Vendor: Isaca

Exam Code:CRISC

Exam Name: Certified in Risk and Information Systems Control

Version: Demo

QUESTION 1

An organization has completed a risk assessment of one of its service providers. Who should be accountable for ensuring that risk responses are implemented?

A. IT risk practitioner

B. Third -partf3ecurity team

C. The relationship owner

D. Legal representation of the business

Correct Answer: C

QUESTION 2

The MAIN reason for creating and maintaining a risk register is to:

A. assess effectiveness of different projects.

B. define the risk assessment methodology.

C. ensure assets have low residual risk.

D. account for identified key risk factors.

Correct Answer: D

QUESTION 3

Which of the following roles is BEST suited to help a risk practitioner understand the impact of IT-related events on business objectives?

A. IT management

B. Internal audit

C. Process owners

D. Senior management

Correct Answer: C

QUESTION 4

Which of the following is the MOST important consideration when determining whether to accept residual risk after

security controls have been implemented on a critical system?

A. Cost versus benefit of additional mitigating controls

B. Annualized loss expectancy (ALE) for the system

C. Frequency of business impact

D. Cost of the Information control system

Correct Answer: A

QUESTION 5

Which of the following are the security plans adopted by the organization? Each correct answer represents a complete solution. (Choose three.)

A. Business continuity plan

B. Backup plan

C. Disaster recovery plan

D. Project management plan

Correct Answer: ABC

QUESTION 6

You are working with a vendor on your project. A stakeholder has requested a change for the project, which will add value to the project deliverables. The vendor that you\\'re working with on the project will be affected by the change. What system can help you introduce and execute the stakeholder change request with the vendor?

A. Contract change control system

B. Scope change control system

C. Cost change control system

D. Schedule change control system

Correct Answer: A

QUESTION 7

Which of the following BEST indicates that additional or improved controls ate needed m the environment?

A. Management, has decreased organisational risk appetite

B. The risk register and portfolio do not include all risk scenarios

C. merging risk scenarios have been identified

D. Risk events and losses exceed risk tolerance

Correct Answer: D

QUESTION 8

Which of the following would be the BEST key performance indicator (KPI) for monitoring the effectiveness of the IT asset management process?

A. Percentage of unpatched IT assets

B. Percentage of IT assets without ownership

C. The number of IT assets securely disposed during the past year

D. The number of IT assets procured during the previous month

Correct Answer: B

QUESTION 9

Which of the following should be included in a risk assessment report to BEST facilitate senior management\\'s understanding of the results?

A. Benchmarking parameters likely to affect the results

B. Tools and techniques used by risk owners to perform the assessments

C. A risk heat map with a summary of risk identified and assessed

D. The possible impact of internal and external risk factors on the assessment results

Correct Answer: C

QUESTION 10

Which of the following is the PRIMARY reason for an organization to ensure the risk register is updated regularly?

A. Risk assessment results are accessible to senior management and stakeholders.

B. Risk mitigation activities are managed and coordinated.

C. Key risk indicators (KRIs) are evaluated to validate they are still within the risk threshold.

D. Risk information is available to enable risk-based decisions.

Correct Answer: D

QUESTION 11

A risk manager has determined there is excessive risk with a particular technology. Who is the BEST person to own the unmitigated risk of the technology?

A. IT system owner

B. Chief financial officer

C. Chief risk officer

D. Business process owner

Correct Answer: D

QUESTION 12

Which of the following could BEST detect an in-house developer inserting malicious functions into a web-based application?

A. Segregation of duties

B. Code review

C. Change management

D. Audit modules

Correct Answer: B