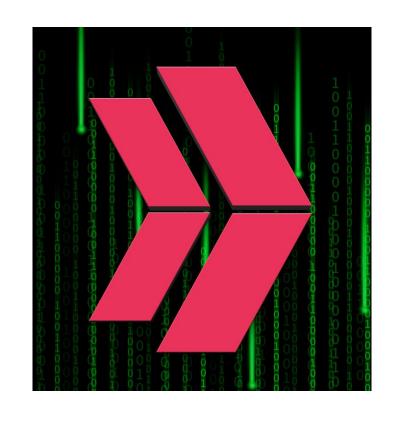


CLARUSWAY

WAY TO REINVENT YOURSELF



CompTIA (1A-1B)

AGENDA



- 1A Security Concepts (4)
- ► 1B Security Controls (8)
- ► TOTAL: 12







NO.1 A healthcare organization wants to provide a web application that allows individuals to digitally report health emergencies. Which of the following is the most important consideration during development?

- A. Scalability
- B. Availability
- C. Cost
- D. Ease of deployment



NO.1 A healthcare organization wants to provide a web application that allows individuals to digitally report health emergencies. Which of the following is the most important consideration during development?

A. Scalability

B. Availability

C. Cost

D. Ease of deployment



NO.2 Which of the following security concepts is the best reason for permissions on a human resources fileshare to follow the principle of least privilege?

- A. Integrity
- B. Availability
- C. Confidentiality
- D. Non-repudiation



NO.2 Which of the following security concepts is the best reason for permissions on a human resources fileshare to follow the principle of least privilege?

(A). Integrity

(B). Availability

(C). Confidentiality

(D). Non-repudiation



NO.3 Two companies are in the process of merging. The companies need to decide how to standardize their information security programs.

Which of the following would best align the security programs?

- A. Shared deployment of CIS baselines
- B. Joint cybersecurity best practices
- C. Both companies following the same CSF
- D. Assessment of controls in a vulnerability report



NO.3 Two companies are in the process of merging. The companies need to decide how to standardize their information security programs.

Which of the following would best align the security programs?

- A. Shared deployment of CIS baselines
- B. Joint cybersecurity best practices
- C. Both companies following the same CSF
- D. Assessment of controls in a vulnerability report



NO.4 Client files can only be accessed by employees who need to know the information and have specified roles in the company.

Which of the following best describes this security concept?

- A. Availability
- B. Confidentiality
- C. Integrity
- D. Non-repudiation

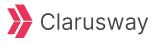


NO.4 Client files can only be accessed by employees who need to know the information and have specified roles in the company.

Which of the following best describes this security concept?

- A. Availability
- **B.** Confidentiality
- C. Integrity
- D. Non-repudiation







NO.1 A company is planning to set up a SIEM system and assign an analyst to review the logs on a weekly basis Which of the following types of controls is the company setting up?

- A. Corrective
- B. Preventive
- C. Detective
- D. Deterrent



NO.1 A company is planning to set up a SIEM system and assign an analyst to review the logs on a weekly basis Which of the following types of controls is the company setting up?

A. Corrective

B. Preventive

C. Detective

D. Deterrent



NO.2 Which of the following has been implemented when a host-based firewall on a legacy Linux system allows connections from only specific internal IP addresses?

- A. Compensating control
- B. Network segmentation
- C. Transfer of risk
- D. SNMP traps



NO.2 Which of the following has been implemented when a host-based firewall on a legacy Linux system allows connections from only specific internal IP addresses?

- A. Compensating control
- B. Network segmentation
- C. Transfer of risk
- D. SNMP traps



NO.3 Which of the following security control types does an acceptable use policy best represent?

- A. Detective
- B. Compensating
- C. Corrective
- D. Preventive



NO.3 Which of the following security control types does an acceptable use policy best represent?

- A. Detective
- B. Compensating
- C. Corrective
- D. Preventive



NO.4 Visitors to a secured facility are required to check in with a photo ID and enter the facility through an access control vestibule Which of the following but describes this form of security control?

- A. Physical
- B. Managerial
- C. Technical
- D. Operational



NO.4 Visitors to a secured facility are required to check in with a photo ID and enter the facility through an access control vestibule Which of the following but describes this form of security control?

- A. Physical
- B. Managerial
- C. Technical
- D. Operational



NO.5 After a recent ransomware attack on a company's system, an administrator reviewed the log files. Which of the following control types did the administrator use?

A. Compensating

B. Detective

C. Preventive

D. Corrective



NO.5 After a recent ransomware attack on a company's system, an administrator reviewed the log files. Which of the following control types did the administrator use?

A. Compensating

B. Detective

C. Preventive

D. Corrective



NO.6 Which of the following security controls is most likely being used when a critical legacy server is segmented into a private network?

- A. Deterrent
- B. Corrective
- C. Compensating
- D. Preventive



NO.6 Which of the following security controls is most likely being used when a **critical legacy** server is <u>segmented into a private network?</u>

- A. Deterrent
- B. Corrective
- C. Compensating
- D. Preventive



NO.7 A security manager is implementing MFA and patch management.

Which of the following would best describe the control type and category? (Select two).

- A. Physical
- B. Managerial
- C. Detective
- D. Administrator
- E. Preventative
- F. Technical



NO.7 A security manager is implementing MFA and patch management.

Which of the following would best describe the control type and category? (Select two).

- A. Physical
- B. Managerial
- C. Detective
- D. Administrator
- E. Preventative
- F. Technical



NO.8 A network administrator deployed a DNS logging tool that togs suspicious websites that are visited and then sends a daily report based on various weighted metrics.

Which of the following best describes the type of control the administrator put in place?

- A. Preventive
- B. Deterrent
- C. Corrective
- D. Detective



NO.8 A network administrator deployed a **DNS logging tool** that togs suspicious websites that are visited and then sends a daily report based on various weighted metrics.

Which of the following best describes the type of control the administrator put in place?

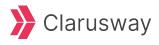
- A. Preventive
- B. Deterrent
- C. Corrective
- D. Detective



THANKS!

Any questions?





Our Graduates are Hired By





Google Deloitte. AT&T ally













































