CISSP Free Exam Questions & Answers PDF Updated on Dec-2023 [Q21-Q40
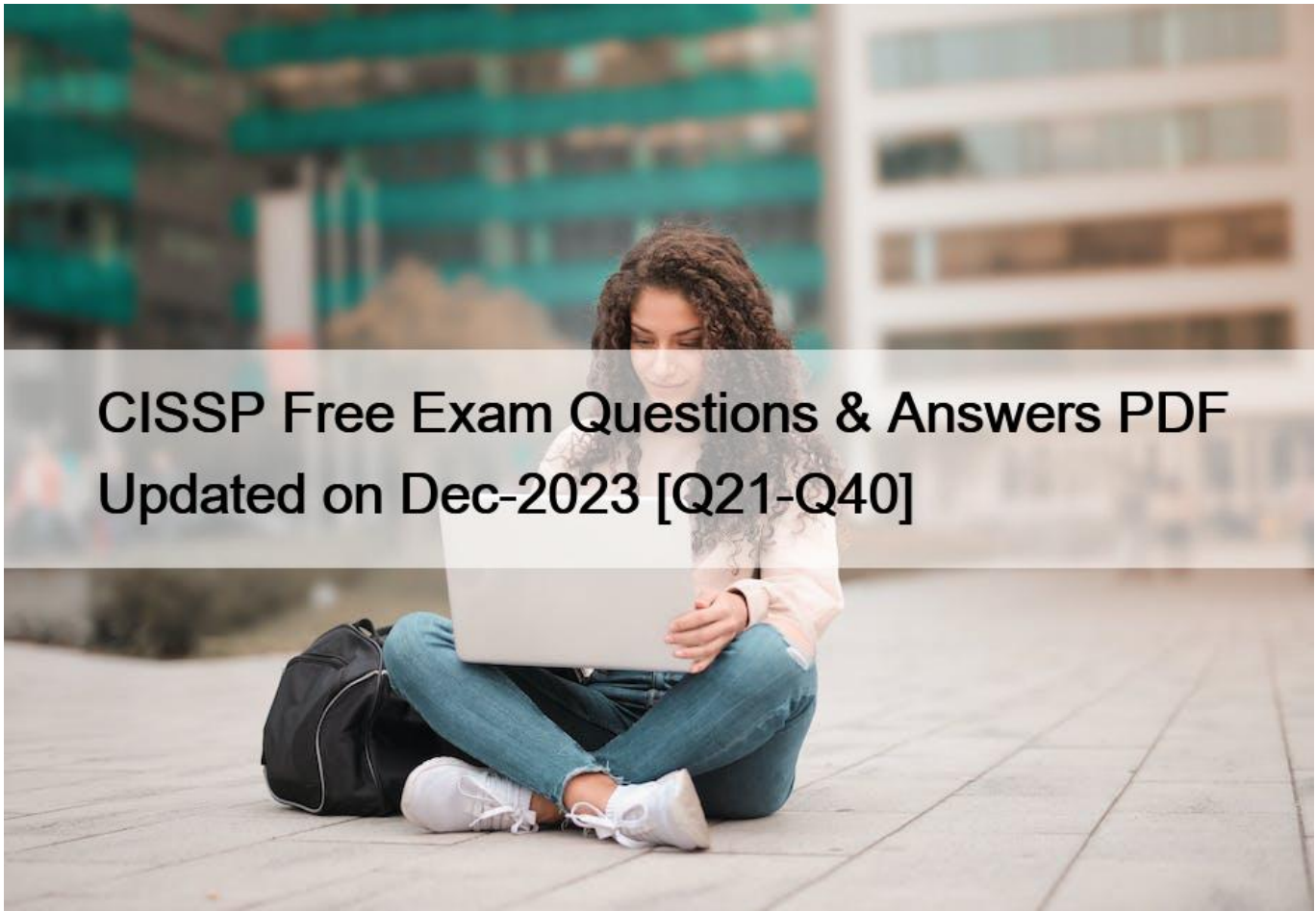

CISSP Free Exam Questions and Answers PDF Updated on Dec-2023
Latest CISSP Exam Dumps Recently Updated 1481 Questions

NEW QUESTION 21

What is the second step in the identity and access provisioning lifecycle?
* Provisioning
* Review
* Approval
* Revocation
Section: Identity and Access Management (IAM)

NEW QUESTION 22

As users switch roles within an organization, their accounts are given additional permissions to perform the duties of their new position. After a recent audit, it was discovered that many of these accounts maintained their old permissions as well. The obsolete permissions identified by the audit have been remediated and accounts have only the appropriate permissions to complete their jobs.

Which of the following is the BEST way to prevent access privilege creep?

* Implementing Identity and Access Management (IAM) solution
* Time-based review and certification
* Internet audit
* Trigger-based review and certification

Section: Mixed questions

NEW QUESTION 23

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

* Restrict use of SELECT command.
* Restrict stored procedures.
* Enforce boundary checking.
* Restrict Hyper Text Markup Language (HTML) source code access.

NEW QUESTION 24

Refer to the information below to answer the question.

A large organization uses unique identifiers and requires them at the start of every system session. Application access is based on job classification. The organization is subject to periodic independent reviews of access controls and violations. The organization uses wired and wireless networks and remote access. The organization also uses secure connections to branch offices and secure backup and recovery strategies for selected information and processes.

What MUST the access control logs contain in addition to the identifier?

* Time of the access
* Security classification
* Denied access attempts
* Associated clearance

NEW QUESTION 25

Which choice below is NOT an example of a media control?

* Printing to a printer in a secured room
* Conducting background checks on individuals
* Sanitizing the media before disposition
* Physically protecting copies of backup media

The answer is a personnel control. Most support and operations

staff have special access to the system. Some organizations conduct

background checks on individuals filling these positions to screen

out possibly untrustworthy individuals.

*Answer “Sanitizing the media before disposition”: The process of removing information from media before disposition is called sanitization. Three techniques are commonly used

for media sanitization: overwriting, degaussing, and destruction.

*Answer “Printing to a printer in a secured room”: It may be necessary to actually output data to the media in a secure location, such as printing to a printer in a locked room

instead of to a general-purpose printer in a common area.

*Answer “Physically protecting copies of backup media”: Physical protection of copies of backup media stored offsite should be accorded a level of protection equivalent to media

containing the same information stored onsite.

Source: National Institute of Standards and Technology, An Introduction to Computer Security: The NIST Handbook Special Publication 800-12.

NEW QUESTION 26

The security term that is concerned with the same primary key existing at different classification levels in the same database is:
* Polymorphism.
* Inheritance.
* Polyinstantiation.
* Normalization.
The security term that is concerned with

the same primary key existing at different classification levels in the same database is polyinstantiation.

Answer Polymorphism is incorrect because

polymorphism is defined as objects of many different classes that are

related by some common superclass; thus, any object denoted by this

name is able to respond to some common set of operations in a different way.

Answer Normalization is incorrect because normalization refers to

removing redundant or incorrect data from a database.

Answer Inheritance is incorrect because inheritance refers to methods from a class inherited by another subclass.

NEW QUESTION 27

Which of the following is the MOST important element of change management documentation?
* List of components involved
* Number of changes being made
* Business case justification
* A stakeholder communication

NEW QUESTION 28

Which statement is NOT true about the SOCKS protocol?

* It operates in the transport layer of the OSI model.
* It uses an ESP for authentication and encryption.
* It is sometimes referred to as an application-level proxy.
* Network applications need to be SOCKS-ified to operate.

The correct answer is “It uses an ESP for authentication and encryptio”. The Encapsulating

Security Payload, (ESP) is a component of IPSec. Socket Security (SOCKS) is a transport layer, secure networking proxy protocol. SOCKS replaces the standard network systems calls with its own calls. These calls open connections to a SOCKS proxy server for client authentication, transparently to the user.

Common network utilities, like TELNET or FTP, need to be SOCKSified,

or have their network calls altered to recognize SOCKS proxy calls.

Source: Designing Network Security by Merike Kaeo (Cisco Press, 1999).

NEW QUESTION 29

Contingency plan exercises are intended to do which of the following?
* Train personnel in roles and responsibilities
* Validate service level agreements
* Train maintenance personnel
* Validate operation metrics

NEW QUESTION 30

Which of the following controls related to physical security is not an administrative control?
* Personnel controls
* Alarms
* Training
* Emergency response and procedures

Physical security involves administrative, technical and physical controls.

All of the choices presented are part of Administrative Controls except Alarms which is a technical control.

Administrative Controls are mostly on paper. Senior management must decide what role security will play in the organization, including the security goals and objectives. These directives will dictate how all the supporting mechanisms will fall into place. Basically, senior management provides the skeleton of a security infrastructure and then appoints the proper entities to fill in the rest. Publishing the company security plan or security policy would be one of the first step under the administrative controls.

Personnel controls are part of Administrative Controls, it indicate how employees are expected to interact with security mechanisms and address noncompliance issues pertaining to these expectations. These controls indicate what security actions should be taken when an employee is hired, terminated, suspended, moved into another department, or promoted. Specific procedures must be developed for each situation, and many times the human resources and legal departments are involved with making these decisions.

Reference(s) used for this question:

Harris, Shon (2012-10-18). CISSP All-in-One Exam Guide, 6th Edition (p. 242). McGraw-

Hill . Kindle Edition.

and

Harris, Shon (2012-10-18). CISSP All-in-One Exam Guide, 6th Edition (p. 242). McGraw-

Hill . Kindle Edition.

NEW QUESTION 31

Which of the following technologies is a target of XSS or CSS (Cross-Site Scripting) attacks?
* Web Applications
* Intrusion Detection Systems
* Firewalls
* DNS Servers
XSS or Cross-Site Scripting is a threat to web applications where malicious code is

placed on a website that attacks the use using their existing authenticated session status.

Cross-Site Scripting attacks are a type of injection problem, in which malicious scripts are injected

into the otherwise benign and trusted web sites. Cross-site scripting (XSS) attacks occur when an

attacker uses a web application to send malicious code, generally in the form of a browser side

script, to a different end user. Flaws that allow these attacks to succeed are quite widespread and

occur anywhere a web application uses input from a user in the output it generates without

validating or encoding it.

An attacker can use XSS to send a malicious script to an unsuspecting user. The end user’s

browser has no way to know that the script should not be trusted, and will execute the script.

Because it thinks the script came from a trusted source, the malicious script can access any

cookies, session tokens, or other sensitive information retained by your browser and used with

that site. These scripts can even rewrite the content of the HTML page.

Mitigation:

-Configure your IPS – Intrusion Prevention System to detect and suppress this traffic.

-Input Validation on the web application to normalize inputted data.

-Set web apps to bind session cookies to the IP Address of the legitimate user and only permit that IP Address to use that cookie.

See the XSS (Cross Site Scripting) Prevention Cheat Sheet See the Abridged XSS Prevention Cheat Sheet See the DOM based XSS Prevention Cheat Sheet See the OWASP Development Guide article on Phishing. See the OWASP Development Guide article on

Data Validation.

The following answers are incorrect:

-Intrusion Detection Systems: Sorry. IDS Systems aren’t usually the target of XSS attacks but a properly-configured IDS/IPS can “detect and report on malicious string and suppress the TCP connection in an attempt to mitigate the threat.

-Firewalls: Sorry. Firewalls aren’t usually the target of XSS attacks.

-DNS Servers: Same as above, DNS Servers aren’t usually targeted in XSS attacks but they play a key role in the domain name resolution in the XSS attack process.

The following reference(s) was used to create this question:

https://www.owasp.org/index.php/Cross-site_Scripting_%28XSS%29

NEW QUESTION 32

Which of the following media sanitization techniques is MOST likely to be effective for an organization using public cloud services?
* Low-level formatting
* Secure-grade overwrite erasure
* Cryptographic erasure
* Drive degaussing

NEW QUESTION 33

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?
* Connect the device to another network jack
* Apply remediation’s according to security requirements
* Apply Operating System (OS) patches
* Change the Message Authentication Code (MAC) address of the network interface

NEW QUESTION 34

Which of the following answer specifies the correct sequence of levels within the Capability Maturity Model (CMM)?
* Initial, Managed, Defined, Quantitatively managed, optimized
* Initial, Managed, Defined, optimized, Quantitatively managed
* Initial, Defined, Managed, Quantitatively managed, optimized
* Initial, Managed, Quantitatively managed, Defined, optimized
Maturity model A maturity model can be viewed as a set of structured levels that describe how well the behaviors, practices and processes of an organization can reliably and sustainable produce required outcomes.

CMMI Staged Maturity Levels

Image Source – http://www.cmmilevels.com/cmmi-levels.jpg

A maturity model can be used as a benchmark for comparison and as an aid to understanding – for

example, for comparative assessment of different organizations where there is something in

common that can be used as a basis for comparison. In the case of the CMM, for example, the

basis for comparison would be the organizations’ software development processes.

Structure

The model involves five aspects:

Maturity Levels: a 5-level process maturity continuum – where the uppermost (5th) level is a

notional ideal state where processes would be systematically managed by a combination of

process optimization and continuous process improvement.

Key Process Areas: a Key Process Area identifies a cluster of related activities that, when

performed together, achieve a set of goals considered important.

Goals: the goals of a key process area summarize the states that must exist for that key process

area to have been implemented in an effective and lasting way. The extent to which the goals

have been accomplished is an indicator of how much capability the organization has established

at that maturity level. The goals signify the scope, boundaries, and intent of each key process

area.

Common Features: common features include practices that implement and institutionalize a key

process area. There are five types of common features: commitment to perform, ability to perform,

activities performed, measurement and analysis, and verifying implementation.

Key Practices: The key practices describe the elements of infrastructure and practice that

contribute most effectively to the implementation and institutionalization of the area.

Levels

There are five levels defined along the continuum of the model and, according to the SEI:

“Predictability, effectiveness, and control of an organization’s software processes are believed to

improve as the organization moves up these five levels. While not rigorous, the empirical evidence

to date supports this belief”.

Initial (chaotic, ad hoc, individual heroics) – the starting point for use of a new or undocumented

repeat process.

Repeatable – the process is at least documented sufficiently such that repeating the same steps

may be attempted.

Defined – the process is defined/confirmed as a standard business process, and decomposed to

levels 0, 1 and 2 (the last being Work Instructions).

Managed – the process is quantitatively managed in accordance with agreed-upon metrics.

Optimizing – process management includes deliberate process optimization/improvement.

Within each of these maturity levels are Key Process Areas which characteristic that level, and for

each such area there are five factors: goals, commitment, ability, measurement, and verification.

These are not necessarily unique to CMM, representing – as they do – the stages that

organizations must go through on the way to becoming mature.

The model provides a theoretical continuum along which process maturity can be developed

incrementally from one level to the next. Skipping levels is not allowed/feasible.

Level 1 – Initial (Chaotic)

It is characteristic of processes at this level that they are (typically) undocumented and in a state of dynamic change, tending to be driven in an ad hoc, uncontrolled and reactive manner by users or events. This provides a chaotic or unstable environment for the processes.

Level 2 – Repeatable

It is characteristic of processes at this level that some processes are repeatable, possibly with consistent results. Process discipline is unlikely to be rigorous, but where it exists it may help to ensure that existing processes are maintained during times of stress.

Level 3 – Defined

It is characteristic of processes at this level that there are sets of defined and documented standard processes established and subject to some degree of improvement over time. These standard processes are in place (i.e., they are the AS-IS processes) and used to establish consistency of process performance across the organization.

Level 4 – Managed

It is characteristic of processes at this level that, using process metrics, management can effectively control the AS-IS process (e.g., for software development). In particular, management can identify ways to adjust and adapt the process to particular projects without measurable losses of quality or deviations from specifications. Process Capability is established from this level.

Level 5 – Optimizing

It is a characteristic of processes at this level that the focus is on continually improving process performance through both incremental and innovative technological changes/improvements.

At maturity level 5, processes are concerned with addressing statistical common causes of process variation and changing the process (for example, to shift the mean of the process performance) to improve process performance. This would be done at the same time as maintaining the likelihood of achieving the established quantitative process-improvement

objectives.

The following answers are incorrect:

The other option specified in the option does not provide correct sequence.

The following reference(s) were/was used to create this question:

CISA review manual 2014 Page number 188

CISSP Official study guide page number 693

Topic 5, Security Operations

NEW QUESTION 35

A reference monitor is a system component that enforces access controls on an object. Specifically, the reference monitor concept is an abstract machine that mediates all access of subjects to objects. The hardware, firmware, and software elements of a trusted computing base that

implement the reference monitor concept are called:
* Identification and authentication (I & A) mechanisms
* The auditing subsystem
* The security kernel
* The authorization database
The security kernel implements the reference model concept. The

reference model must have the following characteristics:

It must mediate all accesses.

It must be protected from modification.

It must be verifiable as correct.

Answer “the authorization database” is used by the reference monitor

to mediate accesses by subjects to objects. When a request for access

is received, the reference monitor refers to entries in the authorization database to verify that the operation requested by a subject for application to an object is permitted. The authorization database has entries or authorizations of the form subject, object, access mode.

In answer “Identification and authentication (I & A) mechanisms”, the

I & A operation is separate from the reference monitor. The user enters his/her identification to the I & A function. Then the user must be authenticated. Authentication is verification that the user’s claimed identity is valid. Authentication is based on the following three factor types:

Type 1. Something you know, such as a PIN or password

Type 2. Something you have, such as an ATM card or smart card

Type 3. Something you are (physically), such as a fingerprint or

retina scan

Answer "The auditing subsystem" is a key complement to the reference

monitor. The auditing subsystem is used by the reference

monitor to keep track of the reference monitor's activities. Examples

of such activities include the date and time of an access request, identification of the subject and objects involved, the access privileges requested and the result of the request.

NEW QUESTION 36

The Simple Security Property and the Star Property are key principles in

which type of access control?
* Mandatory
* Discretionary
* Rule-based
* Role-based
Two properties define fundamental principles of mandatory access control. These properties are: Simple Security Property. A user at one clearance level cannot read data from a higher classification level. Star Property. A user at one clearance level cannot write data to a lower classification level

NEW QUESTION 37

Which of the following is MOST appropriate for protecting confidentially of data stored on a hard drive?
* Triple Data Encryption Standard (3DES)
* Advanced Encryption Standard (AES)
* Message Digest 5 (MD5)
* Secure Hash Algorithm 2(SHA-2)

NEW QUESTION 38

What is the PRIMARY use of a password?
* Allow access to files.
* Identify the user.
* Authenticate the user.
* Segregate various user's accesses.
Source: TIPTON, Hal, (ISC)2, Introduction to the CISSP Exam presentation.

NEW QUESTION 39

A 1999 law that addresses privacy issues related to health care,

insurance and finance and that will be implemented by the states is:

* Kennedy-Kassebaum
* Gramm-Leach-Bliley (GLB)
* Insurance Reform Act
* Medical Action Bill

See the answers to

Question 15

for a discussion of GLb.

* Answer Kennedy-Kassebaum refers to the HIPAA legislation (US Kennedy-Kassebaum Health

Insurance and Portability Accountability Act HIPAA-Public Law 104-19).

Answers Medical Action Bill and Insurance Reform Act are distracters.

NEW QUESTION 40

What does the * (star) integrity axiom mean in the Biba model?
* No read up
* No write down
* No read down
* No write up

Explanation/Reference:

Explanation:

The Biba model was developed after the Bell-LaPadula model. It is a state machine model similar to the Bell-LaPadula model. Biba addresses the integrity of data within applications.

The Biba model uses a lattice of integrity levels. If implemented and enforced properly, the Biba model prevents data from any integrity level from flowing to a higher integrity level.

Biba has three main rules to provide this type of protection:

*-integrity axiom: A subject cannot write data to an object at a higher integrity level (referred to as “no

.

write up”).

Simple integrity axiom: A subject cannot read data from a lower integrity level (referred to as “no read

.

down”).

Invocation property: A subject cannot request service (invoke) of higher integrity.

.

Incorrect Answers:

A: The * (star) integrity axiom means “no write up”, not “no read up”.

B: The * (star) integrity axiom means “no write up”, not “no write down”.

C: The * (star) integrity axiom means “no write up”, not “no read down”.

References:

Harris, Shon, All In One CISSP Exam Guide, 6th Edition, McGraw-Hill, New York, 2013, p. 372

ISC CISSP Real 2023 Braindumps Mock Exam Dumps: https://www.vceprep.com/CISSP-latest-vce-prep.html]