

Question 1

What does a security professional use to create guidelines and plans that educate employees about how they can help protect the organization? 1 / 1 point

Security framework

Security audit

Security hardening

Security posture

Correct

Question 2

Fill in the blank: An employee using multi-factor authentication to verify their identity is an example of the _____ process. 1 / 1 point

authentication

integrity

encryption

confidentiality

Correct

Question 3

A person's fingerprint, eye or palm scan are examples of what? 1 / 1 point

Passwords

Statistics

Codes

Biometrics

Correct

Question 4

You work as a security analyst for a community organization that has large amounts of private data. Which core principle of the CIA triad do you use to ensure private information is kept safe? 1 / 1 point

Consistency

Availability

Integrity

Confidentiality

Correct

Question 5

Which of the following statements accurately describe the CSF? Select all that apply. 1 / 1 point

The protect function of the CSF involves returning affected systems back to normal operation.

The identify function of the CSF involves managing cybersecurity risk and its effects on an organization's people and assets.

Correct

Implementing improvements to a security process is part of the respond function of the CSF.

Correct

The CSF is a voluntary framework that consists of standards, guidelines, and best practices to manage cybersecurity risk.

Correct

Question 6

A security team establishes controls, including permission settings that will be used to create multiple security points that a threat actor must get through to breach their organization. Which OWASP principle does this scenario describe? 1 / 1 point

Principle of least privilege

Separation of duties

Defense in depth

Keep security simple

Correct

Question 7

What are some of the primary objectives of an internal security audit? Select three answers. 1 / 1 point

Help security teams identify organizational risk

Correct

Improve security posture

Correct

Develop a guiding security statement for the business

Avoid fines due to a lack of compliance

Correct

Question 8

Fill in the blank: In an internal security audit, _____ involves identifying potential threats, risks, and vulnerabilities in order to decide what security measures should be implemented. 1 / 1 point

- assessing compliance
- establishing the scope and goals
- conducting a risk assessment**
- communicating to stakeholders

Correct

Question 9

A security analyst performs an internal security audit. They focus on the human component of cybersecurity, such as the policies and procedures that define how their company manages data. What are they working to establish? 1 / 1 point

- Administrative controls**
- Technical controls
- Physical controls
- Compliance controls

Correct

Question 10

What information is typically communicated to stakeholders after completion of an internal security audit? Select three answers. 1 / 1 point

- A summary of the scope**
- Correct
- A list of existing risks**
- Correct
- Results and recommendations**
- Correct

Questions about specific controls