased performance to reduce crosstalk and signal noise than Category 5 and 3, thus suitable for Gigabit and 10-Gigabit Ethernet in a LAN environment (up to 100 meters)Note: Category 5e and 5 may be capable of carrying Gigabit Ethernet signals, but they are not certified and capable of carrying 10-Gigabit Ethernet signals. |
| 1. What radio frequency (RF) local area network (LAN) communications standard that operates in the open 2.4GHz frequency band and uses orthogonal frequency-division multiplexing (OFDM) method for managing communication signals?
	1. Bluetooth
	2. IEEE 802.11a
	3. IEEE 802.11b
	4. IEEE 802.11g
 | Domain: Telecommunications & Network SecurityBest answer: **D*** **IEEE 802.11g** operates in 2.4GHz and uses orthogonal frequency-division multiplexing (OFDM).
* **IEEE 802.11b** operates in 2.4GHz, but uses direct-sequence spread spectrum (DSSS).
* **IEEE 802.11a** operates in 5GHz, and uses OFDM
* **Bluetooth** operates in 2.4GHz and uses frequency-hopping spread spectrum (FHSS)
 |
| 1. In the OSI data-link layer for local area network (LAN) protocols, what is the length of unique address for the media access control (MAC) that is assigned as the vender code?
	1. 48-bit
	2. 24-bit
	3. 16-bit
	4. 8-bit
 | Domain: Telecommunications & Network SecurityBest answer: **B**Media access control (MAC) address is a 48-bit address for hardware. First 3 bytes (24-bit) are the vendor code assigned by IEEE, the second 3 bytes are the serial numbers from the manufacturer. |
| 1. What is the best media access method to use by communication packets to access the wireless radio frequency (RF) network medium?
	1. Carrier sensing multiple access with collision avoidance (CSMA/CA)
	2. Carrier sensing multiple access with collision detection (CSMA/CD)
	3. Polling
	4. Token passing
 | Domain: Telecommunications & Network SecurityBest answer: **A**Carrier sensing multiple access with collision avoidance (**CSMA/CA**) is usually the best media access method for RF network protocols. Primarily, this is because RF medium must have some ways to know if the frequency channels are in-use or available.  |
| 1. What is the wide area network (WAN) protocol that packetizes digital voice, video, and data information into 53-byte cell units and requires no clocking mechanism?
	1. Frame relay
	2. Integrated Services Digital Network (ISDN)
	3. Asynchronous Transfer Mode (ATM)
	4. Synchronous Data Link Control (SDLC)
 | Domain: Telecommunications & Network SecurityBest answer: **C**Asynchronous Transfer Mode (ATM) is a asynchronous (clocking not required) WAN protocol that packetizes digital voice, video, and data information into 53-byte cell units. |
| 1. What is the wireless protocol suite that enables your smart phone to access Internet application services?
	1. Enhanced Data rates for GSM Evolution (EDGE)
	2. Evolution-Data Optimized (EV-DO)
	3. IEEE 802.16, Worldwide Interoperability for Microwave Access (WiMAX)
	4. Wireless Application Protocol (WAP)
 | Domain: Telecommunications & Network SecurityBest answer: **D****Wireless Application Protocol (WAP)** is a suite of interoperability protocols from OSI Data-Link layer to Application layer that enables smart phones to access Internet-based application services.All others (EDGE, EV-DO, WiMAX) are the 3rd Generation (3G) design for interoperability primarily at the physical “interface” level (OSI Physical layer). |
| 1. What is the wide area network (WAN) device that interprets analog signals into digital signals and vice versa so the data packets can be transmitted over circuit switched plain old telephone service (POTS) network?
	1. Modem
	2. Channel Service Unit/Digital Service Unit (CSU/DSU)
	3. Wide area network (WAN) switch
	4. Gateway
 | Domain: Telecommunications & Network SecurityBest answer: **A*** **Modem** is the wide area network (WAN) device that interprets analog signals into digital signals and vice versa over the circuit switched POTS line.
* **Channel Service Unit (CSU)** is a line bridging device that enables the **Digital Service Unit (DSU)** to use channelized digital circuits such as T-carriers.
* **WAN switch** provides packet switching at Layer 2
* **Gateway** does not interpret analog and digital signals. Gateway enables interoperability of digital packets between two or multiple types of physical medium. (e.g., Satcom and TCP/IP)
 |
| 1. What are the considerations for designing and provisioning virtual local area networks (VLANs)?
	1. Performance
	2. Simplified administration
	3. Improve security by limiting network broadcasts
	4. All of the above
 | Domain: Telecommunications & Network SecurityBest answer: **D**All of the above. Virtual local area network (VLAN) improves network performance and security by limiting network broadcasts; hence reduce collision. VLAN simplifies network administration; hence, reduce costs. |
| 1. In the TCP/IP Protocol Architecture, what is the mandatory protocol that provides control messages as a part of Internet Protocol (IP) header?
	1. Internet Protocol (IP)
	2. Internet Control Message Protocol (ICMP)
	3. Address Resolution Protocol (ARP)
	4. Reverse Address Resolution Protocol (RARP)
 | Domain: Telecommunications & Network SecurityBest answer: **B**Per RFC792 and RFC2463 (for IPv6), the Internet Control Message Protocol (ICMP) is used to report IP control messages for status and error of datagrams. |
| 1. Which one of radio frequency (RF) network communication protocol is not designed to operate in the open industrial, scientific, and medial (ISM) radio band of 2.4 – 2.5GHz?
	1. IEEE 802.11a
	2. IEEE 802.11b
	3. IEEE 802.11c
	4. Bluetooth
 | Domain: Telecommunications & Network SecurityBest answer: **A**IEEE 802.11a uses the open ISM radio band of 5GHz.IEEE 802.11b/g and Bluetooth operate in the open 2.4GHz radio band. |
| 1. What is the length of Internet Protocol version 6 (IPv6) address?
	1. 32-bit
	2. 64-bit
	3. 128-bit
	4. 256-bit
 | Domain: Telecommunications & Network SecurityBest answer: **C**The length of **IPv6** address is **128-bit**, which amounts to 2128 = 3.40282367 x 1038 unique addresses.The length of **IPv4** address is **32-bit**, which amounts to 232 = 4,294,967,296 unique addresses. |
| 1. In IPv4, what class of IP address: 128.10.5.254 is in?
	1. Class A
	2. Class B
	3. Class C
	4. Class D
 | Domain: Telecommunications & Network SecurityBest answer: **B*** **Class A**: 1.0.0.0 – 127.255.255.255
* **Class B**: 128.0.0.0 – 191.255.255.255
* **Class C**: 192.0.0.0 – 223.255.255.255
* **Class D**: 224.0.0.0 – 239.255.255.255 (Multicast)
* **Class E**: 240.0.0.0 – 254.255.255.255 (Experimental)
 |
| 1. In IPv4, per RFC 1918, *Address Allocation for Private Internets*, which of the following is a private, (none Internet routable) IP address?
	1. 11.32.68.5
	2. 168.155.32.36
	3. 193.168.254.254
	4. 172.30.10.10
 | Domain: Telecommunications & Network SecurityBest answer: **D**Per RFC 1918, the following IP addresses are reserved as private IP addresses:* **Class A: 10.0.0.0 – 10.255.255.255**
* **Class B: 172.16.0.0 – 172.31.255.255**
* **Class C: 192.168.0.0 – 192.168.255.255**
 |
| 1. In the Internet Protocol (IP) addressing and transmission methods, which of the following expression describes the transmission method of multicast?
	1. Datagram is sent from a single source to a single destination
	2. Datagram is copied, then sent to all the nodes on the network
	3. Datagram is copied, then they are sent to a group of destinations on a network
	4. Datagram sent is routed to one of several available locations.
 | Domain: Telecommunications & Network SecurityBest answer: **C*** **Multicast**: Datagram is copied, then sent to a group of destinations on a network
* **Broadcast**: Datagram is copied, then sent to all the nodes on the network
* **Unicast**: Datagram is sent from a single source to a single destination
* **Anycast**: Datagram sent is routed to one of several available locations
 |
| 1. Which of the following protocols is not an interior routing protocol?
	1. Routing Information Protocol (RIP)
	2. Open Shortest Path First (OSPF)
	3. Integrated Intermediate System-to-Intermediate System (IS-IS)
	4. Border Gateway Protocol (BGP)
 | Domain: Telecommunications & Network SecurityBest answer: **D**RIP, OSPF, and IS-IS are interior routing protocols.BGP is an exterior routing protocol design for routing between autonomous systems (AS) on the Internet. |
| 1. Which of the following protocols is a link-state routing protocol?
	1. Routing Information Protocol (RIP)
	2. Open Shortest Path First (OSPF)
	3. Interior Gateway Routing Protocol (IGRP)
	4. Border Gateway Protocol (BGP)
 | Domain: Telecommunications & Network SecurityBest answer: **B**OSPF and IS-IS are link-state routing protocols.RIP and IGRP are distance-vector routing protocols.BGP is a path-vector routing protocol. |
| 1. Which of the following routed protocols uses a connectionless transmission of User Datagram Protocol (UDP)?
	1. Domain Name System (DNS)
	2. File Transfer Protocol (FTP)
	3. Hypertext Transfer Protocol (HTTP)
	4. Simple Mail Transfer Protocol (SMTP)
 | Domain: Telecommunications & Network SecurityBest answer: **A**DNS uses UDP at the Transport Layer.FTP, HTTP, and SMTP are protocols that use stateful Transmission Control Protocol (TCP) at the Transport Layer.  |
| 1. In the Open System Interconnection (OSI) reference model, what layer provides services to establish connection between two presentation entities, support orderly data exchanges, and release the connection in an orderly manner?
	1. Application Layer
	2. Presentation Layer
	3. Session Layer
	4. Transport Layer
 | Domain: Telecommunications & Network SecurityBest answer: **C**OSI **Session Layer** provides services to establish a session-connection between two presentation entities, support orderly data exchange interactions, and to release the connection in an orderly manner. |
| 1. American Standard Code for Information Interchange (ASCII), Joint Photographic Experts Group (JPEG), and Tagged Image File Format (TIFF) are example data formats in which layer of the Open System Interconnection (OSI) Reference Model?
	1. Application Layer
	2. Presentation Layer
	3. Session Layer
	4. Transport Layer
 | Domain: Telecommunications & Network SecurityBest answer: **B**ASCII, EBCDIC, TIFF, JPEG, and MPEG are example data formats in the OSI **Presentation Layer**.  |
| 1. Hypertext Transfer Protocol (HTTP), Telnet, Simple Network Management Protocol (SNMP), Simple Mail Transfer Protocol (SMTP), and File Transfer Protocol (FTP) are example of services in which layer of the Open System Interconnection (OSI) Reference Model?
	1. Application Layer
	2. Presentation Layer
	3. Session Layer
	4. Transport Layer
 | Domain: Telecommunications & Network SecurityBest answer: **A**HTTP, SNMP, SMTP, and FTP are example of application level services in the OSI **Application Layer**. |
| 1. Loss of signal strength over distance is?
	1. Crosstalk
	2. Radio frequency interference (RFI)
	3. Transient
	4. Attenuation
 | Domain: Telecommunications & Network SecurityBest answer: **D****Attenuation** is loss of signal strength over distance**Transient** is disturbance of power traveling across transport mediumRadio frequency interference (**RFI**) is also known as electromagnetic interference (**EMI**). It is a disturbance affects an electrical circuit to conduct or a radio to emit electrical signals.  |
| 1. When describing the advantages of Point-to-Point Protocol (PPP) over Serial Line Internet Protocol (SLIP), which of the following statement is not true?
	1. PPP supports multiple authentication methods, SLIP does not.
	2. PPP can be implemented on top of virtual circuit network, but SLIP does not.
	3. PPP supports multiple network protocols in a connected session, but SLIP only supports one network protocol per connected session.
	4. PPP has options for authentication, but SLIP does not.
 | Domain: Telecommunications & Network SecurityBest answer: **B**Both PPP and SLIP can be implemented on top of circuit switched networks. |
| 1. A security engineer is implementing an authenticated remote access service for Company A, which of the following data-link layer protocol allows him to provision the service endpoints on various devices?
	1. Serial Line Internet Protocol (SLIP)
	2. Point-to-Point Protocol (PPP)
	3. Layer 2 Tunneling Protocol (L2TP)
	4. Extensible Authentication Protocol (EAP)
 | Domain: Telecommunications & Network SecurityBest answer: **C**L2TP extends the PPP by allowing endpoints to reside on different devices, such as workstation in a home wireless network linked to an ISP to a corporate access gateway.EAP is an authentication protocol, not a data-link lay protocol. |
|  | Domain: Telecommunications & Network Security |
|  | Domain: Telecommunications & Network Security |
|  | Domain: Telecommunications & Network Security |
|  | Domain: Telecommunications & Network Security |
|  | Domain: Telecommunications & Network Security |
|  | Domain: Telecommunications & Network Security |
|  | Domain: Telecommunications & Network Security |
|  | Domain: Telecommunications & Network Security |
|  | Domain: Telecommunications & Network Security |
|  | Domain: Telecommunications & Network Security |
|  | Domain: Telecommunications & Network Security |
|  | Domain: Telecommunications & Network Security |
|  | Domain: Telecommunications & Network Security |
|  | Domain: Telecommunications & Network Security |
|  | Domain: Telecommunications & Network Security |
|  | Domain: Telecommunications & Network Security |
|  | Domain: Telecommunications & Network Security |
|  | Domain: Telecommunications & Network Security |
|  | Domain: Telecommunications & Network Security |
|  | Domain: Telecommunications & Network Security |
|  | Domain: Telecommunications & Network Security |
|  | Domain: Telecommunications & Network Security |
|  | Domain: Application Security |
|  | Domain: Application Security |
|  | Domain: Application Security |
|  | Domain: Application Security |
|  | Domain: Application Security |
|  | Domain: Application Security |
|  | Domain: Application Security |
|  | Domain: Application Security |
|  | Domain: Application Security |
|  | Domain: Application Security |
|  | Domain: Application Security |
|  | Domain: Application Security |
|  | Domain: Application Security |
|  | Domain: Application Security |
|  | Domain: Application Security |
|  | Domain: Access Control |
|  | Domain: Access Control |
|  | Domain: Access Control |
|  | Domain: Access Control |
|  | Domain: Access Control |
|  | Domain: Access Control |
|  | Domain: Access Control |
|  | Domain: Access Control |
|  | Domain: Access Control |
|  | Domain: Access Control |
|  | Domain: Access Control |
|  | Domain: Access Control |
|  | Domain: Access Control |
|  | Domain: Access Control |
|  | Domain: Access Control |
|  | Domain: Access Control |
|  | Domain: Access Control |
|  | Domain: Access Control |
|  | Domain: Access Control |
|  | Domain: Access Control |
|  | Domain: Cryptography |
|  | Domain: Cryptography |
|  | Domain: Cryptography |
|  | Domain: Cryptography |
|  | Domain: Cryptography |
|  | Domain: Cryptography |
|  | Domain: Cryptography |
|  | Domain: Cryptography |
|  | Domain: Cryptography |
|  | Domain: Cryptography |
|  | Domain: Cryptography |
|  | Domain: Cryptography |
|  | Domain: Cryptography |
|  | Domain: Cryptography |
|  | Domain: Cryptography |
|  | Domain: Cryptography |
|  | Domain: Cryptography |
|  | Domain: Cryptography |
|  | Domain: Cryptography |
|  | Domain: Cryptography |
|  | Domain: Cryptography |
|  | Domain: Cryptography |
|  | Domain: Cryptography |
|  | Domain: Cryptography |
|  | Domain: Cryptography |
|  | Domain: Cryptography |
|  | Domain: Cryptography |
|  | Domain: Cryptography |
|  | Domain: Cryptography |
|  | Domain: Cryptography |
|  | Domain: Cryptography |
|  | Domain: Cryptography |
|  | Domain: Cryptography |
|  | Domain: Cryptography |
|  | Domain: Cryptography |
|  | Domain: Cryptography |
|  | Domain: Cryptography |
|  | Domain: Cryptography |
|  | Domain: Cryptography |
|  | Domain: Cryptography |
|  | Domain: Cryptography |
|  | Domain: Cryptography |
|  | Domain: Cryptography |
|  | Domain: Cryptography |
|  | Domain: Cryptography |
|  | Domain: Cryptography |
|  | Domain: Cryptography |
|  | Domain: Cryptography |
|  | Domain: Cryptography |
|  | Domain: Cryptography |
|  | Domain: Operations Security |
|  | Domain: Operations Security |
|  | Domain: Operations Security |
|  | Domain: Operations Security |
|  | Domain: Operations Security |
|  | Domain: Operations Security |
|  | Domain: Operations Security |
|  | Domain: Operations Security |
|  | Domain: Operations Security |
|  | Domain: Operations Security |
|  | Domain: Operations Security |
|  | Domain: Operations Security |
|  | Domain: Operations Security |
|  | Domain: Operations Security |
|  | Domain: Operations Security |
|  | Domain: Physical Security |
|  | Domain: Physical Security |
|  | Domain: Physical Security |
|  | Domain: Physical Security |
|  | Domain: Physical Security |
|  | Domain: Physical Security |
|  | Domain: Physical Security |
|  | Domain: Physical Security |
|  | Domain: Physical Security |
|  | Domain: Physical Security |
|  | Domain: Physical Security |
|  | Domain: Physical Security |
|  | Domain: Physical Security |
|  | Domain: Physical Security |
|  | Domain: Physical Security |
|  | Domain: Business Continuity & Disaster Recovery Planning |
|  | Domain: Business Continuity & Disaster Recovery Planning |
|  | Domain: Business Continuity & Disaster Recovery Planning |
|  | Domain: Business Continuity & Disaster Recovery Planning |
|  | Domain: Business Continuity & Disaster Recovery Planning |
|  | Domain: Business Continuity & Disaster Recovery Planning |
|  | Domain: Business Continuity & Disaster Recovery Planning |
|  | Domain: Business Continuity & Disaster Recovery Planning |
|  | Domain: Business Continuity & Disaster Recovery Planning |
|  | Domain: Business Continuity & Disaster Recovery Planning |
|  | Domain: Business Continuity & Disaster Recovery Planning |
|  | Domain: Business Continuity & Disaster Recovery Planning |
|  | Domain: Business Continuity & Disaster Recovery Planning |
|  | Domain: Business Continuity & Disaster Recovery Planning |
|  | Domain: Business Continuity & Disaster Recovery Planning |
|  | Domain: Business Continuity & Disaster Recovery Planning |
|  | Domain: Business Continuity & Disaster Recovery Planning |
|  | Domain: Business Continuity & Disaster Recovery Planning |
|  | Domain: Business Continuity & Disaster Recovery Planning |
|  | Domain: Business Continuity & Disaster Recovery Planning |
|  | Domain: Business Continuity & Disaster Recovery Planning |
|  | Domain: Business Continuity & Disaster Recovery Planning |
|  | Domain: Business Continuity & Disaster Recovery Planning |
|  | Domain: Business Continuity & Disaster Recovery Planning |
|  | Domain: Business Continuity & Disaster Recovery Planning |
|  | Domain: Business Continuity & Disaster Recovery Planning |
|  | Domain: Business Continuity & Disaster Recovery Planning |
|  | Domain: Business Continuity & Disaster Recovery Planning |
|  | Domain: Business Continuity & Disaster Recovery Planning |
| 1. U.S. Export Administration Regulations (EAR) and European Union Council (EC) Regulation No. 1334/2000: *Setting up a Community Regime for the Control of Exports of Dual-use Items and Technology* are examples of what type of law?
	1. Civil law
	2. Customary law
	3. Mixed law
	4. Administrative law
 | Domain: Legal, Regulations, Compliance & InvestigationsBest Answer: **D*** Civil laws are rule-based; they are not based on precedence. Administrative laws are a type of civil law.
* Common laws are based on precedence.
* Customary laws are based on cultural customs, and traditions.
* Religious laws are based on religions.
* Mixed law system is based on civil, customary, and religious laws.
 |
| 1. Industrial properties, patents, trademarks, and industrial designs are considered as what type of intellectual property?
	1. Industrial property.
	2. Copyright.
	3. Trade secrets.
	4. None of the above.
 | Domain: Legal, Regulations, Compliance & InvestigationsBest Answer: **A**There are two types of intellectual property:* Industrial property. (Inventions, trademarks, industrial designs, and geographic indications of source.)
* Copyright. (Literary works, e.g., books, articles, architecture designs, etc. And artistic works, e.g., music, songs, films, paintings, photo/ graphs, and sculptures, etc.)
 |
| 1. Which of the following intellectual property is protected by U.S. law for 20 years from the filing date?
	1. Trademark.
	2. Trade secret.
	3. Patent.
	4. Copyright
 | Domain: Legal, Regulations, Compliance & InvestigationsBest Answer: **C**In U.S., the patent law protects inventions for 20 years from the filing date. Patent term can be extended. |
| 1. What is the importance of Wassenaar Arrangement?
	1. Restrict export of cryptographic products based on key lengths.
	2. Enforcement of international copyright.
	3. Mutual legal assistance between international law enforcement agencies.
	4. There is no such international treaty.
 | Domain: Legal, Regulations, Compliance & InvestigationsBest Answer: **A**Importance of Wassenaar Arrangement is restriction on exporting of cryptographic products based on key lengths.* 56-bit for symmetric cryptographic systems.
* 512-bit for asymmetric cryptographic systems.

Reference:* EAR, Part 774, Category 5 (Part 2) – Information Security: *Mass market & retail cryptography can be exported without a license*.
* European Union Council (EC) Regulation No. 1334/2000: *Setting up a Community Regime for the Control of Exports of Dual-use Items and Technology*.
 |
| 1. What is the best way to preserve integrity of digital evidence to support forensic activities?
	1. Make a “bit-for-bit” copy of the original media.
	2. Generate a hash value of the original source.
	3. Document the “chain-of-custody”.
	4. All of the above.
 | Domain: Legal, Regulations, Compliance & InvestigationsBest Answer: **D**To ensure the reliability and durability of digital evidence, a security professional shall generate a hash value of the original source, make a “bit-for-bit” copy of the original media, and document all subjects that have accessed the digital evidence throughout its life cycle. |
| 1. In general, privacy laws usually include which of the following provision?
	1. Government agencies may not use the privacy data for a purpose other than that for which it was initially collected.
	2. Government agencies must ensure accuracy of their data records.
	3. Government agencies must share the privacy data with all other agencies.
	4. Individuals have the right to remove data that they do not wish disclosed.
 | Domain: Legal, Regulations, Compliance & InvestigationsBest Answer: **A**Per Privacy Act of 1974…* Government agencies must restrict disclosure of personal system of records.
* Government agencies must provide individuals the ability to modify their system of records. Therefore, the Government agencies must establish a “code of fair information practice” policy on the collection, maintenance, dissemination and sharing of personal system of records.
 |
| 1. In general, a copyright work created after January 1, 1978 is protected for how long?
	1. 95 years from the year of its first publication.
	2. 120 years from the year of its creation.
	3. The life of the author and 70 years after the author’s death.
	4. A copyright never expires.
 | Domain: Legal, Regulations, Compliance & InvestigationsBest Answer: **C**Per 17 U.S.C. 302, *Duration of copyright: Works created on or after January 1, 1978*, “*Copyright in a work created on or after January 1, 1978, subsists from its creation and, except as provided by the following subsections, endures for a term consisting of* ***the life of the author and 70 years after the author’s death****.*”“*In the case of an anonymous work, a pseudonymous work, or a work made for hire, the copyright endures for a term of 95 years from the year of its first publication, or a term of 120 years from the year of its creation, whichever expires first.*” |
| 1. According to *Computer Fraud and Abuse Act of 1984*, what are the three categories of computer crime?
	1. Unauthorized access, unauthorized alteration, and insertion of malicious code.
	2. Computer assisted, computer targeted, and computer is incidental.
	3. Crimes directed at computer or network.
	4. None of the above.
 | Domain: Legal, Regulations, Compliance & InvestigationsBest Answer: **B**Per *Computer Fraud and Abuse Act of 1984*, there are three categories of computer crime:* Computer assisted crime (i.e., computer as a tool.)
* Computer targeted crime (i.e., crime directed at computer.)
* Computer is incidental (i.e., computer data from criminal activities.)
 |
| 1. What is the primary difference between an intellectual property protected by copyright and an intellectual property protected as a trade secret?
	1. A trade secret is not a formal protection, as copyright is a formal protection defined by law.
	2. A trade secret has much longer term of protection than copyright.
	3. A trade secret applies to industrial property and copyright protects only “expression of ideas”.
	4. No difference. All trade secrets are protected by copyright.
 | Domain: Legal, Regulations, Compliance & InvestigationsBest Answer: **A**Trade secret has no formal protection. It is a proprietary information that its owner must take “reasonable” security precaution to keep it proprietary.Copyright is protected by law. And copyrighted material is usually public. |
| 1. Business records may be considered as hearsay evidence, unless…
	1. the information is related to regular business activities.
	2. the information is auto-generated computer data.
	3. the integrity of information is preserved.
	4. All of the above.
 | Domain: Legal, Regulations, Compliance & InvestigationsBest Answer: **D**Business records may be exempt as a hearsay evidence, if the business records are:* related to regular business activities;
* automatically computer generated with:
	+ no human intervention;
	+ the system was operating correctly; and
	+ no one has change the data.
 |
| 1. When handling digital evidence, how is the chain-of-custody implemented?
	1. A judge must first determine whether the digital evidence is admissible.
	2. The digital evidence must be submitted by the originator.
	3. A copy of digital evidence must be produced and submitted for record.
	4. A procedure must be implemented to account for everyone that has handled the digital evidence.
 | Domain: Legal, Regulations, Compliance & InvestigationsBest Answer: DChain-of-custody a procedure that produces an audit trail that accounts for everyone handled the evidence. |
| 1. What type of evidence where it is presented to jury in a form of model, illustration, chart, or experiment outcome?
	1. Direct evidence.
	2. Real evidence.
	3. Documentary evidence.
	4. Demonstrative evidence.
 | Domain: Legal, Regulations, Compliance & InvestigationsBest Answer: **D*** Direct evidence is oral testimony by witness.
* Real is physical evidence made up by tangible objects that prove or disprove guilt.
* Documentary is in form of business records, manuals, or print outs, etc.
* Demonstrative evidence is evidence used to aid the jury. In a form of model, illustration, chart or experiment offered as proof.
 |
| 1. When determining the admissibility of evidence, what are the rules?
	1. Relevancy.
	2. Reliability.
	3. Durability.
	4. All of the above.
 | Domain: Legal, Regulations, Compliance & InvestigationsBest Answer: **D**Rules of evidence. The evidence must be:* Relevant. To proof a crime occurred.
* Reliable. To ensure the legally obtained evidence is trustworthy.
* Durable. To preserve integrity of the evidence.
 |
| 1. Oral testimony by a subject matter expert (SME) on a computer crime is considered as what type of evidence?
	1. Direct evidence.
	2. Real evidence.
	3. Documentary.
	4. Demonstrative evidence.
 | Domain: Legal, Regulations, Compliance & InvestigationsBest Answer: **A*** Direct evidence is oral testimony by witness.
* Real is physical evidence made up by tangible objects that prove or disprove guilt.
* Documentary is in form of business records, manuals, or print outs, etc.
* Demonstrative evidence is evidence used to aid the jury. In a form of model, illustration, chart or experiment offered as proof.
 |
| 1. In 1989, Defense Advanced Research Project Agency (DARPA) Internet Activities Board (IAB) submitted RFC 1087, *Ethics and the Internet* as an ethics guideline. Which of the following activity is not considered as unethical?
	1. To gain unauthorized access to the resources of the Internet.
	2. To disrupt the intended use of the Internet.
	3. To destroy the integrity of computer-based information.
	4. To decrypt encrypted information.
 | Domain: Legal, Regulations, Compliance & InvestigationsBest Answer: **D**RFC 1087 characterizes the following activities as unethical and unacceptable on the Internet:1. Seeks to gain unauthorized access to the resources of the Internet,
2. Disrupts the intended use of the Internet,
3. Wastes resources (people, capacity, computer) through such actions,
4. Destroys the integrity of computer-based information, and/or
5. Compromises the privacy of users.
 |
| 1. When a CISSP faces with an ethical conflict, what is the order of priority for resolving ethical conflicts?
	1. Duties to public safety, principals, individuals, and profession.
	2. Duties to principals, profession, public safety, and individuals.
	3. Duties to profession, public safety, individuals, and principals.
	4. Duties to public safety, profession, individuals, and principals.
 | Domain: Legal, Regulations, Compliance & InvestigationsBest Answer: **A****(ISC)2 Code of Ethics…**Act honorably, honestly, justly, responsibly, and legally.* Tell the truth; make all stakeholders aware of your actions on a timely basis.
* Observe all contracts and agreements, express or implied.
* **Treat all members fairly. In resolving conflicts, consider public safety and duties to principals, individuals, and the profession in that order**.
* Give prudent advice; avoid raising unnecessary alarm or giving unwarranted comfort. Take care to be truthful, objective, cautious, and within your competence.
* When resolving differing laws in different jurisdictions, give preference to the laws of the jurisdiction in which you render your service.
 |