Exam : **SY0-801**

Title : CompTIA Security+ V8

Version : DEMO

1.A company requires employees to digitally sign purchase orders before they are approved. Later, an employee claims they never submitted one of the orders.
Which security principle prevents the employee from successfully denying they sent the document?
A. Confidentiality
B. Least privilege
C. Non-repudiation
D. Availability
Answer: C
Explanation:
The correct answer is option C. Non-repudiation provides proof that a specific individual performed an action, preventing them from denying they created or approved a digitally signed document.

2.One of the file servers of an organization has suffered an attack. The organization's IT administrator is searching the log files to understand what happened.
What type of control are they implementing when carrying out the investigation?
A. Operational
B. Technical
C. Detective
D. Physical
Answer: C
Explanation:
The correct answer is option C. Detective controls help in uncovering issues and anomalies that have already occurred. Therefore, log files being searched is a detective control.

3.A financial organization requires every employee to verify their identity and device health before accessing any application, even when connected to the corporate network.
Which security model is being implemented?
A. Implicit trust
B. Zero trust
C. Network segmentation
D. Defense in depth
Answer: B
Explanation:
The correct answer is option B. Zero trust assumes no user or device is trusted by default. Every access request must be continuously verified regardless of its location.

4.During a monthly team meeting, an IT manager instructs the mail administrator and network administrator to create a standard operating procedure (SOP) that documents the required steps for performing routine administrative tasks. Once approved, the SOP provides specific instructions that employees are expected to follow.
What type of control does the SOP represent?
A. Directive
B. Managerial
C. Operational

D. Technical
Answer: A
Explanation:
The correct answer is option A. A directive control provides policies, procedures, or instructions that guide employees on how tasks should be performed. The SOP documents the required steps that staff are expected to follow.

5.Which control type focuses on eliminating or minimizing potential threats before they can cause harm?
A. Preventive
B. Compensating
C. Deterrent
D. Corrective
Answer: A
Explanation:
The correct answer is option A. Preventive controls are designed to prevent problems or risks from occurring by eliminating or minimizing potential threats.