Vendor: ISACA

Exam Code: CISA

Exam Name: Certified Information Systems Auditor

Version: DEMO

QUESTION 1
Which of the following antispam filtering techniques would BEST prevent a valid, variable- length e-mail message containing a heavily weighted spam keyword from being labeled as spam?

A. Heuristic (rule-based)
B. Signature-based
C. Pattern matching
D. Bayesian (statistical)

Answer: D

QUESTION 2
An offsite information processing facility with electrical wiring, air conditioning and flooring, but no computer or communications equipment, is a:

A. cold site.
B. warm site.
C. dial-up site
D. duplicate processing facility.

Answer: A

QUESTION 3
Which of the following is MOST directly affected by network performance monitoring tools?

A. Integrity
B. Availability
C. Completeness
D. Confidentiality

Answer: B

QUESTION 4
An IS auditor invited to a development project meeting notes that no project risks have been documented. When the IS auditor raises this issue, the project manager responds that it is too early to identify risks and that, if risks do start impacting the project, a risk manager will be hired. The appropriate response of the IS auditor would be to:

A. stress the importance of spending time at this point in the project to consider and document risks, and to develop contingency plans.
B. accept the project manager's position as the project manager is accountable for the outcome of the project.
C. offer to work with the risk manager when one is appointed.
D. inform the project manager that the IS auditor will conduct a review of the risks at the completion of the requirements definition phase of the project.

Answer: A

QUESTION 5

In a public key infrastructure, a registration authority:

A. verifies information supplied by the subject requesting a certificate
B. issues the certificate after the required attributes are verified and the keys are generated.
C. digitally signs a message to achieve nonrepudiation of the signed message.
D. registers signed messages to protect them from future repudiation.

Answer: A

QUESTION 6
Which of the following should be of MOST concern to an IS auditor reviewing the BCP?

A. The disaster levels are based on scopes of damaged functions, but not on duration.
B. The difference between low-level disaster and software incidents is not clear.
C. The overall BCP is documented, but detailed recovery steps are not specified.
D. The responsibility for declaring a disaster is not identified.

Answer: D

QUESTION 7
Which of the following is the key benefit of control self-assessment (CSA)?

A. Management ownership of the internal controls supporting business objectives is reinforced.
B. Audit expenses are reduced when the assessment results are an input to external audit work.
C. Improved fraud detection since internal business staff are engaged in testing controls
D. Internal auditors can shift to a consultative approach by using the results of the assessment.

Answer: A

QUESTION 8
An IS auditor evaluating logical access controls should FIRST:

A. document the controls applied to the potential access paths to the system.
B. test controls over the access paths to determine if they are functional.
C. evaluate the security environment in relation to written policies and practices.
D. obtain an understanding of the security risks to information processing.

Answer: D

QUESTION 9
The logical exposure associated with the use of a checkpoint restart procedure is:

A. denial of service.
B. an asynchronous attack.
C. wire tapping.
D. computer shutdown.

Answer: B

QUESTION 10
Many organizations require an employee to take a mandatory vacation (holiday) of a week or more to:

A. ensure the employee maintains a good quality of life, which will lead to greater productivity.
B. reduce the opportunity for an employee to commit an improper or illegal act.
C. provide proper cross-training for another employee.
D. eliminate the potential disruption caused when an employee takes vacation one day at a time.

Answer: B

QUESTION 11
To determine how data are accessed across different platforms in a heterogeneous environment, an IS auditor should FIRST review:

A. business software.
B. infrastructure platform tools.
C. application services.
D. system development tools.

Answer: C

QUESTION 12
An integrated test facility is considered a useful audit tool because it:

A. is a cost-efficient approach to auditing application controls.
B. enables the financial and IS auditors to integrate their audit tests.
C. compares processing output with independently calculated data.
D. provides the IS auditor with a tool to analyze a large range of information.

Answer: C

QUESTION 13
An IS auditor evaluates the test results of a modification to a system that deals with payment computation. The auditor finds that 50 percent of the calculations do not match predetermined totals. Which of the following would MOST likely be the next step in the audit?

A. Design further tests of the calculations that are in error.
B. Identify variables that may have caused the test results to be inaccurate.
C. Examine some of the test cases to confirm the results.
D. Document the results and prepare a report of findings, conclusions and recommendations.

Answer: C

QUESTION 14
The PRIMARY objective of performing a postincident review is that it presents an opportunity to:

A. improve internal control procedures.

B. harden the network to industry best practices.
C. highlight the importance of incident response management to management.
D. improve employee awareness of the incident response process.

Answer: A

QUESTION 15
When conducting a penetration test of an organization's internal network, which of the following approaches would BEST enable the conductor of the test to remain undetected on the network?

A. Use the IP address of an existing file server or domain controller.
B. Pause the scanning every few minutes to allow thresholds to reset.
C. Conduct the scans during evening hours when no one is logged-in.
D. Use multiple scanning tools since each tool has different characteristics.

Answer: B

QUESTION 16
An organization has implemented a disaster recovery plan. Which of the following steps should be carried out next?

A. Obtain senior management sponsorship.
B. Identify business needs.
C. Conduct a paper test.
D. Perform a system restore test.

Answer: C

QUESTION 17
This question refers to the following diagram.E-mail traffic from the Internet is routed via firewall-1 to the mail gateway. Mail is routed from the mail gateway, via firewall-2, to the mail recipients in the internal network. Other traffic is not allowed. For example, the firewalls do not

allow direct traffic from the Internet to the internal network.The intrusion detection system (IDS) detects traffic for the internal network that did not originate from the mail gateway. The FIRST action triggered by the IDS should be to:

A. alert the appropriate staff.
B. create an entry in the log.
C. close firewall-2.
D. close firewall-1.

Answer: C

QUESTION 18
What is the MOST prevalent security risk when an organization implements remote virtual private network (VPN) access to its network?

A. Malicious code could be spread across the network

B. VPN logon could be spoofed
C. Traffic could be sniffed and decrypted
D. VPN gateway could be compromised

Answer: A

QUESTION 19
When developing a business continuity plan (BCP), which of the following tools should be used to gain an understanding of the organization's business processes?

A. Business continuity self-audit
B. Resource recovery analysis
C. Risk assessment
D. Gap analysis

Answer: C

QUESTION 20
The PRIMARY objective of implementing corporate governance by an organization's management is to:

A. provide strategic direction.
B. control business operations.
C. align IT with business.
D. implement best practices.

Answer: A