DUMPSARENA

Disaster Recovery Professional Practice Test

ECCouncil 312-76

Version Demo

Total Demo Questions: 37

Total Premium Questions: 370

Buy Premium PDF

https://dumpsarena.co

sales@dumpsarena.co

sales@dumpsarena.co
dumpsarena.co

Topic Break Down

Topic	No. of Questions
Topic 1, Introduction to Disaster Recovery and Business Continuity	51
Topic 2, Business Impact Analysis	23
Topic 3, Risk Assessment	39
Topic 4, Development of Disaster Recovery and Business Continuity Plans	66
Topic 5, Implementation of Disaster Recovery and Business Continuity Plans	84
Topic 6, Development of Disaster Recovery and Business Continuity Policies and Procedures	18
Topic 7, Disaster Recovery and Business Continuity Plan Testing, Assessment, and Maintenance	28
Topic 8, Disaster Recovery and Business Continuity Management	14
Topic 9, Mix Questions	47
Total	370

QUESTION NO: 1

Configuration Management (CM) is an Information Technology Infrastructure Library (ITIL) IT Service Management (ITSM) process. Configuration Management is used for which of the following?

Each correct answer represents a part of the solution. Choose all that apply.

A. To verify configuration records and correct any exceptions

B. To account for all IT assets

C. To provide precise information support to other ITIL disciplines

D. To provide a solid base only for Incident and Problem Management

ANSWER: A B C

Explanation:

Configuration Management maintains reliable, current information about configuration items and the relationships between them, traditionally through a configuration management database. A central purpose is *to account for all IT assets* and the relevant configuration items that support services. This provides visibility into what exists, its status, ownership, version, and dependencies, enabling the organization to manage service infrastructure in a controlled manner.

It is also used *to verify configuration records and correct any exceptions*. Configuration verification and audit activities compare the recorded configuration information with the actual environment, identify discrepancies, and ensure that records remain accurate enough to support operational and governance decisions.

Accurate configuration information is intended *to provide precise information support to other ITIL disciplines*. For example, service teams can use configuration-item relationships and history when assessing change impact, investigating incidents, resolving problems, planning releases, managing availability, and evaluating risks. This shared, trustworthy information is the operational value of Configuration Management: it supports service-management decision-making across processes rather than being limited to a narrow set of activities. ITIL guidance describes service configuration management as ensuring that accurate and reliable information about configuration items is available when and where needed. See AXELOS service configuration management guidance and IBM configuration management documentation.

QUESTION NO: 2

Which of the following practices are consistent with the 3-2-1 backup strategy?

Each correct answer represents a complete solution. Choose three.

A. Maintain at least three copies of data

B. Use at least two different storage media or technologies

C. Keep at least one copy offsite

D. Store every backup copy on the same production storage array

ANSWER: A B C

Explanation:

Maintaining at least three copies of data, **using at least two different storage media or technologies**, and **keeping at least one copy offsite** are consistent with the 3-2-1 backup strategy. The approach is intended to reduce the likelihood that a single hardware failure, site-level disaster, accidental deletion, malware event, or storage-platform problem will eliminate all recoverable copies.

An offsite copy should be protected from the same threats that could affect the primary environment. Organizations may supplement the 3-2-1 approach with immutable, offline, or logically isolated backup copies to improve resilience against ransomware. Backup procedures should also include regular restoration testing to verify that data can be recovered within

required objectives. CISA recommends maintaining protected backups and testing restoration as part of ransomware resilience. See CISA StopRansomware Guide.

QUESTION NO: 3

Which of the following terms refers to the act, manner, or practice of an organization to bring systems, applications, and data back to "normal" conditions in a prescribed and acceptable time frame?

A. Disaster Recovery Management

B. Business Continuity Management (BCM)

C. Risk Management

D. Recovery Management

ANSWER: A

Explanation:

Disaster Recovery Management is the correct term because it encompasses the governance, planning, procedures, resources, and coordinated activities used to restore an organization's IT capabilities after a disruptive incident. Its objective is to return systems, applications, and data to an agreed operational state within defined recovery requirements. Those requirements commonly include the recovery time objective, which establishes the maximum acceptable downtime, and the recovery point objective, which establishes the maximum acceptable amount of data loss. Effective disaster recovery management therefore does more than perform a technical restoration: it establishes recovery strategies, assigns responsibilities, maintains recovery documentation, conducts tests, and improves plans based on test results and changing business needs. This aligns directly with the question's emphasis on restoring technology and information assets to normal conditions in a prescribed, acceptable time frame. NIST describes contingency planning as a coordinated strategy for recovering information systems and identifies recovery objectives as central planning inputs. ISO's business-continuity guidance likewise recognizes recovery of prioritized activities and resources as a managed discipline. See NIST SP 800-34 Rev. 1, Contingency Planning Guide for Federal Information Systems and ISO 22301:2019, Security and resilience—Business continuity management systems.

QUESTION NO: 4

Which of the following services provides mail and calendar services?

A. Application Server

B. Web Server

C. Exchange Server

D. Domain Controller

ANSWER: C

Explanation:

Exchange Server is the correct answer because Microsoft Exchange is a messaging and collaboration server platform designed to provide organizational email, calendaring, contacts, tasks, mailbox access, and scheduling features. It stores and manages user mailboxes and calendars and enables users to send and receive messages, share availability information, schedule meetings, reserve resources such as meeting rooms, and access these services through clients including Outlook and Outlook on the web. In a disaster-recovery context, Exchange is a critical workload because an interruption can affect both routine communication and the ability of personnel to coordinate response and recovery activities. Recovery planning for this service should therefore address mailbox databases, transaction logs, server roles, service dependencies such as Active Directory and DNS, backup and restoration procedures, and defined recovery objectives. Microsoft describes Exchange Server as an enterprise platform for email and calendaring, and its documentation

provides architecture and deployment information relevant to maintaining service availability. See Microsoft Learn: Plan and deploy Exchange Server and Microsoft Learn: Exchange Server architecture.

QUESTION NO: 5

BS 7799 is an internationally recognized ISM standard that provides high level, conceptual recommendations on enterprise security. BS 7799 is basically divided into three parts.

Which of the following statements are true about BS 7799?

Each correct answer represents a complete solution. Choose all that apply.

A. BS 7799 Part 3 was published in 2005, covering risk analysis and management.

B. BS 7799 Part 1 was a standard originally published as BS 7799 by the British Standards

Institute (BSI) in 1995.

C. BS 7799 Part 2 was adopted by ISO as ISO/IEC 27001 in November 2005.

D. BS 7799 Part 1 was adopted by ISO as ISO/IEC 27001 in November 2005.

ANSWER: A B C

Explanation:

BS 7799 developed as a British Standards Institution information-security management standard and later became a key foundation for the ISO/IEC 27000 family. **BS 7799 Part 1 was a standard originally published as BS 7799 by the British Standards Institute (BSI) in 1995.** This initial publication established a code of practice for information-security management, supplying the security-control guidance that shaped the subsequent international standardization work. **BS 7799 Part 2 was adopted by ISO as ISO/IEC 27001 in November 2005.** Part 2 was the specification for establishing, implementing, and assessing an information security management system, so it formed the basis of the certifiable ISO/IEC 27001 requirements standard. ISO's record identifies ISO/IEC 27001:2005 as the first edition, published in November 2005. **BS 7799 Part 3 was published in 2005, covering risk analysis and management.** Its purpose was to provide ISMS-focused guidance for identifying, assessing, treating, and managing information-security risks, an area later represented internationally by ISO/IEC 27005. This historical progression explains why BS 7799 is commonly cited as the predecessor of modern ISO/IEC information-security management standards. See the ISO record for ISO/IEC 27001:2005 and BSI's overview of ISO/IEC 27001 information security management.

QUESTION NO: 6

A project plan includes the Work Breakdown Structure (WBS) and cost estimates. Which of the following are the parts of a project plan?

Each correct answer represents a complete solution. Choose all that apply.

A. Risk identification

B. Project schedule

C. Risk analysis

D. Team members list

E. Security Threat

ANSWER: A B C D

Explanation:

A complete project plan documents how project work will be organized, resourced, scheduled, monitored, and controlled. **Risk identification** is a necessary planning activity because it records conditions or events that could affect scope, schedule, cost, quality, or recovery objectives. The identified risks provide the basis for planned responses and ongoing risk monitoring. **Risk analysis** evaluates the likelihood and potential impact of those identified risks, allowing the project team to prioritize treatment and assign appropriate contingency actions.

A **project schedule** translates work defined in the WBS into planned activities, dependencies, durations, milestones, and delivery dates. It enables progress measurement and supports coordination of recovery-project tasks. A **team members list** is also an important project-plan component because the plan must establish the people and roles responsible for completing work, making decisions, managing risks, and communicating status. Together, these elements support effective execution and control of the project. PMI describes project management planning as covering areas such as schedule, resources, and risk; its standards overview is available at PMI PMBOK Guide and Standards. NIST also emphasizes identifying, analyzing, and managing risk as foundational to organizational planning in NIST SP 800-30 Rev. 1.

QUESTION NO: 7

Which of the following is prepared by the business and serves as a starting point for producing the IT Service Continuity Strategy?

A. Business Continuity Strategy

B. Index of Disaster-Relevant Information

C. Disaster Invocation Guideline

D. Availability/ ITSCM/ Security Testing Schedule

ANSWER: A

Explanation:

Business Continuity Strategy is correct because IT service continuity management is driven by the organization's broader business continuity requirements. The business prepares its continuity strategy after identifying critical business processes, recovery priorities, acceptable disruption periods, dependencies, and the resources needed to maintain or restore essential operations. IT then uses those requirements as the foundation for an IT Service Continuity Strategy, defining how technology services, infrastructure, applications, data, suppliers, and recovery capabilities will support the required business recovery objectives.

This relationship ensures that IT recovery investments are proportionate to business need. For example, where the business continuity strategy establishes a short recovery-time requirement for a critical process, the IT strategy can select and implement appropriate resilience and recovery measures to meet that requirement. The resulting IT service continuity arrangements must remain aligned with, and be validated against, the business continuity strategy rather than being developed independently. This reflects the established business-continuity principle that technology continuity planning supports the organization's overall continuity objectives. See the ISO 22301 business continuity management standard overview and AXELOS ITIL guidance.

QUESTION NO: 8

Which of the following defines the communication link between a Web server and Web applications?

A. IETF

B. Firewall

C. PGP

D. CGI

ANSWER: D

Explanation:

CGI is correct because the Common Gateway Interface defines a standard interface through which a web server communicates with an external application or executable program to generate dynamic web content. When a client requests a resource that is handled by a CGI program, the web server starts or invokes that program and supplies request information, such as request method, headers, query data, and environment variables. The application processes that input and returns content, together with appropriate response headers, for the web server to send to the client. This separation provides a well-defined boundary between the server's HTTP-handling responsibilities and application-level processing. CGI was especially important in early dynamic websites and remains a foundational model for understanding how web servers can pass requests to application code. The Internet Engineering Task Force's CGI specification documents the interface, including the use of environment variables and standard input/output streams: RFC 3875: The Common Gateway Interface (CGI) Version 1.1. Apache also documents CGI execution and configuration concepts in its CGI Dynamic Content guide.

QUESTION NO: 9

Which of the following governance bodies provides management, operational, and technical controls to satisfy the security requirements?

A. Chief Information Security Officer

B. Senior Management

C. Business Unit Manager

D. Information Security Steering Committee

ANSWER: D

Explanation:

Information Security Steering Committee is the correct answer because it is the cross-functional governance body that coordinates information-security decisions across business, technology, risk, and operational stakeholders. It translates organizational security requirements into an actionable security program and provides oversight for the selection, implementation, and continuing effectiveness of administrative/management, operational, and technical safeguards. In a disaster-recovery context, this includes ensuring that security requirements are built into recovery strategies, recovery environments, incident coordination, testing, and restoration procedures rather than being treated as isolated technical tasks.

This committee gives security governance the organizational authority and broad representation needed to prioritize risk treatment, allocate resources, resolve conflicts between business needs and security requirements, and monitor whether controls remain appropriate. Control families are commonly categorized as management, operational, and technical in security-control frameworks. NIST describes these control classes and their role in protecting organizational systems and information in NIST SP 800-53 Rev. 5. NIST's Cybersecurity Framework also emphasizes governance as the mechanism for establishing direction, oversight, and accountability for cybersecurity risk management.

QUESTION NO: 10

Remus works as an IT administrator for an organization. An important aspect of his job is to ensure that physical storage space remains available in all host machines at all times. However, recently there was not much physical storage space available in one host machine, so he deleted several snapshots of the virtual machines present. Despite the deletion, free space could not be obtained. What can Remus do to remedy this situation?

A. Delete the child disk of the snapshots present in the host machine

B. Delete the virtual machine database

C. Uninstall the Hypervisor

D. Shut down or restart the virtual machine system

E. Consolidate the virtual machines' snapshot/delta disks after confirming a valid backup

ANSWER: E

Explanation:

Consolidate the virtual machines' snapshot/delta disks after confirming a valid backup is the correct remediation. A snapshot generally creates delta, or redo, disk files that hold changes made after the snapshot was taken. Removing a snapshot is not necessarily an immediate deletion of all related disk data: the platform must commit or merge the delta-disk contents into the appropriate base disk and remove obsolete files. If that operation is incomplete, fails, or the VM indicates that disk consolidation is needed, the host datastore can remain consumed by those files.

The administrator should first verify that the VM has a current, recoverable backup and that the datastore has enough temporary working space for the merge. They should then use the hypervisor's supported snapshot-consolidation or merge operation, monitor the task to successful completion, and confirm that the snapshot and delta files have been removed and capacity is available again. This is a storage-maintenance action performed through the virtualization platform; manually deleting a child or delta disk is not a safe substitute because it can break the virtual disk chain and make the VM inconsistent or unavailable.

VMware documents consolidation as the process of merging redundant delta disks after snapshot operations and provides supported procedures for resolving consolidation-needed conditions. See VMware: Consolidating snapshots and Microsoft: Manage Hyper-V checkpoints.

QUESTION NO: 11

Availability Management deals with the day-to-day availability of services. Which of the following takes over when a 'disaster' situation occurs?

A. Capacity Management

B. Service Level Management

C. Service Continuity Management

D. Service Reporting

ANSWER: C

Explanation:

Service Continuity Management is correct because it addresses the organization's ability to maintain or restore essential services following a major disruption or disaster. Whereas routine availability work focuses on preventing and managing normal service interruptions, continuity management prepares for exceptional events that exceed normal operational response capabilities, such as loss of a data center, widespread infrastructure failure, natural disasters, or other incidents requiring invocation of recovery arrangements.

This discipline performs business impact analysis and risk assessment, defines continuity and recovery requirements, develops and maintains recovery plans, and tests those plans to verify that critical services can be recovered within agreed time objectives. It also coordinates the transition from a disaster response into the recovery and restoration of services at an alternate or recovered site. The objective is to protect business operations by ensuring that agreed service levels for vital services can be re-established after a severe disruption.

This relationship between continuity planning, recovery capabilities, and resilience is consistent with the guidance in the ISO 22301 business continuity management standard and the NIST contingency-planning guidance, both of which emphasize planning, exercising, and recovering critical systems after disruptive events.

QUESTION NO: 12

Katie was setting up disaster recovery teams in her organization to combat any disaster that occurred. One of the most important teams was the disaster recovery coordinator. Having two names in mind for the post, Katie interviewed the two people for the roles and responsibilities of the disaster recovery coordinator. Which of the following statements should either of the interviewees use to get the post?

A. Responsible for disaster recovery planning verification and compliance

B. Day-to-day management control over the execution and maintenance of the disaster recovery program

C. Responsible for the specification and design of all technology-based disaster recovery solutions

D. Executive authority over the disaster recovery program

ANSWER: B

Explanation:

The disaster recovery coordinator is appropriately responsible for the day-to-day management control over execution and maintenance of the disaster recovery program. This role turns the organization's recovery strategy into an operating capability: coordinating plan development and updates, maintaining recovery documentation and contact information, arranging training and exercises, tracking corrective actions, and ensuring that teams are prepared to perform their assigned recovery activities when an incident occurs. During a disruption, the coordinator also serves as a central point for organizing recovery work, monitoring progress, escalating issues, and keeping recovery activities aligned with approved procedures and recovery objectives. This ongoing ownership is essential because a disaster recovery plan is not effective as a static document; it must be maintained, tested, and improved as systems, personnel, dependencies, and business requirements change. NIST's contingency-planning guidance describes the need for plan maintenance, testing, training, and coordinated recovery procedures as continuing elements of an effective program. The role also aligns with broader organizational continuity practices that emphasize assigning responsible personnel to implement and sustain emergency and recovery plans. See NIST SP 800-34 Rev. 1, Contingency Planning Guide for Federal Information Systems and Ready.gov business continuity planning guidance.

QUESTION NO: 13

Which of the following subphases are defined in the maintenance phase of the life cycle models?

Each correct answer represents a part of the solution. Choose all that apply.

A. Change control

B. Request control

C. Release control

D. Configuration control

ANSWER: A B C

Explanation:

The maintenance phase keeps a disaster-recovery capability usable after it has been designed, implemented, and tested. **Request control** is the intake and tracking mechanism for maintenance requests, ensuring that identified needs, issues, and proposed updates are formally recorded and evaluated. **Change control** provides the disciplined review, authorization, documentation, and tracking of approved changes so that updates to recovery procedures, technical components, contact information, and dependencies remain controlled. **Release control** governs packaging, communicating, deploying, and validating the approved updates as a usable version of the recovery capability. Together, these subphases ensure that maintenance is traceable and that operational recovery documentation and supporting resources remain current rather than changing informally. This aligns with the broader contingency-planning principle that plans must be maintained as organizational processes, systems, personnel, and risks change. NIST describes contingency-plan maintenance as an ongoing activity in the system development life cycle and calls for plans to be reviewed and updated when relevant changes occur. See NIST SP 800-34 Rev. 1 and the EC-Council overview of the Certified Disaster Recovery Professional (EDRP) program.

QUESTION NO: 14

Which of the following refers to a moveable operating environment that can be set up or installed at any place on transportable units?

A. Mobile Recovery Center

B. Crisis Command Center

C. Cold Site

D. Colocation Facilities

ANSWER: A

Explanation:

Mobile Recovery Center is the correct term for a portable recovery capability that can be transported to, positioned, and made operational at a suitable location after a disruptive event. It commonly consists of trailer-mounted or other transportable units that provide workspace, communications, technology infrastructure, and related facilities needed to continue critical business or IT operations. This approach is valuable when a primary facility is unavailable and an organization needs an alternate environment without relying on a permanently constructed recovery location. The mobility of the unit is the defining characteristic: recovery resources can be delivered to an affected area or another approved location, then configured to support the organization's prioritized recovery requirements. In disaster-recovery planning, the arrangement must be supported by logistics, access to power and communications, physical security, staffing, and periodic testing to ensure that deployment time and operational capabilities meet recovery objectives. NIST contingency-planning guidance describes alternate processing arrangements and emphasizes selecting, documenting, and testing recovery capabilities that meet organizational requirements; see NIST SP 800-34 Rev. 1. FEMA also provides continuity-planning resources that address maintaining essential functions from alternate locations: FEMA Continuity Program.

QUESTION NO: 15

Which of the following factors should be considered while selecting an alternate processing site for a disaster recovery plan?

Each correct answer represents a part of the solution. Choose three.

A. Recovery time requirements

B. Recovery point requirements

C. Geographic separation from the primary site

D. The lowest available rental cost only

ANSWER: A B C

Explanation:

Recovery time requirements, **recovery point requirements**, and **geographic separation from the primary site** are correct considerations when selecting an alternate processing site. The alternate capability must be able to support the organization's required recovery time objective and recovery point objective for the systems and business services assigned to it.

Geographic separation is also important because an alternate facility located within the same hazard area as the primary site may be affected by the same natural disaster, utility outage, or regional emergency. Site selection should also account for capacity, communications, security, staffing, supplier dependencies, and the ability to test and invoke the recovery arrangement. NIST contingency-planning guidance discusses alternate processing facilities and recovery strategies selected according to system and business requirements. See NIST SP 800-34 Rev. 1.

QUESTION NO: 16

Which of the following alternate processing sites provides physical space and basic infrastructure but does not contain preinstalled computer equipment?

A. Hot site

B. Warm site

C. Cold site

D. Mirrored site

ANSWER: C

Explanation:

Cold site is correct because it generally provides a facility with basic infrastructure, such as space, power, environmental controls, and communications capability, but does not have the necessary computer hardware, software, and current data already installed for immediate processing. The organization must transport, procure, or install the required resources before operations can resume.

A cold site is usually less expensive than a warm or hot site, but it has a longer recovery time and is therefore suitable only when the business can tolerate the delay required to configure the environment and restore systems. The selected site type must be consistent with the recovery objectives established through the business impact analysis. See NIST SP 800-34 Rev. 1 for alternate-site and recovery-strategy guidance.

QUESTION NO: 17

Against which of the following does SSH provide protection?

Each correct answer represents a complete solution. Choose two.

A. Broadcast storm

B. Password sniffing

C. DoS attack

D. IP spoofing

ANSWER: B D

Explanation:

SSH provides protection against **Password sniffing** because it establishes an encrypted channel before credentials and interactive session data are transmitted. Instead of sending a reusable password or terminal traffic in clear text, SSH encrypts the connection and uses cryptographic integrity protection, preventing a passive observer on the network from reading captured authentication data or commands. SSH can also use public-key authentication, which avoids transmitting a password for that login method altogether.

IP spoofing is addressed through SSH's authenticated key exchange, host-key verification, and integrity-protected session traffic. A forged source address alone does not allow an attacker to successfully impersonate the SSH server or participate in the protected session: the attacker must complete the cryptographic exchange and prove possession of the appropriate private key material. The client's verification of the server host key is especially important for detecting an attempted impersonation of the destination system.

The SSH transport protocol is specified to provide server authentication, confidentiality, and integrity for the connection. See RFC 4253: The Secure Shell Transport Layer Protocol and the OpenSSH ssh manual.

QUESTION NO: 18

Which of the following are common applications that help in replicating and protecting critical information at the time of disaster?

Each correct answer represents a complete solution. Choose all that apply.

A. Asynchronous replication

B. Synchronous replication

C. Tape backup

D. Disk mirroring

ANSWER: A B C D

Explanation:

Asynchronous replication, synchronous replication, tape backup, and disk mirroring are all established techniques for protecting critical information and supporting disaster recovery. Synchronous replication commits data to a secondary location as part of the write operation, providing very low data loss exposure when the replica remains available. Asynchronous replication transfers changes to the recovery location after the primary write completes, making it practical for longer-distance recovery designs while accepting a defined recovery-point gap. Disk mirroring maintains a duplicate copy of data on separate disks or storage systems, improving availability and preserving a current copy when a component fails. Tape backup creates an independent backup copy that can be retained offline and transported to a secure alternate facility; this is particularly valuable for long-term retention and recovery from incidents that affect online systems. A resilient recovery strategy commonly combines replication for rapid restoration with backup media for independent, recoverable copies. NIST disaster-recovery guidance identifies data backup and alternate processing/storage arrangements as key recovery capabilities: NIST SP 800-34 Rev. 1. Microsoft also documents synchronous and asynchronous replication as recovery approaches with distinct latency and recovery-point characteristics: Azure Site Recovery documentation.

QUESTION NO: 19

Which of the following should the administrator ensure during the test of a disaster recovery plan?

A. Ensure that all client computers in the organization are shut down.

B. Ensure that each member of the disaster recovery team is aware of their responsibility.

C. Ensure that the plan works properly

D. Ensure that all the servers in the organization are shut down.

ANSWER: B C

Explanation:

During a disaster recovery plan test, the administrator should ensure that each member of the disaster recovery team is aware of their responsibility and that the plan works properly. A recovery plan is operational only when assigned personnel understand their roles, escalation paths, decision authority, communications duties, and the specific recovery tasks they must perform. Testing validates that these responsibilities can be carried out in a coordinated manner under realistic conditions rather than merely existing as documented assignments.

The test must also demonstrate that the recovery procedures work properly. This includes confirming that recovery steps can restore required services and data, that dependencies are addressed in the correct order, that recovery objectives can be met, and that test findings are documented for corrective action. NIST contingency-planning guidance identifies testing, training, and exercises as essential for validating a plan and identifying deficiencies before an actual disruption. The test results should be used to update procedures, contact information, technical runbooks, and team training as needed. See NIST SP 800-34 Rev. 1, Contingency Planning Guide and Ready.gov Business Continuity Planning Suite.

QUESTION NO: 20

Which of the following command line tools are available in Helix Live acquisition tool on

Windows?

Each correct answer represents a complete solution. Choose all that apply.

A. netstat

B. whois

C. cab extractors

D. ipconfig

ANSWER: A C D

Explanation:

Helix Live for Windows is intended to support live-response and acquisition work by providing command-line utilities that can collect or reveal volatile system and network information without requiring a full software installation on the target. **netstat** is available for identifying active network connections, listening ports, and associated protocol activity—information that can change quickly during an incident. **ipconfig** is also available and provides the host's IP addressing and adapter configuration, which helps establish the system's network context at the time of acquisition. Microsoft documents the information exposed by netstat and ipconfig as Windows command-line networking utilities. Helix Live's Windows tool collection also includes **cab extractors**, enabling investigators to work with Microsoft Cabinet archives when required during evidence collection or examination. These utilities fit live forensic practice because responders should record relevant volatile network and system-state artifacts before shutdown, reboot, or other remediation changes the evidence.

QUESTION NO: 21

Della works as a security manager for SoftTech Inc. She is training some of the newly recruited personnel in the field of security management. She is giving a tutorial on DRP.

She explains that the major goal of a disaster recovery plan is to provide an organized way to make decisions if a disruptive event occurs and asks for the other objectives of the DRP. If you are among some of the newly recruited personnel in SoftTech Inc, what will be your answer for her question?

Each correct answer represents a part of the solution. Choose three.

A. Maximize the decision-making required by personnel during a disaster.

B. Guarantee the reliability of standby systems through testing and simulation.

C. Protect an organization from major computer services failure.

D. Minimize the risk to the organization from delays in providing services.

ANSWER: B C D

Explanation:

A disaster recovery plan is designed to preserve or restore essential technology capabilities after a disruptive event so that the organization can continue delivering required services within acceptable recovery objectives. "Protect an organization from major computer services failure" is therefore a core DRP objective: the plan establishes recovery procedures, alternate capabilities, responsibilities, and priorities for restoring affected IT services. "Minimize the risk to the organization from delays in providing services" is also central because prolonged outages can create operational, financial, legal, and reputational harm; recovery strategies are selected to meet defined recovery-time and recovery-point objectives. "Guarantee the reliability of standby systems through testing and simulation" reflects the need to validate that alternate processing facilities, backups, procedures, and personnel can support recovery in practice. Regular exercises and simulations identify gaps before a real incident and provide evidence that recovery capabilities are workable. NIST contingency-planning guidance emphasizes recovery strategies, alternate sites, plan testing, training, and exercises as essential components of IT contingency planning. CISA likewise recommends exercising plans to validate recovery arrangements and improve organizational resilience. See NIST SP 800-34 Rev. 1, Contingency Planning Guide for Federal Information Systems and CISA Resilience Services.

QUESTION NO: 22

An organization is recovering from a ransomware incident. Which of the following actions should be performed before restoring affected production systems?

Each correct answer represents a part of the solution. Choose three.

A. Isolate affected systems

B. Validate that backup data is usable and free from compromise

C. Identify and remove the cause of the compromise

D. Restore systems before assessing the attack vector

ANSWER: A B C

Explanation:

Isolating affected systems, **validating that backup data is usable and free from compromise**, and **identifying and removing the cause of the compromise** are correct recovery actions. Isolation helps prevent ransomware from continuing to spread or encrypt additional systems and backups. Before restoration, recovery personnel should validate backup integrity, confirm that backup copies are within the required recovery point, and ensure restored systems will not be immediately reinfected.

Recovery also requires eradication of the attack vector, such as compromised credentials, vulnerable services, malicious persistence mechanisms, or insecure configurations. Payment of a ransom does not demonstrate that systems are safe to restore and does not replace containment, eradication, and validated recovery procedures. CISA provides ransomware response and recovery guidance at StopRansomware Guide.

QUESTION NO: 23

Which of the following backup methods copies only the data that has changed since the most recent backup of any type?

A. Full backup

B. Differential backup

C. Incremental backup

D. Mirror backup

ANSWER: C

Explanation:

Incremental backup is correct because it captures data that has changed since the last completed backup, whether that prior backup was full or incremental. This approach usually reduces the amount of backup data and the time needed to perform daily backup operations.

However, recovery from incremental backups can require the most recent full backup and every subsequent incremental backup in sequence. A differential backup instead copies changes made since the last full backup, while a full backup copies all selected data. Backup selection should be based on recovery objectives, restoration complexity, available backup windows, and retention requirements. NIST discusses backup and restoration capabilities as key elements of contingency planning in NIST SP 800-34 Rev. 1.

QUESTION NO: 24

Which of the following terms refers to third-party backup, and offsite replication?

A. Continuous Data Protection

B. Managed Disaster Recovery

C. Tape Vaulting

D. Disk Shadowing

ANSWER: B

Explanation:

Managed Disaster Recovery is the correct term because it describes a disaster-recovery capability delivered and operated by an external service provider. In this model, the provider commonly manages protected backups, replication of workloads or data to a geographically separate recovery location, recovery infrastructure, monitoring, and recovery support. The organization retains responsibility for defining its recovery objectives and priorities, while using the provider's facilities, platforms, operational expertise, and managed processes to meet those objectives. This approach is particularly useful when an organization does not want to build, staff, and maintain its own secondary site and replication environment. Offsite replication is a core component because a usable recovery capability requires data and systems to be available away from the primary site if that site becomes unavailable. Third-party management also distinguishes this service model from technologies that describe only a backup or storage mechanism. IBM describes managed disaster recovery as a service that helps organizations protect and recover workloads using provider-operated resources and expertise. Recovery objectives and the need for an alternate recovery location are also central themes in the NIST contingency-planning guidance. See IBM: Disaster Recovery as a Service and NIST SP 800-34 Rev. 1.

QUESTION NO: 25

ISO 17799 has two parts. The first part is an implementation guide with guidelines on how to build a comprehensive information security infrastructure and the second part is an auditing guide based on requirements that must be met for an organization to be deemed compliant with ISO 17799. What are the ISO 17799 domains?

Each correct answer represents a complete solution. Choose all that apply.

A. Business continuity management

B. Information security policy for the organization

C. Personnel security

D. System architecture management

E. System development and maintenance

ANSWER: A B C E

Explanation:

ISO/IEC 17799 was the predecessor guidance standard to today's ISO/IEC 27002 and organized information-security controls into defined domains (called control clauses or control areas in some editions). **Business continuity management** is a domain because organizations must establish and maintain plans to continue critical activities and recover information-processing capabilities following disruption. **Information security policy for the organization** corresponds to the security-policy domain, which establishes management direction and the basis for security governance. **Personnel security** is a recognized domain addressing security responsibilities associated with employees, contractors, and other users throughout their engagement. **System development and maintenance** is also a domain, covering the incorporation of security requirements and controls into information systems across their life cycle. These domains reflect the broad control structure used by ISO 17799 rather than only technical safeguards. ISO 17799 was subsequently renumbered and evolved into ISO/IEC 27002; ISO notes this historical relationship in its ISO/IEC 27002 publication information. See ISO/IEC 27002:2022 and the ISO/IEC 27002:2013 standard pages for the continuing information-security controls guidance lineage.

QUESTION NO: 26

Which of the following features of the Cisco MDS 9000 SAN Extension over IP Package help in implementing efficient FCIP-based business-continuity and disaster-recovery solutions?

Each correct answer represents a complete solution. Choose all that apply.

A. FCIP write acceleration

B. IVR

C. FCIP compression

D. SAN extension tuner

ANSWER: A C D

Explanation:

The Cisco MDS 9000 SAN Extension over IP Package includes FCIP-focused capabilities intended to make remote SAN replication and recovery traffic more practical across WAN links. **FCIP write acceleration** improves the performance of write-intensive replication by reducing the impact of WAN latency on Fibre Channel write operations. This is particularly valuable when synchronous or latency-sensitive replication workflows must operate between geographically separated sites. **FCIP compression** reduces the amount of data transmitted through an FCIP tunnel, helping organizations use WAN bandwidth more efficiently and potentially reducing the network capacity required to meet replication objectives. **SAN extension tuner** provides tuning support for SAN-extension configurations, allowing administrators to optimize FCIP behavior for the available WAN characteristics and application requirements. Together, these functions address the key FCIP concerns of latency, bandwidth consumption, and configuration optimization, supporting resilient business-continuity and disaster-recovery designs. Cisco describes FCIP and associated SAN-extension capabilities in its MDS documentation and SAN-extension product materials; see the Cisco MDS 9000 Series overview and the Cisco NX-OS FCIP configuration documentation.

QUESTION NO: 27

Which of the following levels of RAID provides security features that are availability, enhanced performance, and fault tolerance?

A. RAID-10

B. RAID-5

C. RAID-0

D. RAID-1

ANSWER: A

Explanation:

RAID-10 is the correct choice because it combines mirroring and striping to provide a practical balance of availability, performance, and fault tolerance for disaster-recovery-oriented storage. Data is first mirrored across paired disks, meaning each block has a duplicate copy on a separate drive. It is then striped across those mirrored pairs, allowing reads and writes to be distributed across multiple disks for improved throughput and lower latency compared with a single mirrored pair. This architecture preserves service availability when a disk fails, because the surviving member of an affected mirror continues to supply the data. In arrays with multiple mirror pairs, RAID-10 can potentially sustain more than one disk failure provided the failed disks are not both members of the same mirror pair. RAID itself is not a substitute for backups, encryption, access controls, or a full disaster recovery plan; its contribution is storage redundancy and continuity against disk-device failures. The U.S. National Institute of Standards and Technology describes RAID as a mechanism that combines disks to improve reliability and/or performance, while vendor RAID documentation identifies RAID 10 as striped mirrors. See NIST's RAID glossary entry and Intel's RAID level overview.

QUESTION NO: 28

Which of the following control measures are considered while creating a disaster recovery plan?

Each correct answer represents a part of the solution. Choose three.

A. Detective measures

B. Supportive measures

C. Corrective measures

D. Preventive measures

ANSWER: A C D

Explanation:

A disaster recovery plan should account for preventive measures, detective measures, and corrective measures because these control categories work together to reduce disruption and restore operations following an incident. Preventive measures are incorporated to reduce the likelihood of an event or to limit its potential impact before it occurs. In a recovery context, this includes practices such as redundancy, resilient architecture, protected backups, environmental safeguards, and well-defined operational procedures. Detective measures provide timely identification of an outage, compromise, or other disruptive condition. Monitoring, alerting, logging, health checks, and incident escalation processes enable the organization to invoke recovery procedures promptly and on the basis of reliable information. Corrective measures address restoration after a disruption has been identified, including failover, system repair, data restoration, rebuilding affected services, and validating that recovered systems function as intended. Together, these measures support the lifecycle of reducing risk, recognizing a disruption, and recovering business capabilities. This approach is consistent with NIST contingency-planning guidance, which emphasizes controls and procedures for responding to disruptions and recovering information systems and services. See NIST SP 800-34 Rev. 1 and CISA cybersecurity resources.

QUESTION NO: 29

Which of the following procedures is designed to contain data, hardware, and software that can be critical for a business?

A. Disaster Recovery Plan

B. Crisis Communication Plan

C. Cyber Incident Response Plan

D. Occupant Emergency Plan

ANSWER: A

Explanation:

Disaster Recovery Plan is correct because it establishes the documented procedures, resources, and recovery priorities required to restore an organization’s critical technology environment after a disruptive event. Its scope includes the information assets and supporting infrastructure essential to business operations, such as applications, data, servers, network components, storage, operating environments, backups, alternate processing capabilities, and the personnel actions needed to recover them. A usable plan identifies which systems and datasets are most critical, defines recovery time and recovery point objectives, assigns recovery responsibilities, and specifies the sequence for restoring services to an acceptable operational state. This preparation enables the organization to protect and recover the hardware, software, and data on which vital business processes depend. NIST describes contingency planning as preparing for the recovery and restoration of information systems following a disruption, and identifies disaster recovery planning as a key technical recovery activity. The NIST Cybersecurity Framework likewise recognizes recovery planning as necessary to restore assets and operations after an incident. See NIST SP 800-34 Rev. 1, Contingency Planning Guide and NIST Cybersecurity Framework.

QUESTION NO: 30

Peter works as a Technical Representative in a CSIRT for SecureEnet Inc. His team is called to investigate the computer of an employee, who is suspected for classified data theft. Suspect's computer runs on Windows operating system. Peter

wants to collect data and evidences for further analysis. He knows that in Windows operating system, the data is searched in pre-defined steps for proper and efficient analysis. Which of the following is the correct order for searching data on a Windows based system?

Volatile data, file slack, registry, system state backup, internet traces, file system, memory dumps

B. Volatile data, file slack, internet traces, registry, memory dumps, system state backup, file system

C. Volatile data, file slack, registry, memory dumps, file system, system state backup, internet traces

D. Volatile data, file slack, file system, registry, memory dumps, system state backup, internet traces

Answer: D

A. Volatile data, file slack, internet traces, registry, memory dumps, system state backup, file system

B. Volatile data, file slack, registry, memory dumps, file system, system state backup, internet traces

C. Volatile data, file slack, file system, registry, memory dumps, system state backup, internet traces

ANSWER: C

Explanation:

The correct sequence is **"Volatile data, file slack, file system, registry, memory dumps, system state backup, internet traces."** This sequence reflects a structured Windows forensic examination workflow that begins with the most time-sensitive evidence. Volatile data is addressed first because active processes, network connections, logged-on sessions, and other live-state artifacts can disappear when a system is powered down or changes state. The examiner then proceeds through storage-based artifacts, including file slack and the file system, to identify files, metadata, deleted-content traces, and unallocated-space evidence. Windows Registry examination follows as a central source of configuration, user activity, device history, program execution, and persistence information. Memory dumps and system-state backups provide additional preservation and analysis sources for operating-system and application artifacts. Internet traces are subsequently reviewed to reconstruct browser usage, downloads, searches, communications, and other web-related activity relevant to the suspected data theft. This ordering supports a disciplined investigation by prioritizing evidence preservation and then examining artifacts in a consistent, repeatable manner. NIST's guidance on integrating forensic techniques into incident response emphasizes preserving and collecting digital evidence methodically: NIST SP 800-86. Additional Windows forensic artifact guidance is available from CISA.

QUESTION NO: 31

Which of the following best describes the identification, analysis, and ranking of risks?

A. Design of experiments

B. Fast tracking

C. Fixed-price contract

D. Plan Risk management

E. Risk assessment

ANSWER: E

Explanation:

Risk assessment is the correct term for the systematic process of identifying risks, analyzing their likelihood and potential impact, and ranking or prioritizing them so that the organization can direct recovery-planning resources to the most significant threats. In a disaster-recovery context, this work establishes which events could disrupt critical services, what assets and business processes may be affected, and the relative severity of each scenario. The resulting prioritized risk information supports proportionate risk treatment decisions, including preventive controls, response measures, and recovery capabilities.

This usage is consistent with NIST guidance: risk assessment incorporates risk identification and risk analysis to determine risk, which can then be compared and prioritized to support risk-management decisions. ISO guidance likewise treats risk assessment as a structured activity involving risk identification, risk analysis, and risk evaluation. The ranking element is especially important because recovery programs must focus first on risks that could most seriously affect the organization's people, operations, systems, data, and ability to meet recovery objectives. See NIST SP 800-30 Rev. 1 and ISO 31000:2018 Risk Management.

QUESTION NO: 32

Which of the following terms refers to a backup that is taken when the database is offline?

A. Online Data Backup

B. Hot Backup

C. Full System Backup

D. Cold Backup

ANSWER: D

Explanation:

Cold Backup is the term for a backup performed while a database is shut down or otherwise offline. Because the database is not accepting transactions or modifying data files during the operation, its files represent a consistent state that can be copied together for recovery. This approach avoids the need to coordinate active transactions and associated recovery information during the backup itself. In disaster-recovery planning, cold backups can be appropriate where a maintenance window is available and the organization can tolerate the temporary service interruption required to stop the database. The resulting backup is commonly called an offline backup and may include the database data files, control or configuration files, and other components needed to restore the database to the point at which it was cleanly closed. Backup terminology and implementation details can vary by database platform, but the defining characteristic of a cold backup remains that the database is offline while the backup is created. Oracle's documentation describes consistent backups as backups made after the database has been shut down cleanly, and its backup-and-recovery guidance distinguishes these from backups made while the database is open. See Oracle Database Backup and Recovery User's Guide and IBM Db2 backup and recovery overview.

QUESTION NO: 33

Which of the following terms refers to a data storage and processing facility that is virtualized and provided as a service?

A. Cloud-based Storage

B. Virtual Machines

C. Software Defined Data Center

D. Data Virtualization

ANSWER: C

Explanation:

Software Defined Data Center is correct because it describes a complete data-center architecture in which the principal infrastructure domains—compute, storage, networking, and associated management services—are abstracted from underlying physical hardware and controlled through software. This virtualization and policy-driven automation allows the environment to be provisioned, managed, scaled, and delivered as a service rather than being tied to manually configured physical infrastructure. In disaster-recovery planning, this model is particularly valuable because defined infrastructure policies, workloads, and configurations can be automated and reproduced in another suitable environment, improving recovery agility and consistency. VMware describes a software-defined data center as an architecture that virtualizes and delivers compute, storage, and networking as services, with management and automation across those resources. See

VMware's Software-Defined Data Center overview. The broader cloud characteristic of on-demand resource provisioning is also consistent with NIST's cloud-computing model, which emphasizes rapidly provisioned and released configurable resources: NIST SP 800-145. Thus, the term accurately covers both virtualized data storage and processing in a service-delivery model.

QUESTION NO: 34

You want to use PGP files for steganography. Which of the following tools will you use to accomplish the task?

A. Snow

B. ImageHide

C. Blindside

D. Stealth

ANSWER: D

Explanation:

Stealth is the appropriate tool because it was designed to conceal information within carrier files while supporting PGP-based protection of the hidden payload. In this use case, the data can first be protected using Pretty Good Privacy encryption and then embedded so that its existence is less apparent than an ordinary encrypted file. This combines cryptography, which protects the content from disclosure, with steganography, which attempts to obscure the presence of that protected content. PGP is an OpenPGP implementation family that uses a packet-based message format for encrypted and signed data, as specified in RFC 4880. Stealth is specifically associated with using PGP-encrypted content in a steganographic workflow, making it the best match for the stated requirement. Operationally, the recipient needs both knowledge of the steganographic extraction process and the applicable PGP private key or passphrase to recover and decrypt the concealed information. This layered approach is useful when simply transmitting an encrypted file could itself attract attention. For background on the distinction and relationship between hiding data and encrypting it, see the NIST overview of steganography and digital watermarking.

QUESTION NO: 35

Which of the following statements are true about classless routing protocols?

Each correct answer represents a complete solution. Choose two.

A. The same subnet mask is used everywhere on the network.

B. They extend the IP addressing scheme.

C. IGRP is a classless routing protocol.

D. They support VLSM and discontiguous networks.

ANSWER: B D

Explanation:

"They extend the IP addressing scheme" is correct because classless routing protocols carry subnet-mask or prefix-length information with route advertisements. This removes the former dependency on the default Class A, B, or C network mask and lets routers make forwarding decisions using the actual network prefix. In practical terms, the route is represented as a network address plus its prefix length, such as 192.0.2.0/24, rather than being inferred solely from the first octet of the address.

"They support VLSM and discontiguous networks" is also correct. Variable Length Subnet Masking allows an organization to use differently sized subnets where needed, conserving IPv4 address space and matching allocation to host requirements. Because a classless protocol advertises the precise prefix length, it can distinguish and route those different subnet sizes correctly. That same prefix-aware behavior enables operation across discontiguous networks: portions of an address range

can be separated by other networks without requiring a single contiguous, classful topology. CIDR and VLSM are foundational classless-addressing concepts, described in RFC 4632. Cisco's routing documentation also explains that classless routing protocols include mask information in updates and thereby support VLSM and discontiguous networks: Cisco IP routing documentation.

QUESTION NO: 36

Which of the following activities should be performed during the reconstitution phase after a disaster recovery operation?

Each correct answer represents a part of the solution. Choose three.

A. Validate that recovered systems operate correctly

B. Return operations to the primary environment when appropriate

C. Document lessons learned and required plan updates

D. Disable all monitoring until the next scheduled test

ANSWER: A B C

Explanation:

During reconstitution, the organization should **validate that recovered systems operate correctly**, **return operations to the primary environment when appropriate**, and **document lessons learned and required plan updates**. Validation confirms that applications, infrastructure, interfaces, security controls, and restored data meet operational requirements before normal processing is fully resumed.

Returning to the primary environment may be necessary after temporary alternate-site operations, provided the primary site is repaired and ready. Lessons learned from the event should be recorded and used to improve recovery procedures, technical documentation, training, contracts, and recovery capabilities. NIST identifies reconstitution as the activity of returning systems to normal operation and updating contingency planning based on recovery experience. See NIST SP 800-34 Rev. 1.

QUESTION NO: 37

Which of the following statements about disaster recovery plan documentation are true?

Each correct answer represents a complete solution. Choose all that apply.

A. The documentation regarding a disaster recovery plan should be stored in backup tapes.

B. The documentation regarding a disaster recovery plan should be stored in floppy disks.

C. The disaster recovery plan documentation should be stored onsite only.

D. The disaster recovery plan documentation should be stored offsite only.

E. Current disaster recovery plan documentation should be maintained both onsite and at a secure offsite location.

ANSWER: A E

Explanation:

Disaster-recovery documentation must itself be protected as a recoverable business asset. Storing an archived copy on backup tapes can provide a durable, portable backup medium, particularly when the tapes are retained securely, protected from unauthorized alteration, and included in the organization's backup retention process. The documentation must be available even when the primary facility, its systems, or ordinary document repositories are unavailable. A resilient documentation approach therefore maintains controlled, current copies at the primary location for normal operations and at a geographically separate, secure location for use during a site-level disruption. The offsite copy may be maintained through a secure cloud repository, a recovery site, or protected physical media, provided authorized recovery personnel can access it

during an emergency. Version control, access control, periodic review, and testing are essential so that responders use an accurate plan rather than an obsolete copy. NIST contingency-planning guidance emphasizes protecting contingency-plan information and ensuring it is available to personnel who must execute recovery activities. CISA likewise recommends maintaining and protecting recovery plans and critical information as part of organizational resilience. See NIST SP 800-34 Rev. 1 and CISA Business Resilience.