EXAM CRAM

CompTIA

Security+™

SY0-401

Fourth Edition

Save 10% on Exam Voucher

See Inside

DIANE BARRETT
MARTIN WEISS
KIRK HAUSMAN

PEARSON IT
CERTIFICATION

EXAM CRAM

CompTIA® Security+™ SY0-401

Fourth Edition

Diane Barrett,
Kalani K. Hausman,
Martin Weiss

800 East 96th Street, Indianapolis, Indiana 46240 USA

Cram Quiz

Answer these questions. The answers follow the last question. If you cannot answer these questions correctly, consider reading this section again until you can.

1. Which type of fire extinguisher would be best for putting out burning wires?

○ **A.** Foam

○ **B.** Carbon dioxide

○ **C.** Sodium chloride

○ **D.** Copper powder

2. What is the plenum?

○ **A.** A mesh enclosure designed to block EMI

○ **B.** A mechanism for controlling condensation

○ **C.** A type of dry-pipe fire control system

○ **D.** A mechanism for thermal management

3. The ASHRAE recommends humidity levels in which range?

○ **A.** 25% to 40%

○ **B.** 40% to 55%

○ **C.** 55% to 70%

○ **D.** 70% to 85%

4. Which of these is not a concern for environmental monitoring systems?

○ **A.** Able to sustain operations during an environmental disaster

○ **B.** Able to communicate even if the email service was involved

○ **C.** Able to reach responders in a timely manner

○ **D.** Include signage noting live or automated review only

Cram Quiz Answers

1. **B**. The carbon-dioxide extinguisher replaces the Halon extinguisher for putting out electrical (Class C) fires. Answer A is incorrect because foam is used for Class A fires (trash, wood, and paper). Answers C and D are incorrect because both sodium chloride and copper-based dry powder extinguishers are used for Class D (combustible materials) fires.
2. **D**. A plenum is the space below a raised floor or above a drop ceiling that can be used in hot-aisle/cold-aisle server rooms to efficiently manage thermal dissipation. Answer A is incorrect because a grounded mesh enclosure for EMI shielding is called a Faraday cage. Answer B is incorrect because management of condensation is handled as part of the HVAC function as air is cooled. Answer C is incorrect because a dry-pipe system is a fire extinguishing system that uses pressurized air as a triggering mechanism for water.
3. **B**. The Air-Conditioning Engineers (ASHRAE) recommendation for optimal humidity levels between 40% and 55% to minimize electrostatic discharge and condensation. Answer A is incorrect because it specifies a range too low that would be dangerous for static discharge, whereas answers C and D are incorrect because they represent too high a humidity level that would be susceptible to the buildup of condensation on cool components and boards.
4. **D**. Video surveillance might require signage noting whether cameras are monitored live or not, to avoid a legal complaint if someone tries unsuccessfully to signal for aid during an emergency. Answers A, B, and C are valid concerns because environmental monitoring systems must be able to operate even during a disaster and communicate with responders in a timely manner even if the servers hosting the usual communication services (email, SMS, and so on) are involved in the disaster.

Summarize Risk Management Best Practices

- **Business continuity concepts**
- **Fault tolerance**
- **Disaster recovery concepts**

CramSaver

If you can correctly answer these questions before going through this section, save time by skimming the Exam Alerts in this section and then completing the Cram Quiz at the end of the section.

1. Which type of recovery allows a business to sustain operations following an incident?
2. How much time can a service be unavailable to meet a “five nines” uptime requirement?
3. Which form of RAID would be best if single-user performance were the sole consideration?

Answers

1. Business continuity planning (BCP) and continuity of operation planning (COOP) are used to ensure organizational functional restoration in the shortest possible time even if services resume at a reduced level of effectiveness or availability. Disaster recovery plans (DRPs) extend this process to ensure a full recovery of operational capacity following a disaster (natural or manmade). Instructions and details for recovery should occur before an incident. Not only should plans be set forth, but they should be regularly updated and tested, as well, to ensure that communication plans can be implemented and that responders can execute response and recovery plans properly. These should address different scenarios for incident handling responses and notification procedures following identification, short-term recovery of key service, and operational data access functions as part of continuity of operation preparedness, and long-term sustained recovery to full operational status in disaster recovery planning. A business recovery plan, business resumption plan, and contingency plan are also considered part of business continuity planning. In the event of an incident, an organization might also need to restore equipment (in addition to data) or personnel lost or rendered unavailable due to the nature or scale of the disaster.

2. 5.3 minutes per year. Service level agreements (SLAs) have thresholds for acceptable levels of downtime, based on the overall percentage of operational time. Five nines refers to 99.999% of total operational potential. So, for a 24x7 service such as an online auction site available to global consumers, across a year that translates to less than 5.3 minutes of downtime combined.
3. RAID 0 is the best from a performance-only perspective. All other varieties trade additional time calculating and storing parity data to protect redundancy and gain fault tolerance in the event of hardware failure in one or more drives, or to share access loads across multiple drives for high-throughput requirements.

Business Continuity Concepts

In any planning, safety of human life must be paramount. BCP involves identification of risks and threats to operation and implementing strategies to mitigate the effect of each. Beyond backup and restoration of data, disaster recovery planning must include a detailed analysis of underlying business practices and support requirements. This is called business continuity planning. BCP is a more comprehensive approach to provide guidance so that the organization can continue making sales and collecting revenue. As with disaster recovery planning, it covers natural and manmade disasters. BCP should identify required services, such as network access and utility agreements, and arrange for automatic failover of critical services to redundant offsite systems.

Business Impact Analysis

A business impact analysis (BIA) is the process for determining the potential impacts resulting from the interruption of time-sensitive or critical business processes. IT contingency planning for both disaster recovery and operational continuity rely on conducting a BIA as part of the overall DR/BC planning process. Unlike a risk assessment, the BIA is not focused as much on the relative likelihood of potential threats to an organization, but instead focuses on the relative impact on critical business functions due to the loss of operational capability due to the threats. Conducting a business impact analysis involves identification of critical business functions and the services and technologies required for each, along with the cost associated with the loss of each and the maximum acceptable outage period.

For hardware-related outages, the assessment should also include the current age of existing solutions along with standards for the expected mean time between failures based on vendor data or accepted industry standards. Strategies for the DR/BC plan are intended to minimize this cost by arranging recovery actions to restore critical functions in the most effective manner based on cost, legal or statutory mandates, and mean-time-to-restore calculations.

Identification of Critical Systems and Components

BCP must include identification of critical systems and components. In the event that a disaster is widespread or targeted at an Internet service provider (ISP) or key routing hardware point, an organization's continuity plan should include options for alternative network access, including dedicated administrative connections that might be required for recovery. Continuity planning should include considerations for recovery in the event that existing hardware and facilities are rendered inaccessible or unrecoverable. You should include hardware configuration details, network requirements, and utilities agreements for alternative sites (that is, warm and cold sites) in this planning consideration.

Removing Single Points of Failure

A single point of failure is a potential risk posed by a flaw in business continuity planning in which one fault or malfunction causes an entire system or enterprise to stop operating. Single points of failure are avoided by means of redundancy and various fault-tolerance protocols. Examples of removing single points of failure include the use of server clustering technology, redundant switches, and redundant network connections.

Business Continuity Planning and Testing

BCP and COOP are used to ensure organizational functional restoration in the shortest possible time even if services resume at a reduced level of effectiveness or availability. Disaster recovery plans (DRPs) extend this process to ensure a full recovery of operational capacity following a disaster (natural or manmade). Instructions and details for recovery should occur before an incident. Not only should plans be set forth, but they should be regularly updated and tested as well to ensure that communication plans can be implemented and that responders can execute response and recovery plans properly. These should address different scenarios for incident handling responses and notification procedures following identification, short-term recovery of key service and operational data access functions as part of continuity of operation preparedness, and long-term sustained recovery to full operational status in disaster recovery planning. A business recovery plan, business resumption plan, and contingency plan are also considered part of business continuity planning.

In the event of an incident, an organization might also need to restore equipment (in addition to data) or personnel lost or rendered unavailable due to the nature or scale of the disaster.

Risk Assessment

Risk assessments identify potential vulnerabilities and analyze what could happen if an incident occurs. Risk assessments are conducted to plan recovery appropriately, determining the scope and criticality of organizational services and data. In addition, an order (a priority) of recovery must be established, with recovery time and recovery measures of success identified, documented, shared, and tested during training to function properly during the operational window following an incident.

Continuity of Operations

Continuity of operations is an initiative issued by the President of the United States in 2007 to be sure that government departments and agencies are able to continue operation of their essential functions under circumstances involving natural, manmade, and technological threats and national security emergencies. Continuity of operations is generally viewed as the same as business continuity, although it primarily focused on government and public sectors. Policies and procedures are designed to ensure that an organization can recover from a potentially destructive incident and resume operations as quickly as possible following that event.

Disaster Recovery

Disaster recovery involves many aspects, including the following:

- **Disaster recovery plan:** A DRP is a written document that defines how the organization will recover from a disaster and how to restore business with minimum delay. The document also explains how to evaluate risks; how data backup and restoration procedures work; and the training required for managers, administrators, and users. A detailed disaster recovery should address various processes, including backup, data security, and recovery.
- **Disaster recovery policies:** These policies detail responsibilities and procedures to follow during disaster recovery events, including how to contact key employees, vendors, customers, and the press. They should also include instructions for situations in which it might be necessary to bypass the normal chain of command to minimize damage or the effects of a disaster.