All of the following controls are important to specify when defining a data classification scheme, except:

A) Marking, labeling, and handling procedures

B) Physical security protections

C) Backup and recovery procedures

D) Personnel clearance procedures

D is correct. The clearance of personnel should be conducted independently of the classification of the data that may be accessed.

Which of the following firewall types keeps track of each ongoing dialog between internal and external systems?

A) Packet filtering

B) Circuit-level proxy

C) Stateful

D) Application-level proxy

C is correct. Stateful firewalls use state tables to keep track of each step of communication between systems. This provides a higher level of protection than packet filtering, because it makes access decisions based on the steps that have already been completed in the dialog.

Which of the following is NOT a recommended procedure to enact as part of an employee termination process?

A) Immediately disable all of the employee's accounts and passwords.

B) Ensure the employee surrenders any of the company's badges and keys in their possession.

C) Confiscate all devices in the employee's possession that contain company data.

D) Ensure the employee leaves immediately upon termination, escorted by a supervisor.

C is correct. While the other procedures listed are reasonable, proper, and within the company's purview, it simply may not be possible—or even reasonable—to collect from the employee all devices

which are known to contain company data. Particularly in a bring your own device (BYOD) environment, it is almost certain that the employee's personal mobile device contains corporate data, and such devices most likely will not be surrendered willingly. It may be possible for the company to remotely wipe some mobile devices, but only if the employee consented in advance to such measures as part of a signed employment agreement.

Nancy is a new network administrator and has been faced with decision of implementing either direct access backup systems or sequential access backup storage devices. Which of the following does not properly describe these types of technologies?

A) Any point on a Direct Access Storage Device may be promptly reached, whereas every point in between the current position and the desired position of a Sequential Access Storage Device must be traversed in order to reach the desired position

B) Any point on a Sequential Access Storage Device may be promptly reached, whereas every point in between the current position and the desired position of a Direct Access Storage Device must be traversed in order to reach the desired position

C) Some tape drives have minimal amounts of Direct Access intelligence built in

D) Tape drives are Sequential Access Storage Devices

B is correct. The key distinction between Direct Access and Sequential Access storage devices is that any point on a Direct Access Storage Device may be promptly reached, whereas every point in between the current position and the desired position of a Sequential Access Storage Device must be traversed in order to reach the desired position. Tape drives are Sequential Access Storage Devices. Some tape drives have minimal amounts of Direct Access intelligence built in. These include multitrack tape devices that store at specific points on the tape and cache in the tape drive information about where major sections of data on the tape begin, allowing the tape drive to more quickly reach a track and a point on the track from which to begin the now much shorter traversal of data from that indexed point to the desired point. While this makes such tape drives noticeably faster than their purely sequential peers, the difference in performance between Sequential and Direct Access Storage Devices is orders of magnitude.

There are different types of biometric systems in the industry today. Some make authentication decisions based on behavior and some make authentication decisions based on physical attributes. Which of the following is the best description of their differences?

A) **A system that uses physical attributes provides more accuracy than one that uses behavior attributes.**

B) A system that uses behavior attributes provides more accuracy than one that uses physical attributes.

C) A fingerprint system is an example of a physical attribute and an iris system is an example of a behavior system.

D) A voice print system is an example of a behavior and signature dynamics is an example of a physical attribute.

A is correct. A biometric system can make authentication decisions based on an individual's behavior, as in signature dynamics and voice prints, but these can change over time and possibly be forged. Biometric systems that base authentication decisions on physical attributes (iris, retina, fingerprint) provide more accuracy, because they do not change as often and are harder to impersonate.

MSP, PGP, PEM, and S/MIME are examples of which of the following?

A) Digital signing algorithms

B) E-mail standards

C) Asymmetric cryptography algorithms

D) Hashing standards

B is correct. These are examples of different e-mail standards: MSP (Message Security Protocol) PGP (Pretty Good Privacy) PEM: (Privacy Enhanced Mail) S/MIME (Secure Multipurpose Internet Mail Extensions)

Tom is setting up computers at a trade show for his company's booth. The computers will give customers the opportunity to access a new product but will also take them onto a live network. Which control would be the best fit to offer the necessary protection from public users gaining privileged access?

A) **Constrained user interface.**

B) Role-based.

C) Discretionary-based.

D) Network segregation.

A is correct. Constrained user interfaces would be the perfect choice for this trade show scenario. The interface can be physically constrained, as in a kiosk system, or logically constrained through the use of properly configured profiles, menus, and shells.

Who has the primary responsibility of determining the classification level for information?

A) Senior management

B) Owner

C) User

D) Functional manager

C is correct. A company can have one specific data owner or different data owners who have been delegated the responsibility of protecting specific sets of data. One of the responsibilities that goes into protecting this information is properly classifying it.

One mode that triple-DES can work in uses three DES operations with an encrypt/decrypt/encrypt sequence and three separate keys. What is this called?

A) Double DES

B) DES-EE3

C) DES-EDE3

D) DES-EDE2

C is correct. Triple-DES is an extension of DES which offers much stronger protection. It can be used a number of modes including DES-EDE3, which utilizes three keys and an encrypt/decrypt/encrypt sequence.

Which of the following items does not provide physical protection?

A) Smart card

B) Token

C) Biometric device

D) Single sign-on system

D is correct. Each of the other answers contain technologies or devices that can be used for identification and authorization purposes for access control into a facility or sensitive area. Single sign-on technologies are used to logically control users' access to network resources, which does not fall under the physical security umbrella.

Which types of data are considered protected privacy data by the General Data Protection Regulation (GDPR)?

A) Name and address

B) Health and biometric data

C) Political opinions

D) All of the above

D is correct. The GDPR defines personal data as "…any information that relates to an identified or identifiable living individual. Different pieces of information, which collected together can lead to the identification of a particular person, also constitute personal data." The protection of personal data under the GDPR not only encompasses the U.S. equivalent protections of personally identifiable information (PII) under the Privacy Act and protected health information (PHI) under the Health Insurance Portability and Accountability Act (HIPAA), but also extends to such information as political opinions and web cookie IDs, which is information that is not considered private in the United States or elsewhere outside the EU.

Which of the following has/have an incorrect definition?

i. Foreign key: An attribute of one table that is related to the cell of another table

ii. Cell: An intersection of a row and column

iii. Schema: Defines the structure of the database

iv. Data dictionary: Central repository of data elements and their relationships

---

A) **i**

B) i, ii, ii

C) i, ii, iv

D) i, ii, iii, iv

A is correct. A foreign key is an attribute of one table that is related to the primary key of another table.

Corruption/modification is one of the biggest threats to an operations environment. Which of the following is the typical culprit in this type of threat?

A) **Employees**

B) Viruses

C) Bad code

D) Poor maintenance procedures

A is correct. Employees are the number one threat to organizations and operations environments. Obviously, this is not to say that all employees are bad, but because they have access to the systems and the data, as well as the knowledge of internal processes, employees as a whole instantly become the biggest threat.

Paul is a new network administrator. He has found that the current network needs an intelligent unit to balance traffic and provide fault-tolerance. Which of the following technologies should Paul implement?

A) Grid computing

B) Server farming

C) Federated servers

D) Clustering

D is correct. Clustering is a fault-tolerant server technology that is similar to redundant servers, except each server takes part in processing services that are requested. Clusters work as an intelligent unit to balance traffic, and users who access the cluster do not know they may be accessing different systems at different times. To the users, all servers within the cluster are seen as one unit.

What is the most important reason war dialing is still a concern for modern security assessments?

A) Free tools exist that make it easy for an attacker to scan huge blocks of phone numbers.

B) Some tools are relatively sophisticated and can fingerprint the systems that answer, enabling further automation.

C) Many organizations still employ modems for backup communications in a way that is not well secured.

D) Modern, advanced private branch exchanges (PBXs) can make an attacker's job even easier through telephony diagnostic tools.

C is correct. The primary reason modern security assessments still must evaluate exposure to war dialing is that many organizations still employ modems for backup communications yet don't secure them well because of the common misunderstanding that the vulnerability of an exposed modem is no longer a worry. Although the modern war dialing tools available do contribute to this concern, they are ineffective against a properly secured modem.

The concept of data hiding is used for what purpose?

A) To prevent a requesting service from accessing an object when it asks

B) To obscure the object label from the requestor, so it doesn't know how to ask for it

C) To permit access to objects only in the requestor's layer

D) All of the choices

C is correct. Data hiding restricts a requestor from accessing objects outside its security layer by obscuring the fact that they exist as all.

What is true about a physical access control transponder?

A) **It is a card that can be read without sliding it through a card reader.**

B) It is a passive proximity device.

C) It is a card that a user swipes through a card reader to gain access to a facility.

D) It exchanges tokens with an authentication server.

A is correct. A transponder is a type of physical access control device that does not require the user to slide a card through a reader. The reader and card communicate directly. The card and reader has a receiver, transmitter, and battery. The reader sends signals to the card to request information. The card sends the reader an access code.

When work product satisfies real-world requirements and concepts, this is known as:

A) **Validation**

B) Verification

C) Concurrence

D) Accuracy

A is correct. Validation ensures that the final product meets a real-world requirement and is providing the necessary function to the end user.

What type of attack would alter a configuration file after the system looked to see if it had that specific file?

A) Covert channel

B) Backdoor

C) Fraggle

D) TOC/TOU

D is correct. Time-of-check versus time-of-use (TOC/TOU) attacks take advantage of timing differences between when a system checks for files and when it actually executes the files. It is an asynchronous attack.

Which of the following identifies a row within a relational database and is used for indexing?

A) Foreign key

B) Primary key

C) Cell

D) Tuple

B is correct. The primary key is an identifier of a row and is used for indexing in relational databases. Each row must have a unique primary key to properly represent the row as one entity. When a user makes a request to view a record, the database tracks this record by its unique primary key.

Systems that are built on the OSI framework are considered open systems. What does this mean?

A) They do not have authentication mechanisms configured by default.

B) They have interoperability issues.

C) They are built with international protocols and standards so they can easily communicate with other systems.

D) They are built with international protocols and standards so they can choose what types of systems they will communicate with.

C is correct. An open system is a system that has been developed based on standardized protocols and interfaces. Following these standards allows the systems to interoperate more effectively with other systems that follow the same standards.

Which of the following is not a denial-of-service attack?

A) Teardrop

B) Dictionary

C) Smurf

D) TCP SYN flood

B is correct. Dictionary attacks are password-related attacks that can be categorized as brute-force attacks as well. The other types are all geared to bring down a service or attack a network's availability.

What is the term used to describe the systematic evaluation of the exchange points between a graphical data system and the system's user?

A) Black box testing

B) Administrative testing

C) Stress testing

D) Interface testing

D is correct. Interface testing is the systematic evaluation of the data exchange points between a user and a software program's graphical user interface (GUI).

A program that receives too much data so that it cannot execute instructions properly has been exploited by a _____ attack.

A) **Buffer overflow.**

B) TOC/TOU.

C) Covert channel.

D) Data validation.

A is correct. Buffer overflows are common tactics used by hackers to get systems to execute their malicious code. They identify an application or operating system that is not performing proper bounds

checking and input a large amount of data that will write over current memory segments. The data usually contains malicious code that will then be executed by the system.

Paul has been asked to evaluate implementing soft tokens across the enterprise. What exactly are soft tokens?

A) **One-time password generators that reside in software**

B) Synchronous cognitive passwords generated in software

C) Components that are required in SESAME implementations that provide the single-sign on component

D) The authenticator portion of Kerberos

A is correct. One-time passwords can be generated in software, instead of requiring a piece of hardware as in a token device. These are referred to as soft tokens and require that the authentication service and application contain the same base secrets, which are used to generate the one-time passwords.

Part of operational recovery is designing backup facility configurations to work in an acceptable manner so that business can continue. Which of the following is a setup that allows services to be distributed over two or more in-house centers?

A) Hot site

B) Multi-processing center

C) Mobile site

D) Reciprocal agreements

B is correct. A multi-processing center allows a company to have backup over multiple facilities where services have been distributed.

Referring to the TCP/IP model, which of the following are application layer protocols?

A) IEEE 802.3 Ethernet and PPP

B) DNS, DHCP, and SNMP

C) TCP and UDP

D) IPv4 and IPv6

B is correct. DNS, DHCP, and SNMP are application layer protocols. 802.3 Ethernet and PPP are data link layer protocols, TCP and UDP are transport layer protocols, and IPv4 and IPv6 are Internet layer protocols.

Which of the following is something that should be required of an off-site backup facility that stores backed-up media for companies?

- The facility should be within 10 to 15 minutes of the original facility to ensure easy access.
- The facility should contain all necessary PCs, servers, and raised flooring.
- The facility should be protected by an armed guard.
- **The facility should protect against unauthorized access and entry.**

D is correct. This question is addressing a facility that is used to store backed-up data; it is not talking about an off-site facility used for disaster recovery purposes. The facility should not be 10 to 15 minutes away because if there was some type of disaster, the company's main facility and this facility could both be destroyed and the company would lose all of their information. The facility should have the same security standards as the company's security, including protecting against unauthorized access.

Packet routing takes place at which OSI layer?

- **Layer 3 (network)**
- Layer 2 (data link)
- Layer 4 (transport)
- Layer 1 (physical)

A is correct. Packet routing takes place at the network layer. Layer 2 is the data link layer, where stations on a local area network communicate, but cannot communicate with other networks. Layer 4 is the transport layer, which can provide end-to-end connectivity based on packets being routed. And layer 1 is the physical layer upon which all other layers depend.

Which of the following roles is responsible for classifying data?

A) User

B) Data owner

C) Data custodian

D) System owner

B is correct. The data's owner, either through acquisition or creation—and with supervision, is the best entity able to assign classification. The other roles must be relied upon to provide the designated level of protection.

Which of the following statements is true with respect to full volume encryption?

A) The decryption key must reside in memory, but is not accessible.

B) The decryption key may be accessible in memory during the time it is being used.

C) The decryption key must reside in memory, but is only accessible and recoverable while it is being used.

D) The decryption key may reside in memory long past its last use, and be accessible and recoverable.

D is correct. Until power has been removed from primary memory for a sufficient amount of time, encryption/decryption keys for any process may remain recoverable directly from memory, where they must necessarily reside during processing. Additionally, the memory pages that contain the keys may continue to be present after their use if they are not subsequently reused.

A virtual private network is a tunneling protocol plus _____.

A) **Encryption**

B) Digital signature

C) DSL connection

D) Bus topology

A is correct. A tunneling protocol alone does not make a VPN. This is a common misunderstanding. A VPN must include both a tunneling protocol and encryption.

Which of the following is not a reason why data should be classified?

A) Classification forces valuation, which can be used to determine risk.

B) Classification is required to determine appropriate access controls.

C) Classification can be used to optimize security budget.

D) Classification is required to develop secure systems.

D is correct. Data classification is not a requirement of secure systems. Systems can be made secure without any regard to the sensitivity of the data they will handle. However, system investment can be optimized if the data classification, representing its underlying value, is known. Systems handling low-sensitivity information, for instance, can require fewer or less-rigorous security controls than ones that handle top secret information. Knowledge of data classification, therefore, can optimize security budgets on development projects, putting money where it is most needed.

Which model introduced five levels with which the development of an organization's software process is evaluated?

A) Total Quality Model (TQM)

B) IDEAL Model

C) Capability Maturity Model Integration

D) Spiral Model

C is correct. The Capability Maturity Model Integration (CMMI) features five maturity levels that serve as a foundation for conducting continuous process improvement and as an ordinal scale for measuring the maturity of the organization involved in the software processes.

If there are automated tools for risk analysis, why does it take so much time to complete?

A) **A lot of data has to be gathered to be inputted into the automated tool.**

B) Management has to approve it and then a team has to be built.

C) Risk analysis cannot be automated because of the nature of the assessment.

D) Many people have to agree on the same data.

A is correct. An analysis usually takes a long time to complete because of all the data that must be properly gathered. There are usually a lot of different sources for this type of data and properly extracting it is extremely time consuming. In most situations, it involves setting up meetings with specific personnel and going through a question and answer process.

Which of the following is not a physical access control?

A) Turnstiles.

B) Fencing.

C) Host-based IDS.

D) Exterior lighting.

C is correct. Host-based intrusion detection systems (IDS) are considered technical or logical controls because they exist within computer systems and monitor activities. The other controls all exist to provide some type of physical protection.

Administrative controls include all but which of the following?

A) Mandatory vacations.

B) Audit trails.

C) Background checks.

D) Separation of duties.

B is correct. Audit trails are controls that exist within devices and are thereby considered technical or logical controls. Administrative controls are management-driven actions that usually reveal themselves

in the form of policies, directives, advisories, and procedures. Security policies, awareness training, and incident response planning are all examples of administrative controls.

What is “egress monitoring”?

A) **Inspecting outbound connections to determine if they are the result of appropriate behavior**

B) Inspecting inbound connections to determine if they are the result of appropriate behavior

C) Inspecting employees for incoming contraband as they enter the workplace

D) Inspecting employees for outgoing contraband as they leave the workplace

A is correct. “Egress” means outgoing, and in this context of monitoring it applies to network connections that should be monitored to ensure that no critical data is flowing out to destinations in ways that should be deemed suspicious. It is most commonly associated with data loss detection and/or prevention, but can also indicate outbound command and control sessions established by adversaries to maintain the persistence of their control over compromised systems.

In biometrics, what is the difference between an iris scan and a retinal scan?

A) There is no practical difference. Both are interchangeable technologies for a biometric recording of the eyeball.

B) They are very similar in that both use a laser beam to scan aspects of the eyeball, but they scan different parts of the eye.

C) A retinal scan uses a laser to inspect the pattern of capillaries inside the eyeball, whereas an iris scan uses a camera to capture the pattern of colors in the ring surrounding the eye’s pupil.

D) An iris scan uses a laser to inspect the pattern of capillaries inside the eyeball, whereas a retinal scan uses a camera to capture the pattern of colors in the ring surrounding the eye’s pupil.

C is correct. The retina is the back of the inside of the eyeball, and the pattern of the small blood vessels (capillaries) visible there is unique to the individual. It can only be recorded with the precision of a laser beam projected through the pupil and lens of the eye. The iris is the muscular ring around the pupil of the eye, and the color pattern it possesses is also unique to the individual. This can be recorded with a high-resolution camera, and so is less intrusive.

Which would require the lowest level of protection?

A) System logs

B) Backup copies of system logs

C) Hard copies of sensitive company information

D) User training documentation

D is correct. Training documentation would receive the lowest priority in this list. System logs and the backups of these logs keep valuable data about the activities that take place on these devices. Administrators can use these logs to troubleshoot problems or, more importantly, identify security breaches. Hard copies of sensitive information should be kept under tight control as well.

What does the term “data at rest” refer to, and how is it best protected?

A) Data that is not being actively used, though is encrypted during use

B) Data that may be in use, but is decrypted on disk so that it is accessible

C) Data that may be used later, and so is stored decrypted for when it is needed

D) Data that is not being actively used, and is encrypted while static

D is correct. “At rest” means that the data is not actively in use. Such data is best protected via encrypted storage, only to be decrypted during its use.

Switches marry the technologies of _____ and _____.

- **Hubs and bridges**
- Bridges and routers
- Network adapters and hubs
- Bridges and network adapters

A is correct. Switches combine the technologies of hubs and bridges. They act as hubs by enhancing performance and act as bridges by distributing traffic to different networks.

When crafting a technical security report for management, how long should the executive summary be, and what should it contain?

A) No more than a page or two, highlighting only what senior leaders need to understand about the contents, which could run to hundreds of pages

B) No more than five pages, highlighting only what senior leaders need to understand about the contents, which could run to hundreds of pages

C) No more than a page or two, highlighting the most important technical details

D) No more than five pages, highlighting the most important technical details

A is correct. Senior-level management is unlikely to be willing to read more than a page or two of a technical report, and do not need technical details. The report can be lengthy, but the contents need to be concisely summarized.

Which of the following refers to the assessment of a system by someone with no advance knowledge of how it was designed or implemented?

A) White box testing

B) Gray box testing

C) Black box testing

D) Blue box testing

C is correct. Black box testing refers to the assessment of a system by someone with no a priori knowledge of how it was designed or constructed. White box testing refers to the assessment of a system by someone who has access to any and all details of its inner workings, including the source code of relevant software. Gray box testing refers to a system assessment where the tester has some, but incomplete, knowledge of how the system works. There is no such thing as “blue box” testing.

Disaster recovery drills and tests should be performed at least:

A) Once a quarter

B) Once a year

C) Twice a year

D) Every two years

B is correct. Tests and disaster recovery drills should be performed at least once a year. The company should have no confidence in an untested plan. Since systems and processes can change, frequent testing will aid in ensuring a plan will succeed.

Alice needs to hire a third party to conduct a test of her company's security posture. If she needs an exhaustive enumeration of her company's vulnerabilities for prioritization of mitigation, which of the following services should she select?

A) Vulnerability assessment

B) Penetration test

C) Regulatory audit

D) DSS audit

A is correct. Vulnerability assessments seek to exhaustively enumerate all possible vulnerabilities for prioritization of mitigation. Penetration tests are not intended to exhaustively enumerate vulnerabilities, but rather to demonstrate the viability of exploitation by an adversary. Audits against regulations are designed to determine the level of an organization's compliance. Likewise, a PCI DSS audit, which is contractual and not regulatory, is expected to ensure that a Qualified Security Assessor (QSA) deems a payment card processor is compliant with the Data Security Standard (DSS).

Alice is responsible for ensuring that enterprise data is backed up and recoverable. Which of the following is the most critical duty that Alice must perform?

A) Backing up user data files on a daily basis

B) Ensuring that the enterprise databases have replicated

C) Testing recovery procedures with data backups

D) Backing up mailbox data to satisfy e-discovery requirements

C is correct. It doesn't matter what data gets backed up, or how frequently, if the restoration procedures are not demonstrably viable.

During a post-mortem incident evaluation, it is discovered that coercion was used by an attacker to infiltrate the company and obtain confidential information. This tactic would best be characterized as:

A) Eavesdropping

B) Passive

C) Active

D) Sniffing

C is correct. Using coercion is an active type of attack in which the intruder uses aggressive tactics to achieve the intended goal. Using coercion is an example of social engineering, which is an active attack.

The network topology in which all computers are connected together in a nonuniform formation is called what?

A) Mesh

B) Ring

C) Star

D) Bus

A is correct. A mesh topology is one that does not provide the network structure of the other three mentioned topologies (bus, star, ring). In a partial mesh topology, all computers are connected in some way (the Internet is a good example). In a full mesh, each computer is connected to each and every other computer. A full mesh topology provides full redundancy, but requires a lot of cabling.

IPSec uses _____ for key management.

A) IKE

B) MPLS

C) PPP

D) NAT

A is correct. Internet Key Exchange (IKE) is used within IPSec to negotiate and authenticate keys.

Which of the following best describes a centralized repository of information about data such as meaning, relationships to other data, origin, usage, and format?

- Meta-data
- **Data dictionary**
- Cross data
- DBMS

B is correct. A **data dictionary, or a metadata repository**, is a centralized repository of information about data, such as its meaning, relationships to other data, origin, usage, and format. It is a tool used to centrally manage parts of a database by controlling the metadata within the database.

How does the Diameter protocol provide more security than RADIUS?

A) For interoperability issues, the both provide the same level of security.

B) Diameter has been developed to work directly with TLS and IPSec.

C) Diameter works within the S/MIME standard.

D) RADIUS only encrypts the username.

B is correct. Diameter provides end-to-end security through the use of IPSec or TLS, which is not available in RADIUS.

Your company's CIO has stressed the need for an immediate incident response plan to be created. What is the best reason for this mandate?

A) To improve the company's reputation with stockholders

B) To improve the executive team's compliance with due diligence regulations

C) To improve employee morale and retention

D) To improve the likelihood that the company could effectively react to a disruption

D is correct. Incident response plans are created to ensure that when an attack, virus, or some other type of disruption is experienced, the company can effectively and efficiently react and mitigate any potential damages. All the other answers may come true as a result of an incident response plan, but are not the core reason for developing this type of plan.

Which of the following NIST document is used specifically for risk management?

A) SP 800-53

B) SP 800-63

C) SP 800-30

D) SP 800-90

C is correct. NIST Special Publication 800-30 is the Risk Management Guide for Information Technology Systems.

Which of the following roles has the responsibility for implementing and maintaining firewalls?

A) Security supervisor

B) System owner

C) Data custodian

D) Security administrator

D is correct. Implementing and maintaining all security controls, whether network, software, or endpoint based, is the explicit role of the security administrator.

What is the best way to avoid introducing vulnerabilities such as injection, broken authentication, cross-site scripting (XSS), and insecure de-serialization?

A) Employ only secure integrated development environments (IDEs).

B) Avoid using open source libraries or frameworks.

C) Implement secure coding practices.

D) Perform rigorous quality assurance tests.

C is correct. Only a comprehensive approach of secure coding practices can avoid introducing the vulnerabilities listed in the question, which otherwise can be introduced regardless of the IDE

employed and regardless of whether the libraries and frameworks used are open source or proprietary, and commonly go undiscovered despite thorough quality assurance testing alone.

Who does the security auditor report to?

A) Data owners

B) Data custodians

C) External audit organization

D) Senior management

D is correct. The security auditor is responsible for reporting to senior management about the effectiveness of security controls and their compliance with security policy objectives.

Sensitive data is classified based upon all of the following factors, except:

A) Security policy

B) Amount of data

C) Age of data

D) Content of data

B is correct. The amount of data should have no bearing on whether or not it is deemed sensitive. The age of data is significant as it relates to the declassification process. The content of the data and the details of the security policy also dictate how data is classified.

Some organizations over-issue privileged access to ensure that users can have access to devices in emergency situations or unconventional scenarios. This practice violates what standard security principle?

A) Separation of duties

B) Job rotation

C) Least privilege

D) Due diligence

C is correct. Least privilege is a common security principle that dictates that all users should have the lowest access level necessary to do their job. Every user should be configured with the least possible permission to ensure high security throughout the organization.

Which best describes the IP protocol?

- Connectionless protocol that deals with dialog establishment, maintenance, and destruction
- **Connectionless protocol that deals with addressing and routing of packets**
- Connection-oriented protocol that deals with addressing and routing of packets
- Connection-oriented protocol that deals with sequencing, error detection, and flow control

B is correct. The IP protocol is connectionless and works at the network layer. It adds source and destination addresses to a packet as it goes through its data encapsulation process. IP can also make routing decisions based on the destination address.

A digital identity is made up of attributes, entitlements, and traits. Which of the following has the incorrect mapping when considering these identity characteristics?

A) Attributes = department, role in company, shift time, clearance type

B) Entitlements = resources available to user, authoritative rights in the company

C) Traits = biometric information, height, sex

D) None of the above

D is correct. A user's identity can be a collection of her attributes (department, role in company, shift time, clearance, and others), her entitlements (resources available to her, authoritative rights in the company, and so on) and her traits (biometric information, height, sex, and so forth). So if a user requests access to a database that contains sensitive employee information, an IdM (Identity Management) solution could need to pull together the necessary identity information and her supplied credentials before she is authorized access. If the user is a senior manager (attribute), with a Secret clearance (attribute), and has access to the database (entitlement)-she is granted the permissions Read and Write to certain records in the database Monday through Friday, 8 A.M. to 5 P.M. (attribute).

Which of the following statements is correct regarding the designated retention period for data?

A) Business documents (e.g., meeting minutes) must be retained for 7 years.

B) Invoices must be retained for 5 years

C) Requirements may vary, so consult an attorney.

D) There are no designated standards, only best practice.

C is correct. Laws regarding records retention exist and must be adhered to, but vary by jurisdiction. Consequently, legal counsel should be consulted to ensure compliance.

The _____is responsible for getting the alternate site into a working and functioning environment, and the _____is responsible for starting the recovery of the original site.

A) Restoration team, salvage team

B) Salvage team, restoration team

C) Recovery team, restoration team

D) Recovery team, salvage team

A is correct. The restoration team should be responsible for getting the alternate site into a working and functioning environment, and the salvage team should be responsible for starting the recovery of the original site.

Which of the following is not a form of identification?

A) Token device.

B) Fingerprint.

C) User ID.

D) Badge systems.

A is correct. Token devices are authenticating devices that are used in combination with an identification component, such as a user name. Fingerprints and user IDs are examples of identification components. Token devices commonly generate one-time passwords, which is one way to authenticate individuals.

The operating system performs all except which of the following tasks?

A) Memory allocation

B) Input and output tasks

C) Resource allocation

D) User access to database views

D is correct. The operating system has a long list of responsibilities, but implementing database views is not one of them. This is the responsibility of the database management software.

A critical company asset would most likely have which of the following MTD (maximum tolerable downtime) values?

A) Minutes to hours

B) Days

C) Weeks

D) Months

A is correct. According to NIST guidelines, a critical company asset would have a maximum tolerable downtime of a few minutes to hours.

Hiding messages within the text of this question would be considered what type of encryption method?

A) Steganography

B) Running key cipher

C) Concealment cipher

D) Frequency analysis

C is correct. Concealment ciphers disguise messages within the text or body of a message, such as using every other word in a sentence to form a different message. Steganography hides messages within the slack bits of pictures, music files, etc.

What is a pretext?

A) A false scenario presented to an employee by management with the intent to socially engineer the employee into better performance of their duties

B) Textual information designed to facilitate future instant messaging

C) A false scenario presented to an employee by an attacker with the intent to socially engineer the employee into violating security controls on the attacker's behalf

D) The banner information presented via a text-based protocol prior to the body of the message

C is correct. Pretexting is a social engineering technique designed to leverage an employee's trust relationships and usual work flows in order to convince them to do something that is both unusual and detrimental.

Isochronous processes rely on _____.

A) Time constraints

B) Content variables

C) Error checking

D) Malformed packets

A is correct. Isochronous processes must deliver data within set time constraints. Applications are typically video related where audio and video must match perfectly. VoIP is another example.

Alice needs to hire a third party to conduct a test of her company's security posture. If she needs an independent comparison against statutory requirements, which of the following services should she select?

A) Vulnerability assessment

B) Penetration test

C) Regulatory audit

D) DSS audit

C is correct. Audits against regulations are designed to determine the level of an organization's compliance. A PCI DSS audit is contractual, not regulatory, and is expected to ensure that a Qualified Security Assessor (QSA) deems a payment card processor is compliant with the Data Security Standard (DSS). Vulnerability assessments seek to exhaustively enumerate all possible vulnerabilities for prioritization of mitigation. Penetration tests are intended to demonstrate the viability of exploitation by an adversary.

When purchasing a biometric system, one of the considerations that should be reviewed is the processing speed. Which of the following best describes what it is meant by processing?

A) How long it takes to set up individual user accounts

B) The amount of time it takes to convert biometric data into a template on a smart card

C) When an individual provides identification and authentication information and the amount of time it takes to either be accepted or rejected

D) The amount of time and resources that are necessary to maintain a biometric system

C is correct. When reviewing biometric devices for purchase, one component to take into consideration is the length of time it takes to actually authenticate users. From the time a user inserts data until she receives an accept or reject response should take between 5-10 seconds.

What is the difference between a pharming attack and a phishing attack?

A) Pharming involves DNS poisoning and phishing involves social engineering.

B) Phishing involves DNS poisoning and pharming involves social engineering.

C) Pharming involves DNSSEC and phishing involves TOC\TOU.

D) Pharming involves DNSSEC and phishing involves social engineering.

A is correct. Phishing is a type of social engineering with the goal of obtaining personal information, credentials, credit card number, or financial data. The attackers lure, or fish, for sensitive data through various different methods. A similar type of attack is called pharming, which redirects a victim to a seemingly legitimate, yet fake, web site. In this type of attack, the attacker carries out something called DNS poisoning, in which a DNS server resolves a host name into an incorrect IP address.

Business continuity management means taking the necessary steps to increase a company's _____ to service disruption.

A) Resilience

B) Perceived reaction

C) Attitude

D) Means

A is correct. Business continuity management is the steps deployed to ensure that a company would be able to sustain a service disruption while minimizing the effect of the disruption on critical business functions.

What is the Network Time Protocol (NTP), and why is it important in security assessments?

A) It is a peer-to-peer protocol for system time synchronization, and it is important to ensure that peer systems' time-based authentication functions properly.

B) It is a client/server protocol for system time synchronization, and it is important to ensure that peer systems' time-based authentication functions properly.

C) It is a peer-to-peer protocol for system time synchronization, and it is important to ensure that system logs have timestamps that are consistent across all critical systems.

D) It is a client/server protocol for system time synchronization, and it is important to ensure that system logs have timestamps that are consistent across all critical systems.

D is correct. NTP provides a hierarchical architecture for client/server time synchronization, which is critical to ensure that logging activities performed by multiple disparate systems provide records with consistent timestamps. This is especially important when investigating incidents involving activities across multiple systems.

Which of the following is the best description of a “honeypot”?

A) It is a system that contains critical data that is attractive to an attacker.

B) It is a system developed to deceive an attacker into believing it is important.

C) It is a system that contains special tokens called “honeytokens.”

D) It is a system that “black holes” attacker activities in a way that they can’t spread.

B is correct. A honeypot is a system that serves no legitimate production services and contains no legitimate production data, and so should never be interacted with by internal users in any way. It is also not a preventive device. It exists only so that any interaction with it can be monitored, with the knowledge that all such interactions are illegitimate and indicate the presence of an adversary.

Which role is accountable for information security?

A) Information security professionals

B) Senior management

C) Security management

D) Security auditors

B is correct. Senior management is ultimately accountable for all organizational risk. As security is an organizational risk, senior management is ultimately accountable for information security.

McKenna performs the following data tasks: 1) Assigns data classification levels to meet her business unit’s specific needs. 2) Determines which users can access data. 3) Verifies security controls are in place and working correctly. Which of the following roles is McKenna performing?

A) Data custodian

B) Data user

C) Data owner

D) Process owner

C is correct. Data owners decide how data sets will be classified and protected, and ensure that the agreed-upon mechanisms are in place and working correctly. Data owners are typically department heads.

Alice, Bob, and many of their colleagues have spent months constructing a business continuity plan (BCP) for their enterprise. What is the first test of their findings that should be conducted?

A) Checklist test

B) Structured walk-through test

C) Simulation test

D) Parallel test

A is correct. A checklist test, or "desk check test," is done to ensure that nothing has been left out of the plan. A structured walk-through is a drill performed by representatives of each functional area to ensure that the recovery can actually be performed correctly. A simulation test seeks to emulate the performance of recovery steps in real time. A parallel test involves the actual operation of the alternate processing facilities in parallel with the primary site remaining online and functional.

Which of the following protocols is considered connection oriented?

A) IP

B) ICMP

C) UDP

D) TCP

D is correct. Transmission Control Protocol (TCP) is the only connection-oriented protocol listed. A connection-oriented protocol provides reliable connectivity and data transmission, while a connectionless protocol provides unreliable connections and does not promise or ensure data transmission.

Alice needs to hire a third party to conduct a test of her company's security posture. If she needs to determine whether and how an attacker could truly penetrate her company's defenses, which of the following services should she select?

A) Vulnerability assessment

B) Penetration test

C) Regulatory audit

D) DSS audit

B is correct. Penetration tests (pen-tests) are intended to demonstrate the viability of exploitation by an adversary. Unlike vulnerability assessments, pen tests are not intended to exhaustively enumerate all possible vulnerabilities for prioritization of mitigation. Audits against regulations are designed to determine the level of an organization's compliance. Likewise, a PCI DSS audit, which is contractual and not regulatory, is expected to ensure that a Qualified Security Assessor (QSA) deems a payment card processor is compliant with the Data Security Standard (DSS).

Bob is a hacker who intends to use social engineering strategies to infiltrate a former employer. After doing thorough research, he begins calling the customer service line to find the weakest representatives to attack. He calls over and over again trying to talk to many different representatives. What phase of this social engineering attack is Bob involved in?

A) Dumpster diving

B) Target selection

C) Intelligence gathering

D) Attack mode

B is correct. Bob has already completed the intelligence gathering phase and is now executing the target selection phase. By surfing through all the different customer service representatives, he is deciding which one will provide the easiest avenue for his exploit.

Business continuity and disaster recovery fall under which category of security control?

A) Preventive

B) Detective

C) Corrective

D) Compensating

D is correct. Business continuity and disaster recovery do not contribute directly to organizational security, but they can serve to compensate for security disasters by reducing the time it takes to respond to a security incident that interrupts business productivity.

Which method is the most certain way of ensuring that data cannot be recovered?

A) Deletion

B) Destruction

C) Degaussing

D) Declassifying

B is correct. Destruction of the physical medium is the surest way of ensuring that data cannot be recovered, regardless of the way it is stored.

What is the difference between disaster recovery and business continuity?

A) Disaster recovery deals with the actions that need to take place right after a disaster, and business continuity deals with the actions that need to take place to keep operations running over a longer period of time.

B) Business continuity deals with the actions that need to take place right after a disaster, and disaster recovery deals with the actions that need to take place to keep operations running over a longer period of time.

C) They are one and the same

D) Disaster recovery deals with operations, and business continuity deals with mitigating risks.

A is correct. Disaster recovery has the goal of minimizing the effects of a disaster and taking the necessary steps to ensure that the resources, personnel, and business processes are able to resume operation in a timely matter. This is different from business continuity planning, which deals with providing methods and procedures for dealing with longer-term outages and disasters and keeping the company in business.

The responsibility of the classification of data within an organization rests with whom?

A) Data custodians

B) Senior management

C) Data classifiers

D) Unit managers

B is correct. The senior management of an organization is ultimately responsible for the classification and proper handling of data assets.

California 1386, Sarbanes-Oxley, and HIPAA are examples of what kinds of security policy directives?

A) Regulatory

B) Administrative

C) Advisory

D) Informative

A is correct. Directives and mandates typically coming from outside the company from the government, legal, or industry authorities are called regulatory policy objectives. Administrative is not one of the three types of policies. Advisory policies address requirements for certain types of behaviors or activities among the workforce. Informative policies address educational awareness.