CSUDH   anizations   Portfolios   MyBb   Library   Mail   Brandon Mao   elp

Com Systems Security CTC362-01_2194_22066   Tests   Review Test Submission: Quiz #4a

Review Test Submission: Quiz #4a

User	Brandon Ethan Mao
Course	Com Systems Security
Test	Quiz #4a
Started	2/20/19 2:24 PM
Submitted	2/20/19 3:26 PM
Status	Completed
Attempt Score	53 out of 54 points
Time Elapsed	1 hour, 1 minute out of 1 hour and 30 minutes
Instructions	Read each question carefully before answering.
Results Displayed	All Answers, Submitted Answers, Correct Answers, Feedback, Incorrectly Answered Questions

Question 1   1 out of 1 points

Implementing multiple types of technology and thereby precluding that the failure of one system will compromise the security of information is referred to as _____.

Selected Answer: ✅ redundancy

Correct Answer:

Evaluation Method	Correct Answer	Case Sensitivity
✅ Exact Match	redundancy	
✅ Exact Match	defense in depth	

Question 2   1 out of 1 points

A(n) _____ plan ensures that critical business functions continue if a catastrophic incident or disaster occurs.

Selected Answer: ✅ business continuity

Correct Answer:

Evaluation Method	Correct Answer	Case Sensitivity
✅ Exact Match	business continuity	
✅ Exact Match	business continuity (BC)	
✅ Exact Match	BC	

Question 3

1 out of 1 points

_____ is a strategy for the protection of information assets that uses multiple layers and different types of controls (managerial, operational, and technical) to provide optimal protection.

Selected Answer: ✅ c. Defense in depth

Answers: a. Networking

       b. Best-effort

       ✅ c. Defense in depth

       d. Proxy

Question 4

1 out of 1 points

Incident _____ is the set of activities taken to plan for, detect, and correct the impact of an incident on information assets.

Selected Answer: ✅ response

Correct Answer:

Evaluation Method	Correct Answer	Case Sensitivity
✅ Exact Match	response	

Question 5

3 out of 4 points

Compare electronic vaulting and remote journaling.

Selected Answer: Electronic vaulting is the transfer of large batches of data to an offsite facility. Likewise, remote journaling is the transfer of live transactions to an offsite facility.

Correct Answer: ✅
The transfer of large batches of data to an offsite facility is called electronic vaulting. The transfer of live transactions to an offsite facility is called remote journaling. It differs from electronic vaulting in that 1) only transactions are transferred, not archived data, and 2) the transfer is in real-time. Electronic vaulting is much like a traditional backup, with a dump of data to the off-site storage, but remote journaling involves activities on a systems level, much like server fault tolerance, with the data written to two locations simultaneously.

Response Feedback: [None Given]

Question 6

1 out of 1 points

_____ controls are information security safeguards focusing on lower-level planning that deals with the functionality of the organization's security. These safeguards include disaster recovery and incident response planning.

Selected Answer: ✅ Operational

Correct Answer:

Evaluation Method	Correct Answer	Case Sensitivity
✅ Exact Match	Operational	

Question 7

1 out of 1 points

A(n) _____ is a document containing contact information for the people to be notified in the event of an incident.

Selected Answer: ✅ d. alert roster

Answers: a. emergency notification system

                  b. phone list

                  c. call register

                  ✅ d. alert roster

Question 8

1 out of 1 points

A(n) _____ is a scripted description of an incident, usually just enough information so that each individual knows what portion of the IRP to implement, and not enough to slow down the notification process.

Selected Answer: ✅ alert message

Correct Answer:

Evaluation Method	Correct Answer	Case Sensitivity
✅ *Exact Match*	alert message	

Question 9

1 out of 1 points

Security _____ are the areas of trust within which users can freely communicate.

Selected Answer: ✅ b. domains

Answers: a. perimeters

                  ✅ b. domains

                  c. layers

                  d. rectangles

Question 10

1 out of 1 points

RAID is an acronym for a _____ array of independent disk drives that stores information across multiple units to spread out data and minimize the impact of a single drive failure.

Selected Answer: ✅ d. redundant

Answers: a. replicated

                  b. resistant

                  c. random

                  ✅ d. redundant

Question 11
1 out of 1 points

A(n) _____ is a plan or course of action that conveys instructions from an organization's senior management to those who make decisions, take actions, and perform other duties.

Selected Answer: ✅ policy

Correct Answer:

Evaluation Method	Correct Answer	Case Sensitivity
✅ *Exact Match*	policy	

Question 12
1 out of 1 points

The spheres of security are the foundation of the security framework and illustrate how information is under attack from a variety of sources, with far fewer protection layers between the information and potential attackers on the _____ side of the organization.

Selected Answer: ✅ d. people

Answers:　　　a. Internet

　　　　　　　b. technology

　　　　　　　c. operational

　　　　　　✅ d. people

Question 13
7 out of 7 points

What is an ACL? What does it regulate?

Selected Answer: ACL stands for access control lists. They are a specification of an organization's information asset, the users who may access and use it, and their rights and privileges for using the asset. They restrict access for a particular user, computer, time, duration, and file. In general, they regulate who can use the system, what authorized users can access, when authorized users can access the system, and where authorized users can access the system from.

Correct Answer: ✅
Access Control List- Constist of details about user access and use permissions and priveileges for an organizational assset or resource, such as a file storage system, software component, or network communication device.
ACL regulates-
Who can use the system.
What authorized users can access.
When authorized users can access the system.
Where authorized users can access the system.

Response Feedback: [None Given]

Question 14
1 out of 1 points

A(n) _____ is an adverse event that could result in loss of an information asset or assets, but does not currently threaten the viability of the entire organization.

Selected Answer: ✅ incident

Correct Answer:

Evaluation Method	Correct Answer	Case Sensitivity
✅ Exact Match	incident	

Question 15

1 out of 1 points

Many organizations have policies that prohibit _____ tools, often used by those who attack systems, to explicitly prohibit the installation of such tools without the written permission of the CISO.

Selected Answer: ✅ hacker

Correct Answer:

Evaluation Method	Correct Answer	Case Sensitivity
✅ Exact Match	hacker	
✅ Exact Match	hacking	

Question 16

1 out of 1 points

_____ management is the set of actions taken by an organization in response to an emergency to minimize injury or loss of life, preserve the organization's image and market share, and complement its disaster recovery and business continuity processes.

Selected Answer: ✅ Crisis

Correct Answer:

Evaluation Method	Correct Answer	Case Sensitivity
✅ Exact Match	crisis	

Question 17

1 out of 1 points

_____often function as standards or procedures to be used when configuring or maintaining systems.

Selected Answer: ✅ d. SysSPs

Answers: a. ESSPs

b. ISSPs

c. EISPs

✅ d. SysSPs

Question 18

1 out of 1 points

The _____is based on and directly supports the mission, vision, and direction of the organization and sets the strategic direction, scope, and tone for all security efforts.

Selected Answer: ✅ c. EISP

Answers: a. ISSP

            b. GSP

            ✅ c. EISP

            d. SysSP

Question 19
1 out of 1 points

A fundamental difference between a BIA and risk management is that risk management focuses on identifying the threats, vulnerabilities, and attacks to determine which controls can protect the information, while the BIA assumes _____.

Selected Answer: ✅ a. All of the above

Answers: ✅ a. All of the above

            b. controls have been bypassed

            c. controls have proven ineffective

            d. controls have failed

Question 20
1 out of 1 points

Redundancy can be implemented at a number of points throughout the security architecture, such as in _____

Selected Answer: ✅ d. All of the above

Answers: a. firewalls

            b. proxy servers

            c. access controls

            ✅ d. All of the above

Question 21
1 out of 1 points

The _____ of an organization are the intermediate states obtained to achieve progress toward a goal or goals.

Selected Answer: ✅ objectives

Correct Answer:

Evaluation Method	Correct Answer	Case Sensitivity
✅ Exact Match	objectives	

Question 22
1 out of 1 points

Computer _____ is the process of collecting, analyzing, and preserving computer-related evidence.

Selected Answer: ✅ forensics

Correct Answer:

Evaluation Method	Correct Answer	Case Sensitivity
✅ *Exact Match*	forensics	

Question 23
1 out of 1 points

The security _____ is an outline or structure of the organization's overall information security strategy that is used as a road map for planned changes to its information security environment

Selected Answer: ✅ framework

Correct Answer:

Evaluation Method	Correct Answer	Case Sensitivity
✅ *Exact Match*	framework	

Question 24
1 out of 1 points

A(n) _____ plan is a plan for the organization's intended strategic efforts over the next several years.

Selected Answer: ✅ c. strategic

Answers: a. standard

                  b. tactical

                  ✅ c. strategic

                  d. operational

Question 25
1 out of 1 points

A security _____ is an outline of the overall information security strategy for the organization and a roadmap for planned changes to the information security environment of the organization.

Selected Answer: ✅ a. framework

Answers: ✅ a. framework

                  b. plan

                  c. policy

                  d. model

Question 26
1 out of 1 points

A(n) _____ site is a fully configured computer facility, with all services, communications links, and physical plant operations including heating and air conditioning.

Selected Answer: ❌ hot site

Correct Answer:

Evaluation Method	Correct Answer	Case Sensitivity
✅ Exact Match	hot	

Question 27

1 out of 1 points

The SETA program is a control measure designed to reduce the instances of _____ security breaches by employees.

Selected Answer: ✅ a. accidental

Answers: ✅ a. accidental

b. intentional

c. external

d. physical

Question 28

1 out of 1 points

Incident _____ is the process of examining a potential incident, or incident candidate, and determining whether or not the candidate constitutes an actual incident.

Selected Answer: ✅ classification

Correct Answer:

Evaluation Method	Correct Answer	Case Sensitivity
✅ Exact Match	classification	

Question 29

1 out of 1 points

_____ controls address personnel security, physical security, and the protection of production inputs and outputs.

Selected Answer: ✅ b. Operational

Answers: a. Technical

✅ b. Operational

c. Informational

d. Managerial

Question 30

1 out of 1 points

Some policies may need a(n) _____ indicating their expiration date.

Selected Answer: ✅ sunset clause

Correct Answer:

Evaluation Method	Correct Answer	Case Sensitivity

        ✅ *Exact Match*   sunset clause

Question 31

1 out of 1 points

Incident _____ is the rapid determination of the scope of the breach of the confidentiality, integrity, and availability of information and information assets during or just following an incident.

Selected Answer:	✅ d. damage assessment
Answers:	a. disaster assessment
	b. containment strategy
	c. incident response
	✅ d. damage assessment

Question 32

1 out of 1 points

_____-specific security policies often function as standards or procedures to be used when configuring or maintaining systems.

Selected Answer: ✅ Systems

Correct Answer:

Evaluation Method	Correct Answer	Case Sensitivity
✅ *Exact Match*	Systems	

Question 33

3 out of 3 points

What three purposes does the ISSP serve?

Selected Answer:	1) Addresses specific areas of technology. 2) Requires frequent updates. 3) Contains statements on the organization's position on a specific issue.
Correct Answer:	✅ The issue-specific security policy, or ISSP, 1) addresses specific areas of technology as listed below, 2) requires frequent updates, and 3) contains a statement on the organization's position on a specific issue.
Response Feedback:	[None Given]

Question 34

1 out of 1 points

A _____ site provides only rudimentary services and facilities.

Selected Answer:	✅ c. cold
Answers:	a. commercial
	b. hot
	✅ c. cold

d. warm

Question 35

1 out of 1 points

_____ controls are information security safeguards that focus on the application of modern technologies, systems, and processes to protect information assets..

Selected Answer: ✅ Technical

Correct Answer:

Evaluation Method	Correct Answer	Case Sensitivity
✅ Exact Match	Technical	

Question 36

1 out of 1 points

A(n) _____ backup is the storage of all files that have changed or been added since the last full backup.

Selected Answer: ✅ differential

Correct Answer:

Evaluation Method	Correct Answer	Case Sensitivity
✅ Exact Match	differential	

Question 37

1 out of 1 points

_____ controls are security processes that are designed by strategic planners and implemented by the security administration of the organization.

Selected Answer: ✅ Managerial

Correct Answer:

Evaluation Method	Correct Answer	Case Sensitivity
✅ Exact Match	Managerial	

Question 38

1 out of 1 points

A security _____ defines the boundary between the outer limit of an organization's security and the beginning of the outside world.

Selected Answer: ✅ perimeter

Correct Answer:

Evaluation Method	Correct Answer	Case Sensitivity
✅ Exact Match	perimeter	

Question 39

1 out of 1 points

_____ controls cover security processes that are designed by strategic planners and implemented by the security administration of the organization.

Selected Answer: ✅ b. Managerial

Answers: a. Operational

                  ✅ b. Managerial

                  c. Technical

                  d. Informational

Question 40

1 out of 1 points

A(n) _____ is a contract between two or more organizations that specifies how each will assist the other in the event of a disaster.

Selected Answer: ✅ mutual agreement

Correct Answer:

Evaluation Method	Correct Answer	Case Sensitivity
✅ *Exact Match*	mutual agreement	

Question 41

0 out of 6 points (Extra Credit)

Describe a method to set up an ACL for a Windows file system.

Selected Answer: Administrators can configure ACLs to determine accessibility for someone in their systems. As admin, go to the user accounts menu. Select a user and start configuring their properties of access.

Correct Answer: [None]

Response Feedback: [None Given]

Question 42

1 out of 1 points

A(n) _____ is a detailed examination of the events that occurred from first detection to final recovery.

Selected Answer: ✅ after-action review

Correct Answer:

Evaluation Method	Correct Answer	Case Sensitivity
✅ *Exact Match*	AAR	
✅ *Exact Match*	after-action review	
✅ *Exact Match*	AAR (after-action review)	
✅ *Exact Match*	after-action review (AAR)	

Question 43

1 out of 1 points

_____ is a strategy of using multiple types of technology that prevent the failure of one system from compromising the security of information.

Selected Answer: ✓ a. Redundancy

Answers: ✓ a. Redundancy

                         b. Firewalling

                         c. Hosting

                         d. Domaining

Question 44

1 out of 1 points

RAID Level 1 is commonly called disk _____.

Selected Answer: ✓ mirroring

Correct Answer:

Evaluation Method	Correct Answer	Case Sensitivity
✓ Exact Match	mirroring	

Monday, March 4, 2019 7:57:19 PM PST

← OK