GETCERTKEY

GETCERTKEY
100% guarantee you pass IT cert exam!

http://www.getcertkey.com

No help, Full refund!

Exam : **312-76**

Title : EC-Council Disaster Recovery Professional (EDRP)

Vendor : EC-COUNCIL

Version : DEMO

NO.1 What is the name of the shared directory in the Microsoft Server OS, which contains the copy of commonly shared and replicated public files of that particular domain?

A. ADFS

B. SYSVOL

C. inetpub

D. Public Files

Answer: B

Explanation:

SYSVOL (System Volume) is a shared directory in Microsoft Server OS that stores domain public files, such as Group Policy objects and scripts, replicated across domain controllers.

* Option A (ADFS):Active Directory Federation Services, unrelated to file storage.
* Option C (inetpub):Hosts web server files, not domain-shared files.
* Option D (Public Files):Too generic, not a specific directory.
* "SYSVOL is a critical directory in Windows domains, replicating shared files across controllers for consistency and accessibility" (Module: Server Management, Section: Domain Operations).

NO.2 Sam was working on an Ubuntu OS-based system and accidentally deleted some of his official project files.

Fortunately, he had taken a backup of his system previously. Which of the following native Ubuntu options should he use to recover his deleted files?

A. Deja Dup

B. Checkpoints

C. Shadow Copy

D. Snapshots

Answer: A

Explanation:

Deja Dup is Ubuntu's native backup and restore tool, allowing Sam to recover deleted files from a previous backup.

* Option B (Checkpoints):Hyper-V term, not Ubuntu.
* Option C (Shadow Copy):Windows feature, not Ubuntu.
* Option D (Snapshots):General term, not Ubuntu-specific.
* "Deja Dup, Ubuntu's native backup utility, enables file recovery from prior backups, simplifying restoration on Linux systems" (Module: System Recovery, Section: OS-Specific Tools).

NO.3 Which of the following terms refers to a set of tasks that organizations must continue throughout or resume rapidly after a disruptive incident?

A. Business Impact Analysis

B. Risk Mitigation

C. Mission Essential Functions (MEF)

D. Maximum Allowed Downtime (MAD)

Answer: C

Explanation:

Mission Essential Functions (MEF) are critical tasks an organization must maintain or quickly resume post- disruption to ensure continuity.

* Option A (BIA):Identifies impacts, not tasks.
* Option B (Mitigation):Reduces risks, not task-focused.
* Option D (MAD):Downtime limit, not tasks.
* "Mission Essential Functions (MEF) are vital tasks requiring continuous or rapid resumption to sustain operations post-incident" (Module: Business Continuity Planning, Section: MEF Definition).

NO.4 Which of the following terms refers to the training milestones that must be achieved in order to meet the BC training program's aim?

A. Time-Related Objectives

B. Development Objectives

C. Routine Objectives

D. Terminal Objectives

Answer: D

Explanation:

Terminal Objectives are the specific milestones or end goals of a training program, ensuring the BC training aim is met.
* Option A (Time-Related):Time-focused, not milestones.
* Option B (Development):Process-oriented, not end goals.
* Option C (Routine):Daily tasks, not training-specific.
* "Terminal Objectives define the key milestones to achieve BC training goals, ensuring preparedness aligns with program aims" (Module: Training and Awareness, Section: Training Objectives).

NO.5 Which of the following terms refers to the recommencement of business functions and operations as the systems are gradually made available after the occurrence of a disaster?

A. Return

B. Resume

C. Reduce

D. Recover

Answer: B

Explanation:

"Resume" refers to restarting or recommencing business operations post-disaster as systems become available, aligning with business continuity goals.
* Option A (Return):Too vague, not a specific DR term.
* Option C (Reduce):Unrelated to restarting operations.
* Option D (Recover):Focuses on data/system restoration, not operational resumption.
* EDRP v3 uses "resume" to describe the phase of restoring business functions after recovery (Module:
Business Continuity Management).

NO.6 Which of the following terms measures the number of applications or data sets handled by the recovery solution and the maximum size of the data it can store?

A. Recovery Service Scalability (RSS)

B. Recovery Location Scope (RLS)

C. Recovery Point Objective (RPO)

D. Recovery Service Resiliency (RSR)

Answer: A
Explanation:
Recovery Service Scalability (RSS) measures a recovery solution's capacity to handle multiple applications or data sets and the maximum data size it can manage, reflecting its scalability.
* Option B (RLS):Refers to the geographic scope of recovery, not capacity.
* Option C (RPO):Measures data loss tolerance, not scalability.
* Option D (RSR):Focuses on resilience, not size or number of applications.
* EDRP v3 defines RSS as a metric for evaluating recovery solution scalability, critical for large-scale environments (Module: Recovery Metrics).

NO.7 When information confidentiality increases in PASIS architecture, what else also increases as a direct result?
A. Reaction
B. Latency
C. Storage Requirement
D. Durability
Answer: C
Explanation:
In PASIS architecture, increasing confidentiality (e.g., via encryption) increases storage requirements due to added overhead (e.g., metadata, keys).
* Option A (Reaction):Not a PASIS feature.
* Option B (Latency):May increase, but not direct as storage.
* Option D (Durability):Unaffected by confidentiality.
* "Higher confidentiality in PASIS, through encryption, directly increases storage needs due to additional data overhead" (Module: Survivable Storage Systems, Section: PASIS Trade-offs).

NO.8 Which of the following is also known as the doomsday recovery level in 3DR?
A. Local Data Protection
B. Archiving of Data
C. Backup of Data
D. Remote Backup of Data Protection
Answer: D
Explanation:
In the 3DR (Data Protection, Disaster Recovery, Doomsday Recovery) model, Remote Backup of Data Protection is termed the "doomsday recovery level," representing the ultimate offsite safeguard against catastrophic loss.
* Option A:Basic local protection, not doomsday-level.
* Option B:Long-term storage, not recovery-focused.
* Option C:General backup, not remote-specific.
* "Remote Backup of Data Protection, dubbed the doomsday recovery level in 3DR, ensures data survival through offsite replication" (Module: Data Protection Strategies, Section: 3DR Model).

NO.9 What is the main objective of a BC test plan?
A. To demonstrate proficiency in management response and crisis conditions
B. To ensure the plan is accurate and relevant under adverse circumstances

C. To diverge from the test storyboard to include unplanned events or circumstances

D. Not threaten the normal business operations of an organization

Answer: B

Explanation:

The main objective of a Business Continuity (BC) test plan is to ensure the plan's accuracy and relevance under adverse conditions, validating its effectiveness.

* Option A:Secondary, not the primary goal.
* Option C:Unplanned events may occur, but not the objective.
* Option D:A consideration, not the main purpose.
* "The primary objective of a BC test plan is to confirm its accuracy and relevance, ensuring it performs under disaster conditions" (Module: Testing Disaster Recovery Plans, Section: BC Testing Goals).

NO.10 Which layer of the Recovery Management Model would provide hassle-free recovery of systems in case of a disaster and would enable the control of data protection technologies such as replication and backup?

A. Protection Technologies Layer

B. Testing Simulation Layer

C. Common Management Layer

D. Analytics and Reporting Layer

Answer: A

Explanation:

The Protection Technologies Layer in a Recovery Management Model manages tools like replication and backup, ensuring hassle-free system recovery, as described.

* Option B (Testing Simulation):Validates plans, not recovery execution.
* Option C (Common Management):Coordinates, not tech-specific.
* Option D (Analytics):Monitors, not recovery-focused.
* "The Protection Technologies Layer controls replication and backup, enabling seamless system recovery post-disaster" (Module: Recovery Processes, Section: Recovery Management Model).

NO.11 Seth wants to get an approximate picture of the likelihood of the risks that were identified by his organization.

After getting a high-level understanding of their probability, he could dedicate his resources to risk mitigation according to the priorities since he was a bit under-staffed. He was told that out of the identified risks, the occurrence of an earthquake was highly unlikely owing to the geography of their location. Furthermore, he learned that the chances of a fire breaking out in his building were high and his facility also faced a risk of physical intrusion but that was partly under control owing to the physical guards. What kind of risk assessment is Seth essentially conducting?

A. Quantitative Risk Assessment

B. Qualitative Risk Assessment

C. Semi-Qualitative Risk Assessment

D. Semi-Quantitative Risk Assessment

Answer: B

Explanation:

Qualitative Risk Assessment evaluates risks based on subjective likelihood (e.g., "high," "low") and

impact, without precise numerical values, fitting Seth's high-level probability approach.
* Option A (Quantitative):Uses numerical data (e.g., percentages), not applicable here.
* Option C (Semi-Qualitative):A hybrid, but Seth's method is fully qualitative.
* Option D (Semi-Quantitative):Combines numbers with qualitative, not evident here.
* "Qualitative Risk Assessment prioritizes risks using descriptive scales (e.g., high, low) for probability and impact, ideal for resource-constrained planning" (Module: Risk Management, Section: Assessment Types).

NO.12 ABC Investment Bank is implementing a security and disaster recovery plan. As part of the plan, it sets up several remote data centers across the globe. The objective was to not have all the records of any one important client at one location but to distribute chunks of it throughout these centers. This was so if any one of the centers is compromised, the attacker will not have only chunks of data and will not be able to use it maliciously against the bank's clients. One other advantage of this is that if a center is struck by a disaster, all the data about a client's portfolio is not lost. For this plan to work, a percentage of deviation should not exist between the actual and targeted business data. Which recovery metric best defines this percentage of deviation?

A. Recovery Consistency Objective (RCO)

B. Recovery Object Granularity (ROG)

C. Recovery Location Scope (RLS)

D. Recovery Service Resiliency (RSR)

Answer: A

Explanation:
Recovery Consistency Objective (RCO) measures the allowable deviation between actual and target data consistency, critical for ABC's distributed data plan.
* Option B (ROG):Data recovery detail level, not consistency.
* Option C (RLS):Geographic recovery scope, not deviation.
* Option D (RSR):Service resilience, not data consistency.
* "RCO ensures minimal deviation in data consistency across distributed centers, vital for security and partial loss prevention" (Module: Recovery Metrics, Section: RCO Definition).

NO.13 An organization is facing issues with updating its data since it has been the culture of the organization for employees to create individual backups for the same data. This is not only consuming a lot of virtual storage space but is also eating into the bandwidth of the organization. Additionally, this can also lead to a potential data leak in the organization. What can be done to contain this situation?

A. Data Erasure

B. Data Remanence

C. Failover

D. Deduplication

Answer: D

Explanation:
Deduplication eliminates redundant data copies, reducing storage and bandwidth usage while minimizing data leak risks by centralizing control. It's ideal for this scenario where multiple individual backups exist.
* Option A (Data Erasure):Deletes data, not a solution for redundancy.

* Option B (Data Remanence):Refers to residual data, not a fix here.
* Option C (Failover):Switches to a backup system, unrelated to data management.
* EDRP v3 highlights deduplication as a storage optimization technique to enhance efficiency and security (Module: Data Backup and Recovery).

NO.14 ABC Inc. has a host of servers, each serving a different purpose. Almost all of them are critical to the functioning of the business. Most of the servers were virtualized and had backup virtual components. Thus, when the memory of one server crashed in the middle of a busy business day, it did not affect the operations as the server quickly switched to a different virtual memory, which was kept as a backup for this purpose precisely. What is such a feature called?

A. Deduplication

B. High Availability

C. Fault Tolerance

D. Mirroring

Answer: B

Explanation:
High Availability (HA) ensures continuous operation by automatically switching to backup components (like virtual memory) during a failure, minimizing downtime, as in ABC Inc.'s case.
* Option A (Deduplication):Removes redundant data, not a failover feature.
* Option C (Fault Tolerance):Prevents failure impact but typically implies no interruption, not a switch.
* Option D (Mirroring):Duplicates data, a component of HA, but not the full feature.
* "High Availability maintains operations through automatic failover to backup resources, ensuring business continuity during component failures" (Module: System Resilience, Section: Availability Features).

NO.15 In which scenario training phase is a debrief conducted with the participants to obtain more feedback?

A. Execution Phase

B. Review Phase

C. Warning Phase

D. Planning Phase

Answer: B

Explanation:
The Review Phase of scenario training occurs after execution and involves a debrief with participants to gather feedback, assess performance, and identify improvements. This aligns with the question's focus on obtaining feedback post-training.
* Option A (Execution Phase):The active running of the scenario, no debrief yet.
* Option C (Warning Phase):Not a standard phase; implies pre-event alerts.
* Option D (Planning Phase):Prepares the scenario, not for feedback collection.
* "The Review Phase follows scenario execution, involving a debrief to collect participant feedback and refine the training process" (Module: Training and Awareness, Section: Training Phases).