CSUDH Organizations Portfolios MyBb Library Mail System Check Help Brandon Mao

Com Systems Security CTC362-01_2194_22066 Tests Review Test Submission: Quiz #5a

Review Test Submission: Quiz #5a

User	Brandon Ethan Mao
Course	Com Systems Security
Test	Quiz #5a
Started	2/27/19 8:17 AM
Submitted	2/27/19 9:13 AM
Status	Completed
Attempt Score	56 out of 50 points
Time Elapsed	55 minutes 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

✓ A(n) ____________________ is a performance value or metric used to compare changes in the object being measured.

Selected Answer: ✓ baseline

Correct Answer:

Evaluation Method	Correct Answer	Case Sensitivity
✓ *Exact Match*	baseline	

Question 2

1 out of 1 points

✓ Management of classified data includes its storage and _________.

Selected Answer: ✓ d. All of the above

Answers:

a. distribution

b. portability

c. destruction

✓ d. All of the above

Question 3

1 out of 1 points

✓ Overriding an employee’s security clearance requires that the employee meet the _________________________ standard be met.

Selected Answer: ✓ need-to-know

Correct Answer:

Evaluation Method	Correct Answer	Case Sensitivity
✓ *Exact Match*	need-to-know	
✓ *Exact Match*	need to know	

Question 4

1 out of 1 points

✓ Using the simplified information classification scheme outlined in the text, all information that has been approved by management for public release has a(n) ____________________ classification.

Selected Answer: ✓ external

Correct Answer:

Evaluation Method	Correct Answer	Case Sensitivity
✓ *Exact Match*	external	

Question 5

1 out of 1 points

✓ The first phase of risk management is _________.

Selected Answer: ✓ c. risk identification

Answers:

a. risk evaluation

b. design

✓ c. risk identification

d. risk control

Question 6

1 out of 1 points

✓ The _________ control strategy that attempts to eliminate or reduce any remaining uncontrolled risk through the application of additional controls and safeguards.

Selected Answer: ✓ a. defense

Answers:

✓ a. defense

b. termination

c. transfer

d. mitigate

Question 7

1 out of 1 points

✓ A(n) _________ is a formal access control methodology used to assign a level of confidentiality to an information asset and thus restrict the number of people who can access it..

Selected Answer: ✓ d. data classification scheme

Answers: a. security clearance scheme

b. data recovery scheme

c. risk management scheme

✓ d. data classification scheme

Question 8

1 out of 1 points

✓ __________ equals the probability of a successful attack times the expected loss from a successful attack plus an element of uncertainty.

Selected Answer: ✓ d. Risk

Answers: a. Loss Frequency

b. Loss

c. Loss Magnitude

✓ d. Risk

Question 9

1 out of 1 points

✓ A(n) __________ is an authorization issued by an organization for the repair, modification, or update of a piece of equipment.

Selected Answer: ✓ a. FCO

Answers: ✓ a. FCO

b. CTO

c. HTTP

d. IP

Question 10

1 out of 1 points

✓ ______________________ measures are generally less focused on numbers and are more strategic than metrics-based measures.

Selected Answer: ✓ Process-based

Correct Answer:

Evaluation Method	Correct Answer	Case Sensitivity
✓ *Exact Match*	process-based	

Question 11

1 out of 1 points

✓ ___________ is an asset valuation approach that uses categorical or non-numeric values rather than absolute numerical measures.

Selected Answer: ✓ b. Qualitative assessment

Answers: a. Quantitative assessment

✓ b. Qualitative assessment

c. Value-specific constant

d. Metric-centric model

Question 12

1 out of 1 points

____________________ is the process of identifying risk, as represented by vulnerabilities, to an organization’s information assets and infrastructure, and taking steps to reduce this risk to an acceptable level.

Selected Answer: ✓ Risk management

Correct Answer:

Evaluation Method	Correct Answer	Case Sensitivity
✓ *Exact Match*	Risk management	

Question 13

1 out of 1 points

Behavioral feasibility is also known as ____________________.

Selected Answer: ✓ operational feasibility

Correct Answer:

Evaluation Method	Correct Answer	Case Sensitivity
✓ *Exact Match*	operational feasibility	

Question 14

1 out of 1 points

__________ plans usually include all preparations for the recovery process, strategies to limit losses during the disaster, and detailed steps to follow when the smoke clears, the dust settles, or the flood waters recede.

Selected Answer: ✓ c. DR

Answers: a. BR

b. BC

✓ c. DR

d. IR

Question 15

1 out of 1 points

Risk _________ defines the quantity and nature of risk that organizations are willing to accept as they evaluate the tradeoffs between perfect security and unlimited accessibility.

Selected Answer: ✓ d. appetite

Answers: a. acceptance

b. avoidance

c. benefit

✓ d. appetite

Question 16

1 out of 1 points

✓ The combination of an asset’s value and the percentage of the asset that might be lost in an attack is known as the loss ____________________.

Selected Answer: ✓ magnitude

Correct Answer:

Evaluation Method	Correct Answer	Case Sensitivity
✓ *Exact Match*	magnitude	

Question 17

1 out of 1 points

✓ _________ addresses are sometimes called electronic serial numbers or hardware addresses.

Selected Answer: ✓ c. MAC

Answers:

a. HTTP

b. IP

✓ c. MAC

d. DHCP

Question 18

1 out of 1 points

✓ The __________ strategy is the choice to do nothing to protect a vulnerability and to accept the outcome of its exploitation.

Selected Answer: ✓ c. acceptance

Answers:

a. defense

b. transfer

✓ c. acceptance

d. mitigation

Question 19

1 out of 1 points

✓ The __________ plan specifies the actions an organization can and should take while 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) is in progress.

Selected Answer: ✓ b. IR

Answers:

a. BR

✓ b. IR

c. BC

d. DR

Question 20

1 out of 1 points

__________ assigns a status level to employees to designate the maximum level of classified data they may access.

Selected Answer: ✓ b. security clearance scheme

Answers:

a. data recovery scheme

✓ b. security clearance scheme

c. data classification scheme

d. risk management scheme

Question 21

1 out of 1 points

____________________ is the process of comparing other organizations' activities against the practices used in one's own organization to produce results it would like to duplicate..

Selected Answer: ✓ Benchmarking

Correct Answer:

Evaluation Method	Correct Answer	Case Sensitivity
✓ *Exact Match*	Benchmarking	

Question 22

1 out of 1 points

____________________ is the process of assigning financial value or worth to each information asset.

Selected Answer: ✓ Asset valuation

Correct Answer:

Evaluation Method	Correct Answer	Case Sensitivity
✓ *Exact Match*	Asset valuation	
✓ *Exact Match*	Information asset valuation	

Question 23

1 out of 1 points

The __________ is the difference between an organization's observed and desired performance.

Selected Answer: ✓ a. performance gap

Answers:

✓ a. performance gap

b. objective

c. issue delta

d. risk assessment

Question 24

1 out of 1 points

__________ is simply how often you expect a specific type of attack to occur.

Selected Answer: ✓ d. ARO

Answers:

a. SLE

b. ALE

c. CBA

✓ d. ARO

Question 25

1 out of 1 points

Risk _________ is the application of security mechanisms to reduce the risks to an organization’s data and information systems.

Selected Answer: ✓ d. control

Answers:

a. management

b. security

c. identification

✓ d. control

Question 26

1 out of 1 points

When organizations adopt security measures for a legal defense, they may need to show that they have done what any prudent organization would do in similar circumstances. This is referred to as __________.

Selected Answer: ✓ c. standards of due care

Answers:

a. baselining

b. benchmarking

✓ c. standards of due care

d. best practices

Question 27

1 out of 1 points

____________________ is the probability that a specific vulnerability within an organization's assets will be successfully attacked.

Selected Answer: ✓ Likelihood

Correct Answer:

Evaluation Method	Correct Answer	Case Sensitivity
✓ *Exact Match*	Likelihood	

Question 28

1 out of 1 points

Federal agencies such as the NSA, FBI, and CIA use specialty classification schemes. For materials that are not considered 'National Security Information', ___________ data is the lowest level classification.

Selected Answer: ✓ c. Unclassified

Answers:

a. Sensistive

b. Confidential

✓ c. Unclassified

d. Public

Question 29

1 out of 1 points

Once the inventory and value assessment are complete, you can prioritize each asset using a straightforward process known as ______________________ analysis.

Selected Answer: ✓ weighted factor

Correct Answer:

Evaluation Method	Correct Answer	Case Sensitivity
✓ *Exact Match*	weighted factor	
✓ *Exact Match*	weighted table	

Question 30

1 out of 1 points

______________________ feasibility analysis is an assessment of which controls can and cannot occur based on the consensus and relationships among communities of interest.

Selected Answer: ✓ Political

Correct Answer:

Evaluation Method	Correct Answer	Case Sensitivity
✓ *Exact Match*	Political	

Question 31

6 out of 6 points (Extra Credit)

One of the first components of risk identification is identification. inventory and categorization of assets, including all elements, or attributes, of an organization's information system. List and describe these asset attributes.

Selected Answer:

Asset attributes can include:
1) People: Can be accounted towards employees (trusted employees and other staff) and nonemployees (people at trusted organizations or stangers and visitors). Includes the position name, number, and ID of people, supervisor, security clearance level, and special skills.
2) Procedures: Can be split between IT and business standard procedures or IT and business-sensitive procedures. Includes a description, purpose, relation of software, hardware, and network, storage location for reference and update. They either don't expose knowledge useful to a potential attacker, or are sensitive and could allow adversaries to gain advantage.
3) Data: Involves the management of information within the transmission, processing, and storage states. Includes the classification, manager, size of data structure, location, and backup procedures.
4) Software: Can be assigned towards applications, operating systems, and security components.
5) Hardware: Involves usual system devices and peripherals (security devices and peripherals), or information security control systems and networking components (intranet, internet, or DMZ components).

Correct Answer: ✓
People comprise employees and nonemployees.
Procedures fall into two categories: IT and business standard procedures, and IT and business sensitive procedures.
Data components account for the management of information in all its states: transmission, processing, and storage.
Software components are assigned to one of three categories: applications, operating systems, or security components.
Hardware is assigned to one of two categories: the usual systems devices and their peripherals, and the devices that are part of information security control systems.
Hardware components are separated into two categories: devices and peripherals, and networks.

Response Feedback: [None Given]

Question 32

1 out of 1 points

✓ The ___________ control strategy attempts to shift risk to other assets, other processes, or other organizations.

Selected Answer: ✓ a. transfer

Answers: ✓ a. transfer

b. defend

c. accept

d. mitigate

Question 33

1 out of 1 points

✓ After identifying and performing the preliminary classification of an organization's information assets, the analysis phase moves on to an examination of the ____________________ facing the organization.

Selected Answer: ✓ threats

Correct Answer:

Evaluation Method	Correct Answer	Case Sensitivity
✓ *Exact Match*	threats	

Question 34

1 out of 1 points

✓ There are individuals who search trash and recycling — a practice known as _________ — to retrieve information that could embarrass a company or compromise information security.

Selected Answer: ✓ b. dumpster diving

Answers:

a. corporate espionage

✓ b. dumpster diving

c. pretexting

d. shoulder surfing

Question 35

1 out of 1 points

✓ The formal decision making process used when considering the economic feasibility of implementing information security controls and safeguards is called a(n) __________.

Selected Answer: ✓ d. CBA

Answers:

a. ARO

b. SLE

c. ALE

✓ d. CBA

Question 36

1 out of 1 points

✓ The concept of competitive _________ refers to falling behind the competition.

Selected Answer: ✓ d. disadvantage

Answers:

a. drawback

b. failure

c. shortcoming

✓ d. disadvantage

Question 37

1 out of 1 points

✓ The calculation of the likelihood of an attack coupled with the attack frequency to determine the expected number of losses within a specified time range is called the __________.

Selected Answer: ✓ a. loss frequency

Answers:

✓ a. loss frequency

b. benefit of loss

c. annualized loss expectancy

d. likelihood

Question 38

1 out of 1 points

✓ A single loss ____________________ is the calculation of the value associated with the most likely loss from an attack.

Selected Answer: ✓ expectancy

Correct Answer:

Evaluation Method	Correct Answer	Case Sensitivity
✓ *Exact Match*	expectancy	

Question 39

1 out of 1 points

✓ __________ feasibility analysis examines user acceptance and support, management acceptance and support, and the overall requirements of the organization's stakeholders.

Selected Answer: ✓ b. Operational

Answers:

a. Technical

✓ b. Operational

c. Political

d. Organizational

Question 40

1 out of 1 points

✓ You can determine the relative risk for each of the organization's information assets by a process called risk ____________________.

Selected Answer: ✓ assessment

Correct Answer:

Evaluation Method	Correct Answer	Case Sensitivity
✓ *Exact Match*	assessment	

Question 41

1 out of 1 points

✓ Of the three types of mitigation plans, the ____________________ plan is the most strategic and long term, as it focuses on the steps to ensure the continuation of the organization.

Selected Answer: ✓ business continuity

Correct Answer:

Evaluation Method	Correct Answer	Case Sensitivity
✓ *Exact Match*	BC	
✓ *Exact Match*	Business Continuity	
✓ *Exact Match*	BC (business	

	continuity)	
✓ *Exact Match*	business continuity (BC)	

Question 42

1 out of 1 points

✓ Cost ____________________ is the process of preventing the financial impact of an incident by implementing a control.

Selected Answer: ✓ avoidance

Correct Answer:

Evaluation Method	Correct Answer	Case Sensitivity
✓ *Exact Match*	avoidance	

Question 43

1 out of 1 points

✓ The ____________________ control strategy attempts to reduce the impact caused by the exploitation of vulnerability through planning and preparation.

Selected Answer: ✓ mitigation

Correct Answer:

Evaluation Method	Correct Answer	Case Sensitivity
✓ *Exact Match*	mitigation	

Question 44

1 out of 1 points

✓ A(n) ____________________ policy requires that employees secure all information in appropriate storage containers at the end of each day.

Selected Answer: ✓ clean desk

Correct Answer:

Evaluation Method	Correct Answer	Case Sensitivity
✓ *Exact Match*	clean desk	

Question 45

6 out of 6 points

✓ When valuing information assets, what criteria could be considered in establishing or determining the value of the assets?

Selected Answer:

One should consider whether the information asset:
1) Is the most critical to the organization's success.
2) Generates the most revenue and profitability.
3) Plays the biggest role in generating revenue or delivering services.
4) Would be the most expensive to replace or protect.
5) Would be the most embarrassing or cause the greatest liability if ever revealed.

Correct Answer: ✓

Which information asset is most critical to the organization’s success?
Which information asset generates the most revenue?
Which of these assets plays the biggest role in generating revenue or delivering services?
Which information asset would be the most expensive to replace?
Which information asset would be the most expensive to protect?
Which information asset would most expose the company to liability or embarrassment if revealed?

Response Feedback: [None Given]

Question 46

1 out of 1 points

✓ In a(n) ___________, assets or threats can be prioritized by identifying criteria with differing levels of importance, assigning a score for each of the criteria and then summing and ranking those scores.

Selected Answer: ✓ d. weighted factor analysis

Answers:

a. threat assessment

b. data classification scheme

c. risk management program

✓ d. weighted factor analysis

Monday, March 4, 2019 7:56:39 PM PST

← OK