Free Questions for CSSLP by actualtestdumps

Shared by Barlow on 06-06-2022

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: **MultipleChoice**

Which of the following describes the acceptable amount of data loss measured in time?

Options:

A- Recovery Point Objective (RPO)

B- Recovery Time Objective (RTO)

C- Recovery Consistency Objective (RCO)

D- Recovery Time Actual (RTA)

Answer:

A

Explanation:

The Recovery Point Objective (RPO) describes the acceptable amount of data loss measured in time. It is the point in time to which data must be recovered as defined by the organization. The RPO is generally a definition of what an organization determines is an 'acceptable loss' in a disaster situation. If the RPO of a company is 2 hours and the time it takes to get the data back into production is 5 hours, the RPO is still 2 hours. Based on this RPO the data must be restored to within 2 hours of the disaster.

Answer B is incorrect. The Recovery Time Objective (RTO) is the duration of time and a service level within which a business process must be restored after a disaster or disruption in order to avoid unacceptable consequences associated with a break in business continuity. It includes the time for trying to fix the problem without a recovery, the recovery itself, tests and the communication to the users. Decision time for user representative is not included. The business continuity timeline usually runs parallel with an incident management timeline and may start at the same, or different, points.

In accepted business continuity planning methodology, the RTO is established during the Business Impact Analysis (BIA) by the owner of a process (usually in conjunction with the Business Continuity planner). The RTOs are then presented to senior management for acceptance.

The RTO attaches to the business process and not the resources required to support the process.

Answer D is incorrect. The Recovery Time Actual (RTA) is established during an exercise, actual event, or predetermined based on

recovery methodology the technology support team develops. This is the time frame the technology support takes to deliver the recovered

infrastructure to the business.

Answer C is incorrect. The Recovery Consistency Objective (RCO) is used in Business Continuity Planning in addition to Recovery Point

Objective (RPO) and Recovery Time Objective (RTO). It applies data consistency objectives to Continuous Data Protection services.

Question 2

Question Type: MultipleChoice

Copyright holders, content providers, and manufacturers use digital rights management (DRM) in order to limit usage of digital media and devices. Which of the following security challenges does DRM include? Each correct answer represents a complete solution. Choose all that apply.

Options:

A- OTA provisioning

B- Access control

C- Key hiding

D- Device fingerprinting

Answer:

A, C, D

Explanation:

The security challenges for DRM are as follows:

Key hiding: It prevents tampering attacks that target the secret keys. In the key hiding process, secret keys are used for authentication, encryption, and node-locking.

Device fingerprinting: It prevents fraud and provides secure authentication. Device fingerprinting includes the summary of hardware and software characteristics in order to uniquely identify a device.

OTA provisioning: It provides end-to-end encryption or other secure ways for delivery of copyrighted software to mobile devices.

Answer B is incorrect. Access control is not a security challenge for DRM.

Question 3

Question Type: MultipleChoice

Which of the following terms refers to the protection of data against unauthorized access?

Options:

A- Integrity

B- Recovery

C- Auditing

D- Confidentiality

Answer:

D

Explanation:

Confidentiality is a term that refers to the protection of data against unauthorized access. Administrators can provide confidentiality by encrypting data. Symmetric encryption is a relatively fast encryption method. Hence, this method of encryption is best suited for encrypting

large amounts of data such as files on a computer.

Answer A is incorrect. Integrity ensures that no intentional or unintentional unauthorized modification is made to data.

Answer C is incorrect. Auditing is used to track user accounts for file and object access, logon attempts, system shutdown etc. This

enhances the security of the network. Before enabling auditing, the type of event to be audited should be specified in the Audit Policy in User

Manager for Domains.

Question 4

Question Type: MultipleChoice

Which of the following are the responsibilities of a custodian with regard to data in an information classification program? Each correct answer represents a complete solution. Choose three.

Options:

A- Performing data restoration from the backups when necessary

B- Running regular backups and routinely testing the validity of the backup data

C- Determining what level of classification the information requires

D- Controlling access, adding and removing privileges for individual users

Answer:

A, B, D

Explanation:

The owner of information delegates the responsibility of protecting that information to a custodian. The following are the responsibilities of a

custodian with regard to data in an information classification program:

Running regular backups and routinely testing the validity of the backup data

Performing data restoration from the backups when necessary

Controlling access, adding and removing privileges for individual users

Answer C is incorrect. Determining what level of classification the information requires is the responsibility of the owner.

Question 5

Question Type: MultipleChoice

Which of the following DoD directives defines DITSCAP as the standard C&A process for the Department of Defense?

Options:

A- DoD 8910.1

B- DoD 5200.22-M

C- DoD 8000.1

D- DoD 5200.40

Answer:

D

Explanation:

DITSCAP stands for DoD Information Technology Security Certification and Accreditation Process. The DoD Directive 5200.40 (DoD Information

Technology Security Certification and Accreditation Process) established the DITSCAP as the standard C&A process for the Department of

Defense. The Department of Defense Information Assurance Certification and Accreditation Process (DIACAP) is a process defined by the

United States Department of Defense (DoD) for managing risk. DIACAP replaced the former process, known as DITSCAP, in 2006.

Answer B is incorrect. This DoD Directive is known as National Industrial Security Program Operating Manual.

Answer C is incorrect. This DoD Directive is known as Defense Information Management (IM) Program.

Answer A is incorrect. This DoD Directive is known as Management and Control of Information Requirements.

Question 6

Question Type: **MultipleChoice**

Which of the following elements of the BCP process emphasizes on creating the scope and the additional elements required to define the parameters of the plan?

Options:

A- Business continuity plan development

B- Plan approval and implementation

C- Business impact analysis

D- Scope and plan initiation

Answer:

D

Explanation:

The scope and plan initiation process in BCP symbolizes the beginning of the BCP process. It emphasizes on creating the scope and the

additional elements required to define the parameters of the plan.

The scope and plan initiation phase embodies a check of the company's operations and support services. The scope activities include creating

a detailed account of the work required, listing the resources to be used, and defining the management practices to be employed.

Answer C is incorrect. The business impact assessment is a method used to facilitate business units to understand the impact of a

disruptive event. This phase includes the execution of a vulnerability assessment. This process makes out the mission-critical areas and

business processes that are important for the survival of business.

It is similar to the risk assessment process. The function of a business impact assessment process is to create a document, which is used to

help and understand what impact a disruptive event would have on the business.

Answer A is incorrect. The business continuity plan development refers to the utilization of the information collected in the Business

Impact Analysis (BIA) for the creation of the recovery strategy plan to support the critical business functions. The information gathered from

the BIA is mapped out to make a strategy for creating a continuity plan. The business continuity plan development process includes the areas

of plan implementation, plan testing, and ongoing plan maintenance. This phase also consists of defining and documenting the continuity

strategy.

Answer B is incorrect. The plan approval and implementation process involves creating enterprise-wide awareness of the plan, getting

the final senior management signoff, and implementing a maintenance procedure for updating the plan as required.

20%
DISCOUNT