

More about frameworks and controls

The CIA triad: Confidentiality, integrity, and availability

NIST frameworks

OWASP principles and security audits

Review: Security frameworks and controls

Video: Wrap-up
1 min

Reading: Glossary terms from week 2
10 min

Quiz: Weekly challenge 2
10 questions

🎉 Congratulations! You passed!

Grade received 100%
Latest submission made 10 min
Quiz • 50 min

To pass 80% or higher

Go to next item

Weekly challenge 2

Review Learning Objectives

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 hardening
- ☐ Security posture
- ☒ Security framework
- ☐ Security audit

Submit your assignment

Due Jun 11, 11:59 PM +08 Attempts 3 every 24 hours

Try again

Receive grade

To Pass 80% or higher

✔ Correct

Your grade
100%

View Feedback
We keep your highest score

2. Fill in the blank: A security professional uses _____ to convert data from a readable format to an encoded format.

1 / 1 point

- ☐ authorization
- ☒ encryption
- ☐ confidentiality
- ☐ authentication

✔ Correct

3. A person's fingerprint, eye or palm scan are examples of what?

1 / 1 point

- ☒ Biometrics
- ☐ Passwords
- ☐ Statistics
- ☐ Codes

✔ Correct

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

5. Which of the following statements accurately describe the CSF? Select all that apply.

1 / 1 point

☒ The detect function of the CSF involves improving monitoring capabilities to increase the speed and efficiency of detections.

✔ Correct

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

☒ Restoring affected files or data is part of the recover function of the CSF.

✔ Correct

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

✔ Correct

6. A security team has just finished addressing a recent security incident. They now conduct tests to ensure that all of their repairs were successful. Which OWASP principle does this scenario describe?

1 / 1 point

- ☒ Fix security issues correctly
- ☐ Principle of least privilege
- ☐ Separation of duties
- ☐ Minimize attack surface area

✔ Correct

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

1 / 1 point

☒ Avoid fines due to a lack of compliance

✔ Correct

☒ Improve security posture

✔ Correct

☐ Develop a guiding security statement for the business

☒ Help security teams identify organizational risk

✔ Correct

8. Fill in the blank: In an internal security audit, _____ refers to identifying people, assets, policies, procedures, and technologies that might impact an organization's security posture.

1 / 1 point

- ☐ goals
- ☐ completing a controls assessment
- ☐ implementing administrative controls
- ☒ scope

✔ Correct

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

- ☐ Technical controls
- ☐ Compliance controls
- ☐ Physical controls
- ☒ Administrative controls

✔ Correct

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

1 / 1 point

☐ Questions about specific controls

☒ A list of existing risks

✔ Correct

☒ A summary of the scope

✔ Correct

☒ Results and recommendations

✔ Correct