Question 1

According to MA guidance on IT. which of the following controls the routing of data packets to link computers?

Options:

A- Operating system.

B- Control environment.

C- Network.

D- Application program code.

Answer:

C

Question 2

Which of the following is the best example of a compliance risk that is likely to arise when adopting a bring-your-own-device (BYOD) policy?

Options:

A- The risk that users try to bypass controls and do not install required software updates.

B- The risk that smart devices can be lost or stolen due to their mobile nature.

C- The risk that an organization intrusively monitors personal information stored on smart devices.

D- The risk that proprietary information is not deleted from the device when an employee leaves.

Answer:

C

Question 3

Question Type: **MultipleChoice**

Which of the following IT-related activities is most commonly performed by the second line of defense?

A- Block unauthorized traffic.

B- Encrypt data.

C- Review disaster recovery test results.

D- Provide independent assessment of IT security.

Answer:

C

Question 4

Question Type: **MultipleChoice**

An internal auditor is investigating a potential fraudulent activity. What is the first test the auditor should perform on the transaction data under scrutiny?

Options:

A- Digital analysis for statistically unlikely occurrences that may indicate system tampering.

B- Verification of the completeness and integrity of the obtained data.

C- Detailed review of the data contents to strategize the best analytical techniques.

D- Calculation of statistical parameters to identify outliers requiring further scrutiny.

Answer:

B

Question 5

Question Type: **MultipleChoice**

During an audit of the organization's annual financial statements, the internal auditor notes that the current cost of goods sold percentage is substantially higher than in prior years. Which of the following is the most likely explanation for this increase?

Options:

A- Cost of raw material inventory items is decreasing.

B- Process to manufacture goods is more efficient.

C- Labor productivity to produce goods is increasing.

D- Write-off of inventory is increasing.

Question 6

Question Type: **MultipleChoice**

Which of the following describes the most appropriate set of tests for auditing a workstation's logical access controls?

Options:

A- Review the list of people with access badges to the room containing the workstation and a log of those who accessed the room.

B- Review the password length, frequency of change, and list of users for the workstation's login process.

C- Review the list of people who attempted to access the workstation and failed, as well as error messages.

D- Review the passwords of those who attempted unsuccessfully to access the workstation and the log of their activity.

Answer:

A

Question 7

The board has requested that the internal audit activity be involved in all phases of the organization's outsourcing of its network management. During which of the following stages is the internal auditor most likely to verify that the organization's right-to-audit clause is drafted effectively?

Options:

A- Implementation and transition phase.

B- Monitoring and reporting phase

C- Decision-making and business-case phase.

D- Tendering and contracting phase.

Answer:

D

Question 8

For employees, the primary value of implementing job enrichment is which of the following?

Options:

A- Validation of the achievement of their goals and objectives.

B- Increased knowledge through the performance of additional tasks.

C- Support for personal growth and a meaningful work experience.

D- An increased opportunity to manage better the work done by their subordinates.

Answer:

C

Question 9

Which of the following is an example of a phishing attack?

Options:

A- An employee receives an email that appears to be from the organization's bank, though it is not. The employee replies to the email and sends the requested confidential information.

B- An organization's website has been hacked. The hacker added political content that is not consistent with the organization's views.

C- An organization's systems have been compromised by malicious software. The software locks the organization's operating system until d ransom is paid.

D- An organization's communication systems have been intercepted. A communication session is controlled by an unauthorized third party.

Answer:

A