DUMPSBOSS.

# Certified in Risk and Information Systems Control

## Isaca CRISC

### Version Demo

**Total Demo Questions: 20**

**Total Premium Questions: 1799**

**Buy Premium PDF**

https://dumpsboss.co

support@dumpsboss.co

support@dumpsboss.co
dumpsboss.co

# Topic Break Down

| Topic | No. of Questions |
|---|---|
| Topic 1, New Update | 710 |
| Topic 2, Volume A | 100 |
| Topic 3, Volume B | 100 |
| Topic 4, Volume C | 99 |
| Topic 5, Volume D | 790 |
| Total | 1799 |

## QUESTION NO: 1

Which of the following are the responsibilities of Enterprise risk committee?

Each correct answer represents a complete solution. (Choose three.)

**A.** React to risk events

**B.** Analyze risk

**C.** Risk aware decision

**D.** Articulate risk

## ANSWER: B C D

**Explanation:**

Risk aware decision, analyzing risk, and articulating risk are the responsibilities of Enterprise risk committee. They are the executives who are accountable for the enterprise level collaboration and consensus required to support enterprise risk management (ERM) activities and decisions. An IT risk council may be established to consider IT risk in more detail and advise the enterprise risk committee.

ERC ensure that these activities are completed successfully.

Incorrect Answers:

A: ERM is not responsible for reaction over risk events. Business process owners are accounted for this task.

## QUESTION NO: 2

Which of the following would provide executive management with the BEST information to make risk decisions as a result of a risk assessment?

**A.** A quantitative presentation of risk assessment results

**B.** A qualitative presentation of risk assessment results

**C.** A comparison of risk assessment results to the desired state

**D.** An assessment of organizational maturity levels and readiness

## ANSWER: A

## QUESTION NO: 3

Which of the following is the MAIN purpose of monitoring risk?

**A.** Benchmarking

**B.** Risk analysis

**C.** Decision support

**D.** Communication

**ANSWER: B**

## QUESTION NO: 4

What are the two MAJOR factors to be considered while deciding risk appetite level? Each correct answer represents a part of the solution. (Choose two.)

**A.** The amount of loss the enterprise wants to accept

**B.** Alignment with risk-culture

**C.** Risk-aware decisions

**D.** The capacity of the enterprise's objective to absorb loss.

**ANSWER: A D**

**Explanation:**

Risk appetite is the amount of risk a company or other entity is willing to accept in pursuit of its mission. This is the responsibility of the board to decide risk appetite of an enterprise. When considering the risk appetite levels for the enterprise, the following two major factors should be taken into account:

The enterprise's objective capacity to absorb loss, e.g., financial loss, reputation damage, etc.

The culture towards risk taking-cautious or aggressive. In other words, the amount of loss the enterprise wants to accept in pursue of its objective fulfillment.

Incorrect Answers:

B: Alignment with risk-culture is also one of the factors but is not as important as these two.

C: Risk aware decision is not the factor, but is the result which uses risk appetite information as its input.

## QUESTION NO: 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

**ANSWER: A B C**

**Explanation:**

Organizations create different security plans to address different scenarios. Many of the security plans are common to most organizations.

Most used security plans found in many organizations are:

- Business continuity plan
- Disaster recovery plan
- Backup plan
- Incident response plan

Incorrect Answers:

D: Project management plan is not a security plan, but a plan which describes the implementation of the project.

## QUESTION NO: 6

Which of the following is MOST important for mitigating ethical risk when establishing accountability for control ownership?

**A.** Ensuring processes are documented to enable effective control execution

**B.** Ensuring regular risk messaging is Included in business communications from leadership

**C.** Ensuring schedules and deadlines for control-related deliverables are strictly monitored

**D.** Ensuring performance metrics balance business goals with risk appetiie

**ANSWER: B**

## QUESTION NO: 7

You are the project manager of GHT project. A stakeholder of this project requested a change request in this project. What are your responsibilities as the project manager that you should do in order to approve this change request?

Each correct answer represents a complete solution. (Choose two.)

**A.** Archive copies of all change requests in the project file.

**B.** Evaluate the change request on behalf of the sponsor

**C.** Judge the impact of each change request on project activities, schedule and budget.

**D.** Formally accept the updated project plan

**ANSWER: A C**

**Explanation:**

Project manager responsibilities related to the change request approval process is judging the impact of each change request on project activities, schedule and budget, and also archiving copies of all change requests in the project file.

Incorrect Answers:

B: This is the responsibility of Change advisory board.

D: Pm has not the authority to formally accept the updated project plan. This is done by project sponsors so as to approve the change request.

## QUESTION NO: 8

Which of the following are the common mistakes while implementing KRIs?

Each correct answer represents a complete solution. (Choose three.)

**A.** Choosing KRIs that are difficult to measure

**B.** Choosing KRIs that has high correlation with the risk

**C.** Choosing KRIs that are incomplete or inaccurate due to unclear specifications

**D.** Choosing KRIs that are not linked to specific risk

**ANSWER: A C D**

**Explanation:**

A common mistake when implementing KRIs other than selecting too many KRIs includes choosing KRIs that are: ▪ Not linked to specific risk

▪ Incomplete or inaccurate due to unclear specifications

▪ Too generic

▪ Difficult to aggregate, compare and interpret ▪ Difficult to measure

Incorrect Answers:

B: For ensuring high reliability of the KRI, The indicator must possess a high correlation with the risk and be a good predictor or outcome measure. Hence KRIs are chosen that has high correlation with the risk.

## QUESTION NO: 9

Which of the following should be of GREATEST concern when reviewing the results of an independent control assessment to determine the effectiveness of a vendor's control environment?

**A.** The report was provided directly from the vendor.

**B.** The risk associated with multiple control gaps was accepted.

**C.** The control owners disagreed with the auditor's recommendations.

**D.** The controls had recurring noncompliance.

**ANSWER: A**

## QUESTION NO: 10

What are the requirements for creating risk scenarios? Each correct answer represents a part of the solution. (Choose three.)

**A.** Determination of cause and effect

**B.** Determination of the value of business process at risk

**C.** Potential threats and vulnerabilities that could cause loss

**D.** Determination of the value of an asset

**ANSWER: B C D**

**Explanation:**

Creating a scenario requires determination of the value of an asset or a business process at risk and the potential threats and vulnerabilities that could cause loss. The risk scenario should be assessed for relevance and realism, and then entered into the risk register if found to be relevant.

In practice following steps are involved in risk scenario development: ▪ First determine manageable set of scenarios, which include:

- Frequently occurring scenarios in the industry or product area.

- Scenarios representing threat sources that are increasing in count or severity level.

- Scenarios involving legal and regulatory requirements applicable to the business.

▪ After determining manageable risk scenarios, perform a validation against the business objectives of the entity.

▪ Based on this validation, refine the selected scenarios and then detail them to a level in line with the criticality of the entity.

▪ Lower down the number of scenarios to a manageable set. Manageable does not signify a fixed number, but should be in line with the overall importance and criticality of the unit.

- Risk factors kept in a register so that they can be reevaluated in the next iteration and included for detailed analysis if they have become relevant at that time.

- Risk factors kept in a register so that they can be reevaluated in the next iteration and included for detailed analysis if they have become relevant at that time. - Include an unspecified event in the scenarios, that is, address an incident not covered by other scenarios.

Incorrect Answers:

A: Cause-and-effect analysis is a predictive or diagnostic analytical tool used to explore the root causes or factors that contribute to positive or negative effects or outcomes. It is used during the process of exposing risk factors.

## QUESTION NO: 11

You are the project manager of GHT project. Your project team is in the process of identifying project risks on your current project. The team has the option to use all of the following tools and techniques to diagram some of these potential risks EXCEPT for which one?

**A.** Process flowchart

**B.** Ishikawa diagram

**C.** Influence diagram

**D.** Decision tree diagram

## ANSWER: D

**Explanation:**

Decision tree diagrams are used during the Quantitative risk analysis process and not in risk identification.

Incorrect Answers:

A, B, C: All these options are diagrammatical techniques used in the Identify risks process.

## QUESTION NO: 12

Which of the following aspects are included in the Internal Environment Framework of COSO ERM? Each correct answer represents a complete solution. (Choose three.)

**A.** Enterprise's integrity and ethical values

**B.** Enterprise's working environment

**C.** Enterprise's human resource standards

**D.** Enterprise's risk appetite

## ANSWER: A C D

**Explanation:**

The internal environment for risk management is the foundational level of the COSO ERM framework, which describes the philosophical basics of managing risks within the implementing enterprise. The different aspects of the internal environment include the enterprise's:

- Philosophy on risk management
- Risk appetite
- Attitudes of Board of Directors
- Integrity and ethical values
- Commitment to competence
- Organizational structure
- Authority and responsibility
- Human resource standards

## QUESTION NO: 13

Which of the following assets are the examples of intangible assets of an enterprise?

Each correct answer represents a complete solution. (Choose two.)

**A.** Customer trust

**B.** Information

**C.** People

**D.** Infrastructure

## ANSWER: A B

**Explanation:**

Assets are the economic resources owned by business or company. Anything tangible or intangible that one possesses, usually considered as applicable to the payment of one's debts, is considered an asset. An asset can also be defined as a resource, process, product, computing infrastructure, and so forth that an organization has determined must be protected.

Tangible asset: Tangible are those assets that has physical attributes and can be detected with the senses, e.g., people, infrastructure, and finances.

Intangible asset: Intangible are those assets that has no physical attributes and cannot be detected with the senses, e.g., information, reputation and customer trust.

## QUESTION NO: 14

Which of the following activities would BEST contribute to promoting an organization-wide risk-aware culture?

**A.** Communicating components of risk and their acceptable levels

**B.** Performing a benchmark analysis and evaluating gaps

**C.** Participating in peer reviews and implementing best practices

**D.** Conducting risk assessments and implementing controls

**ANSWER: D**

**Explanation:**

Reference: https://m.isaca.org/Certification/CRISC-Certified-in-Risk-and-Information-Systems-Control/Documents/CRISC-Additional-Verification-Form-2015-Later-frm_Eng_0818.pdf

## QUESTION NO: 15

Which of the following steps ensure effective communication of the risk analysis results to relevant stakeholders? Each correct answer represents a complete solution. (Choose three.)

**A.** The results should be reported in terms and formats that are useful to support business decisions

**B.** Provide decision makers with an understanding of worst-case and most probable scenarios,due diligence exposures and significant reputation, legal or regulatory considerations

**C.** Communicate the negative impacts of the events only, it needs more consideration

**D.** Communicate the risk-return context clearly

**ANSWER: A B D**

**Explanation:**

The result of risk analysis process is being communicated to relevant stakeholders. The steps that are involved in communication are:

- The results should be reported in terms and formats that are useful to support business decisions.
- Coordinate additional risk analysis activity as required by decision makers, like report rejection and scope adjustment
- Communicate the risk-return context clearly, which include probabilities of loss and/or gain, ranges, and confidence levels (if possible) that enable management to balance risk-return.
- Identify the negative impacts of events that drive response decisions as well as positive impacts of events that represent opportunities which should channel back into the strategy and objective setting process.
- Provide decision makers with an understanding of worst-case and most probable scenarios, due diligence exposures and significant reputation, legal or regulatory considerations.

Incorrect Answers:

C: Communicate the negative impacts of events that drive response decisions as well as positive impacts of events that represent opportunities which should channel back into the strategy and objective setting process, for effective communication. Only negative impacts are not considered alone.

## QUESTION NO: 16

An organization has outsourced a critical process involving highly regulated data to a third party with servers located in a foreign country. Who is accountable for the confidentiality of this data?

**A.** Third-party data custodian

**B.** Data custodian

**C.** Regional office executive

**D.** Data owner

## ANSWER: D

## QUESTION NO: 17

Which of the following are true for threats?

Each correct answer represents a complete solution. (Choose three.)

**A.** They can become more imminent as time goes by, or it can diminish

**B.** They can result in risks from external sources

**C.** They are possibility

**D.** They are real

**E.** They will arise and stay in place until they are properly dealt.

## ANSWER: A B D

**Explanation:**

Threat is an act of coercion wherein an act is proposed to elicit a negative response. Threats are real, while the vulnerabilities are a possibility. They can result in risks from external sources, and can become imminent by time or can diminish.

Incorrect Answers:

C, E: These two are true for vulnerability, but not threat. Unlike the threat, vulnerabilities are possibility and can result in risks from internal sources. They will arise and stay in place until they are properly dealt.

## QUESTION NO: 18

You are the project manager in your enterprise. You have identified risk that is noticeable failure threatening the success of certain goals of your enterprise. In which of the following levels do this identified risk exists?

**A.** Moderate risk

**B.** High risk

**C.** Extremely high risk

**D.** Low risk

**ANSWER: A**

**Explanation:**

Moderate risks are noticeable failure threatening the success of certain goals.

Incorrect Answers:

B: High risk is the significant failure impacting in certain goals not being met.

C: Extremely high risk are the risks that has large impact on enterprise and are most likely results in failure with severe consequences.

D: Low risks are the risk that results in certain unsuccessful goals.

## QUESTION NO: 19

Which of the following is a risk practitioner's MOST important responsibility in managing risk acceptance that exceeds risk tolerance?

**A.** Verify authorization by senior management.

**B.** Increase the risk appetite to align with the current risk level

**C.** Ensure the acceptance is set to expire over lime

**D.** Update the risk response in the risk register.

**ANSWER: A**

## QUESTION NO: 20

Which of the following provides the MOST useful information to assess the magnitude of identified deficiencies in the IT control environment?

**A.** Peer benchmarks

**B.** Internal audit reports

**C.** Business impact analysis (BIA) results

**D.** Threat analysis results

**ANSWER: D**