Started on	Wednesday, 20 July 2022, 10:36 AM
State	Finished
Completed on	Wednesday, 20 July 2022, 10:56 AM
Time taken	20 mins 2 secs
Marks	34.00/35.00
Grade	**9.71** out of 10.00 (**97**%)

Question **1**

Complete

Mark 1.00 out of 1.00

Which one of the following properly defines total risk?

Select one:

- a. Threat X Mitigation
- b. Vulnerability X Controls
- c. Vulnerability - Controls
- d. Threat X Vulnerability X Asset Value

Question 2

Complete

Mark 1.00 out of 1.00

What is the primary goal of an information security grogram?

Select one:

- a. To eliminate losses related to risk
- b. To reduce losses related to residual risk
- c. To reduce losses related to loss of confidentiality, integrity, and availability
- d. To eliminate losses related to employee actions

Question 3

Complete

Mark 1.00 out of 1.00

Which of the following is a goal of risk management?

Select one:

- a. To eliminate the loss associated with risk
- b. To identify the correct cost balance between risk and controls
- c. To calculate value associated with residual risk
- d. to eliminate risk by implementing controls

Question **4**

Complete

Mark 1.00 out of 1.00

You want to ensure that users are granted only the rights to perform actions required only the rights to perform actions required for their jobs. What should you use?

Select one:

- a. Principle of limited rights
- b. Principle of least privilege
- c. Principle of need to know
- d. Separation of duties

Question **5**

Complete

Mark 1.00 out of 1.00

Which of the following security principles divides jobs responsibilities to reduce fraud?

Select one:

- a. Least privilege
- b. Separation of duties
- c. Mandatory vacations
- d. Need to know

Question **6**

Complete

Mark 1.00 out of 1.00

What are two type of intrusion detection systems?

Select one:

- a. Intentional and unintentional
- b. Technical and physical
- c. Natural and man-make
- d. Host-based and network-based

Question **7**

Complete

Mark 1.00 out of 1.00

What allows an attacker to gain additional privileges on a system by sending unexpected code to the system?

Select one:

- a. Input validation
- b. MAC flood
- c. Spiders
- d. Buffer overflow

Question 8

Complete

Mark 1.00 out of 1.00

Which government agency includes the Information Technology Laboratory and publishes SP 800-30?

Select one:

- a. DHS
- b. NCCIC
- c. US-CERT
- d. NIST

Question 9

Complete

Mark 1.00 out of 1.00

What law applies to organizations handling health care information?

Select one:

- a. GLBA
- b. HIPAA
- c. SOX
- d. FISMA

Question **10**

Complete

Mark 1.00 out of 1.00

What law requires schools and libraries to limit offensive content on their computers?

Select one:

- a. SSCP
- b. HIPAA
- c. CIPA
- d. FERPA

Question **11**

Complete

Mark 1.00 out of 1.00

The National Institute of Standards and Technology published Special Publication 800-300. What does this cover?

Select one:

- a. Maturity levels
- b. A framework of good practices
- c. Certification and accreditation
- d. Risk assessments

Question 12

Complete

Mark 1.00 out of 1.00

This standard is focused on maintaining a balance between benefits, risk, and asset use. It is based on five principles and seven enablers. What is this standard?

Select one:

- a. ITIL
- b. CMMI
- c. GAISP
- d. COBIT

Question 13

Complete

Mark 1.00 out of 1.00

A risk management plan includes steps to mitigate risk. Who is responsible for choosing what steps to implement?

Select one:

- a. Management
- b. The POAM manager
- c. The project manager
- d. Risk management team

Question **14**

Complete

Mark 1.00 out of 1.00

What three elements should be included in the findings of the risk management report?

Select one:

- a. Threats, causes, and effects
- b. Criteria, vulnerabilities, and effects
- c. Causes, criteria, and milestones
- d. Causes, criteria, and effects

Question **15**

Complete

Mark 1.00 out of 1.00

What is a POAM?

Select one:

- a. Project objectives and milestones
- b. Plan of action and milestones
- c. Planned objectives and milestones
- d. Project of action milestones

Question **16**

Complete

Mark 1.00 out of 1.00

What elements are included in a quantitative analysis?

Select one:

- a. Probability and impact
- b. SLE, ALE, ARO
- c. Threats and vulnerabilities
- d. ALE, ARO, ARP

Question **17**

Complete

Mark 1.00 out of 1.00

What must you define when performing a qualitative risk assessment?

Select one:

- a. Scales used to define SLE an ALE
- b. Formulas used for ALE
- c. Scales used to define probability and impact
- d. Acceptable level of risk

Question **18**

Complete

Mark 1.00 out of 1.00

When defining the system for the risk assessment, what should you ensure is included?

Select one:

- a. A list of possible attacks
- b. Only the title of the system
- c. The current configuration of the system
- d. A list of previous risk assessments

Question **19**

Complete

Mark 1.00 out of 1.00

Which type of assessment can you perform to identify weaknesses in a system without exploiting the weaknesses?

Select one:

- a. Penetration test
- b. Vulnerability assessment
- c. Exploit assessment
- d. Risk assessment

Question 20

Complete

Mark 1.00 out of 1.00

Which of the following should you match with a control to mitigate a relevant risk?

Select one:

- a. Threat/vulnerability pair
- b. Threats
- c. Residual risk
- d. Vulnerabilities

Question 21

Complete

Mark 1.00 out of 1.00

What does a quantitative RA use to prioritize a risk?

Select one:

- a. Probability and impact
- b. Cost-benefit analysis
- c. Safeguard value
- d. SLE, ARO and ALE

Question 22

Complete

Mark 1.00 out of 1.00

What is included in an RA that helps justify the cost of control?

Select one:

- a. CBA
- b. Probability and impact
- c. ALE
- d. POAM

Question 23

Complete

Mark 1.00 out of 1.00

What determines if an organization is governed by HIPAA?

Select one:

- a. If it is registered with the Securities and Exchange commission.
- b. If it is a federal agency.
- c. If employees handle health-related information.
- d. If it receives E-Rate funding.

Question 24

Complete

Mark 1.00 out of 1.00

What determines if an organization is governed by CIPA?

Select one:

- a. If it receives E-Rate funding.
- b. If it is registered with the Securities and Exchange commission.
- c. If it is a federal agency.
- d. If employees handle health-related information.

Question 25

Complete

Mark 1.00 out of 1.00

What can you use to determine the priority of countermeasures?

Select one:

- a. Disaster recovery plan.
- b. Best guess method.
- c. Cost-benefit analysis.
- d. Threat/likelihood-impact matrix.

Question **26**

Complete

Mark 1.00 out of 1.00

You are evaluating two possible countermeasures to mitigate a risk. Management only wants to purchase one. What can you use to determine which countermeasure provides the best cost benefits?

Select one:

- a. CBA.
- b. Threat score.
- c. Threat/likelihood-impact matrix.
- d. CIA.

Question **27**

Complete

Mark 1.00 out of 1.00

What defines the boundaries of a business impact analysis?

Select one:

- a. Recovery objectives.
- b. MAO.
- c. BCP.
- d. Scope.

Question 28

Complete

Mark 0.00 out of 1.00

You have identified the MAO for a system. You now want to specify the time required for a system to be recovered. What if this called?

Select one:

- a. BIA time.
- b. Maximum acceptable outage.
- c. Recovery point objectives.
- d. Recovery time objectives.

Question 29

Complete

Mark 1.00 out of 1.00

After a BCP has been activated, who will assess the damages?

Select one:

- a. BCP coordinator.
- b. TRT.
- c. EMT.
- d. DAT.

Question 30

Complete

Mark 1.00 out of 1.00

What are the three phases of a BCP?

Select one:

- a. Recovery, renewal, reconstitution.
- b. Notification/activation, transfer, recovery.
- c. Transfer, recovery, notification.
- d. Notification/activation, recovery, reconstitution.

Question 31

Complete

Mark 1.00 out of 1.00

You are considering an alternate location for a DRP. you want to minimize cost for the site. What type of site would you choose?

Select one:

- a. Warm site.
- b. Cold site.
- c. DRP site.
- d. Hot site.

Question 32

Complete

Mark 1.00 out of 1.00

You are considering an alternate location for a DRP. You want to use a business location that is already running noncritical business functions as the alternate location. This location has most of the equipment needed. What type of site is this?

Select one:

- a. DRP site.
- b. Cold site.
- c. Hot site.
- d. Warm site.

Question 33

Complete

Mark 1.00 out of 1.00

Many steps are taken before, during, and after an incident. Of the following choices, what accurately identifies the incident response life cycle?

Select one:

- a. Preparation, deletion and analysis, eradication and recovery, and post-incident recovery.
- b. Detection and analysis, containment, backup and eradication, and post-incident recovery.
- c. Preparation, detection, deletion and analysis, containment and recovery, and post-incident recovery.
- d. Preparation, detection and analysis containment, eradication and recovery, and post-incident recovery.

Question **34**

Complete

Mark 1.00 out of 1.00

After an incident has been verifies, you need to ensure that it doesn't spread to other systems. What is this called?

Select one:

- a. Impact and priority calculation.
- b. Spread avoidance.
- c. Containment.
- d. Incident response.

Question **35**

Complete

Mark 1.00 out of 1.00

Attackers attempt a DoS attack on servers in your organization. The CIRT responds and mitigates the attack. What should be the last step that the CIRT will complete in response to this incident?

Select one:

- a. Containment the threat.
- b. Attack the attacker.
- c. Document the incident.
- d. Report the incident.