ISC CISSP

Certified Information Systems Security Professional

Version: 5.0

Topic 1, Security and Risk Management

QUESTION NO: 1

All of the following items should be included in a Business Impact Analysis (BIA) questionnaire EXCEPT questions that

A.
determine the risk of a business interruption occurring

B.
determine the technological dependence of the business processes

C.
identify the operational impacts of a business interruption

D.
identify the financial impacts of a business interruption

Answer: B
Reference:
https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&uact=8&ved=0ahUKEwjbktbTp-LaAhVIr48KHZuhB0UQFggmMAA&url=http%3A%2F%2Fwww.oregon.gov%2Fdas%2FProcurement%2FGuiddoc%2FBusImpAnalysQs.doc&usg=AOvVaw1wBxcnLP8ceI_yhv2rsI9h

QUESTION NO: 2

Which of the following actions will reduce risk to a laptop before traveling to a high risk area?

A.
Examine the device for physical tampering

B.
Implement more stringent baseline configurations

C.
Purge or re-image the hard disk drive

D.
Change access codes

Answer: B

Explanation:

QUESTION NO: 3

Which of the following represents the GREATEST risk to data confidentiality?

A.
Network redundancies are not implemented

B.
Security awareness training is not completed

C.
Backup tapes are generated unencrypted

D.
Users have administrative privileges

Answer: C

Explanation:

QUESTION NO: 4

What is the MOST important consideration from a data security perspective when an organization plans to relocate?

A.
Ensure the fire prevention and detection systems are sufficient to protect personnel

B.
Review the architectural plans to determine how many emergency exits are present

C.
Conduct a gap analysis of a new facilities against existing security requirements

D.
Revise the Disaster Recovery and Business Continuity (DR/BC) plan

Answer: C

Explanation:

QUESTION NO: 5

A company whose Information Technology (IT) services are being delivered from a Tier 4 data center, is preparing a companywide Business Continuity Planning (BCP). Which of the following failures should the IT manager be concerned with?

A.
Application

B.
Storage

C.
Power

D.
Network

Answer: C
Reference: https://www.colocationamerica.com/data-center/tier-standards-overview.htm

QUESTION NO: 6

When assessing an organization's security policy according to standards established by the International Organization for Standardization (ISO) 27001 and 27002, when can management responsibilities be defined?

A.
Only when assets are clearly defined

B.
Only when standards are defined

C.
Only when controls are put in place

D.

Only procedures are defined

Answer: A

Explanation:

QUESTION NO: 7

Which of the following types of technologies would be the MOST cost-effective method to provide a reactive control for protecting personnel in public areas?

A.
Install mantraps at the building entrances

B.
Enclose the personnel entry area with polycarbonate plastic

C.
Supply a duress alarm for personnel exposed to the public

D.
Hire a guard to protect the public area

Answer: C

Explanation:

QUESTION NO: 8

An important principle of defense in depth is that achieving information security requires a balanced focus on which PRIMARY elements?

A.
Development, testing, and deployment

B.
Prevention, detection, and remediation

C.
People, technology, and operations

D.

Certification, accreditation, and monitoring

Answer: C
Reference: https://www.giac.org/paper/gsec/3873/information-warfare-cyber-warfare-future-warfare/106165 (14)

QUESTION NO: 9

Intellectual property rights are PRIMARY concerned with which of the following?

A.
Owner's ability to realize financial gain

B.
Owner's ability to maintain copyright

C.
Right of the owner to enjoy their creation

D.
Right of the owner to control delivery method

Answer: A
Explanation:

QUESTION NO: 10

A control to protect from a Denial-of-Service (DoS) attach has been determined to stop 50% of attacks, and additionally reduces the impact of an attack by 50%. What is the residual risk?

A.
25%

B.
50%

C.
75%

D.
100%

Answer: A
Explanation:

QUESTION NO: 11

In the Open System Interconnection (OSI) model, which layer is responsible for the transmission of binary data over a communications network?

A.
Physical Layer

B.
Application Layer

C.
Data-Link Layer

D.
Network Layer

Answer: A
Explanation:

QUESTION NO: 12

What is the term commonly used to refer to a technique of authentication one machine to another by forging packets from a trusted source?

A.
Smurfing

B.
Man-in-the-Middle (MITM) attack

C.
Session redirect

D.
Spoofing

Answer: D
Explanation:

QUESTION NO: 13

Which of the following entails identification of data and links to business processes, applications, and data stores as well as assignment of ownership responsibilities?

A.
Security governance

B.
Risk management

C.
Security portfolio management

D.
Risk assessment

Answer: B
Explanation:

QUESTION NO: 14

Which of the following mandates the amount and complexity of security controls applied to a security risk?

A.
Security vulnerabilities

B.
Risk tolerance

C.
Risk mitigation

D.
Security staff

Answer: B

Explanation:

QUESTION NO: 15

When determining who can accept the risk associated with a vulnerability, which of the following is **MOST** important?

A.
Countermeasure effectiveness

B.
Type of potential loss

C.
Incident likelihood

D.
Information ownership

Answer: C

Explanation:

QUESTION NO: 16

A security professional determines that a number of outsourcing contracts inherited from a previous merger do not adhere to the current security requirements. Which of the following **BEST** minimizes the risk of this happening again?

A.
Define additional security controls directly after the merger

B.
Include a procurement officer in the merger team

C.

Verify all contracts before a merger occurs

D.
Assign a compliancy officer to review the merger conditions

Answer: D
Explanation:

QUESTION NO: 17

Which of the following is a direct monetary cost of a security incident?

A.
Morale

B.
Reputation

C.
Equipment

D.
Information

Answer: C
Explanation:

QUESTION NO: 18

Which of the following would **MINIMIZE** the ability of an attacker to exploit a buffer overflow?

A.
Memory review

B.
Code review

C.
Message division

D.
Buffer division

Answer: B
Explanation:

QUESTION NO: 19

Which of the following mechanisms will **BEST** prevent a Cross-Site Request Forgery (CSRF) attack?

A.
parameterized database queries

B.
whitelist input values

C.
synchronized session tokens

D.
use strong ciphers

Answer: C
Explanation:

QUESTION NO: 20

What is the PRIMARY purpose for an organization to conduct a security audit?

A.
To ensure the organization is adhering to a well-defined standard

B.
To ensure the organization is applying security controls to mitigate identified risks

C.
To ensure the organization is configuring information systems efficiently

D.

To ensure the organization is documenting findings

Answer: B

Explanation:

QUESTION NO: 21

How does security in a distributed file system using mutual authentication differ from file security in a multi-user host?

A.
Access control can rely on the Operating System (OS), but eavesdropping is not a risk

B.
Access control cannot rely on the Operating System (OS), and eavesdropping is a risk

C.
Access control can rely on the Operating System (OS), and eavesdropping is a risk

D.
Access control cannot rely on the Operating System (OS), and eavesdropping is not a risk

Answer: C

Explanation:

QUESTION NO: 22

When defining a set of security controls to mitigate a risk, which of the following actions MUST occur?

A.
Each control’s effectiveness must be evaluated individually

B.
Each control must completely mitigate the risk

C.
The control set must adequately mitigate the risk

D.

The control set must evenly divide the risk

Answer: C

Explanation:

QUESTION NO: 23

Which of the following provides the BEST method to verify that security baseline configurations are maintained?

A.
Perform regular system security testing

B.
Design security early in the development cycle

C.
Analyze logs to determine user activities

D.
Perform quarterly risk assessments

Answer: A

Explanation:

QUESTION NO: 24

Which of the following is the MOST critical success factor in the security patch management process?

A.
Tracking and reporting on inventory

B.
Supporting documentation

C.
Management review of reports

D.

Risk and impact analysis

Answer: D

Explanation:

QUESTION NO: 25

Which of the following is MOST important when determining appropriate countermeasures for an identified risk?

A.
Interaction with existing controls

B.
Organizational risk tolerance

C.
Patch availability

D.
Cost

Answer: B

Explanation:

QUESTION NO: 26

What is the MAIN reason to ensure the appropriate retention periods are enforced for data stored on electronic media?

A.
To reduce the carbon footprint by eliminating paper

B.
To create an inventory of data assets stored on disk for backup recovery

C.
To declassify information that has been improperly classified

D.

To reduce the risk of loss, unauthorized access, use, modification, and disclosure

Answer: D

Explanation:

QUESTION NO: 27

What is the MAIN objective of risk analysis in Disaster Recovery (DR) planning?

A.
Establish Maximum Tolerable Downtime (MTD) Information Systems (IS)

B.
Define the variable cost for extended downtime scenarios

C.
Identify potential threats to business availability

D.
Establish personnel requirements for various downtime scenarios

Answer: C

Explanation:

QUESTION NO: 28

A security professional is assessing the risk in an application and does not take into account any mitigating or compensating controls. This type of risk rating is an example of which of the following?

A.
Transferred risk

B.
Inherent risk

C.
Residual risk

D.

Avoided risk

Answer: B
Explanation:

Topic 2, Asset Security

QUESTION NO: 29

Which of the following is **MOST** important when assigning ownership of an asset to a department?

A.
The department should report to the business owner

B.
Ownership of the asset should be periodically reviewed

C.
Individual accountability should be ensured

D.
All members should be trained on their responsibilities

Answer: B
Explanation:

QUESTION NO: 30

Which one of the following affects the classification of data?

A.
Assigned security label

B.
Multilevel Security (MLS) architecture

C.
Minimum query size

D.
Passage of time

Answer: D
Explanation:

QUESTION NO: 31

Which of the following BEST describes the responsibilities of a data owner?

A.
Ensuring quality and validation through periodic audits for ongoing data integrity

B.
Maintaining fundamental data availability, including data storage and archiving

C.
Ensuring accessibility to appropriate users, maintaining appropriate levels of data security

D.
Determining the impact the information has on the mission of the organization

Answer: C
Reference: http://resources.infosecinstitute.com/category/certifications-training/cissp/domains/asset-security/data-and-system-ownership/#gref

QUESTION NO: 32

An organization has doubled in size due to a rapid market share increase. The size of the Information Technology (IT) staff has maintained pace with this growth. The organization hires several contractors whose onsite time is limited. The IT department has pushed its limits building servers and rolling out workstations and has a backlog of account management requests.

Which contract is BEST in offloading the task from the IT staff?

A.
Platform as a Service (PaaS)

B.
Identity as a Service (IDaaS)

C.
Desktop as a Service (DaaS)

D.
Software as a Service (SaaS)

Answer: B

Explanation:

QUESTION NO: 33

When implementing a data classification program, why is it important to avoid too much granularity?

A.
The process will require too many resources

B.
It will be difficult to apply to both hardware and software

C.
It will be difficult to assign ownership to the data

D.
The process will be perceived as having value

Answer: A
Reference: http://www.ittoday.info/AIMS/DSM/82-02-55.pdf

QUESTION NO: 34

In a data classification scheme, the data is owned by the

A.
system security managers

B.
business managers

C.
Information Technology (IT) managers

D.
end users

Answer: B

Explanation:

QUESTION NO: 35

Which of the following is an initial consideration when developing an information security management system?

A.
Identify the contractual security obligations that apply to the organizations

B.
Understand the value of the information assets

C.
Identify the level of residual risk that is tolerable to management

D.
Identify relevant legislative and regulatory compliance requirements

Answer: B

Explanation:

QUESTION NO: 36

Which of the following is an effective control in preventing electronic cloning of Radio Frequency Identification (RFID) based access cards?

A.
Personal Identity Verification (PIV)

B.
Cardholder Unique Identifier (CHUID) authentication

C.
Physical Access Control System (PACS) repeated attempt detection

D.
Asymmetric Card Authentication Key (CAK) challenge-response

Answer: D
Explanation:

QUESTION NO: 37

Which factors **MUST** be considered when classifying information and supporting assets for risk management, legal discovery, and compliance?

A.
System owner roles and responsibilities, data handling standards, storage and secure development lifecycle requirements

B.
Data stewardship roles, data handling and storage standards, data lifecycle requirements

C.
Compliance office roles and responsibilities, classified material handling standards, storage system lifecycle requirements

D.
System authorization roles and responsibilities, cloud computing standards, lifecycle requirements

Answer: A
Explanation:

QUESTION NO: 38

When network management is outsourced to third parties, which of the following is the **MOST** effective method of protecting critical data assets?

A.
Log all activities associated with sensitive systems

B.
Provide links to security policies

C.
Confirm that confidentially agreements are signed

D.
Employ strong access controls

Answer: D
Explanation:

QUESTION NO: 39

Which of the following is the **MOST** appropriate action when reusing media that contains sensitive data?

A.
Erase

B.
Sanitize

C.
Encrypt

D.
Degauss

Answer: B
Explanation:

QUESTION NO: 40

An organization recently conducted a review of the security of its network applications. One of the vulnerabilities found was that the session key used in encrypting sensitive information to a third party server had been hard-coded in the client and server applications. Which of the following

would be **MOST** effective in mitigating this vulnerability?

A.
Diffle-Hellman (DH) algorithm

B.
Elliptic Curve Cryptography (ECC) algorithm

C.
Digital Signature algorithm (DSA)

D.
Rivest-Shamir-Adleman (RSA) algorithm

Answer: A
Explanation:

QUESTION NO: 41

Which of the following methods of suppressing a fire is environmentally friendly and the **MOST** appropriate for a data center?

A.
Inert gas fire suppression system

B.
Halon gas fire suppression system

C.
Dry-pipe sprinklers

D.
Wet-pipe sprinklers

Answer: A
Explanation:

QUESTION NO: 42

Unused space in a disk cluster is important in media analysis because it may contain which of the

following?

A.
Residual data that has not been overwritten

B.
Hidden viruses and Trojan horses

C.
Information about the File Allocation table (FAT)

D.
Information about patches and upgrades to the system

Answer: A
Explanation:

QUESTION NO: 43

A company seizes a mobile device suspected of being used in committing fraud. What would be the **BEST** method used by a forensic examiner to isolate the powered-on device from the network and preserve the evidence?

A.
Put the device in airplane mode

B.
Suspend the account with the telecommunication provider

C.
Remove the SIM card

D.
Turn the device off

Answer: A
Explanation:

QUESTION NO: 44

Which of the following is **MOST** appropriate for protecting confidentially of data stored on a hard drive?

A.
Triple Data Encryption Standard (3DES)

B.
Advanced Encryption Standard (AES)

C.
Message Digest 5 (MD5)

D.
Secure Hash Algorithm 2 (SHA-2)

Answer: B

Explanation:

QUESTION NO: 45

Which of the following is the **MOST** effective method to mitigate Cross-Site Scripting (XSS) attacks?

A.
Use Software as a Service (SaaS)

B.
Whitelist input validation

C.
Require client certificates

D.
Validate data output

Answer: B

Explanation:

QUESTION NO: 46

What is the **MOST** significant benefit of an application upgrade that replaces randomly generated session keys with certificate based encryption for communications with backend servers?

A.
Non-repudiation

B.
Efficiency

C.
Confidentially

D.
Privacy

Answer: A

Explanation:

QUESTION NO: 47

A user has infected a computer with malware by connecting a Universal Serial Bus (USB) storage device.

Which of the following is **MOST** effective to mitigate future infections?

A.
Develop a written organizational policy prohibiting unauthorized USB devices

B.
Train users on the dangers of transferring data in USB devices

C.
Implement centralized technical control of USB port connections

D.
Encrypt removable USB devices containing data at rest

Answer: C

Explanation:

QUESTION NO: 48

An organization has a short-term agreement with a public Cloud Service Provider (CSP). Which of the following BEST protects sensitive data once the agreement expires and the assets are reused?

A.
Recommend that the business data owners use continuous monitoring and analysis of applications to prevent data loss

B.
Recommend that the business data owners use internal encryption keys for data-at-rest and data-in-transit to the storage environment

C.
Use a contractual agreement to ensure the CSP wipes and data from the storage environment

D.
Use a National Institute of Standards and Technology (NIST) recommendation for wiping data on the storage environment

Answer: D

Explanation:

QUESTION NO: 49

The MAIN task of promoting security for Personal Computers (PC) is:

A.
understanding the technical controls and ensuring they are correctly installed

B.
understanding the required systems and patching processes for different Operating Systems (OS)

C.
making sure that users are using only valid, authorized software, so that the chance of virus infection is reduced

D.
making users understand the risks to the machines and data, so they will take appropriate steps to protect them

Answer: A

Explanation:

QUESTION NO: 50

The personal laptop of an organization executive is stolen from the office, complete with personnel and project records. Which of the following should be done FIRST to mitigate future occurrences?

A.
Encrypt disks on personal laptops

B.
Issue cable locks for use on personal laptops

C.
Create policies addressing critical information on personal laptops

D.
Monitor personal laptops for critical information

Answer: A
Explanation:

QUESTION NO: 51

Which one of the following can be used to detect an anomaly in a system by keeping track of the state of files that do not normally change?

A.
System logs

B.
Anti-spyware

C.
Integrity checker

D.
Firewall logs

Answer: C

Explanation:

QUESTION NO: 52

Which attack defines a piece of code that is inserted into software to trigger a malicious function?

A.
Phishing

B.
Salami

C.
Back door

D.
Logic bomb

Answer: D
Explanation:

QUESTION NO: 53

Data remanence is the biggest threat in which of the following scenarios?

A.
A physical disk drive has been overwritten and reused within a datacenter

B.
A physical disk drive has been degaussed, verified, and released to a third party for destruction

C.
A flash drive has been overwritten, verified, and reused within a datacenter

D.
A flash drive has been overwritten and released to a third party for destruction

Answer: A
Explanation:

QUESTION NO: 54

Which of the following is used to ensure that data mining activities will NOT reveal sensitive data?

A.
Implement two-factor authentication on the underlying infrastructure

B.
Encrypt data at the field level and tightly control encryption keys

C.
Preprocess the databases to see if information can be disclosed from the learned patterns

D.
Implement the principle of least privilege on data elements so a reduced number of users can access the database

Answer: B
Explanation:

QUESTION NO: 55

How long should the records on a project be retained?

A.
For the duration of the project, or at the discretion of the record owner

B.
Until they are no longer useful or required by policy

C.
Until five years after the project ends, then move to archives

D.
For the duration of the organization fiscal year

Answer: B
Explanation:

QUESTION NO: 56

Which of the following is the MOST effective countermeasure against data remanence?

A.
Destruction

B.
Clearing

C.
Purging

D.
Encryption

Answer: A

Explanation:

QUESTION NO: 57

The application owner of a system that handles confidential data leaves an organization. It is anticipated that a replacement will be hired in approximately six months. During that time, which of the following should the organization do?

A.
Grant temporary access to the former application owner’s account

B.
Assign a temporary application owner to the system

C.
Restrict access to the system until a replacement application owner is hired

D.
Prevent changes to the confidential data until a replacement application owner is hired

Answer: C

Explanation:

QUESTION NO: 58

Assume that a computer was powered off when an information security professional arrived at a crime scene. Which of the following actions should be performed after the crime scene is isolated?

A.
Turn the computer on and collect volatile data

B.
Turn the computer on and collect network information

C.
Leave the computer off and prepare the computer for transportation to the laboratory

D.
Remove the hard drive, prepare it for transportation, and leave the hardware at the scene

Answer: C
Explanation:

QUESTION NO: 59

Which of the following is a MAJOR concern when there is a need to preserve or retain information for future retrieval?

A.
Laws and regulations may change in the interim, making it unnecessary to retain the information

B.
The expense of retaining the information could become untenable for the organization

C.
The organization may lose track of the information and not dispose of it securely

D.
The technology needed to retrieve the information may not be available in the future

Answer: C
Explanation:

QUESTION NO: 60

Which of the following is the BEST way to protect against Structured Query Language (SQL) injection?

A.
Enforce boundary checking

B.
Restrict use of SELECT command

C.
Restrict HyperText Markup Language (HTML) source code access

D.
Use stored procedures

Answer: D

Explanation:

QUESTION NO: 61

What is a common mistake in records retention?

A.
Adopting a retention policy with the longest requirement period

B.
Having the Human Resource (HR) department create a retention policy

C.
Adopting a retention policy based on applicable organization requirements

D.
Having the organization legal department create a retention policy

Answer: A

Explanation:

QUESTION NO: 62

Of the following, which BEST provides non-repudiation with regards to access to a server room?

A.
Fob and Personal Identification Number (PIN)

B.
Locked and secured cages

C.
Biometric readers

D.
Proximity readers

Answer: B

Explanation:

QUESTION NO: 63

What should an auditor do when conducting a periodic audit on media retention?

A.
Check electronic storage media to ensure records are not retained past their destruction date

B.
Ensure authorized personnel are in possession of paper copies containing Personally Identifiable Information (PII)

C.
Check that hard disks containing backup data that are still within a retention cycle are being destroyed correctly

D.
Ensure that data shared with outside organizations is no longer on a retention schedule

Answer: A

Explanation:

QUESTION NO: 64

How should the retention period for an organization's social media content be defined?

A.
By the retention policies of each social media service

B.
By the records retention policy of the organization

C.
By the Chief Information Officer (CIO)

D.
By the amount of available storage space

Answer: B

Explanation:

QUESTION NO: 65

What is the FIRST step required in establishing a records retention program?

A.
Classify records based on sensitivity

B.
Identify and inventory all records storage locations

C.
Identify and inventory all records

D.
Draft a records retention policy

Answer: D

Explanation:

QUESTION NO: 66

An organization is considering outsourcing applications and data to a Cloud Service Provider (CSP). Which of the following is the MOST important concern regarding privacy?

A.
The CSP determines data criticality

B.
The CSP provides end-to-end encryption services

C.
The CSP's privacy policy may be developed by the organization

D.
The CSP may not be subject to the organization's country legislation

Answer: D
Explanation:

QUESTION NO: 67

Which of the following will help prevent improper session handling?

A.
Ensure JavaScript and plugin support is disabled

B.
Ensure that certificates are valid and fail closed

C.
Ensure that tokens are sufficiently long, complex, and pseudo-random

D.
Ensure that all UIWebView calls do not execute without proper input validation

Answer: C
Explanation:

QUESTION NO: 68

Which of the following is the BEST defense against password guessing?

A.
Limit external connections to the network

B.
Disable the account after a limited number of unsuccessful attempts

C.
Force the password to be changed after an invalid password has been entered

D.
Require a combination of letters, numbers, and special characters in the password

Answer: B
Explanation:

QUESTION NO: 69

Which of the following is the MOST secure password technique?

A.
Passphrase

B.
One-time password

C.
Cognitive password

D.
Cipthertext

Answer: B
Explanation:

QUESTION NO: 70

To prevent inadvertent disclosure of restricted information, which of the following would be the LEAST effective process for eliminating data prior to the media being discarded?

A.
Multiple-pass overwriting

B.

Degaussing

C.
High-level formatting

D.
Physical destruction

Answer: C
Explanation:

QUESTION NO: 71

An organization has implemented a new backup process which protects confidential data by encrypting the information stored on backup tapes. Which of the following is a MAJOR data confidentiality concern after the implementation of this new backup process?

A.
Tape backup rotation

B.
Pre-existing backup tapes

C.
Tape backup compression

D.
Backup tape storage location

Answer: B
Explanation:

QUESTION NO: 72

Which of the following objects should be removed FIRST prior to uploading code to public code repositories?

A.
Security credentials

B.
Inefficient algorithms

C.
Coding mistakes

D.
Known vulnerabilities

Answer: A
Explanation:

QUESTION NO: 73

Which media sanitization methods should be used for data with a high security categorization?

A.
Clear or destroy

B.
Clear or purge

C.
Destroy or delete

D.
Purge or destroy

Answer: D
Explanation:

QUESTION NO: 74

How is it possible to extract private keys securely stored on a cryptographic smartcard?

A.
Bluebugging

B.
Focused ion-beam

C.
Bluejacking

D.
Power analysis

Answer: A
Explanation:

QUESTION NO: 75

Which inherent password weakness does a One Time Password (OTP) generator overcome?

A.
Static passwords are too predictable

B.
Static passwords must be changed frequently

C.
Static passwords are difficult to generate

D.
Static passwords are easily disclosed

Answer: D
Explanation:

QUESTION NO: 76

Digital non-repudiation requires which of the following?

A.
A trusted third-party

B.
Appropriate corporate policies

C.
Symmetric encryption

D.
Multifunction access cards

Answer: A
Explanation:

Topic 3, Security Architecture and Engineering

QUESTION NO: 77

Which security service is served by the process of encryption plaintext with the sender's private key and decrypting cipher text with the sender's public key?

A.
Confidentiality

B.
Integrity

C.
Identification

D.
Availability

Answer: C
Explanation:

Only the person having correspondent private key can encrypt the plaintext decrypted (verified) by the public key, so proper identification of the endpoints are maintained.

QUESTION NO: 78

Which of the following mobile code security models relies only on trust?

A.
Code signing

B.
Class authentication

C.
Sandboxing

D.
Type safety

Answer: A
Reference: https://csrc.nist.gov/csrc/media/publications/conference-paper/1999/10/21/proceedings-of-the-22nd-nissc-1999/documents/papers/t09.pdf (11)

QUESTION NO: 79

Which technique can be used to make an encryption scheme more resistant to a known plaintext attack?

A.
Hashing the data before encryption

B.
Hashing the data after encryption

C.
Compressing the data after encryption

D.
Compressing the data before encryption

Answer: D
Explanation:

QUESTION NO: 80

What is the second phase of Public Key Infrastructure (PKI) key/certificate life-cycle management?

A.

Implementation Phase

B.
Initialization Phase

C.
Cancellation Phase

D.
Issued Phase

Answer: D
Explanation:

QUESTION NO: 81

Which component of the Security Content Automation Protocol (SCAP) specification contains the data required to estimate the severity of vulnerabilities identified automated vulnerability assessments?

A.
Common Vulnerabilities and Exposures (CVE)

B.
Common Vulnerability Scoring System (CVSS)

C.
Asset Reporting Format (ARF)

D.
Open Vulnerability and Assessment Language (OVAL)

Answer: B
Explanation:

QUESTION NO: 82

Who in the organization is accountable for classification of data information assets?

A.

Data owner

B.
Data architect

C.
Chief Information Security Officer (CISO)

D.
Chief Information Officer (CIO)

Answer: A
Explanation:

QUESTION NO: 83

The use of private and public encryption keys is fundamental in the implementation of which of the following?

A.
Diffie-Hellman algorithm

B.
Secure Sockets Layer (SSL)

C.
Advanced Encryption Standard (AES)

D.
Message Digest 5 (MD5)

Answer: A
Explanation:

QUESTION NO: 84

Which of the following **MUST** be in place to recognize a system attack?

A.
Stateful firewall

B.
Distributed antivirus

C.
Log analysis

D.
Passive honeypot

Answer: C
Explanation:

QUESTION NO: 85

Which of the following is the **GREATEST** benefit of implementing a Role Based Access Control (RBAC) system?

A.
Integration using Lightweight Directory Access Protocol (LDAP)

B.
Form-based user registration process

C.
Integration with the organizations Human Resources (HR) system

D.
A considerably simpler provisioning process

Answer: D
Explanation:

QUESTION NO: 86

Which Identity and Access Management (IAM) process can be used to maintain the principle of least privilege?

A.
identity provisioning

B.
access recovery

C.
multi-factor authentication (MFA)

D.
user access review

Answer: A
Explanation:

QUESTION NO: 87

A **minima**l implementation of endpoint security includes which of the following?

A.
Trusted platforms

B.
Host-based firewalls

C.
Token-based authentication

D.
Wireless Access Points (AP)

Answer: B
Explanation:

QUESTION NO: 88

What is the expected outcome of security awareness in support of a security awareness program?

A.
Awareness activities should be used to focus on security concerns and respond to those concerns accordingly

B.

Awareness is not an activity or part of the training but rather a state of persistence to support the program

C.
Awareness is training. The purpose of awareness presentations is to broaden attention of security.

D.
Awareness is not training. The purpose of awareness presentation is simply to focus attention on security.

Answer: D

Explanation:

QUESTION NO: 89

Which security modes is **MOST** commonly used in a commercial environment because it protects the integrity of financial and accounting data?

A.
Biba

B.
Graham-Denning

C.
Clark-Wilson

D.
Beil-LaPadula

Answer: C

Explanation:

QUESTION NO: 90

Why is planning in Disaster Recovery (DR) an interactive process?

A.
It details off-site storage plans

B.
It identifies omissions in the plan

C.
It defines the objectives of the plan

D.
It forms part of the awareness process

Answer: B
Explanation:

QUESTION NO: 91

Mandatory Access Controls (MAC) are based on:

A.
security classification and security clearance

B.
data segmentation and data classification

C.
data labels and user access permissions

D.
user roles and data encryption

Answer: A
Explanation:

QUESTION NO: 92

In Disaster Recovery (DR) and Business Continuity (DC) training, which **BEST** describes a functional drill?

A.
a functional evacuation of personnel

B.

a specific test by response teams of individual emergency response functions

C.
an activation of the backup site

D.
a full-scale simulation of an emergency and the subsequent response functions.

Answer: D
Explanation:

QUESTION NO: 93

What is the foundation of cryptographic functions?

A.
Encryption

B.
Cipher

C.
Hash

D.
Entropy

Answer: B
Explanation:

QUESTION NO: 94

Which of the following methods protects Personally Identifiable Information (PII) by use of a full replacement of the data element?

A.
Data tokenization

B.
Volume encryption

C.
Transparent Data Encryption (TDE)

D.
Column level database encryption

Answer: A
Explanation:

QUESTION NO: 95

The organization would like to deploy an authorization mechanism for an Information Technology (IT) infrastructure project with high employee turnover.

Which access control mechanism would be preferred?

A.
Attribute Based Access Control (ABAC)

B.
Discretionary Access Control (DAC)

C.
Mandatory Access Control (MAC)

D.
Role-Based Access Control (RBAC)

Answer: D
Explanation:

QUESTION NO: 96

Which of the following management process allows **ONLY** those services required for users to accomplish their tasks, change default user passwords, and set servers to retrieve antivirus updates?

A.
Configuration

B.
Identity

C.
Compliance

D.
Patch

Answer: A
Explanation:

QUESTION NO: 97

Which security access policy contains fixed security attributes that are used by the system to determine a user's access to a file or object?

A.
Mandatory Access Control (MAC)

B.
Access Control List (ACL)

C.
Discretionary Access Control (DAC)

D.
Authorized user control

Answer: A
Explanation:

QUESTION NO: 98

Which of the following is a common characteristic of privacy?

A.
Provision for maintaining an audit trail of access to the private data

B.

Notice to the subject of the existence of a database containing relevant credit card data

C.
Process for the subject to inspect and correct personal data on-site

D.
Database requirements for integration of privacy data

Answer: A
Explanation:

QUESTION NO: 99

At a **MINIMUM**, audits of permissions to individual or group accounts should be scheduled

A.
annually

B.
to correspond with staff promotions

C.
to correspond with terminations

D.
continually

Answer: A
Explanation:

QUESTION NO: 100

Which of the following **MUST** be part of a contract to support electronic discovery of data stored in a cloud environment?

A.
identification of data location

B.
integration with organizational directory services for authentication

C.
accommodation of hybrid deployment models

D.
tokenization of data

Answer: A
Explanation:

QUESTION NO: 101

Which of the following is part of a Trusted Platform Module (TPM)?

A.
A non-volatile tamper-resistant storage for storing both data and signing keys in a secure fashion

B.
A protected Pre-Basic Input/Output System (BIOS) which specifies a method or a metric for “measuring" the state of a computing platform

C.
A secure processor targeted at managing digital keys and accelerating digital signing

D.
A platform-independent software interface for accessing computer functions

Answer: A
Explanation:

QUESTION NO: 102

In a change-controlled environment, which of the following is **MOST** likely to lead to unauthorized changes to production programs?

A.
Modifying source code without approval

B.
Promoting programs to production without approval

C.
Developers checking out source code without approval

D.
Developers using Rapid Application Development (RAD) methodologies without approval

Answer: B
Explanation:

QUESTION NO: 103

Which of the following combinations would **MOST** negatively affect availability?

A.
Denial of Service (DoS) attacks and outdated hardware

B.
Unauthorized transactions and outdated hardware

C.
Fire and accidental changes to data

D.
Unauthorized transactions and denial of service attacks

Answer: A
Explanation:

QUESTION NO: 104

Which of the following could be considered the **MOST** significant security challenge when adopting DevOps practices compared to a more traditional control framework?

A.
Achieving Service Level Agreements (SLA) on how quickly patches will be released when a security flaw is found.

B.
Maintaining segregation of duties.

C.
Standardized configurations for logging, alerting, and security metrics.

D.
Availability of security teams at the end of design process to perform last-minute manual audits and reviews.

Answer: B

Explanation:

QUESTION NO: 105

A security compliance manager of a large enterprise wants to reduce the time it takes to perform network, system, and application security compliance audits while increasing quality and effectiveness of the results.

What should be implemented to **BEST** achieve the desired results?

A.
Configuration Management Database (CMDB)

B.
Source code repository

C.
Configuration Management Plan (CMP)

D.
System performance monitoring application

Answer: A

Explanation:

QUESTION NO: 106

Which of the following is a characteristic of an internal audit?

A.
An internal audit is typically shorter in duration than an external audit.

B.
The internal audit schedule is published to the organization well in advance.

C.
The internal auditor reports to the Information Technology (IT) department

D.
Management is responsible for reading and acting upon the internal audit results

Answer: D
Explanation:

QUESTION NO: 107

Which of the following is a responsibility of a data steward?

A.
Ensure alignment of the data governance effort to the organization.

B.
Conduct data governance interviews with the organization.

C.
Document data governance requirements.

D.
Ensure that data decisions and impacts are communicated to the organization.

Answer: A
Explanation:

QUESTION NO: 108

Which security approach will **BEST** minimize Personally Identifiable Information (PII) loss from a data breach?

A.
End-to-end data encryption for data in transit

B.

Continuous monitoring of potential vulnerabilities

C.
A strong breach notification process

D.
Limited collection of individuals' confidential data

Answer: D
Explanation:

QUESTION NO: 109

What is the **MAIN** goal of information security awareness and training?

A.
To inform users of the latest malware threats

B.
To inform users of information assurance responsibilities

C.
To comply with the organization information security policy

D.
To prepare students for certification

Answer: B
Explanation:

QUESTION NO: 110

Sensitive customer data is going to be added to a database. What is the **MOST** effective implementation for ensuring data privacy?

A.
Mandatory Access Control (MAC) procedures

B.
Discretionary Access Control (DAC) procedures

C.
Segregation of duties

D.
Data link encryption

Answer: A
Explanation:

QUESTION NO: 111

Proven application security principles include which of the following?

A.
Minimizing attack surface area

B.
Hardening the network perimeter

C.
Accepting infrastructure security controls

D.
Developing independent modules

Answer: A
Explanation:

QUESTION NO: 112

When developing a business case for updating a security program, the security program owner **MUST** do which of the following?

A.
Identify relevant metrics

B.
Prepare performance test reports

C.

Obtain resources for the security program

D.
Interview executive management

Answer: A
Explanation:

QUESTION NO: 113

From a security perspective, which of the following assumptions **MUST** be made about input to an application?

A.
It is tested

B.
It is logged

C.
It is verified

D.
It is untrusted

Answer: D
Explanation:

QUESTION NO: 114

Which of the following is the **BEST** reason for writing an information security policy?

A.
To support information security governance

B.
To reduce the number of audit findings

C.
To deter attackers

D.
To implement effective information security controls

Answer: A
Explanation:

QUESTION NO: 115

What is the **PRIMARY** goal of fault tolerance?

A.
Elimination of single point of failure

B.
Isolation using a sandbox

C.
Single point of repair

D.
Containment to prevent propagation

Answer: A
Explanation:

QUESTION NO: 116

Which of the **BEST** internationally recognized standard for evaluating security products and systems?

A.
Payment Card Industry Data Security Standards (PCI-DSS)

B.
Common Criteria (CC)

C.
Health Insurance Portability and Accountability Act (HIPAA)

D.

Sarbanes-Oxley (SOX)

Answer: B

Explanation:

QUESTION NO: 117

Which one of the following data integrity models assumes a lattice of integrity levels?

A.
Take-Grant

B.
Biba

C.
Harrison-Ruzzo

D.
Bell-LaPadula

Answer: B

Explanation:

QUESTION NO: 118

Even though a particular digital watermark is difficult to detect, which of the following represents a way it might still be inadvertently removed?

A.
Truncating parts of the data

B.
Applying Access Control Lists (ACL) to the data

C.
Appending non-watermarked data to watermarked data

D.
Storing the data in a database

Answer: A

Explanation:

QUESTION NO: 119

Which of the following is the BEST way to mitigate circumvention of access controls?

A.
Multi-layer access controls working in isolation

B.
Multi-vendor approach to technology implementation

C.
Multi-layer firewall architecture with Internet Protocol (IP) filtering enabled

D.
Multi-layer access controls with diversification of technologies

Answer: D

Explanation:

QUESTION NO: 120

When are security requirements the LEAST expensive to implement?

A.
When identified by external consultants

B.
During the application rollout phase

C.
During each phase of the project cycle

D.
When built into application design

Answer: D

Explanation:

QUESTION NO: 121

Which of the following attributes could be used to describe a protection mechanism of an open design methodology?

A.
It exposes the design to vulnerabilities and malicious attacks

B.
It can facilitate independent confirmation of the design security

C.
It can facilitate blackbox penetration testing

D.
It must be tamperproof to protect it from malicious attacks

Answer: D

Explanation:

QUESTION NO: 122

What is the BEST approach for maintaining ethics when a security professional is unfamiliar with the culture of a country and is asked to perform a questionable task?

A.
Exercise due diligence when deciding to circumvent host government requests

B.
Become familiar with the means in which the code of ethics is applied and considered

C.
Complete the assignment based on the customer's wishes

D.
Execute according to the professional's comfort level with the code of ethics

Answer: B

Explanation:

QUESTION NO: 123

What does the term “100-year floodplain" mean to emergency preparedness officials?

A.
The odds of a flood at this level are 1 in 100 in any given year

B.
The area is expected to be safe from flooding for at least 100 years

C.
The last flood of any kind to hit the area was more than 100 years ago

D.
The odds are that the next significant flood will hit within the next 100 years

Answer: A
Explanation:

QUESTION NO: 124

Which one of the following documentation should be included in a Disaster Recovery (DR) package?

A.
Source code, compiled code, firmware updates, operational log book and manuals

B.
Data encrypted in original format, auditable transaction data, and recovery instructions tailored for future extraction on demand

C.
Hardware configuration instructions, hardware configuration software, an operating system image, a data restoration option, media retrieval instructions, and contact information

D.
System configuration including hardware, software hardware interfaces, software Application Programming Interface (API) configuration, data structure, and transaction data from the previous

period

Answer: C
Explanation:

QUESTION NO: 125

An organization is designing a large enterprise-wide document repository system. They plan to have several different classification level areas with increasing levels of controls. The BEST way to ensure document confidentiality in the repository is to:

A.
encrypt the contents of the repository and document any exceptions to that requirement

B.
utilize Intrusion Detection System (IDS) set drop connections if too many requests for documents are detected

C.
keep individuals with access to high security areas from saving those documents into lower security areas

D.
require individuals with access to the system to sign Non-Disclosure Agreements (NDA)

Answer: C
Explanation:

QUESTION NO: 126

Which of the following MUST be considered when developing business rules for a data loss prevention (DLP) solution?

A.
Data availability

B.
Data sensitivity

C.
Data ownership

D.
Data integrity

Answer: B
Explanation:

QUESTION NO: 127

Which of the following is an important requirement when designing a secure remote access system?

A.
Configure a Demilitarized Zone (DMZ) to ensure that user and service traffic is separated

B.
Provide privileged access rights to computer files and systems

C.
Ensure that logging and audit controls are included

D.
Reduce administrative overhead through password self service

Answer: C
Explanation:

QUESTION NO: 128

What is the FIRST step in establishing an information security program?

A.
Identify critical security infrastructure

B.
Establish baseline security controls

C.

Establish an information security policy

D.
Identify factors affecting information security

Answer: A
Explanation:

QUESTION NO: 129

What does the result of Cost-Benefit Analysis (CBA) on new security initiatives provide?

A.
Quantifiable justification

B.
Baseline improvement

C.
Risk evaluation

D.
Formalized acceptance

Answer: A
Explanation:

QUESTION NO: 130

In a large company, a system administrator needs to assign users access to files using Role Based Access Control (RBAC). Which option is an example of RBAC?

A.
Allowing users access to files based on their group membership

B.
Allowing users access to files based on username

C.
Allowing users access to files based on the users location at time of access

D.
Allowing users access to files based on the file type

Answer: A
Explanation:

QUESTION NO: 131

Which of the following access control models is MOST restrictive?

A.
Discretionary Access Control (DAC)

B.
Mandatory Access Control (MAC)

C.
Role Based Access Control (RBAC)

D.
Rule based access control

Answer: B
Explanation:

QUESTION NO: 132

Which of the following is a security weakness in the evaluation of Common Criteria (CC) products?

A.
The manufacturer can state what configuration of the product is to be evaluated

B.
The product can be evaluated by labs in other countries

C.
The Target of Evaluation’s (TOE) testing environment is identical to the operating environment

D.
The evaluations are expensive and time-consuming to perform

Answer: A

Explanation:

QUESTION NO: 133

Which of the following is a canon of the (ISC)2 Code of Ethics?

A.
Integrity first, association before self, and excellence in all we do

B.
Perform all professional activities and duties in accordance with all applicable laws and the highest ethical standards

C.
Provide diligent and competent service to principals

D.
Cooperate with others in the interchange of knowledge and ideas for mutual security

Answer: C

Explanation:

QUESTION NO: 134

In the Common Criteria (CC) for Information Technology (IT) security evaluation, increasing Evaluation Assurance Levels (EAL) results in which of the following?

A.
Increase in evaluated systems

B.
Increased interoperability

C.
Increased functionality

D.
Increase in resource requirement

Answer: A

Explanation:

QUESTION NO: 135

To control the scope of a Business Continuity Management (BCM) system, a security practitioner should identify which of the following?

A.
Size, nature, and complexity of the organization

B.
Business needs of the security organization

C.
All possible risks

D.
Adaptation model for future recovery planning

Answer: A

Explanation:

QUESTION NO: 136

When dealing with shared, privileged accounts, especially those for emergencies, what is the BEST way to assure non-repudiation of logs?

A.
Implement a password vaulting solution

B.
Lock passwords in tamperproof envelopes in a safe

C.
Regularly change the passwords

D.
Implement a strict access control policy

Answer: D
Explanation:

QUESTION NO: 137

Which of the following is a characteristic of a challenge/response authentication process?

A.
Using a password history blacklist

B.
Requiring the use of non-consecutive numeric characters

C.
Presenting distorted graphics of text for authentication

D.
Transmitting a hash based on the user's password

Answer: D
Explanation:

QUESTION NO: 138

Which of the following models uses unique groups contained in unique conflict classes?

A.
Chinese Wall

B.
Bell-LaPadula

C.
Clark-Wilson

D.
Biba

Answer: B

Explanation:

QUESTION NO: 139

Which of the following threats exists with an implementation of digital signatures?

A.
Spoofing

B.
Substitution

C.
Eavesdropping

D.
Content tampering

Answer: C

Explanation:

QUESTION NO: 140

Why should Open Web Application Security Project (OWASP) Application Security Verification Standards (ASVS) Level 1 be considered a MINIMUM level of protection for any web application?

A.
Most regulatory bodies consider ASVS Level 1 as a baseline set of controls for applications

B.
Securing applications at ASVS Level 1 provides adequate protection for sensitive data

C.
ASVS Level 1 ensures that applications are invulnerable to OWASP top 10 threats

D.
Opportunistic attackers will look for any easily exploitable vulnerable applications

Answer: D

Explanation:

QUESTION NO: 141

The Structured Query Language (SQL) implements Discretionary Access Controls (DAC) using:

A.
INSERT and DELETE

B.
GRANT and REVOKE

C.
PUBLIC and PRIVATE

D.
ROLLBACK and TERMINATE

Answer: B

Explanation:

QUESTION NO: 142

In what phase of the System Development Life Cycle (SDLC) should security training for the development team begin?

A.
Development/Acquisition

B.
Initiation

C.
Implementation/Assessment

D.
Disposal

Answer: A

Explanation:

QUESTION NO: 143

What is the PRIMARY purpose of auditing, as it relates to the security review cycle?

A.
To ensure the organization's controls and policies are working as intended

B.
To ensure the organization can still be publicly traded

C.
To ensure the organization's executive team won't be sued

D.
To ensure the organization meets contractual requirements

Answer: A
Explanation:

Topic 4, Communication and Network Security

QUESTION NO: 144

What is the purpose of an Internet Protocol (IP) spoofing attack?

A.
To send excessive amounts of data to a process, making it unpredictable

B.
To intercept network traffic without authorization

C.
To disguise the destination address from a target's IP filtering devices

D.
To convince a system that it is communicating with a known entity

Answer: D

Explanation:

QUESTION NO: 145

At what level of the Open System Interconnection (OSI) model is data at rest on a Storage Area Network (SAN) located?

A.
Link layer

B.
Physical layer

C.
Session layer

D.
Application layer

Answer: D

Explanation:

QUESTION NO: 146

In a Transmission Control Protocol/Internet Protocol (TCP/IP) stack, which layer is responsible for negotiating and establishing a connection with another node?

A.
Transport layer

B.
Application layer

C.
Network layer

D.
Session layer

Answer: A

Explanation:

QUESTION NO: 147

Which of the following is used by the Point-to-Point Protocol (PPP) to determine packet formats?

A.
Layer 2 Tunneling Protocol (L2TP)

B.
Link Control Protocol (LCP)

C.
Challenge Handshake Authentication Protocol (CHAP)

D.
Packet Transfer Protocol (PTP)

Answer: B

Explanation:

QUESTION NO: 148

Which of the following operates at the Network Layer of the Open System Interconnection (OSI) model?

A.
Packet filtering

B.
Port services filtering

C.
Content filtering

D.
Application access control

Answer: A

Reference: https://www.sans.org/reading-room/whitepapers/protocols/applying-osi-layer-network-model-information-security-1309 (10)

QUESTION NO: 149

An external attacker has compromised an organization's network security perimeter and installed a sniffer onto an inside computer. Which of the following is the **MOST** effective layer of security the organization could have implemented to mitigate the attacker's ability to gain further information?

A.
Implement packet filtering on the network firewalls

B.
Install Host Based Intrusion Detection Systems (HIDS)

C.
Require strong authentication for administrators

D.
Implement logical network segmentation at the switches

Answer: D
Explanation:

QUESTION NO: 150

An input validation and exception handling vulnerability has been discovered on a critical web-based system. Which of the following is MOST suited to quickly implement a control?

A.
Add a new rule to the application layer firewall

B.
Block access to the service

C.
Install an Intrusion Detection System (IDS)

D.
Patch the application source code

Answer: A

Explanation:

QUESTION NO: 151

Which of the following is the BEST network defense against unknown types of attacks or stealth attacks in progress?

A.
Intrusion Prevention Systems (IPS)

B.
Intrusion Detection Systems (IDS)

C.
Stateful firewalls

D.
Network Behavior Analysis (NBA) tools

Answer: D

Explanation:

QUESTION NO: 152

Which of the following factors contributes to the weakness of Wired Equivalent Privacy (WEP) protocol?

A.
WEP uses a small range Initialization Vector (IV)

B.
WEP uses Message Digest 5 (MD5)

C.
WEP uses Diffie-Hellman

D.
WEP does not use any Initialization Vector (IV)

Answer: A

Explanation:

QUESTION NO: 153

Which of the following is **BEST** achieved through the use of eXtensible Access Markup Language (XACML)?

A.
Minimize malicious attacks from third parties

B.
Manage resource privileges

C.
Share digital identities in hybrid cloud

D.
Define a standard protocol

Answer: D

Explanation:

QUESTION NO: 154

An organization has discovered that users are visiting unauthorized websites using anonymous proxies.

Which of the following is the **BEST** way to prevent future occurrences?

A.
Remove the anonymity from the proxy

B.
Analyze Internet Protocol (IP) traffic for proxy requests

C.
Disable the proxy server on the firewall

D.

Block the Internet Protocol (IP) address of known anonymous proxies

Answer: C
Explanation:

QUESTION NO: 155

A post-implementation review has identified that the Voice Over Internet Protocol (VoIP) system was designed to have gratuitous Address Resolution Protocol (ARP) disabled.

Why did the network architect likely design the VoIP system with gratuitous ARP disabled?

A.
Gratuitous ARP requires the use of Virtual Local Area Network (VLAN) 1.

B.
Gratuitous ARP requires the use of insecure layer 3 protocols.

C.
Gratuitous ARP requires the likelihood of a successful brute-force attack on the phone.

D.
Gratuitous ARP requires the risk of a Man-in-the-Middle (MITM) attack.

Answer: D
Explanation:

QUESTION NO: 156

Within the company, desktop clients receive Internet Protocol (IP) address over Dynamic Host Configuration Protocol (DHCP).

Which of the following represents a valid measure to help protect the network against unauthorized access?

A.
Implement path management

B.
Implement port based security through 802.1x

C.
Implement DHCP to assign IP address to server systems

D.
Implement change management

Answer: B
Explanation:

QUESTION NO: 157

Transport Layer Security (TLS) provides which of the following capabilities for a remote access server?

A.
Transport layer handshake compression

B.
Application layer negotiation

C.
Peer identity authentication

D.
Digital certificate revocation

Answer: C
Explanation:

QUESTION NO: 158

A chemical plan wants to upgrade the Industrial Control System (ICS) to transmit data using Ethernet instead of RS422. The project manager wants to simplify administration and maintenance by utilizing the office network infrastructure and staff to implement this upgrade.

Which of the following is the **GREATEST** impact on security for the network?

A.
The network administrators have no knowledge of ICS

B.
The ICS is now accessible from the office network

C.
The ICS does not support the office password policy

D.
RS422 is more reliable than Ethernet

Answer: B
Explanation:

QUESTION NO: 159

What does a Synchronous (SYN) flood attack do?

A.
Forces Transmission Control Protocol /Internet Protocol (TCP/IP) connections into a reset state

B.
Establishes many new Transmission Control Protocol / Internet Protocol (TCP/IP) connections

C.
Empties the queue of pending Transmission Control Protocol /Internet Protocol (TCP/IP) requests

D.
Exceeds the limits for new Transmission Control Protocol /Internet Protocol (TCP/IP) connections

Answer: D
Explanation:

QUESTION NO: 160

Which of the following is considered best practice for preventing e-mail spoofing?

A.
Cryptographic signature

B.
Uniform Resource Locator (URL) filtering

C.
Spam filtering

D.
Reverse Domain Name Service (DNS) lookup

Answer: A
Explanation:

QUESTION NO: 161

A Denial of Service (DoS) attack on a syslog server exploits weakness in which of the following protocols?

A.
Point-to-Point Protocol (PPP) and Internet Control Message Protocol (ICMP)

B.
Transmission Control Protocol (TCP) and User Datagram Protocol (UDP)

C.
Address Resolution Protocol (ARP) and Reverse Address Resolution Protocol (RARP)

D.
Transport Layer Security (TLS) and Secure Sockets Layer (SSL)

Answer: B
Explanation:

QUESTION NO: 162

In a High Availability (HA) environment, what is the **PRIMARY** goal of working with a virtual router address as the gateway to a network?

A.
The second of two routers can periodically check in to make sure that the first router is operational.

B.

The second of two routers can better absorb a Denial of Service (DoS) attack knowing the first router is present.

C.
The first of two routers fails and is reinstalled, while the second handles the traffic flawlessly.

D.
The first of two routers can better handle specific traffic, while the second handles the rest of the traffic seamlessly.

Answer: C
Explanation:

QUESTION NO: 163

How does Encapsulating Security Payload (ESP) in transport mode affect in the Internet Protocol (IP)?

A.
Authenticates the IP payload and selected portions of the IP header

B.
Encrypts and optionally authenticates the complete IP packet

C.
Encrypts and optionally authenticates the IP header, but not the IP payload

D.
Encrypts and optionally authenticates the IP payload, but not the IP header

Answer: D
Explanation:

QUESTION NO: 164

A company receives an email threat informing of an Imminent Distributed Denial of Service (DDoS) attack targeting its web application, unless ransom is paid. Which of the following techniques **BEST** addresses that threat?

A.
Deploying load balancers to distribute inbound traffic across multiple data centers

B.
Set Up Web Application Firewalls (WAFs) to filter out malicious traffic

C.
Implementing reverse web-proxies to validate each new inbound connection

D.
Coordinate with and utilize capabilities within Internet Service Provider (ISP)

Answer: D
Explanation:

QUESTION NO: 165

The **MAIN** use of Layer 2 Tunneling Protocol (L2TP) is to tunnel data

A.
through a firewall at the Session layer

B.
through a firewall at the Transport layer

C.
in the Point-to-Point Protocol (PPP)

D.
in the Payload Compression Protocol (PCP)

Answer: C
Explanation:

QUESTION NO: 166

What protocol is often used between gateway hosts on the Internet?

A.
Exterior Gateway Protocol (EGP)

B.
Border Gateway Protocol (BGP)

C.
Open Shortest Path First (OSPF)

D.
Internet Control Message Protocol (ICMP)

Answer: B
Explanation:

QUESTION NO: 167

From a security perspective, which of the following is a best practice to configure a Domain Name Service (DNS) system?

A.
Disable all recursive queries on the name servers

B.
Limit zone transfers to authorized devices

C.
Configure secondary servers to use the primary server as a zone forwarder

D.
Block all Transmission Control Protocol (TCP) connections

Answer: B
Explanation:

QUESTION NO: 168

“Stateful" differs from “Static" packet filtering firewalls by being aware of which of the following?

A.
Difference between a new and an established connection

B.

Originating network location

C.
Difference between a malicious and a benign packet payload

D.
Originating application session

Answer: A
Explanation:

QUESTION NO: 169

Which of the following provides the **MOST** comprehensive filtering of Peer-to-Peer (P2P) traffic?

A.
Application proxy

B.
Port filter

C.
Network boundary router

D.
Access layer switch

Answer: A
Explanation:

QUESTION NO: 170

What can happen when an Intrusion Detection System (IDS) is installed inside a firewall-protected internal network?

A.
The IDS can detect failed administrator logon attempts from servers.

B.
The IDS can increase the number of packets to analyze.

C.
The firewall can increase the number of packets to analyze.

D.
The firewall can detect failed administrator login attempts from servers

Answer: A
Explanation:

QUESTION NO: 171

A security practitioner is tasked with securing the organization's Wireless Access Points (WAP). Which of these is the **MOST** effective way of restricting this environment to authorized users?

A.
Enable Wi-Fi Protected Access 2 (WPA2) encryption on the wireless access point

B.
Disable the broadcast of the Service Set Identifier (SSID) name

C.
Change the name of the Service Set Identifier (SSID) to a random value not associated with the organization

D.
Create Access Control Lists (ACL) based on Media Access Control (MAC) addresses

Answer: A
Explanation:

QUESTION NO: 172

Access to which of the following is required to validate web session management?

A.
Log timestamp

B.
Live session traffic

C.
Session state variables

D.
Test scripts

Answer: C
Explanation:

QUESTION NO: 173

Which of the following would an attacker **BEST** be able to accomplish through the use of Remote Access Tools (RAT)?

A.
Reduce the probability of identification

B.
Detect further compromise of the target

C.
Destabilize the operation of the host

D.
Maintain and expand control

Answer: D
Explanation:

QUESTION NO: 174

Digital certificates used in Transport Layer Security (TLS) support which of the following?

A.
Information input validation

B.
Non-repudiation controls and data encryption

C.

Multi-Factor Authentication (MFA)

D.
Server identity and data confidentially

Answer: D
Explanation:

QUESTION NO: 175

During examination of Internet history records, the following string occurs within a Unique Resource Locator (URL):

http://www.companysite.com/products/products.asp?productid=123 or 1=1

What type of attack does this indicate?

A.
Directory traversal

B.
Structured Query Language (SQL) injection

C.
Cross-Site Scripting (XSS)

D.
Shellcode injection

Answer: B
Explanation:

QUESTION NO: 176

Which testing method requires very limited or no information about the network infrastructure?

A.
White box

B.
Static

C.
Black box

D.
Stress

Answer: C
Explanation:

QUESTION NO: 177

Which of the following will an organization’s network vulnerability testing process BEST enhance?

A.
Firewall log review processes

B.
Asset management procedures

C.
Server hardening processes

D.
Code review procedures

Answer: A
Explanation:

QUESTION NO: 178

Which of the following provides the MOST secure method for Network Access Control (NAC)?

A.
Media Access Control (MAC) filtering

B.
802.1X authentication

C.
Application layer filtering

D.
Network Address Translation (NAT)

Answer: B
Explanation:

QUESTION NO: 179

Individual access to a network is BEST determined based on:

A.
risk matrix

B.
value of the data

C.
business need

D.
data classification

Answer: C
Explanation:

QUESTION NO: 180

A security professional should consider the protection of which of the following elements FIRST when developing a defense-in-depth strategy for a mobile workforce?

A.
Network perimeters

B.
Demilitarized Zones (DMZ)

C.

Databases and back-end servers

D.
End-user devices

Answer: A
Explanation:

QUESTION NO: 181

Why would a security architect specify that a default route pointing to a sinkhole be injected into internal networks?

A.
To have firewalls route all network traffic

B.
To detect the traffic destined to non-existent network destinations

C.
To exercise authority over the network department

D.
To re-inject the route into external networks

Answer: B
Explanation:

QUESTION NO: 182

What is the BEST location in a network to place Virtual Private Network (VPN) devices when an internal review reveals network design flaws in remote access?

A.
In a dedicated Demilitarized Zone (DMZ)

B.
At the Internet Service Provider (ISP)

C.

In its own separate Virtual Local Area Network (VLAN)

D.
Outside the external firewall

Answer: A
Explanation:

QUESTION NO: 183

Which of the following provides the GREATEST level of data security for a Virtual Private Network (VPN) connection?

A.
Internet Protocol Payload Compression (IPComp)

B.
Internet Protocol Security (IPSec)

C.
Extensible Authentication Protocol (EAP)

D.
Remote Authentication Dial-In User Service (RADIUS)

Answer: B
Explanation:

QUESTION NO: 184

What technique used for spoofing the origin of an email can successfully conceal the sender’s Internet Protocol (IP) address?

A.
Virtual Private Network (VPN)

B.
Change In-Reply-To data

C.

Onion routing

D.
Web crawling

Answer: C
Explanation:

QUESTION NO: 185

An organization allows ping traffic into and out of their network. An attacker has installed a program on the network that uses the payload portion of the ping packet to move data into and out of the network. What type of attack has the organization experienced?

A.
Data leakage

B.
Unfiltered channel

C.
Data emanation

D.
Covert channel

Answer: D
Explanation:

QUESTION NO: 186

In a dispersed network that lacks central control, which of the following is the PRIMARY course of action to mitigate exposure?

A.
Implement security policies and standards, data backups, and audit controls

B.
Implement management policies, audit control, and data backups

C.
Implement security policies and standards, access controls, and access limitations

D.
Implement remote access policies, shared workstations, and log management

Answer: A
Explanation:

QUESTION NO: 187

Which of the following actions should be taken by a security professional when a mission critical computer network attack is suspected?

A.
Isolate the network, log an independent report, fix the problem, and redeploy the computer

B.
Isolate the network, install patches, and report the occurrence

C.
Prioritize, report and investigate the occurrence

D.
Turn the router off, perform forensic analysis, apply the appropriate fix, and log incidents

Answer: A
Explanation:

QUESTION NO: 188

Point-to-Point Protocol (PPP) was designed to specifically address what issue?

A.
A common design flaw in telephone modems

B.
Speed and reliability issues between dial-up users and Internet Service Providers (ISP)

C.

Compatibility issues with personal computers and web browsers

D.
The security of dial-up connections to remote networks

Answer: B
Explanation:

QUESTION NO: 189

Which of the following protocols will allow the encrypted transfer of content on the Internet?

A.
Server Message Block (SMB)

B.
Secure copy

C.
Hypertext Transfer Protocol (HTTP)

D.
Remote copy

Answer: B
Explanation:

QUESTION NO: 190

Which of the following is included in the Global System for Mobile Communications (GSM) security framework?

A.
Public-Key Infrastructure (PKI)

B.
Symmetric key cryptography

C.
Digital signatures

D.
Biometric authentication

Answer: B

Explanation:

QUESTION NO: 191

Which of the following is a Key Performance Indicator (KPI) for a security training and awareness program?

A.
The number of security audits performed

B.
The number of attendees at security training events

C.
The number of security training materials created

D.
The number of security controls implemented

Answer: D

Explanation:

QUESTION NO: 192

Which of the following BEST describes a Protection Profile (PP)?

A.
A document that expresses an implementation independent set of security requirements for an Information Technology (IT) product that meets specific consumer needs

B.
A document that is used to develop an Information Technology (IT) security product from its security requirements definition

C.

A document that expresses an implementation dependent set of security requirements which contains only the security functional requirements

D.
A document that represents evaluated products where there is a one-to-one correspondence between a PP and a Security Target (ST)

Answer: A

Explanation:

QUESTION NO: 193

An organization lacks a data retention policy. Of the following, who is the BEST person to consult for such requirement?

A.
Application Manager

B.
Database Administrator

C.
Privacy Officer

D.
Finance Manager

Answer: C

Explanation:

QUESTION NO: 194

Which of the following is the PRIMARY issue when analyzing detailed log information?

A.
Logs may be unavailable when required

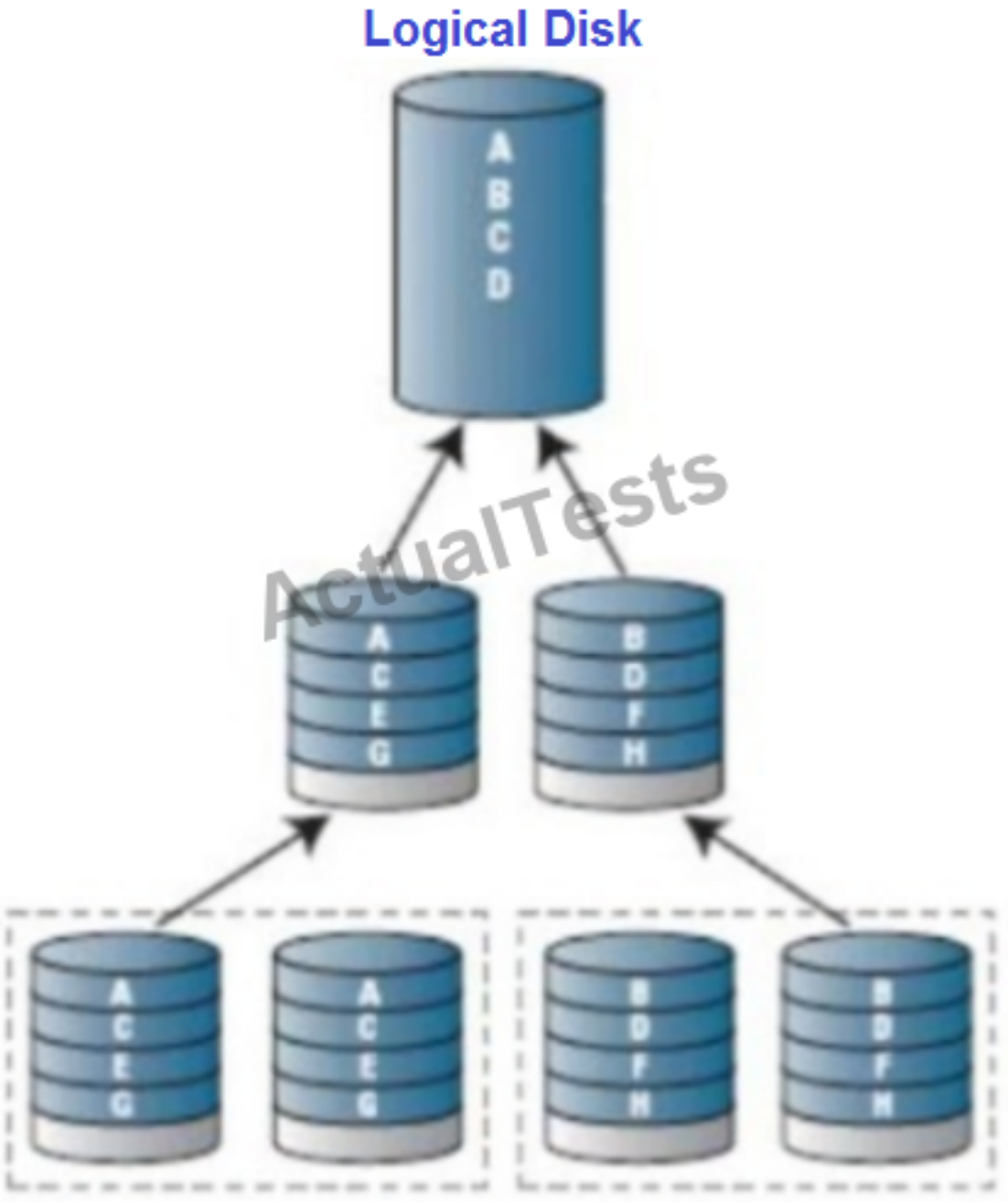
B.
Timely review of the data is potentially difficult

C.
Most systems and applications do not support logging

D.
Logs do not provide sufficient details of system and individual activities

Answer: B
Explanation:

QUESTION NO: 195



Which Redundant Array of Independent Disks (RAID) Level does the following diagram represent?

A.
RAID 0

B.
RAID 1

C.
RAID 5

D.
RAID 10

Answer: D
Explanation:

QUESTION NO: 196

Which of the following MUST be done when promoting a security awareness program to senior management?

A.
Show the need for security; identify the message and the audience

B.
Ensure that the security presentation is designed to be all-inclusive

C.
Notify them that their compliance is mandatory

D.
Explain how hackers have enhanced information security

Answer: A
Explanation:

QUESTION NO: 197

Which of the following BEST describes the objectives of the Business Impact Analysis (BIA)?

A.
Identifying the events and environmental factors that can adversely affect an organization

B.
Identifying what is important and critical based on disruptions that can affect the organization

C.
Establishing the need for a Business Continuity Plan (BCP) based on threats that can affect an organization

D.
Preparing a program to create an organizational awareness for executing the Business Continuity Plan (BCP)

Answer: A

Explanation:

QUESTION NO: 198

Which of the following is considered the PRIMARY security issue associated with encrypted e-mail messages?

A.
Key distribution

B.
Storing attachments in centralized repositories

C.
Scanning for viruses and other malware

D.
Greater costs associated for backups and restores

Answer: C

Explanation:

QUESTION NO: 199

Which one of the following would cause an immediate review and possible change to the security policies of an organization?

A.
Change in technology

B.
Change in senior management

C.
Change to organization processes

D.
Change to organization goals

Answer: A

Explanation:

QUESTION NO: 200

A system with Internet Protocol (IP) address 10.102.10.2 has a physical address of 00:00:08:00:12:13:14:2f. The following static entry is added to its Address Resolution Protocol (ARP) table: 10.102.10.6: 00:00:08:00:12:13:14:2f.

What form of attack could this represent?

A.
A Denial of Service (DoS) attack against the gateway router because the router can no longer accept packets from 10.102.10.2

B.
A transport layer attack that prevents the resolution of 10.102.10.6 address

C.
A Denial of Service (DoS) attack against 10.102.10.2 because it cannot respond correctly to ARP requests

D.
A masquerading attack that sends packets intended for 10.102.10.6 to 10.102.10.2

Answer: D

Explanation:

QUESTION NO: 201

What type of attack sends Internet Control Message Protocol (ICMP) echo requests to the target machine with a larger payload than the target can handle?

A.
Man-in-the-Middle (MITM)

B.
Denial of Service (DoS)

C.
Domain Name Server (DNS) poisoning

D.
Buffer overflow

Answer: D
Explanation:

QUESTION NO: 202

An audit of an application reveals that the current configuration does not match the configuration of the originally implemented application. Which of the following is the FIRST action to be taken?

A.
Recommend an update to the change control process

B.
Verify the approval of the configuration change

C.
Roll back the application to the original configuration

D.
Document the changes to the configuration

Answer: D
Explanation:

QUESTION NO: 203

Configuring a Wireless Access Point (WAP) with the same Service Set Identifier (SSID) as another WAP in order to have users unknowingly connect is referred to as which of the following?

A.
Jamming

B.
Man-in-the-Middle (MITM)

C.
War driving

D.
Internet Protocol (IP) spoofing

Answer: B
Explanation:

QUESTION NO: 204

Which of the following attacks is dependent upon the compromise of a secondary target in order to reach the primary target?

A.
Spear phishing

B.
Address Resolution Protocol (ARP) poisoning

C.
Watering hole

D.
Brute force

Answer: B
Explanation:

QUESTION NO: 205

How is Remote Authentication Dial-In User Service (RADIUS) authentication accomplished?

A.
It uses clear text and firewall rules

B.
It relies on Virtual Private Networks (VPN)

C.
It uses clear text and shared secret keys

D.
It relies on asymmetric encryption keys

Answer: C
Explanation:

QUESTION NO: 206

A project requires the use of an authentication mechanism where playback must be protected and plaintext secret must be used. Which of the following should be used?

A.
Password Authentication Protocol (PAP)

B.
Challenge Handshake Authentication Protocol (CHAP)

C.
Extensible Authentication Protocol (EAP)

D.
Secure Hash Algorithm (SHA)

Answer: B
Explanation:

QUESTION NO: 207

Which of the following MOST applies to Session Initiation Protocol (SIP) security?

A.
It reuses security mechanisms derived from existing protocols

B.
It supports end-to-end security natively

C.
It leverages Hypertext Transfer Protocol (HTTP) over Transport Layer Security (TLS)

D.
It requires a Public Key Infrastructure (PKI)

Answer: A
Explanation:

QUESTION NO: 208

Which of the following is the BEST way to reduce the impact of an externally sourced flood attack?

A.
Block the source address at the firewall

B.
Have the service provider block the source address

C.
Have the source service provider block the address

D.
Block all inbound traffic until the flood ends

Answer: B
Explanation:

QUESTION NO: 209

Which is the RECOMMENDED configuration mode for sensors for an Intrusion Prevention System (IPS) if the prevention capabilities will be used?

A.
Active

B.
Inline

C.
Passive

D.
Span

Answer: A

Explanation:

QUESTION NO: 210

Which of the following techniques is effective to detect taps in fiber optic cables?

A.
Taking baseline signal level of the cable

B.
Measuring signal through external oscillator solution devices

C.
Outlining electromagnetic field strength

D.
Performing network vulnerability scanning

Answer: B

Explanation:

QUESTION NO: 211

Which of the following is a peer entity authentication method for Point-to-Point Protocol (PPP)?

A.
Challenge Handshake Authentication Protocol (CHAP)

B.
Message Authentication Code (MAC)

C.
Transport Layer Security (TLS) handshake protocol

D.
Challenge-response authentication mechanism

Answer: A
Explanation:

QUESTION NO: 212

Which of the following is a standard Access Control List (ACL) element that enables a router to filter Internet traffic?

A.
Media Access Control (MAC) address

B.
Internet Protocol (IP) address

C.
Security roles

D.
Device needs

Answer: B
Explanation:

QUESTION NO: 213

Which of the following is an advantage of Secure Shell (SSH)?

A.

It operates at the network layer

B.
It encrypts transmitted User ID and passwords

C.
It uses challenge-response to authenticate each party

D.
It uses the International Data Encryption Algorithm (IDEA) for data privacy

Answer: C
Explanation:

QUESTION NO: 214

Why are packet filtering routers used in low-risk environments?

A.
They are high-resolution source discrimination and identification tools

B.
They are fast and flexible, and protect against Internet Protocol (IP) spoofing

C.
They are fast, flexible, and transparent

D.
They enforce strong user authentication and audit log generation

Answer: B
Explanation:

QUESTION NO: 215

Which of the following is critical if an employee is dismissed due to violation of an organization's Acceptable Use Policy (AUP)?

A.
Privilege suspension

B.
Appropriate documentation

C.
Internet access logs

D.
Proxy records

Answer: B
Explanation:

QUESTION NO: 216

The Secure Shell (SSH) version 2 protocol supports

A.
availability, accountability, compression, and integrity

B.
authentication, availability, confidentiality, and integrity

C.
accountability, compression, confidentiality, and integrity

D.
authentication, compression, confidentiality, and integrity

Answer: D
Explanation:

QUESTION NO: 217

Which of the following is the MOST secure protocol for remote command access to the firewall?

A.
Secure Shell (SSH)

B.
Trivial File Transfer Protocol (TFTP)

C.
Hypertext Transfer Protocol Secure (HTTPS)

D.
Simple Network Management Protocol (SNMP) v1

Answer: A
Explanation:

QUESTION NO: 218

Which of the following is the reason that transposition ciphers are easily recognizable?

A.
Key

B.
Block

C.
Stream

D.
Character

Answer: D
Explanation:

QUESTION NO: 219

When developing the entitlement review process, which of the following roles is responsible for determining who has a need for the information?

A.
Data Custodian

B.
Data Owner

C.

Database Administrator

D.
Information Technology (IT) Director

Answer: B
Explanation:

QUESTION NO: 220

Which of the following BEST describes botnets?

A.
Computer systems on the Internet that are set up to trap people who attempt to penetrate other computer systems

B.
Set of related programs that protects the resources of a private network from other networks

C.
Small network inserted in a neutral zone between an organization’s private network and the outside public network

D.
Groups of computers that are used to launch destructive attacks

Answer: D
Explanation:

QUESTION NO: 221

A security professional should ensure that clients support which secondary algorithm for digital signatures when a Secure Multipurpose Internet Mail Extension (S/MIME) is used?

A.
Triple Data Encryption Standard (3DES)

B.
Advanced Encryption Standard (AES)

C.
Digital Signature Algorithm (DSA)

D.
Rivest-Shamir-Adleman (RSA)

Answer: B
Explanation:

QUESTION NO: 222

The Rivest-Shamir-Adleman (RSA) algorithm is BEST suited for which of the following operations?

A.
Bulk data encryption and decryption

B.
One-way secure hashing for user and message authentication

C.
Secure key exchange for symmetric cryptography

D.
Creating digital checksums for message integrity

Answer: C
Explanation:

QUESTION NO: 223

An Intrusion Detection System (IDS) is based on the general hypothesis that a security violation is associated with a pattern of system usage, which can be

A.
differentiated from a normal usage pattern

B.
used to detect known violations

C.

used to detect a masquerader

D.
differentiated to detect all security violations

Answer: B
Explanation:

QUESTION NO: 224

Which of the following is the MOST effective countermeasure against Man-in-the-Middle (MITM) attacks while using online banking?

A.
Transport Layer Security (TLS)

B.
Secure Sockets Layer (SSL)

C.
Pretty Good Privacy (PGP)

D.
Secure Shell (SSH)

Answer: A
Explanation:

QUESTION NO: 225

Which of the following needs to be included in order for High Availability (HA) to continue operations during planned system outages?

A.
Redundant hardware, disk spanning, and patching

B.
Load balancing, power reserves, and disk spanning

C.

Backups, clustering, and power reserves

D.
Clustering, load balancing, and fault-tolerant options

Answer: D
Explanation:

QUESTION NO: 226

Organization A is adding a large collection of confidential data records that it received when it acquired Organization B to its data store. Many of the users and staff from Organization B are no longer available.

Which of the following MUST Organization A do to properly classify and secure the acquired data?

A.
Assign data owners from Organization A to the acquired data

B.
Create placeholder accounts that represent former users from Organization B

C.
Archive audit records that refer to users from Organization A

D.
Change the data classification for data acquired from Organization B

Answer: A
Explanation:

Topic 5, Identity and Access Management (IAM)

QUESTION NO: 227

A manufacturing organization wants to establish a Federated Identity Management (FIM) system with its 20 different supplier companies. Which of the following is the **BEST** solution for the manufacturing organization?

A.
Trusted third-party certification

B.
Lightweight Directory Access Protocol (LDAP)

C.
Security Assertion Markup language (SAML)

D.
Cross-certification

Answer: C
Reference: https://www.netiq.com/documentation/access-manager-43/applications-configuration-guide/data/b1ka6lkd.html

QUESTION NO: 228

Which of the following BEST describes an access control method utilizing cryptographic keys derived from a smart card private key that is embedded within mobile devices?

A.
Derived credential

B.
Temporary security credential

C.
Mobile device credentialing service

D.
Digest authentication

Answer: A
Explanation:

QUESTION NO: 229

Users require access rights that allow them to view the average salary of groups of employees.

Which control would prevent the users from obtaining an individual employee's salary?

A.
Limit access to predefined queries

B.
Segregate the database into a small number of partitions each with a separate security level

C.
Implement Role Based Access Control (RBAC)

D.
Reduce the number of people who have access to the system for statistical purposes

Answer: C
Explanation:

QUESTION NO: 230

What is the BEST approach for controlling access to highly sensitive information when employees have the same level of security clearance?

A.
Audit logs

B.
Role-Based Access Control (RBAC)

C.
Two-factor authentication

D.
Application of least privilege

Answer: B
Explanation:

QUESTION NO: 231

The core component of Role Based Access Control (RBAC) must be constructed of defined data

elements.

Which elements are required?

A.
Users, permissions, operations, and protected objects

B.
Roles, accounts, permissions, and protected objects

C.
Users, roles, operations, and protected objects

D.
Roles, operations, accounts, and protected objects

Answer: C
Explanation:

QUESTION NO: 232

Which of the following is the **BEST** metric to obtain when gaining support for an Identify and Access Management (IAM) solution?

A.
Application connection successes resulting in data leakage

B.
Administrative costs for restoring systems after connection failure

C.
Employee system timeouts from implementing wrong limits

D.
Help desk costs required to support password reset requests

Answer: D
Explanation:

QUESTION NO: 233

In an organization where Network Access Control (NAC) has been deployed, a device trying to connect to the network is being placed into an isolated domain. What could be done on this device in order to obtain proper connectivity?

A.
Connect the device to another network jack

B.
Apply remediation's according to security requirements

C.
Apply Operating System (OS) patches

D.
Change the Message Authentication Code (MAC) address of the network interface

Answer: B
Explanation:

QUESTION NO: 234

What is the second step in the identity and access provisioning lifecycle?

A.
Provisioning

B.
Review

C.
Approval

D.
Revocation

Answer: B
Explanation:

QUESTION NO: 235

Which of the following MUST be scalable to address security concerns raised by the integration of third-party identity services?

A.
Mandatory Access Controls (MAC)

B.
Enterprise security architecture

C.
Enterprise security procedures

D.
Role Based Access Controls (RBAC)

Answer: D

Explanation:

QUESTION NO: 236

Which of the following is a common feature of an Identity as a Service (IDaaS) solution?

A.
Single Sign-On (SSO) authentication support

B.
Privileged user authentication support

C.
Password reset service support

D.
Terminal Access Controller Access Control System (TACACS) authentication support

Answer: A

Explanation:

QUESTION NO: 237

An organization’s security policy delegates to the data owner the ability to assign which user roles

have access to a particular resource. What type of authorization mechanism is being used?

A.
Discretionary Access Control (DAC)

B.
Role Based Access Control (RBAC)

C.
Media Access Control (MAC)

D.
Mandatory Access Control (MAC)

Answer: A
Explanation:

QUESTION NO: 238

Extensible Authentication Protocol-Message Digest 5 (EAP-MD5) only provides which of the following?

A.
Mutual authentication

B.
Server authentication

C.
User authentication

D.
Streaming ciphertext data

Answer: C
Explanation:

QUESTION NO: 239

Which of the following is the FIRST step during digital identity provisioning?

A.
Authorizing the entity for resource access

B.
Synchronizing directories

C.
Issuing an initial random password

D.
Creating the entity record with the correct attributes

Answer: D
Explanation:

QUESTION NO: 240

Physical Access Control Systems (PACS) allow authorized security personnel to manage and monitor access control for subjects through which function?

A.
Remote access administration

B.
Personal Identity Verification (PIV)

C.
Access Control List (ACL)

D.
Privileged Identity Management (PIM)

Answer: B
Explanation:

QUESTION NO: 241

An organization seeks to use a cloud Identity and Access Management (IAM) provider whose protocols and data formats are incompatible with existing systems. Which of the following techniques addresses the compatibility issue?

A.
Require the cloud IAM provider to use declarative security instead of programmatic authentication checks

B.
Integrate a Web-Application Firewall (WAF) in reverse-proxy mode in front of the service provider

C.
Apply Transport Layer Security (TLS) to the cloud-based authentication checks

D.
Install an on-premise Authentication Gateway Service (AGS) in front of the service provider

Answer: D
Explanation:

QUESTION NO: 242

Which of the following BEST describes the standard used to exchange authorization information between different identity management systems?

A.
Security Assertion Markup Language (SAML)

B.
Service Oriented Architecture (SOA)

C.
Extensible Markup Language (XML)

D.
Wireless Authentication Protocol (WAP)

Answer: A
Explanation:

QUESTION NO: 243

Which item below is a federated identity standard?

A.
802.11i

B.
Kerberos

C.
Lightweight Directory Access Protocol (LDAP)

D.
Security Assertion Markup Language (SAML)

Answer: D
Explanation:

QUESTION NO: 244

Which of the following problems is not addressed by using Open Authorization Version 2 (OAuth2) to integrate a third-party Identity Provider (IdP) for a service?

A.
Resource servers are required to use passwords to authenticate end users

B.
Revocation of access of some users of the third-party instead of all the users from the third-party

C.
Compromise of the third-party means compromise of all the users in the service

D.
Guest users need to authenticate with the third-party IdP

Answer: C
Explanation:

QUESTION NO: 245

An organization implements a Remote Access Server (RAS). Once users connect to the server, digital certificates are used to authenticate their identity. What type of Extensible Authentication Protocol (EAP) would the organization use during this authentication?

A.
Transport Layer Security (TLS)

B.
Message Digest 5 (MD5)

C.
Lightweight Extensible Authentication Protocol (LEAP)

D.
Subscriber Identity Module (SIM)

Answer: A
Explanation:

QUESTION NO: 246

During a fingerprint verification process, which of the following is used to verify identity and authentication?

A.
A pressure value is compared with a stored template

B.
Sets of digits are matched with stored values

C.
A hash table is matched to a database of stored value

D.
A template of minutiae is compared with a stored template

Answer: D
Explanation:

QUESTION NO: 247

In Identity Management (IdM), when is the verification stage performed?

A.

As part of system sign-on

B.
Before creation of the identity

C.
After revocation of the identity

D.
During authorization of the identity

Answer: A
Explanation:

QUESTION NO: 248

For a federated identity solution, a third-party Identity Provider (IdP) is PRIMARILY responsible for which of the following?

A.
Access Control

B.
Account Management

C.
Authentication

D.
Authorization

Answer: C
Explanation:

QUESTION NO: 249

What is the BEST way to establish identity over the Internet?

A.
Challenge Handshake Authentication Protocol (CHAP) and strong passwords

B.
Remote Authentication Dial-In User Service (RADIUS) server with hardware tokens

C.
Internet Message Access Protocol (IMAP) with Triple Data Encryption Standard (3DES)

D.
Remote user authentication via Simple Object Access Protocol (SOAP)

Answer: B
Explanation:

QUESTION NO: 250

Which of the following authorization standards is built to handle Application Programming Interface (API) access for Federated Identity Management (FIM)?

A.
Remote Authentication Dial-In User Service (RADIUS)

B.
Terminal Access Controller Access Control System Plus (TACACS+)

C.
Open Authorization (OAuth)

D.
Security Assertion Markup Language (SAML)

Answer: C
Explanation:

QUESTION NO: 251

The implementation of which features of an identity management system reduces costs and administration overhead while improving audit and accountability?

A.
Two-factor authentication (2FA)

B.
Single sign-on (SSO)

C.
User self-service

D.
A metadirectory

Answer: C
Explanation:

QUESTION NO: 252

Which of the following will accomplish Multi-Factor Authentication (MFA)?

A.
Issuing a smart card with a user-selected Personal Identification Number (PIN)

B.
Requiring users to enter a Personal Identification Number (PIN) and a password

C.
Performing a palm and retinal scan

D.
Issuing a smart card and a One Time Password (OTP) token

Answer: A
Explanation:

Topic 6, Security Assessment and Testing

QUESTION NO: 253

Which of the following is of GREATEST assistance to auditors when reviewing system configurations?

A.
Change management processes

B.
User administration procedures

C.
Operating System (OS) baselines

D.
System backup documentation

Answer: A
Explanation:

QUESTION NO: 254

In which of the following programs is it MOST important to include the collection of security process data?

A.
Quarterly access reviews

B.
Security continuous monitoring

C.
Business continuity testing

D.
Annual security training

Answer: B
Explanation:

QUESTION NO: 255

A Virtual Machine (VM) environment has five guest Operating Systems (OS) and provides strong isolation. What MUST an administrator review to audit a user’s access to data files?

A.
Host VM monitor audit logs

B.
Guest OS access controls

C.
Host VM access controls

D.
Guest OS audit logs

Answer: B
Explanation:

QUESTION NO: 256

Which of the following is a **PRIMARY** benefit of using a formalized security testing report format and structure?

A.
Executive audiences will understand the outcomes of testing and most appropriate next steps for corrective actions to be taken.

B.
Technical teams will understand the testing objectives, testing strategies applied, and business risk associated with each vulnerability.

C.
Management teams will understand the testing objectives and reputational risk to the organization.

D.
Technical and management teams will better understand the testing objectives, results of each test phase, and potential impact levels.

Answer: D
Explanation:

QUESTION NO: 257

Which of the following could cause a Denial of Service (DoS) against an authentication system?

A.
Encryption of audit logs

B.
No archiving of audit logs

C.
Hashing of audit logs

D.
Remote access audit logs

Answer: B

Explanation:

QUESTION NO: 258

Which type of test would an organization perform in order to locate and target exploitable defects?

A.
Penetration

B.
System

C.
Performance

D.
Vulnerability

Answer: A

Explanation:

QUESTION NO: 259

What is the **MAIN** reason for testing a Disaster Recovery Plan (DRP)?

A.
To ensure Information Technology (IT) staff knows and performs roles assigned to each of them

B.
To validate backup sites' effectiveness

C.
To find out what does not work and fix it

D.
To create a high level DRP awareness among Information Technology (IT) staff

Answer: B
Explanation:

QUESTION NO: 260

When designing a vulnerability test, which one of the following is likely to give the **BEST** indication of what components currently operate on the network?

A.
Ping testing

B.
Mapping tools

C.
Asset register

D.
Topology diagrams

Answer: B
Explanation:

QUESTION NO: 261

Which of the following would **BEST** support effective testing of patch compatibility when patches are applied to an organization's systems?

A.
Standardized configurations for devices

B.
Standardized patch testing equipment

C.
Automated system patching

D.
Management support for patching

Answer: A
Explanation:

QUESTION NO: 262

An international medical organization with headquarters in the United States (US) and branches in France wants to test a drug in both countries. What is the organization allowed to do with the test subject's data?

A.
Aggregate it into one database in the US

B.
Process it in the US, but store the information in France

C.
Share it with a third party

D.
Anonymize it and process it in the US

Answer: D
Explanation:

QUESTION NO: 263

As part of an application penetration testing process, session hijacking can **BEST** be achieved by which of the following?

A.
Known-plaintext attack

B.
Denial of Service (DoS)

C.
Cookie manipulation

D.
Structured Query Language (SQL) injection

Answer: C
Explanation:

QUESTION NO: 264

Assessing a third party's risk by counting bugs in the code may not be the best measure of an attack surface within the supply chain.

Which of the following is **LEAST** associated with the attack surface?

A.
Input protocols

B.
Target processes

C.
Error messages

D.
Access rights

Answer: C
Explanation:

QUESTION NO: 265

What are the steps of a risk assessment?

A.
identification, analysis, evaluation

B.
analysis, evaluation, mitigation

C.
classification, identification, risk management

D.
identification, evaluation, mitigation

Answer: A
Explanation:

QUESTION NO: 266

After following the processes defined within the change management plan, a super user has upgraded a device within an Information system.

What step would be taken to ensure that the upgrade did NOT affect the network security posture?

A.
Conduct an Assessment and Authorization (A&A)

B.
Conduct a security impact analysis

C.
Review the results of the most recent vulnerability scan

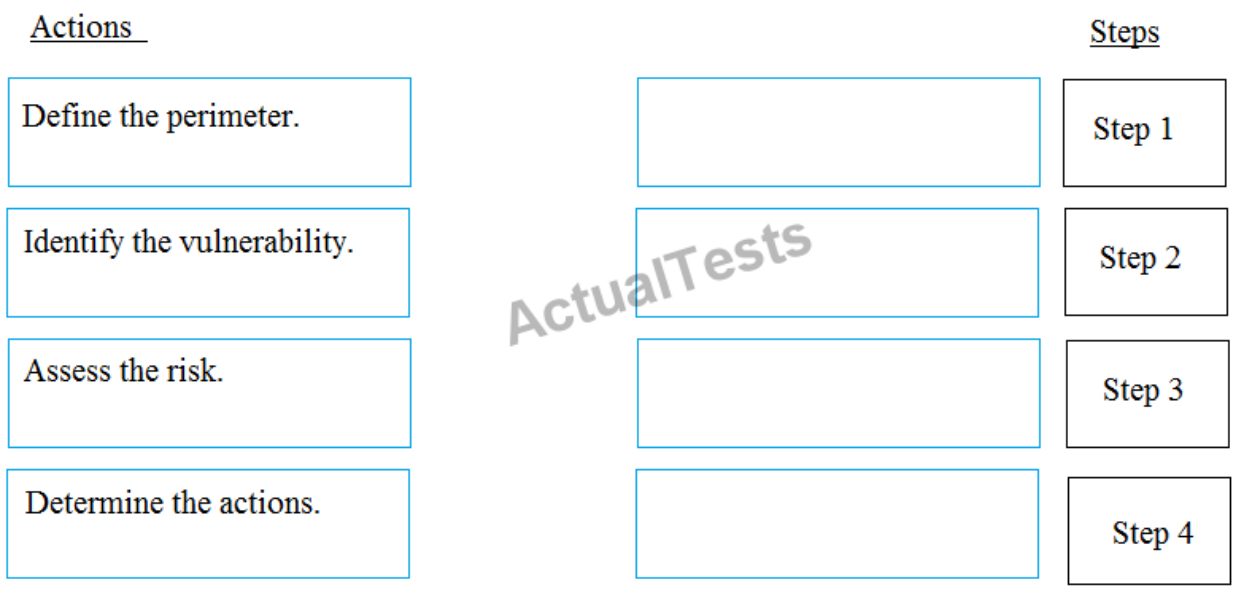
D.
Conduct a gap analysis with the baseline configuration

Answer: B
Explanation:

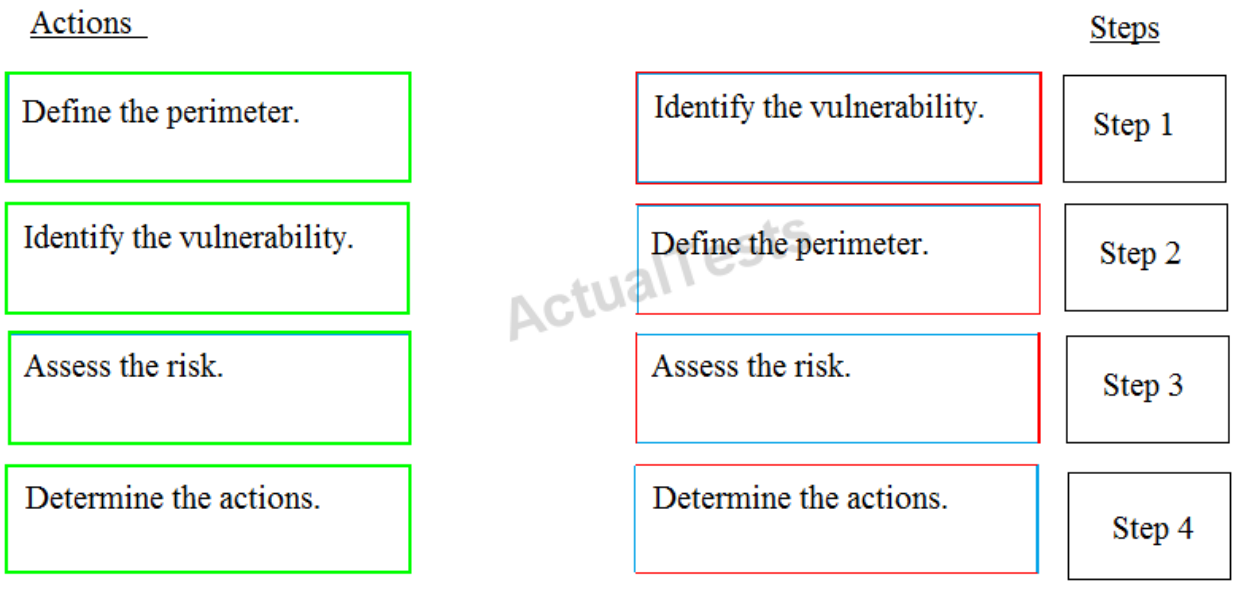
QUESTION NO: 267 DRAG DROP

What is the correct order of steps in an information security assessment?

Place the information security assessment steps on the left next to the numbered boxes on the right in the correct order.



Answer:



Explanation:

Step 1 – Identify the vulnerability

Step 2 – Define the perimeter

Step 3 – Assess the risk

Step 4 – Determine the actions

QUESTION NO: 268

What **MUST** each information owner do when a system contains data from multiple information owners?

A.
Provide input to the Information System (IS) owner regarding the security requirements of the data

B.
Review the Security Assessment report (SAR) for the Information System (IS) and authorize the IS to operate.

C.
Develop and maintain the System Security Plan (SSP) for the Information System (IS) containing the data

D.
Move the data to an Information System (IS) that does not contain data owned by other information owners

Answer: C
Explanation:

QUESTION NO: 269

A vulnerability assessment report has been submitted to a client. The client indicates that one third of the hosts that were in scope are missing from the report.

In which phase of the assessment was this error **MOST** likely made?

A.
Enumeration

B.
Reporting

C.

Detection

D.
Discovery

Answer: C
Explanation:

QUESTION NO: 270

Which of the following is a responsibility of the information owner?

A.
Ensure that users and personnel complete the required security training to access the Information System (IS)

B.
Defining proper access to the Information System (IS), including privileges or access rights

C.
Managing identification, implementation, and assessment of common security controls

D.
Ensuring the Information System (IS) is operated according to agreed upon security requirements

Answer: C
Explanation:

QUESTION NO: 271

Which of the following explains why classifying data is an important step in performing a risk assessment?

A.
To provide a framework for developing good security metrics

B.
To justify the selection of costly security controls

C.

To classify the security controls sensitivity that helps scope the risk assessment

D.
To help determine the appropriate level of data security controls

Answer: D
Explanation:

QUESTION NO: 272

Which of the following activities is MOST likely to be performed during a vulnerability assessment?

A.
Establish caller authentication procedures to verify the identities of users

B.
Analyze the environment by conducting interview sessions with relevant parties

C.
Document policy exceptions required to access systems in non-compliant areas

D.
Review professional credentials of the vulnerability assessment team or vendor

Answer: C
Explanation:

QUESTION NO: 273

What is the PRIMARY objective of an application security assessment?

A.
Obtain information security management approval

B.
Maintain the integrity of the application

C.
Obtain feedback before implementation

D.
Identify vulnerabilities

Answer: D
Explanation:

QUESTION NO: 274

Which of the following is an accurate statement when an assessment results in the discovery of vulnerabilities in a critical network component?

A.
There is little likelihood that the entire network is being placed at a significant risk of attack

B.
There is a low possibility that any adjacently connected components have been compromised by an attacker

C.
A second assessment should immediately be performed after all vulnerabilities are corrected

D.
The fact that every other host is sufficiently hardened does not change the fact that the network is placed at risk of attack

Answer: C
Explanation:

QUESTION NO: 275

Following a penetration test, what should an organization do FIRST?

A.
Review all security policies and procedures

B.
Ensure staff is trained in security

C.

Determine if you need to conduct a full security assessment

D.
Evaluate the problems identified in the test result

Answer: D
Explanation:

QUESTION NO: 276

An organization is outsourcing its payroll system and is requesting to conduct a full audit on the third-party Information Technology (IT) systems. During the due diligence process, the third party provides previous audit reports on its IT systems.

Which of the following MUST be considered by the organization in order for the audit reports to be acceptable?

A.
The audit reports have been issued in the last six months

B.
The audit assessment has been conducted by an independent assessor

C.
The audit assessment has been conducted by an international audit firm

D.
The audit reports have been signed by the third-party senior management

Answer: B
Explanation:

QUESTION NO: 277

What requirement MUST be met during internal security audits to ensure that all information provided is expressed as an objective assessment without risk of retaliation?

A.
The auditor must be independent and report directly to the management

B.
The auditor must utilize automated tools to back their findings

C.
The auditor must work closely with both the Information Technology (IT) and security sections of an organization

D.
The auditor must perform manual reviews of systems and processes

Answer: A

Explanation:

QUESTION NO: 278

A security engineer is designing a Customer Relationship Management (CRM) application for a third-party vendor. In which phase of the System Development Life Cycle (SDLC) will it be MOST beneficial to conduct a data sensitivity assessment?

A.
Development / Acquisition

B.
Initiation

C.
Enumeration

D.
Operation / Maintenance

Answer: D

Explanation:

QUESTION NO: 279

Which of the following is the MOST effective preventative method to identify security flaws in software?

A.
Monitor performance in production environments

B.
Perform a structured code review

C.
Perform application penetration testing

D.
Use automated security vulnerability testing tools

Answer: C
Explanation:

QUESTION NO: 280

Which of the following phases involves researching a target's configuration from public sources when performing a penetration test?

A.
Information gathering

B.
Social engineering

C.
Target selection

D.
Traffic enumeration

Answer: A
Explanation:

QUESTION NO: 281

A company-wide penetration test result shows customers could access and read files through a web browser. Which of the following can be used to mitigate this vulnerability?

A.
Enforce the chmod of files to 755

B.
Enforce the control of file directory listings

C.
Implement access control on the web server

D.
Implement Secure Sockets Layer (SSL) certificates throughout the web server

Answer: D
Explanation:

QUESTION NO: 282

When planning a penetration test, the tester will be MOST interested in which information?

A.
Places to install back doors

B.
The main network access points

C.
Job application handouts and tours

D.
Exploits that can attack weaknesses

Answer: B
Explanation:

QUESTION NO: 283

What is the PRIMARY objective for conducting an internal security audit?

A.
Verify that all systems and Standard Operating Procedures (SOP) are properly documented

B.
Verify that all personnel supporting a system are knowledgeable of their responsibilities

C.
Verify that security controls are established following best practices

D.
Verify that applicable security controls are implemented and effective

Answer: D

Explanation:

QUESTION NO: 284

Which of the following is a characteristic of the independent testing of a program?

A.
Independent testing increases the likelihood that a test will expose the effect of a hidden feature.

B.
Independent testing decreases the likelihood that a test will expose the effect of a hidden feature.

C.
Independent testing teams help decrease the cost of creating test data and system design specifications.

D.
Independent testing teams help identify functional requirements and Service Level Agreements (SLA) to improve program reliability.

Answer: D

Explanation:

QUESTION NO: 285

Which of the following is a characteristic of covert security testing?

A.
Induces less risk than overt testing

B.
Focuses on identifying vulnerabilities

C.
Tests and validates all security controls in the organization

D.
Tests staff knowledge and implementation of the organization’s security policy

Answer: B

Explanation:

QUESTION NO: 286

The security team has been tasked with performing an interface test against a front-end external facing application and needs to verify that all input fields protect against invalid input. Which of the following BEST assists this process?

A.
Application fuzzing

B.
Instruction set simulation

C.
Regression testing

D.
Sanity testing

Answer: D

Explanation:

QUESTION NO: 287

A security professional has been requested by the Board of Directors and Chief Information Security Officer (CISO) to perform an internal and external penetration test. What is the BEST course of action?

A.
Review data localization requirements and regulations

B.
Review corporate security policies and procedures

C.
With notice to the organization, perform an internal penetration test first, then an external test

D.
With notice to the organization, perform an external penetration test first, then an internal test

Answer: A
Explanation:

QUESTION NO: 288

Which of the following is a PRIMARY challenge when running a penetration test?

A.
Determining the cost

B.
Establishing a business case

C.
Remediating found vulnerabilities

D.
Determining the depth of coverage

Answer: C
Explanation:

QUESTION NO: 289

Which type of test suite should be run for fast feedback during application development?

A.
Smoke

B.
Specific functionality

C.
Full regression

D.
End-to-end

Answer: A
Explanation:

Topic 7, Security Operations

QUESTION NO: 290

An organization is found lacking the ability to properly establish performance indicators for its Web hosting solution during an audit. What would be the MOST probable cause?

A.
Absence of a Business Intelligence (BI) solution

B.
Inadequate cost modeling

C.
Improper deployment of the Service-Oriented Architecture (SOA)

D.
Insufficient Service Level Agreement (SLA)

Answer: D
Explanation:

QUESTION NO: 291

Which of the following types of business continuity tests includes assessment of resilience to internal and external risks without endangering live operations?

A.
Walkthrough

B.
Simulation

C.
Parallel

D.
White box

Answer: C
Explanation:

QUESTION NO: 292

What is the PRIMARY reason for implementing change management?

A.
Certify and approve releases to the environment

B.
Provide version rollbacks for system changes

C.
Ensure that all applications are approved

D.
Ensure accountability for changes to the environment

Answer: D
Explanation:

QUESTION NO: 293

Which of the following is a PRIMARY advantage of using a third-party identity service?

A.
Consolidation of multiple providers

B.
Directory synchronization

C.
Web based logon

D.
Automated account management

Answer: D

Explanation:

QUESTION NO: 294

With what frequency should monitoring of a control occur when implementing Information Security Continuous Monitoring (ISCM) solutions?

A.
Continuously without exception for all security controls

B.
Before and after each change of the control

C.
At a rate concurrent with the volatility of the security control

D.
Only during system implementation and decommissioning

Answer: B

Explanation:

QUESTION NO: 295

What should be the FIRST action to protect the chain of evidence when a desktop computer is involved?

A.
Take the computer to a forensic lab

B.
Make a copy of the hard drive

C.
Start documenting

D.
Turn off the computer

Answer: C

Explanation:

QUESTION NO: 296

What is the MOST important step during forensic analysis when trying to learn the purpose of an unknown application?

A.
Disable all unnecessary services

B.
Ensure chain of custody

C.
Prepare another backup of the system

D.
Isolate the system from the network

Answer: D

Explanation:

QUESTION NO: 297

A Business Continuity Plan/Disaster Recovery Plan (BCP/DRP) will provide which of the following?

A.
Guaranteed recovery of all business functions

B.
Minimization of the need decision making during a crisis

C.
Insurance against litigation following a disaster

D.
Protection from loss of organization resources

Answer: D

Explanation:

QUESTION NO: 298

When is a Business Continuity Plan (BCP) considered to be valid?

A.
When it has been validated by the Business Continuity (BC) manager

B.
When it has been validated by the board of directors

C.
When it has been validated by all threat scenarios

D.
When it has been validated by realistic exercises

Answer: D
Reference:
http://www.manchester.gov.uk/info/200039/emergencies/6174/business_continuity_planning/5

QUESTION NO: 299

Recovery strategies of a Disaster Recovery planning (DRIP) MUST be aligned with which of the following?

A.

Hardware and software compatibility issues

B.
Applications' critically and downtime tolerance

C.
Budget constraints and requirements

D.
Cost/benefit analysis and business objectives

Answer: D
Reference: http://www.pearsonitcertification.com/articles/article.aspx?p=1329710&seqNum=3

QUESTION NO: 300

Which of the following is the FIRST step in the incident response process?

A.
Determine the cause of the incident

B.
Disconnect the system involved from the network

C.
Isolate and contain the system involved

D.
Investigate all symptoms to confirm the incident

Answer: D
Explanation:

QUESTION NO: 301

A continuous information security monitoring program can BEST reduce risk through which of the following?

A.
Collecting security events and correlating them to identify anomalies

B.
Facilitating system-wide visibility into the activities of critical user accounts

C.
Encompassing people, process, and technology

D.
Logging both scheduled and unscheduled system changes

Answer: C
Explanation:

QUESTION NO: 302

What would be the MOST cost effective solution for a Disaster Recovery (DR) site given that the organization’s systems cannot be unavailable for more than 24 hours?

A.
Warm site

B.
Hot site

C.
Mirror site

D.
Cold site

Answer: A
Explanation:

QUESTION NO: 303

Who is accountable for the information within an Information System (IS)?

A.

Security manager

B.
System owner

C.
Data owner

D.
Data processor

Answer: B
Explanation:

QUESTION NO: 304

It is **MOST** important to perform which of the following to minimize potential impact when implementing a new vulnerability scanning tool in a production environment?

A.
Negotiate schedule with the Information Technology (IT) operation's team

B.
Log vulnerability summary reports to a secured server

C.
Enable scanning during off-peak hours

D.
Establish access for Information Technology (IT) management

Answer: C
Explanation:

QUESTION NO: 305

A Security Operations Center (SOC) receives an incident response notification on a server with an active intruder who has planted a backdoor. Initial notifications are sent and communications are established.

What MUST be considered or evaluated before performing the next step?

A.
Notifying law enforcement is crucial before hashing the contents of the server hard drive

B.
Identifying who executed the incident is more important than how the incident happened

C.
Removing the server from the network may prevent catching the intruder

D.
Copying the contents of the hard drive to another storage device may damage the evidence

Answer: C
Explanation:

QUESTION NO: 306

Due to system constraints, a group of system administrators must share a high-level access set of credentials.

Which of the following would be **MOST** appropriate to implement?

A.
Increased console lockout times for failed logon attempts

B.
Reduce the group in size

C.
A credential check-out process for a per-use basis

D.
Full logging on affected systems

Answer: C
Explanation:

QUESTION NO: 307

Which of the following is the **MOST** efficient mechanism to account for all staff during a speedy non-emergency evacuation from a large security facility?

A.
Large mantrap where groups of individuals leaving are identified using facial recognition technology

B.
Radio Frequency Identification (RFID) sensors worn by each employee scanned by sensors at each exit door

C.
Emergency exits with push bars with coordinates at each exit checking off the individual against a predefined list

D.
Card-activated turnstile where individuals are validated upon exit

Answer: B

Explanation:

QUESTION NO: 308

What does electronic vaulting accomplish?

A.
It protects critical files.

B.
It ensures the fault tolerance of Redundant Array of Independent Disks (RAID) systems

C.
It stripes all database records

D.
It automates the Disaster Recovery Process (DRP)

Answer: A

Explanation:

QUESTION NO: 309

Who would be the **BEST** person to approve an organizations information security policy?

A.
Chief Information Officer (CIO)

B.
Chief Information Security Officer (CISO)

C.
Chief internal auditor

D.
Chief Executive Officer (CEO)

Answer: B

Explanation:

QUESTION NO: 310

A security analyst for a large financial institution is reviewing network traffic related to an incident. The analyst determines the traffic is irrelevant to the investigation but in the process of the review, the analyst also finds that an applications data, which included full credit card cardholder data, is transferred in clear text between the server and user's desktop. The analyst knows this violates the Payment Card Industry Data Security Standard (PCI-DSS). Which of the following is the analyst's next step?

A.
Send the log file co-workers for peer review

B.
Include the full network traffic logs in the incident report

C.
Follow organizational processes to alert the proper teams to address the issue.

D.
Ignore data as it is outside the scope of the investigation and the analyst's role.

Answer: C

Explanation:

QUESTION NO: 311

An Information Technology (IT) professional attends a cybersecurity seminar on current incident response methodologies.

What code of ethics canon is being observed?

A.
Provide diligent and competent service to principals

B.
Protect society, the commonwealth, and the infrastructure

C.
Advance and protect the profession

D.
Act honorable, honesty, justly, responsibly, and legally

Answer: C

Explanation:

QUESTION NO: 312

An organization adopts a new firewall hardening standard. How can the security professional verify that the technical staff correct implemented the new standard?

A.
Perform a compliance review

B.
Perform a penetration test

C.
Train the technical staff

D.
Survey the technical staff

Answer: B

Explanation:

QUESTION NO: 313

What is the **MAIN** purpose of a change management policy?

A.
To assure management that changes to the Information Technology (IT) infrastructure are necessary

B.
To identify the changes that may be made to the Information Technology (IT) infrastructure

C.
To verify that changes to the Information Technology (IT) infrastructure are approved

D.
To determine the necessary for implementing modifications to the Information Technology (IT) infrastructure

Answer: C
Explanation:

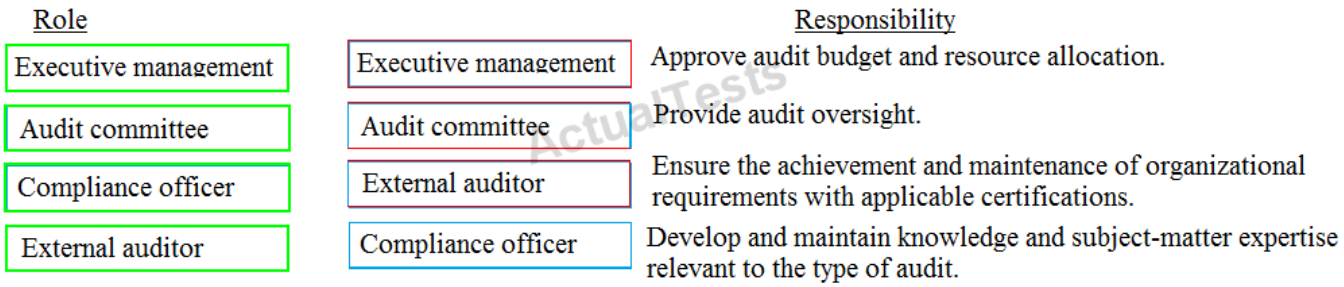
QUESTION NO: 314 DRAG DROP

Match the functional roles in an external audit to their responsibilities.

Drag each role on the left to its corresponding responsibility on the right.

Role		Responsibility
Executive management		Approve audit budget and resource allocation.
Audit committee		Provide audit oversight.
Compliance officer		Ensure the achievement and maintenance of organizational requirements with applicable certifications.
External auditor		Develop and maintain knowledge and subject-matter expertise relevant to the type of audit.

Answer:



Explanation:

Executive management

Audit committee

External auditor

Compliance officer

QUESTION NO: 315

Who is responsible for the protection of information when it is shared with or provided to other organizations?

A.
Systems owner

B.
Authorizing Official (AO)

C.
Information owner

D.
Security officer

Answer: C
Explanation:

QUESTION NO: 316

Which of the following is the **MOST** challenging issue in apprehending cyber criminals?

A.
They often use sophisticated method to commit a crime.

B.
It is often hard to collect and maintain integrity of digital evidence.

C.
The crime is often committed from a different jurisdiction.

D.
There is often no physical evidence involved.

Answer: C
Explanation:

QUESTION NO: 317

What is the BEST way to correlate large volumes of disparate data sources in a Security Operations Center (SOC) environment?

A.
Implement Intrusion Detection System (IDS)

B.
Implement a Security Information and Event Management (SIEM) system

C.
Hire a team of analysts to consolidate data and generate reports

D.
Outsource the management of the SOC

Answer: B
Explanation:

QUESTION NO: 318

Which of the following factors is a PRIMARY reason to drive changes in an Information Security

Continuous Monitoring (ISCM) strategy?

A.
Testing and Evaluation (TE) personnel changes

B.
Changes to core missions or business processes

C.
Increased Cross-Site Request Forgery (CSRF) attacks

D.
Changes in Service Organization Control (SOC) 2 reporting requirements

Answer: D

Explanation:

QUESTION NO: 319

In fault-tolerant systems, what do rollback capabilities permit?

A.
Identifying the error that caused the problem

B.
Isolating the error that caused the problem

C.
Allowing the system to run in a reduced manner

D.
Restoring the system to a previous functional state

Answer: D

Explanation:

QUESTION NO: 320

During a Disaster Recovery (DR) simulation, it is discovered that the shared recovery site lacks adequate data restoration capabilities to support the implementation of multiple plans

simultaneously.

What would be impacted by this fact if left unchanged?

A.
Recovery Point Objective (RPO)

B.
Recovery Time Objective (RTO)

C.
Business Impact Analysis (BIA)

D.
Return on Investment (ROI)

Answer: B
Explanation:

QUESTION NO: 321

When would an organization review a Business Continuity Management (BCM) system?

A.
When major changes occur on systems

B.
When personnel changes occur

C.
Before and after Disaster Recovery (DR) tests

D.
At planned intervals

Answer: C
Explanation:

QUESTION NO: 322

The adoption of an enterprise-wide Business Continuity (BC) program requires which of the following?

A.
Good communication throughout the organization

B.
A completed Business Impact Analysis (BIA)

C.
Formation of Disaster Recovery (DR) project team

D.
Well-documented information asset classification

Answer: B

Explanation:

QUESTION NO: 323

When dealing with compliance with the Payment Card Industry-Data Security Standard (PCI-DSS), an organization that shares card holder information with a service provider MUST do which of the following?

A.
Perform a service provider PCI-DSS assessment on a yearly basis

B.
Validate the service provider’s PCI-DSS compliance status on a regular basis

C.
Validate that the service providers security policies are in alignment with those of the organization

D.
Ensure that the service provider updates and tests its Disaster Recovery Plan (DRP) on a yearly basis

Answer: B

Explanation:

QUESTION NO: 324

During a Disaster Recovery (DR) assessment, additional coverage for assurance is required. What should an assessor do?

A.
Increase the level of detail of the interview questions

B.
Conduct a comprehensive examination of the Disaster Recovery Plan (DRP)

C.
Increase the number and type of relevant staff to interview

D.
Conduct a detailed review of the organization's DR policy

Answer: A

Explanation:

QUESTION NO: 325

Which of the following is the MOST important reason for timely installation of software patches?

A.
Patches are only available for a specific time

B.
Attackers reverse engineer the exploit from the patch

C.
Patches may not be compatible with proprietary software

D.
Attackers may be conducting network analysis

Answer: B

Explanation:

QUESTION NO: 326

Which of the following initiates the systems recovery phase of a Disaster Recovery Plan (DRP)?

A.
Evacuating the disaster site

B.
Activating the organization's hot site

C.
Issuing a formal disaster declaration

D.
Assessing the extent of damage following the disaster

Answer: B

Explanation:

QUESTION NO: 327

In a change-controlled environment, which of the following is MOST likely to lead to unauthorized changes to production programs?

A.
Developers checking out source code without approval

B.
Developers using rapid application development (RAD) methodologies without approval

C.
Promoting programs to production without approval

D.
Modifying source code without approval

Answer: C

Explanation:

QUESTION NO: 328

What is the GREATEST challenge of an agent-based patch management solution?

A.
Time to gather vulnerability information about the computers in the program

B.
Requires that software be installed, running, and managed on all participating computers

C.
The significant amount of network bandwidth while scanning computers

D.
The consistency of distributing patches to each participating computer

Answer: B
Explanation:

QUESTION NO: 329

What should be used immediately after a Business Continuity Plan (BCP) has been invoked?

A.
Emergency procedures describing the necessary actions to be taken following an incident which jeopardizes business operations

B.
Fallback procedures describing what actions are to be taken to move essential business activities to alternative temporary locations

C.
Maintenance schedule specifying how and when the plan will be tested and the process for maintaining the plan

D.
Resumption procedures describing the actions to be taken to return to normal business operations

Answer: A
Explanation:

QUESTION NO: 330

Which of the following actions MUST be performed when using Secure/Multipurpose Internet Mail

Extensions (S/MIME) before sending an encrypted message to a recipient?

A.
Obtain the recipient's private key

B.
Obtain the recipient's digital certificate

C.
Digitally sign the message

D.
Encrypt attachments

Answer: C

Explanation:

QUESTION NO: 331

In order to support the least privilege security principle when a resource is transferring within the organization from a production support system administration role to a developer role, what changes should be made to that resource's access to the production Operating System (OS) directory structure?

A.
From Read Only privileges to No Access privileges

B.
From Author privileges to Administrative privileges

C.
From Administrative privileges to No Access privileges

D.
From No Access privileges to Author privileges

Answer: A

Explanation:

QUESTION NO: 332

According to the Capability Maturity Model Integration (CMMI), which of the following levels is identified by a managed process that is tailored from the organization's set of standard processes according to the organization's tailoring guidelines?

A.
Level 0: Incomplete

B.
Level 1: Performed

C.
Level 2: Managed

D.
Level 3: Defined

Answer: D

Explanation:

QUESTION NO: 333

What is the BEST method if an investigator wishes to analyze a hard drive which may be used as evidence?

A.
Leave the hard drive in place and use only verified and authenticated Operating Systems (OS) utilities to analyze the contents

B.
Log into the system and immediately make a copy of all relevant files to a Write Once, Read Many (WORM) device

C.
Remove the hard drive from the system and make a copy of the hard drive's contents using imaging hardware

D.
Use a separate bootable device to make a copy of the hard drive before booting the system and analyzing the hard drive

Answer: C

Explanation:

QUESTION NO: 334

Which of the following types of data would be MOST difficult to detect by a forensic examiner?

A.
Slack space data

B.
Steganographic data

C.
File system deleted data

D.
Data stored with a different file type extension

Answer: B

Explanation:

QUESTION NO: 335

Which of the following is the BEST approach for a forensic examiner to obtain the greatest amount of relevant information from malicious software?

A.
Analyze the behavior of the program

B.
Analyze the logs generated by the software

C.
Review the code to identify its origin

D.
Examine the file properties and permissions

Answer: A

Explanation:

Topic 8, Software Development Security

QUESTION NO: 336

A Java program is being developed to read a file from computer A and write it to computer B, using a third computer C. The program is not working as expected. What is the MOST probable security feature of Java preventing the program from operating as intended?

A.
Least privilege

B.
Privilege escalation

C.
Defense in depth

D.
Privilege bracketing

Answer: A
Explanation:

QUESTION NO: 337

Which of the following is the PRIMARY risk with using open source software in a commercial software construction?

A.
Lack of software documentation

B.
License agreements requiring release of modified code

C.
Expiration of the license agreement

D.
Costs associated with support of the software

Answer: D

Explanation:

QUESTION NO: 338

When in the Software Development Life Cycle (SDLC) MUST software security functional requirements be defined?

A.
After the system preliminary design has been developed and the data security categorization has been performed

B.
After the vulnerability analysis has been performed and before the system detailed design begins

C.
After the system preliminary design has been developed and before the data security categorization begins

D.
After the business functional analysis and the data security categorization have been performed

Answer: A

Explanation:

QUESTION NO: 339

Which of the following is the BEST method to prevent malware from being introduced into a production environment?

A.
Purchase software from a limited list of retailers

B.
Verify the hash key or certificate key of all updates

C.
Do not permit programs, patches, or updates from the Internet

D.
Test all new software in a segregated environment

Answer: D

Explanation:

QUESTION NO: 340

The configuration management and control task of the certification and accreditation process is incorporated in which phase of the System Development Life Cycle (SDLC)?

A.
System acquisition and development

B.
System operations and maintenance

C.
System initiation

D.
System implementation

Answer: B

Explanation:

QUESTION NO: 341

What is the BEST approach to addressing security issues in legacy web applications?

A.
Debug the security issues

B.
Migrate to newer, supported applications where possible

C.
Conduct a security assessment

D.
Protect the legacy application with a web application firewall

Answer: D

Explanation:

QUESTION NO: 342

Which of the following is a web application control that should be put into place to prevent exploitation of Operating System (OS) bugs?

A.
Check arguments in function calls

B.
Test for the security patch level of the environment

C.
Include logging functions

D.
Digitally sign each application module

Answer: B

Explanation:

QUESTION NO: 343

An Intrusion Detection System (IDS) has recently been deployed in a Demilitarized Zone (DMZ). The IDS detects a flood of malformed packets. Which of the following **BEST** describes what has occurred?

A.
Denial of Service (DoS) attack

B.
Address Resolution Protocol (ARP) spoof

C.
Buffer overflow

D.
Ping flood attack

Answer: A

Explanation:

QUESTION NO: 344

Which of the following command line tools can be used in the reconnaissance phase of a network vulnerability assessment?

A.
dig

B.
ipconfig

C.
ifconfig

D.
nbstat

Answer: A

Explanation:

QUESTION NO: 345

In configuration management, what baseline configuration information **MUST** be maintained for each computer system?

A.
Operating system and version, patch level, applications running, and versions.

B.
List of system changes, test reports, and change approvals

C.
Last vulnerability assessment report and initial risk assessment report

D.
Date of last update, test report, and accreditation certificate

Answer: A

Explanation:

QUESTION NO: 346

Which Radio Frequency Interference (RFI) phenomenon associated with bundled cable runs can create information leakage?

A.
Transference

B.
Covert channel

C.
Bleeding

D.
Cross-talk

Answer: D

Explanation:

QUESTION NO: 347

An organization’s information security strategic plan **MUST** be reviewed

A.
whenever there are significant changes to a major application.

B.
quarterly, when the organization’s strategic plan is updated.

C.
whenever there are major changes to the business.

D.
every three years, when the organization’s strategic plan is updated.

Answer: C

Explanation:

QUESTION NO: 348

When building a data classification scheme, which of the following is the **PRIMARY** concern?

A.
Purpose

B.
Cost effectiveness

C.
Availability

D.
Authenticity

Answer: D

Explanation:

QUESTION NO: 349

Which technology is a prerequisite for populating the cloud-based directory in a federated identity solution?

A.
Notification tool

B.
Message queuing tool

C.
Security token tool

D.
Synchronization tool

Answer: C

Explanation:

QUESTION NO: 350

What is an advantage of Elliptic Curve Cryptography (ECC)?

A.
Cryptographic approach that does not require a fixed-length key

B.
Military-strength security that does not depend upon secrecy of the algorithm

C.
Opportunity to use shorter keys for the same level of security

D.
Ability to use much longer keys for greater security

Answer: C
Explanation:

QUESTION NO: 351

Backup information that is critical to the organization is identified through a

A.
Vulnerability Assessment (VA).

B.
Business Continuity Plan (BCP).

C.
Business Impact Analysis (BIA).

D.
data recovery analysis.

Answer: C
Explanation:

QUESTION NO: 352

When using Generic Routing Encapsulation (GRE) tunneling over Internet Protocol version 4 (IPv4), where is the GRE header inserted?

A.
Into the options field

B.
Between the delivery header and payload

C.
Between the source and destination addresses

D.
Into the destination address

Answer: B
Explanation:

QUESTION NO: 353

An application developer is deciding on the amount of idle session time that the application allows before a timeout. The **BEST** reason for determining the session timeout requirement is

A.
organization policy.

B.
industry best practices.

C.
industry laws and regulations.

D.
management feedback.

Answer: B
Explanation:

QUESTION NO: 354

Knowing the language in which an encrypted message was originally produced might help a cryptanalyst to perform a

A.
clear-text attack.

B.
known cipher attack.

C.
frequency analysis.

D.
stochastic assessment.

Answer: C
Explanation:

QUESTION NO: 355

During the Security Assessment and Authorization process, what is the **PRIMARY** purpose for conducting a hardware and software inventory?

A.
Calculate the value of assets being accredited.

B.
Create a list to include in the Security Assessment and Authorization package.

C.
Identify obsolete hardware and software.

D.
Define the boundaries of the information system.

Answer: A
Explanation:

QUESTION NO: 356

When evaluating third-party applications, which of the following is the **GREATEST** responsibility of Information Security?

A.
Accept the risk on behalf of the organization.

B.
Report findings to the business to determine security gaps.

C.
Quantify the risk to the business for product selection.

D.
Approve the application that best meets security requirements.

Answer: C
Explanation:

QUESTION NO: 357

An employee of a retail company has been granted an extended leave of absence by Human Resources (HR). This information has been formally communicated to the access provisioning team. Which of the following is the **BEST** action to take?

A.
Revoke access temporarily.

B.
Block user access and delete user account after six months.

C.
Block access to the offices immediately.

D.
Monitor account usage temporarily.

Answer: A

Explanation:

QUESTION NO: 358

The goal of a Business Impact Analysis (BIA) is to determine which of the following?

A.
Cost effectiveness of business recovery

B.
Cost effectiveness of installing software security patches

C.
Resource priorities for recovery and Maximum Tolerable Downtime (MTD)

D.
Which security measures should be implemented

Answer: C
Explanation:

QUESTION NO: 359

An organization publishes and periodically updates its employee policies in a file on their intranet. Which of the following is a **PRIMARY** security concern?

A.
Ownership

B.
Confidentiality

C.
Availability

D.
Integrity

Answer: C

Explanation:

QUESTION NO: 360

What does the Maximum Tolerable Downtime (MTD) determine?

A.
The estimated period of time a business critical database can remain down before customers are affected.

B.
The fixed length of time a company can endure a disaster without any Disaster Recovery (DR) planning

C.
The estimated period of time a business can remain interrupted beyond which it risks never recovering

D.
The fixed length of time in a DR process before redundant systems are engaged

Answer: C
Explanation:

QUESTION NO: 361

What is a characteristic of Secure Sockets Layer (SSL) and Transport Layer Security (TLS)?

A.
SSL and TLS provide a generic channel security mechanism on top of Transmission Control Protocol (TCP).

B.
SSL and TLS provide nonrepudiation by default.

C.
SSL and TLS do not provide security for most routed protocols.

D.
SSL and TLS provide header encapsulation over HyperText Transfer Protocol (HTTP).

Answer: A

Explanation:

QUESTION NO: 362

How does a Host Based Intrusion Detection System (HIDS) identify a potential attack?

A.
Examines log messages or other indications on the system.

B.
Monitors alarms sent to the system administrator

C.
Matches traffic patterns to virus signature files

D.
Examines the Access Control List (ACL)

Answer: A

Explanation:

QUESTION NO: 363

From a cryptographic perspective, the service of non-repudiation includes which of the following features?

A.
Validity of digital certificates

B.
Validity of the authorization rules

C.
Proof of authenticity of the message

D.
Proof of integrity of the message

Answer: C

Explanation:

QUESTION NO: 364

Which of the following **BEST** represents the concept of least privilege?

A.
Access to an object is denied unless access is specifically allowed.

B.
Access to an object is only available to the owner.

C.
Access to an object is allowed unless it is protected by the information security policy.

D.
Access to an object is only allowed to authenticated users via an Access Control List (ACL).

Answer: A
Explanation:

QUESTION NO: 365

Which of the following is an advantage of on-premise Credential Management Systems?

A.
Lower infrastructure capital costs

B.
Control over system configuration

C.
Reduced administrative overhead

D.
Improved credential interoperability

Answer: B
Explanation:

QUESTION NO: 366

Which of the following approaches is the **MOST** effective way to dispose of data on multiple hard drives?

A.
Delete every file on each drive.

B.
Destroy the partition table for each drive using the command line.

C.
Degauss each drive individually.

D.
Perform multiple passes on each drive using approved formatting methods.

Answer: D
Explanation:

QUESTION NO: 367

Which of the following **BEST** describes Recovery Time Objective (RTO)?

A.
Time of application resumption after disaster

B.
Time of application verification after disaster.

C.
Time of data validation after disaster.

D.
Time of data restoration from backup after disaster.

Answer: A
Explanation:

QUESTION NO: 368

Which of the following is the **PRIMARY** benefit of a formalized information classification program?

A.
It minimized system logging requirements.

B.
It supports risk assessment.

C.
It reduces asset vulnerabilities.

D.
It drives audit processes.

Answer: B
Explanation:

QUESTION NO: 369

Which of the following is the **BEST** method to reduce the effectiveness of phishing attacks?

A.
User awareness

B.
Two-factor authentication

C.
Anti-phishing software

D.
Periodic vulnerability scan

Answer: A
Explanation:

QUESTION NO: 370

The **PRIMARY** purpose of accreditation is to:

A.
comply with applicable laws and regulations.

B.
allow senior management to make an informed decision regarding whether to accept the risk of operating the system.

C.
protect an organization's sensitive data.

D.
verify that all security controls have been implemented properly and are operating in the correct manner.

Answer: B
Explanation:

QUESTION NO: 371

Which of the following is a weakness of Wired Equivalent Privacy (WEP)?

A.
Length of Initialization Vector (IV)

B.
Protection against message replay

C.
Detection of message tampering

D.
Built-in provision to rotate keys

Answer: A
Explanation:

QUESTION NO: 372

When writing security assessment procedures, what is the **MAIN** purpose of the test outputs and reports?

A.
To force the software to fail and document the process

B.
To find areas of compromise in confidentiality and integrity

C.
To allow for objective pass or fail decisions

D.
To identify malware or hidden code within the test results

Answer: C
Explanation:

QUESTION NO: 373

Which of the following is the **MAIN** reason for using configuration management?

A.
To provide centralized administration

B.
To reduce the number of changes

C.
To reduce errors during upgrades

D.
To provide consistency in security controls

Answer: D
Explanation:

QUESTION NO: 374

Which of the following is **BEST** suited for exchanging authentication and authorization messages

in a multi-party decentralized environment?

A.
Lightweight Directory Access Protocol (LDAP)

B.
Security Assertion Markup Language (SAML)

C.
Internet Mail Access Protocol

D.
Transport Layer Security (TLS)

Answer: B
Explanation:

QUESTION NO: 375

Which of the following is **MOST** important when deploying digital certificates?

A.
Validate compliance with X.509 digital certificate standards

B.
Establish a certificate life cycle management framework

C.
Use a third-party Certificate Authority (CA)

D.
Use no less than 256-bit strength encryption when creating a certificate

Answer: B
Explanation:

QUESTION NO: 376

A user sends an e-mail request asking for read-only access to files that are not considered sensitive. A Discretionary Access Control (DAC) methodology is in place. Which is the **MOST**

suitable approach that the administrator should take?

A.
Administrator should request data owner approval to the user access

B.
Administrator should request manager approval for the user access

C.
Administrator should directly grant the access to the non-sensitive files

D.
Administrator should assess the user access need and either grant or deny the access

Answer: A
Explanation:

QUESTION NO: 377

How should an organization determine the priority of its remediation efforts after a vulnerability assessment has been conducted?

A.
Use an impact-based approach.

B.
Use a risk-based approach.

C.
Use a criticality-based approach.

D.
Use a threat-based approach.

Answer: B
Explanation:

QUESTION NO: 378

Which of the following is the **MOST** important consideration when developing a Disaster Recovery

Plan (DRP)?

A.
The dynamic reconfiguration of systems

B.
The cost of downtime

C.
A recovery strategy for all business processes

D.
A containment strategy

Answer: B
Explanation:

QUESTION NO: 379

A proxy firewall operates at what layer of the Open System Interconnection (OSI) model?

A.
Transport

B.
Data link

C.
Network

D.
Application

Answer: D
Explanation:

QUESTION NO: 380

Which of the following restricts the ability of an individual to carry out all the steps of a particular process?

A.
Job rotation

B.
Separation of duties

C.
Least privilege

D.
Mandatory vacations

Answer: B
Explanation:

QUESTION NO: 381

Although code using a specific program language may not be susceptible to a buffer overflow attack,

A.
most calls to plug-in programs are susceptible.

B.
most supporting application code is susceptible.

C.
the graphical images used by the application could be susceptible.

D.
the supporting virtual machine could be susceptible.

Answer: C
Explanation:

QUESTION NO: 382

What is the **BEST** way to encrypt web application communications?

A.

Secure Hash Algorithm 1 (SHA-1)

B.
Secure Sockets Layer (SSL)

C.
Cipher Block Chaining Message Authentication Code (CBC-MAC)

D.
Transport Layer Security (TLS)

Answer: D
Explanation:

QUESTION NO: 383

Which of the following are effective countermeasures against passive network-layer attacks?

A.
Federated security and authenticated access controls

B.
Trusted software development and run time integrity controls

C.
Encryption and security enabled applications

D.
Enclave boundary protection and computing environment defense

Answer: C
Explanation:

QUESTION NO: 384

What is the **MOST** important element when considering the effectiveness of a training program for Business Continuity (BC) and Disaster Recovery (DR)?

A.
Management support

B.
Consideration of organizational need

C.
Technology used for delivery

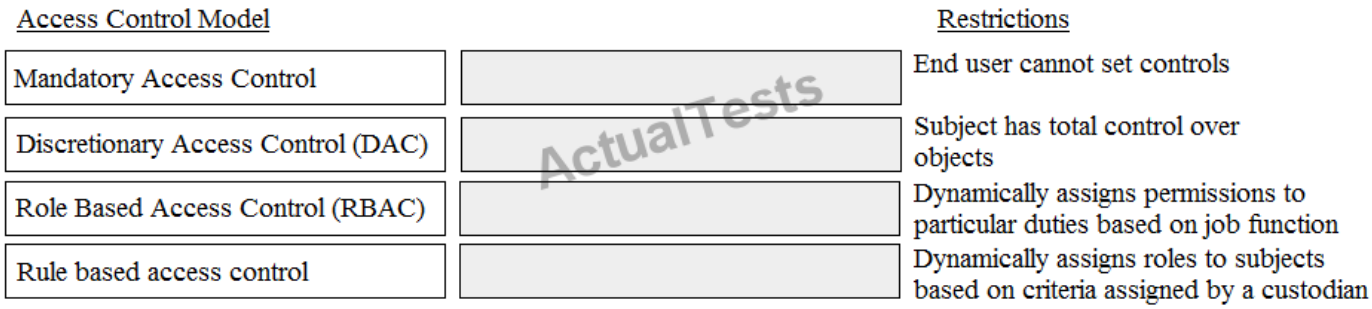
D.
Target audience

Answer: A
Explanation:

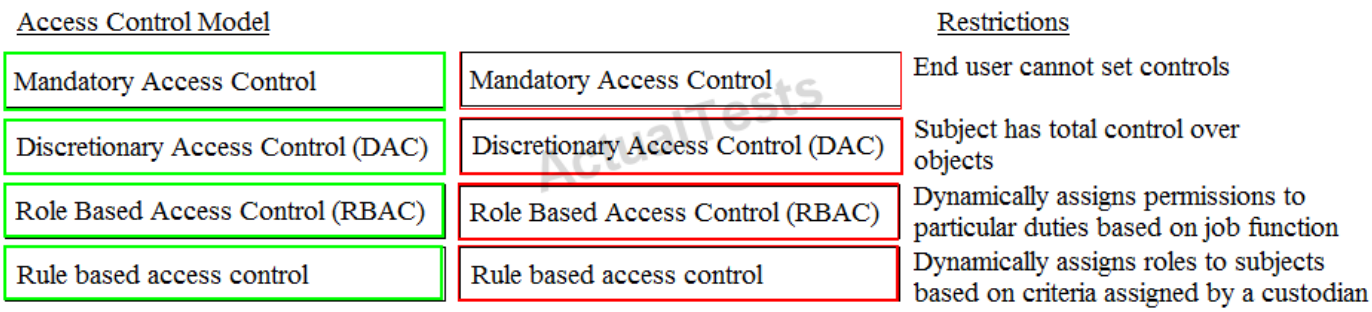
QUESTION NO: 385 DRAG DROP

Match the name of access control model with its associated restriction.

Drag each access control model to its appropriate restriction access on the right.



Answer:



Explanation:

Mandatory Access Control – End user cannot set controls

Discretionary Access Control (DAC) – Subject has total control over objects

Role Based Access Control (RBAC) – Dynamically assigns roles permissions to particular duties based on job function

Rule Based access control – Dynamically assigns roles to subjects based on criteria assigned by a custodian.

QUESTION NO: 386

A database administrator is asked by a high-ranking member of management to perform specific changes to the accounting system database. The administrator is specifically instructed to not track or evidence the change in a ticket. Which of the following is the **BEST** course of action?

A.
Ignore the request and do not perform the change.

B.
Perform the change as requested, and rely on the next audit to detect and report the situation.

C.
Perform the change, but create a change ticket regardless to ensure there is complete traceability.

D.
Inform the audit committee or internal audit directly using the corporate whistleblower process.

Answer: D
Explanation:

QUESTION NO: 387

Which of the following is the **MOST** important goal of information asset valuation?

A.
Developing a consistent and uniform method of controlling access on information assets

B.
Developing appropriate access control policies and guidelines

C.
Assigning a financial value to an organization’s information assets

D.
Determining the appropriate level of protection

Answer: D
Explanation:

QUESTION NO: 388

Which of the following is a strategy of grouping requirements in developing a Security Test and Evaluation (ST&E)?

A.
Tactical, strategic, and financial

B.
Management, operational, and technical

C.
Documentation, observation, and manual

D.
Standards, policies, and procedures

Answer: B
Explanation:

QUESTION NO: 389

Which one of the following activities would present a significant security risk to organizations when employing a Virtual Private Network (VPN) solution?

A.
VPN bandwidth

B.
Simultaneous connection to other networks

C.
Users with Internet Protocol (IP) addressing conflicts

D.
Remote users with administrative rights

Answer: B
Explanation:

QUESTION NO: 390

Which of the following BEST describes a chosen plaintext attack?

A.
The cryptanalyst can generate ciphertext from arbitrary text.

B.
The cryptanalyst examines the communication being sent back and forth.

C.
The cryptanalyst can choose the key and algorithm to mount the attack.

D.
The cryptanalyst is presented with the ciphertext from which the original message is determined.

Answer: A
Explanation:

QUESTION NO: 391

For network based evidence, which of the following contains traffic details of all network sessions in order to detect anomalies?

A.
Alert data

B.
User data

C.
Content data

D.

Statistical data

Answer: D

Explanation:

QUESTION NO: 392

Which of the following is the **PRIMARY** reason to perform regular vulnerability scanning of an organization network?

A.
Provide vulnerability reports to management.

B.
Validate vulnerability remediation activities.

C.
Prevent attackers from discovering vulnerabilities.

D.
Remediate known vulnerabilities.

Answer: B

Explanation:

QUESTION NO: 393

Which of the following would **BEST** describe the role directly responsible for data within an organization?

A.
Data custodian

B.
Information owner

C.
Database administrator

D.

Quality control

Answer: A

Explanation:

QUESTION NO: 394

The restoration priorities of a Disaster Recovery Plan (DRP) are based on which of the following documents?

A.
Service Level Agreement (SLA)

B.
Business Continuity Plan (BCP)

C.
Business Impact Analysis (BIA)

D.
Crisis management plan

Answer: B

Explanation:

QUESTION NO: 395

The **PRIMARY** outcome of a certification process is that it provides documented

A.
interconnected systems and their implemented security controls.

B.
standards for security assessment, testing, and process evaluation.

C.
system weakness for remediation.

D.
security analyses needed to make a risk-based decision.

Answer: D

Explanation:

QUESTION NO: 396

A security architect plans to reference a Mandatory Access Control (MAC) model for implementation. This indicates that which of the following properties are being prioritized?

A.
Confidentiality

B.
Integrity

C.
Availability

D.
Accessibility

Answer: A

Explanation:

Mandatory Access Control (MAC) is system-enforced access control based on a subject's clearance and an object's labels. Subjects and Objects have clearances and labels, respectively, such as confidential, secret, and top secret. A subject may access an object only if the subject's clearance is equal to or greater than the object's label. Subjects cannot share objects with other subjects who lack the proper clearance, or "write down" objects to a lower classification level (such as from top secret to secret). MAC systems are usually focused on preserving the confidentiality of data.

Reference: https://www.sciencedirect.com/topics/computer-science/mandatory-access-control

QUESTION NO: 397

A vulnerability in which of the following components would be **MOST** difficult to detect?

A.
Kernel

B.
Shared libraries

C.
Hardware

D.
System application

Answer: C
Explanation:

QUESTION NO: 398

During which of the following processes is least privilege implemented for a user account?

A.
Provision

B.
Approve

C.
Request

D.
Review

Answer: A
Explanation:

QUESTION NO: 399

Which of the following is a document that identifies each item seized in an investigation, including date and time seized, full name and signature or initials of the person who seized the item, and a detailed description of the item?

A.
Property book

B.
Chain of custody form

C.
Search warrant return

D.
Evidence tag

Answer: B
Explanation:

QUESTION NO: 400

Which of the following is needed to securely distribute symmetric cryptographic keys?

A.
Officially approved Public-Key Infrastructure (PKI) Class 3 or Class 4 certificates

B.
Officially approved and compliant key management technology and processes

C.
An organizationally approved communication protection policy and key management plan

D.
Hardware tokens that protect the user's private key.

Answer: C
Explanation:

QUESTION NO: 401

Reciprocal backup site agreements are considered to be

A.
a better alternative than the use of warm sites.

B.
difficult to test for complex systems.

C.
easy to implement for similar types of organizations.

D.
easy to test and implement for complex systems.

Answer: C
Explanation:

QUESTION NO: 402

In which identity management process is the subject's identity established?

A.
Trust

B.
Provisioning

C.
Authorization

D.
Enrollment

Answer: D
Explanation:

QUESTION NO: 403

In order to assure authenticity, which of the following are required?

A.
Confidentiality and authentication

B.
Confidentiality and integrity

C.
Authentication and non-repudiation

D.
Integrity and non-repudiation

Answer: D
Explanation:

QUESTION NO: 404

At which layer of the Open Systems Interconnect (OSI) model are the source and destination address for a datagram handled?

A.
Transport Layer

B.
Data-Link Layer

C.
Network Layer

D.
Application Layer

Answer: C
Explanation:

QUESTION NO: 405

An organization regularly conducts its own penetration tests. Which of the following scenarios **MUST** be covered for the test to be effective?

A.
Third-party vendor with access to the system

B.
System administrator access compromised

C.
Internal attacker with access to the system

D.
Internal user accidentally accessing data

Answer: B
Explanation:

QUESTION NO: 406

A company was ranked as high in the following National Institute of Standards and Technology (NIST) functions: Protect, Detect, Respond and Recover. However, a low maturity grade was attributed to the Identify function.

In which of the following the controls categories does this company need to improve when analyzing its processes individually?

A.
Asset Management, Business Environment, Governance and Risk Assessment

B.
Access Control, Awareness and Training, Data Security and Maintenance

C.
Anomalies and Events, Security Continuous Monitoring and Detection Processes

D.
Recovery Planning, Improvements and Communications

Answer: A
Explanation:

QUESTION NO: 407

What is the difference between media marking and media labeling?

A.
Media marking refers to the use of human-readable security attributes, while media labeling refers

to the use of security attributes in internal data structures.

B.
Media labeling refers to the use of human-readable security attributes, while media marking refers to the use of security attributes in internal data structures.

C.
Media labeling refers to security attributes required by public policy/law, while media marking refers to security required by internal organizational policy.

D.
Media marking refers to security attributes required by public policy/law, while media labeling refers to security attributes required by internal organizational policy.

Answer: A
Explanation:

QUESTION NO: 408

What balance **MUST** be considered when web application developers determine how informative application error messages should be constructed?

A.
Risk versus benefit

B.
Availability versus auditability

C.
Confidentiality versus integrity

D.
Performance versus user satisfaction

Answer: A
Explanation:

QUESTION NO: 409

What operations role is responsible for protecting the enterprise from corrupt or contaminated

media?

A.
Information security practitioner

B.
Information librarian

C.
Computer operator

D.
Network administrator

Answer: B

Explanation:

QUESTION NO: 410

Which of the following is a characteristic of the initialization vector when using Data Encryption Standard (DES)?

A.
It must be known to both sender and receiver.

B.
It can be transmitted in the clear as a random number.

C.
It must be retained until the last block is transmitted.

D.
It can be used to encrypt and decrypt information.

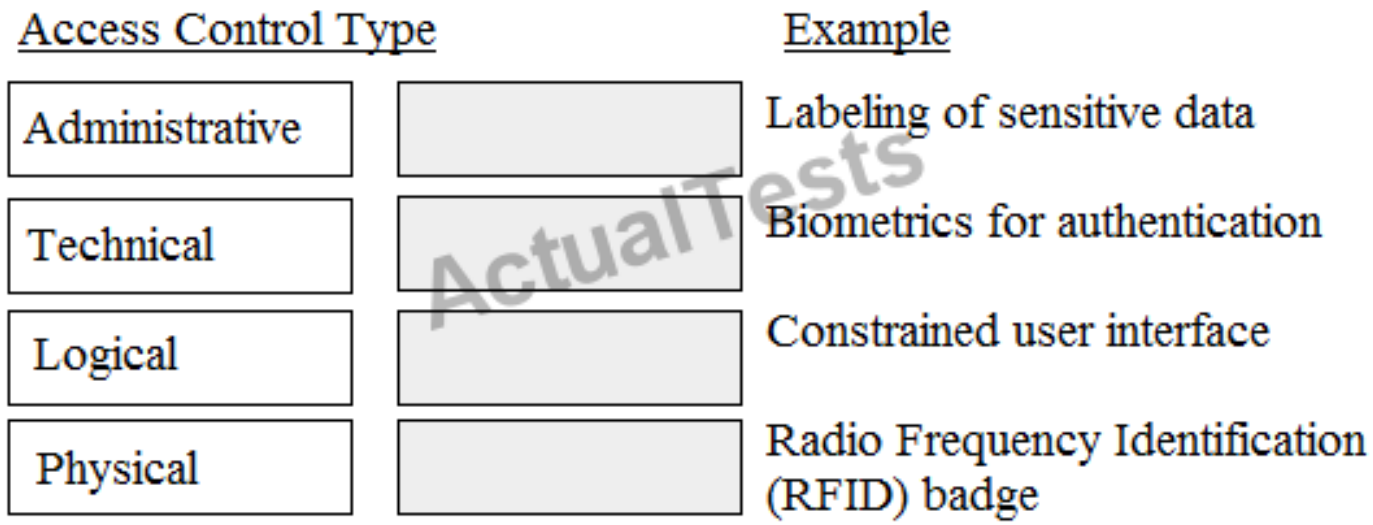
Answer: B

Explanation:

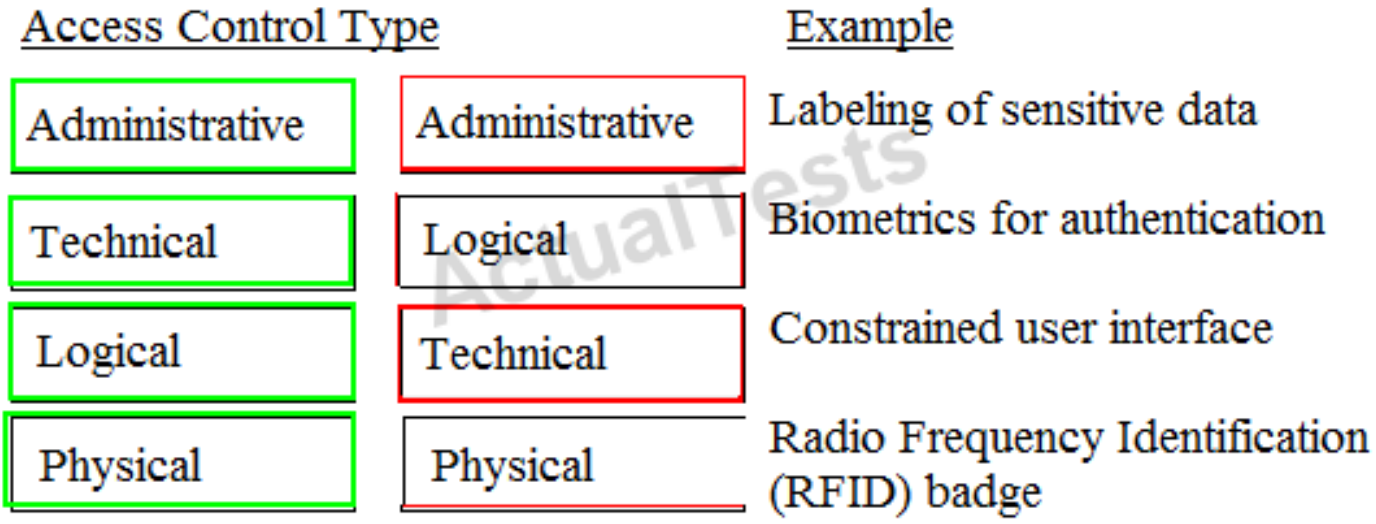
QUESTION NO: 411 DRAG DROP

Match the access control type to the example of the control type.

Drag each access control type net to its corresponding example.



Answer:



Explanation:

Administrative – labeling of sensitive data

Technical – Constrained user interface

Logical – Biometrics for authentication

Physical – Radio Frequency Identification 9RFID) badge

QUESTION NO: 412

In general, servers that are facing the Internet should be placed in a demilitarized zone (DMZ). What is **MAIN** purpose of the DMZ?

A.
Reduced risk to internal systems.

B.
Prepare the server for potential attacks.

C.
Mitigate the risk associated with the exposed server.

D.
Bypass the need for a firewall.

Answer: A

Explanation:

QUESTION NO: 413

Network-based logging has which advantage over host-based logging when reviewing malicious activity about a victim machine?

A.
Addresses and protocols of network-based logs are analyzed.

B.
Host-based system logging has files stored in multiple locations.

C.
Properly handled network-based logs may be more reliable and valid.

D.
Network-based systems cannot capture users logging into the console.

Answer: A

Explanation:

QUESTION NO: 414

Which of the following is the **PRIMARY** reason for employing physical security personnel at entry points in facilities where card access is in operation?

A.
To verify that only employees have access to the facility.

B.
To identify present hazards requiring remediation.

C.
To monitor staff movement throughout the facility.

D.
To provide a safe environment for employees.

Answer: D

Explanation:

QUESTION NO: 415

Between which pair of Open System Interconnection (OSI) Reference Model layers are routers used as a communications device?

A.
Transport and Session

B.
Data-Link and Transport

C.
Network and Session

D.
Physical and Data-Link

Answer: B

Explanation:

QUESTION NO: 416

Which type of security testing is being performed when an ethical hacker has no knowledge about the target system but the testing target is notified before the test?

A.
Reversal

B.
Gray box

C.
Blind

D.
White box

Answer: C
Explanation:

QUESTION NO: 417

Which of the following countermeasures is the **MOST** effective in defending against a social engineering attack?

A.
Mandating security policy acceptance

B.
Changing individual behavior

C.
Evaluating security awareness training

D.
Filtering malicious e-mail content

Answer: C
Explanation:

QUESTION NO: 418

Which of the following information **MUST** be provided for user account provisioning?

A.
Full name

B.
Unique identifier

C.
Security question

D.
Date of birth

Answer: B

Explanation:

QUESTION NO: 419

Which of the following adds end-to-end security inside a Layer 2 Tunneling Protocol (L2TP) Internet Protocol Security (IPSec) connection?

A.
Temporal Key Integrity Protocol (TKIP)

B.
Secure Hash Algorithm (SHA)

C.
Secure Shell (SSH)

D.
Transport Layer Security (TLS)

Answer: B

Explanation:

QUESTION NO: 420

A company has decided that they need to begin maintaining assets deployed in the enterprise. What approach should be followed to determine and maintain ownership information to bring the company into compliance?

A.
Enterprise asset management framework

B.
Asset baseline using commercial off the shelf software

C.
Asset ownership database using domain login records

D.
A script to report active user logins on assets

Answer: A
Explanation:

QUESTION NO: 421

In the Software Development Life Cycle (SDLC), maintaining accurate hardware and software inventories is a critical part of

A.
systems integration.

B.
risk management.

C.
quality assurance.

D.
change management.

Answer: D
Explanation:

QUESTION NO: 422

As a best practice, the Security Assessment Report (SAR) should include which of the following sections?

A.
Data classification policy

B.
Software and hardware inventory

C.
Remediation recommendations

D.
Names of participants

Answer: B

Explanation:

QUESTION NO: 423

The application of a security patch to a product previously validate at Common Criteria (CC) Evaluation Assurance Level (EAL) 4 would

A.
require an update of the Protection Profile (PP).

B.
require recertification.

C.
retain its current EAL rating.

D.
reduce the product to EAL 3.

Answer: B

Explanation:

QUESTION NO: 424

Which of the following media sanitization techniques is **MOST** likely to be effective for an organization using public cloud services?

A.
Low-level formatting

B.
Secure-grade overwrite erasure

C.
Cryptographic erasure

D.
Drive degaussing

Answer: B

Explanation:

QUESTION NO: 425

What type of wireless network attack **BEST** describes an Electromagnetic Pulse (EMP) attack?

A.
Radio Frequency (RF) attack

B.
Denial of Service (DoS) attack

C.
Data modification attack

D.
Application-layer attack

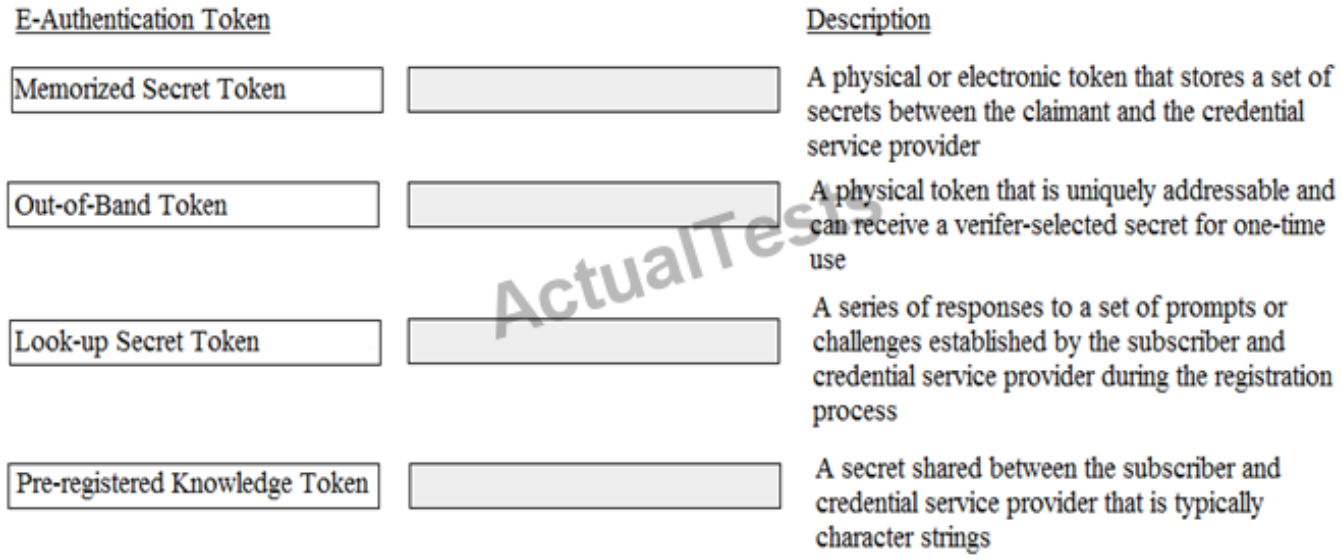
Answer: B

Explanation:

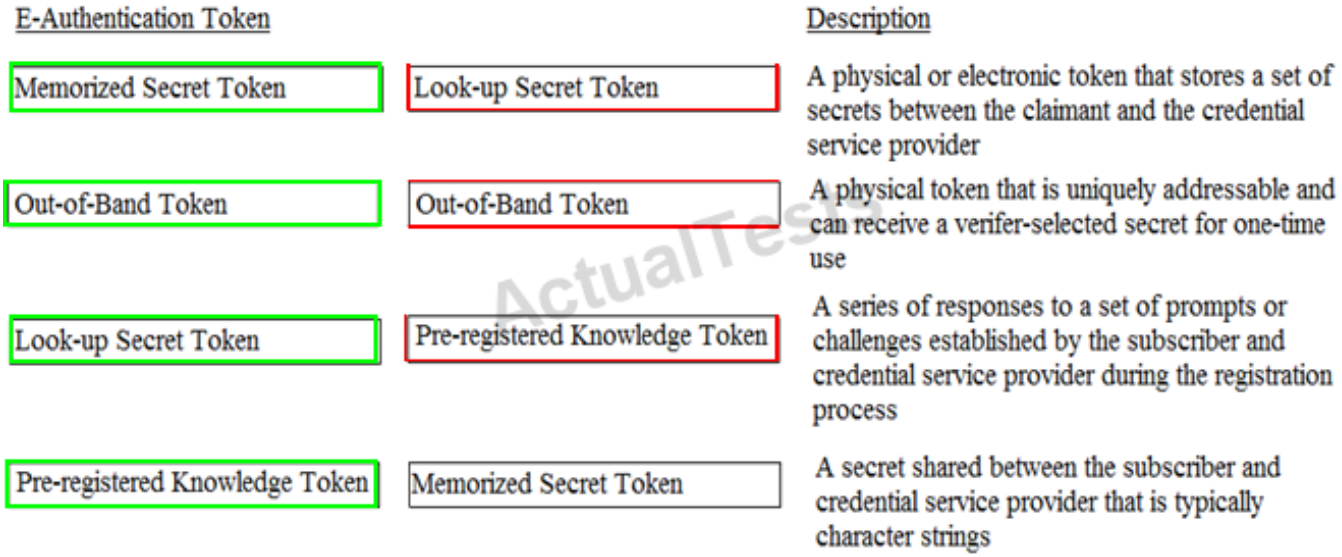
QUESTION NO: 426 DRAG DROP

Match the types of e-authentication tokens to their description.

Drag each e-authentication token on the left to its corresponding description on the right.



Answer:



Explanation:

Look-up secret token - A physical or electronic token that stores a set of secrets between the claimant and the credential service provider

Out-of-Band Token - A physical token that is uniquely addressable and can receive a verifier-selected secret for one-time use

Pre-registered Knowledge Token - A series of responses to a set of prompts or challenges established by the subscriber and credential service provider during the registration process

Memorized Secret Token - A secret shared between the subscriber and credential service provider

that is typically character strings

QUESTION NO: 427

Which of the following is a remote access protocol that uses a static authentication?

A.
Point-to-Point Tunneling Protocol (PPTP)

B.
Routing Information Protocol (RIP)

C.
Password Authentication Protocol (PAP)

D.
Challenge Handshake Authentication Protocol (CHAP)

Answer: C
Explanation:

QUESTION NO: 428

Which of the following sets of controls should allow an investigation if an attack is not blocked by preventive controls or detected by monitoring?

A.
Logging and audit trail controls to enable forensic analysis

B.
Security incident response lessons learned procedures

C.
Security event alert triage done by analysts using a Security Information and Event Management (SIEM) system

D.
Transactional controls focused on fraud prevention

Answer: C
Explanation:

QUESTION NO: 429

Determining outage costs caused by a disaster can **BEST** be measured by the

A.
cost of redundant systems and backups.

B.
cost to recover from an outage.

C.
overall long-term impact of the outage.

D.
revenue lost during the outage.

Answer: C
Explanation:

QUESTION NO: 430

Which of the following is considered a secure coding practice?

A.
Use concurrent access for shared variables and resources

B.
Use checksums to verify the integrity of libraries

C.
Use new code for common tasks

D.
Use dynamic execution functions to pass user supplied data

Answer: B

Explanation:

QUESTION NO: 431

As part of the security assessment plan, the security professional has been asked to use a negative testing strategy on a new website. Which of the following actions would be performed?

A.
Use a web scanner to scan for vulnerabilities within the website.

B.
Perform a code review to ensure that the database references are properly addressed.

C.
Establish a secure connection to the web server to validate that only the approved ports are open.

D.
Enter only numbers in the web form and verify that the website prompts the user to enter a valid input.

Answer: D
Explanation:

QUESTION NO: 432

Who has the **PRIMARY** responsibility to ensure that security objectives are aligned with organization goals?

A.
Senior management

B.
Information security department

C.
Audit committee

D.
All users

Answer: C

Explanation:

QUESTION NO: 433

Which of the following alarm systems is recommended to detect intrusions through windows in a high-noise, occupied environment?

A.
Acoustic sensor

B.
Motion sensor

C.
Shock sensor

D.
Photoelectric sensor

Answer: C

Explanation:

QUESTION NO: 434

Which of the following is the **MOST** effective practice in managing user accounts when an employee is terminated?

A.
Implement processes for automated removal of access for terminated employees.

B.
Delete employee network and system IDs upon termination.

C.
Manually remove terminated employee user-access to all systems and applications.

D.
Disable terminated employee network ID to remove all access.

Answer: D

Explanation:

QUESTION NO: 435

Which of the following is the **MOST** important part of an awareness and training plan to prepare employees for emergency situations?

A.
Having emergency contacts established for the general employee population to get information

B.
Conducting business continuity and disaster recovery training for those who have a direct role in the recovery

C.
Designing business continuity and disaster recovery training programs for different audiences

D.
Publishing a corporate business continuity and disaster recovery plan on the corporate website

Answer: C

Explanation:

QUESTION NO: 436

What is the process of removing sensitive data from a system or storage device with the intent that the data cannot be reconstructed by any known technique?

A.
Purging

B.
Encryption

C.
Destruction

D.
Clearing

Answer: A

Explanation:

QUESTION NO: 437

Which one of the following considerations has the **LEAST** impact when considering transmission security?

A.
Network availability

B.
Node locations

C.
Network bandwidth

D.
Data integrity

Answer: C

Explanation:

QUESTION NO: 438

The security accreditation task of the System Development Life Cycle (SDLC) process is completed at the end of which phase?

A.
System acquisition and development

B.
System operations and maintenance

C.
System initiation

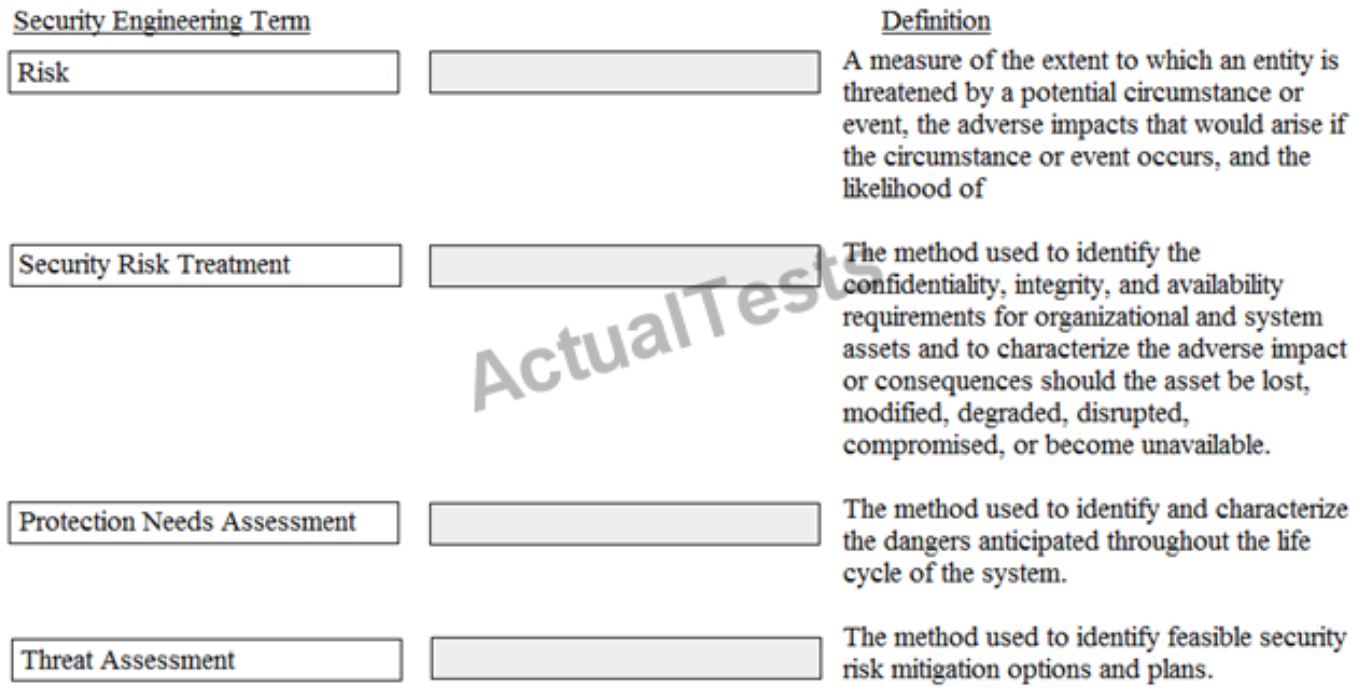
D.
System implementation

Answer: D

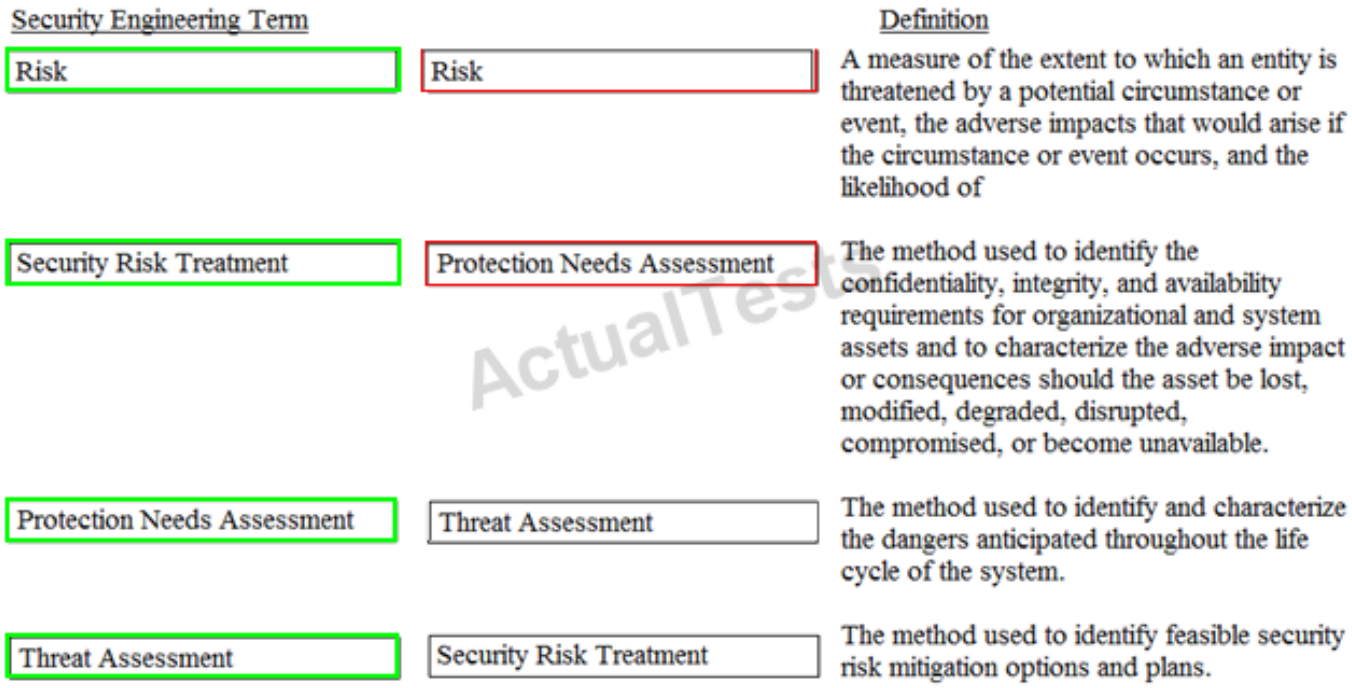
Explanation:

QUESTION NO: 439 DRAG DROP

Drag the following Security Engineering terms on the left to the **BEST** definition on the right.



Answer:



Explanation:

Risk - A measure of the extent to which an entity is threatened by a potential circumstance of event, the adverse impacts that would arise if the circumstance or event occurs, and the likelihood of occurrence.

Protection Needs Assessment - The method used to identify the confidentiality, integrity, and availability requirements for organizational and system assets and to characterize the adverse impact or consequences should be asset be lost, modified, degraded, disrupted, compromised, or become unavailable.

Threat assessment - The method used to identify and characterize the dangers anticipated throughout the life cycle of the system.

Security Risk Treatment - The method used to identify feasible security risk mitigation options and plans.

QUESTION NO: 440

Which of the following is the **BEST** reason for the use of security metrics?

A.
They ensure that the organization meets its security objectives.

B.
They provide an appropriate framework for Information Technology (IT) governance.

C.
They speed up the process of quantitative risk assessment.

D.
They quantify the effectiveness of security processes.

Answer: B
Explanation:

QUESTION NO: 441

Which of the following is a benefit in implementing an enterprise Identity and Access Management (IAM) solution?

A.
Password requirements are simplified.

B.
Risk associated with orphan accounts is reduced.

C.
Segregation of duties is automatically enforced.

D.
Data confidentiality is increased.

Answer: A
Explanation:

QUESTION NO: 442

Which of the following statements is **TRUE** regarding state-based analysis as a functional software testing technique?

A.
It is characterized by the stateless behavior of a process implemented in a function

B.
Test inputs are obtained from the derived boundaries of the given functional specifications

C.
An entire partition can be covered by considering only one representative value from that partition

D.
It is useful for testing communications protocols and graphical user interfaces

Answer: D
Explanation:

QUESTION NO: 443

Which of the following are important criteria when designing procedures and acceptance criteria for acquired software?

A.
Code quality, security, and origin

B.
Architecture, hardware, and firmware

C.
Data quality, provenance, and scaling

D.
Distributed, agile, and bench testing

Answer: A
Explanation:

QUESTION NO: 444

Which of the following steps should be performed **FIRST** when purchasing Commercial Off-The-Shelf (COTS) software?

A.
undergo a security assessment as part of authorization process

B.
establish a risk management strategy

C.
harden the hosting server, and perform hosting and application vulnerability scans

D.
establish policies and procedures on system and services acquisition

Answer: D
Explanation:

QUESTION NO: 445

An organization has outsourced its financial transaction processing to a Cloud Service Provider (CSP) who will provide them with Software as a Service (SaaS). If there was a data breach who is responsible for monetary losses?

A.
The Data Protection Authority (DPA)

B.
The Cloud Service Provider (CSP)

C.
The application developers

D.
The data owner

Answer: D
Explanation:

QUESTION NO: 446

What is the **PRIMARY** role of a scrum master in agile development?

A.
To choose the primary development language

B.
To choose the integrated development environment

C.
To match the software requirements to the delivery plan

D.
To project manage the software delivery

Answer: D
Explanation:

QUESTION NO: 447

What capability would typically be included in a commercially available software package designed for access control?

A.
Password encryption

B.
File encryption

C.
Source library control

D.
File authentication

Answer: A
Explanation:

QUESTION NO: 448

An organization plan on purchasing a custom software product developed by a small vendor to support its business model.

Which unique consideration should be made part of the contractual agreement potential long-term risks associated with creating this dependency?

A.
A source code escrow clause

B.
Right to request an independent review of the software source code

C.
Due diligence form requesting statements of compliance with security requirements

D.
Access to the technical documentation

Answer: B

Explanation: