|  |  |
| --- | --- |
|  | Which of the following is a procedural control? |
| a. | Session timeout |
| b. | Reasonableness check |
| c. | Water detection |
| d. | **DRP** |

|  |  |
| --- | --- |
|  | What would you use to identify mission-critical systems? |
| a. | Critical outage times. |
| b. | **Critical business functions.** |
| c. | PCI DSS review. |
| d. | Disaster recovery plan. |

|  |  |
| --- | --- |
|  | What determines if an organization is governed by HIPAA? |
| a. | If it is registered with the Securities and Exchange commission. |
| b. | **If employees handle health-related information.** |
| c. | If it receives E-Rate funding. |
| d. | If it is a federal agency. |

|  |  |
| --- | --- |
|  | The process used to demonstrate that the costs of implementing controls can be justified by the reduction of a risk level is \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_. |
| a. | Probability and impact |
| b. | Vulnerability assessment |
| c. | Compliance checking |
| d. | **Cost benefit** |

|  |  |
| --- | --- |
|  | Which of the following is a valid formula used to identify the projected benefits of a control? |
| a. | Loss After Control - Loss Before Control. |
| b. | **Loss Before Control - Loss After Control.** |
| c. | Cost of Control + Losses. |
| d. | Cost of Control/12. |

|  |  |
| --- | --- |
|  | Which of the following are considered facility cost for the implementation of a countermeasure? |
| a. | Installation and air conditioning. |
| b. | Installation and training. |
| c. | **Power and air conditioning.** |
| d. | Power and training. |

|  |  |
| --- | --- |
|  | What can you use to determine the priority of countermeasures? |
| a. | Cost-benefit analysis. |
| b. | **Threat/likelihood-impact matrix.** |
| c. | Disaster recovery plan. |
| d. | Best guess method. |

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

|  |  |
| --- | --- |
|  | What defines the boundaries of a business impact analysis? |
| a. | MAO. |
| b. | BCP. |
| c. | Recovery objectives. |
| d. | **Scope.** |

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

|  |  |
| --- | --- |
|  | You are working on BIA. You are calculating cost to determine the impact of an outage for a specific system. Which one of the following is a direct cost? |
| a. | Loss of customers. |
| b. | loss of public goodwill. |
| c. | **Loss of sales.** |
| d. | Lost opportunities. |

|  |  |
| --- | --- |
|  | After a BCP has been activated, who will assess the damages? |
| a. | BCP coordinator. |
| b. | EMT. |
| c. | **DAT.** |
| d. | None of the mentioned. |

|  |  |
| --- | --- |
|  | What are the three phases of a BCP? |
| a. | Notification/activation, transfer, recovery. |
| b. | **Notification/activation, recovery, reconstitution.** |
| c. | Recovery, renewal, reconstitution. |
| d. | Transfer, recovery, notification. |

|  |  |
| --- | --- |
|  | A major disruption has forced you to move operations to an alternate location. The disruption is over and you need to begin normalizing operations. What operations should you move back to the original location first? |
| a. | **Least critical business functions.** |
| b. | Most critical business functions. |
| c. | Non-mission-critical personnel. |
| d. | Mission-critical personnel. |

|  |  |
| --- | --- |
|  | A business impact analysis (BIA) includes a maximum acceptable Outage (MAO). The MAO is used to determine the amount of time in which a system must be recovered. What term is used in the DRP instead of the MAO? |
| a. | Critical business function (CBP). |
| b. | DRP action item (DRPAI). |
| c. | Recovery action item (RAI). |
| d. | **Recovery time objective (RTO).** |

|  |  |
| --- | --- |
|  | The potential for a particular event to successfully exercise a particular vulnerability is called \_\_\_\_\_\_\_\_\_\_. |
| **a.** | **Threat** |
| b. | Risk |
| c. | Impact |
| d. | Probability |

|  |  |
| --- | --- |
|  | What is the first process in the risk management methodology? |
| a. | Records retention |
| **b.** | **Risk analysis** |
| c. | Likelihood |
| d. | Fault tolerance |

|  |  |
| --- | --- |
|  | Many steps are taken before, during, and after an incident. Of the following choices, what accurately identifies the incident response life cycle? |
| 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 and analysis containment, eradication and recovery, and post-incident recovery.** |
| d. | Preparation, detection, deletion and analysis, containment and recovery, and post-incident recovery. |

|  |  |
| --- | --- |
|  | After an incident has been verifies, you need to ensure that it does NOT spread to other systems. What is this called? |
| a. | Spread avoidance. |
| **b.** | **Containment.** |
| c. | Incident response. |
| d. | Impact and priority calculation. |

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