

Quiz #1



Varshit Chirag Jain (username: varshitjain)

Attempt 1

Written: Mar 14, 2023 6:45 PM - Mar 14, 2023 7:09 PM

Submission View

Question 1

1 / 1 point

The CIA Triangle includes confidentiality, availability, and integrity.

- ✓ ☒ 1) True
- ☐ 2) False

▶ [View question 1 feedback](#)

Question 2

0 / 1 point

Wardriving is a form of an active EMSEC attack.

- ✗ ☐ 1) True
- ➡ ☐ 2) False

Question 3

1 / 1 point

All electronic devices emit radiation which may contain information.

- ✓ ☒ 1) True
- ☐ 2) False

▶ [View question 3 feedback](#)

Question 4

1 / 1 point

Users own the data they store on the organization's computers and servers.

- ☐ 1) True
- ✓ ☒ 2) False

▶ [View question 4 feedback](#)

Question 5

1 / 1 point

User piracy is a liability to organizations.

- ✓ ☒ 1) True
☐ 2) False

▶ [View question 5 feedback](#)

Question 6

1 / 1 point

Software such as Cain & Abel and John the Ripper are commonly used for IA assessments.

- ✓ ☒ 1) True
☐ 2) False

▶ [View question 6 feedback](#)

Question 7

1 / 1 point

When destroying the data on a hard drive, the DoD requires a minimum of 10 passes.

- ☐ 1) True
✓ ☒ 2) False

▶ [View question 7 feedback](#)

Question 8

1 / 1 point

Information Assurance is defined as the set of measures intended to protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation.

- ✓ ☒ 1) True
☐ 2) False

▶ [View question 8 feedback](#)

Question 9**1 / 1 point**

Blue team versus red team is a security exercise used to determine potential vulnerabilities and discover how to protect against them.

- ✓ ☒ 1) True
☐ 2) False

▶ [View question 9 feedback](#)

Question 10**1 / 1 point**

There are two IA domains: system assurance and hardware assurance.

- ☐ 1) True
✓ ☒ 2) False

▶ [View question 10 feedback](#)

Question 11**1 / 1 point**

The five pillars of information assurance include:

- ☐ availability, security, authentication, confidentiality, and non-repudiation
✓ ☒ availability, integrity, authentication, confidentiality, and non-repudiation
☐ availability, security, encryption, confidentiality, and non-repudiation
☐ availability, integrity, authentication, confidentiality, and encryption

▶ [View question 11 feedback](#)

Question 12**1 / 1 point**

When performing due diligence, which investigative tools are used by the system administrator?

- ☐ Evidence Collection

- ☐ Information Retrieval
- ☐ System Testing & Evaluation
- ☒ Both A and B
- ☐ Both A and C

▶ [View question 12 feedback](#)

Question 13

1 / 1 point

When was TEMPEST declassified by the U.S. Government?

- ☐ 1992
- ☒ 1995
- ☐ 1999
- ☐ 2003

Question 14

1 / 1 point

Information assurance is important because it covers the following areas:

- ☐ Privacy
- ☐ Theft
- ☐ Malicious Intent
- ☒ All of the Above

▶ [View question 14 feedback](#)

Question 15**1 / 1 point**

The focus areas of Defense-in-Depth include:

- ☐ Network & Infrastructure
- ☐ Computing Environment
- ☐ Reporting Infrastructure
- ✓ ☒ None of the Above

▶ [View question 15 feedback](#)

Question 16**1 / 1 point**

Timely, reliable access to data and information services for authorized users.

- ☐ Confidentiality
- ✓ ☒ Availability
- ☐ Integrity
- ☐ Security

▶ [View question 16 feedback](#)

Question 17**1 / 1 point**

Who owns the data created and stored on a corporate network?

- ✓ ☒ The Corporation

- ☐ The Government
- ☐ The User Who Created the Data
- ☐ The System Administrator

▶ [View question 17 feedback](#)

Question 18

1 / 1 point

When addressing the zone of control, which of the following is NOT considered a physical zone?

- ☐ Networking/Telecommunications Closets
- ☐ Server/Equipment Rooms
- ☐ Media Storage & Handling
- ✓ ☒ Network Resources

▶ [View question 18 feedback](#)

Question 19

1 / 1 point

Generally Accepted Information Security Principles were developed by the Information Systems Security Association and include which of the following?

- ☐ Accountability
- ☐ Awareness
- ☐ Assessment
- ✓ ☒ All of the Above

[▶ View question 19 feedback](#)

Question 20

1 / 1 point

Which of the following is NOT a step during system testing and evaluation?

- ☐ Determine the System is Candidate for IA
- ☐ High Mission Criticality = High Need for IA
- ☐ Certification & Accreditation
- ☒ Vulnerabilities Identified & Repaired Before Assessment by Blue Team

[▶ View question 20 feedback](#)

Attempt Score: 19 / 20 - 95 %

Overall Grade (highest attempt): 19 / 20 - 95 %

Done