QUESTION 1

How is Remote Authentication Dial-In User Service (RADIUS) authentication accomplished?

A. It uses clear text and firewall rules.
B. It relies on Virtual Private Networks (VPN).
C. It uses clear text and shared secret keys.
D. It relies on asymmetric encryption keys.

Correct Answer: C

QUESTION 2

What is the **MAIN** objective of risk analysis in Disaster Recovery (DR) planning?

A. Establish Maximum Tolerable Downtime (MTD) Information Systems (IS).
B. Define the variable cost for extended downtime scenarios.
C. Identify potential threats to business availability.
D. Establish personnel requirements for various downtime scenarios.

Correct Answer: C

QUESTION 3

Which of the following is an important requirement when designing a secure remote access system?

A. Configure a Demilitarized Zone (DMZ) to ensure that user and service traffic is separated.
B. Provide privileged access rights to computer files and systems.
C. Ensure that logging and audit controls are included.
D. Reduce administrative overhead through password self service.

Correct Answer: C

QUESTION 4

An audit of an application reveals that the current configuration does not match the configuration of the originally implemented application. Which of the following is the FIRST action to be taken?

A. Recommend an update to the change control process.
B. Verify the approval of the configuration change.

C. Roll back the application to the original configuration.
D. Document the changes to the configuration.

QUESTION 5

For a federated identity solution, a third-party Identity Provider (IdP) is **PRIMARILY** responsible for which of the following?

A. Access Control
B. Account Management
C. Authentication
D. Authorization