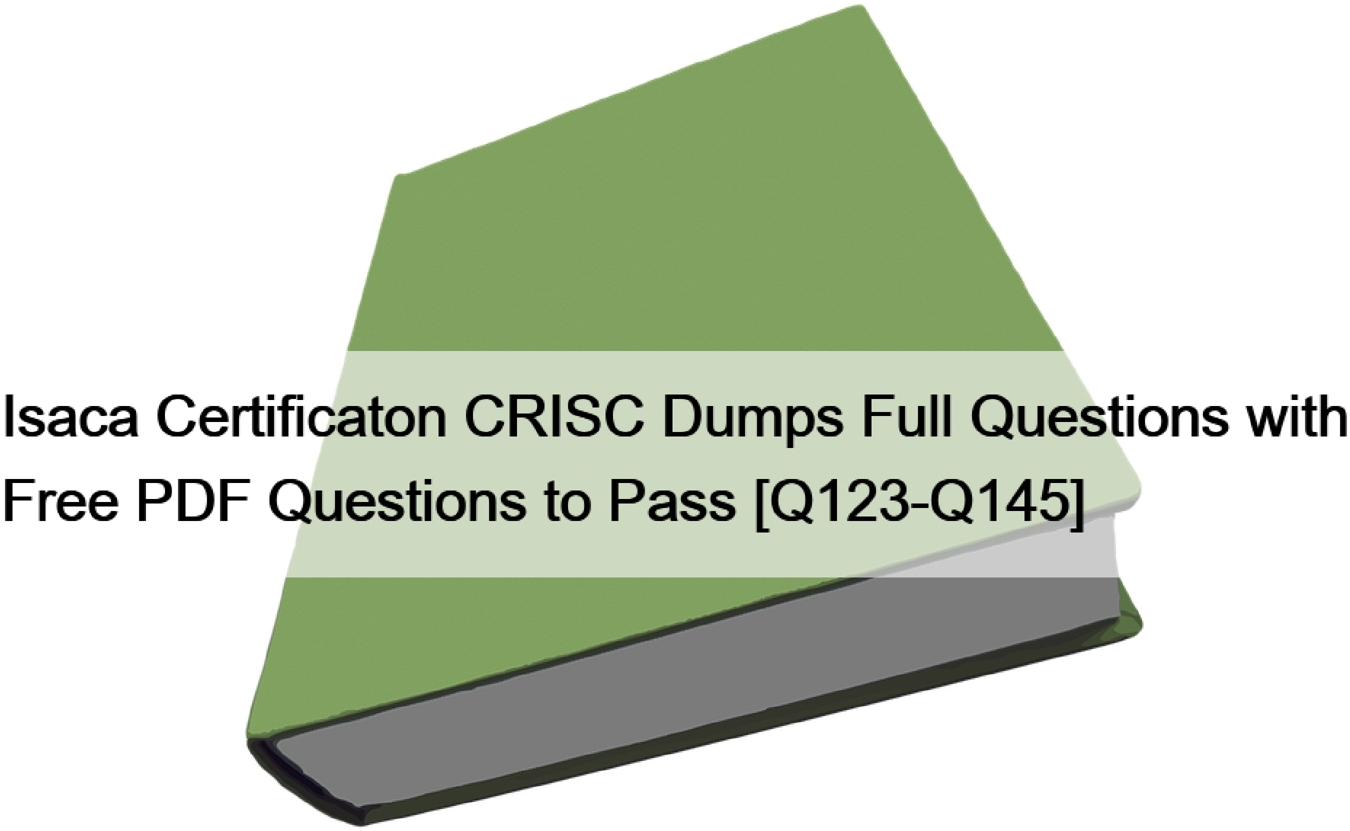
Isaca Certificaton CRISC Dumps Full Questions with Free PDF Questions to Pass [Q123-Q145



Isaca Certificaton CRISC Dumps Full Questions with Free PDF Questions to Pass
100% Updated ISACA CRISC Enterprise PDF Dumps

ISACA Risk and Information Systems Control Exam Syllabus Topics:

TopicDetailsWeightsIT Risk Assessment**A. IT Risk Identification**- Risk Events (e.g., contributing conditions, loss result)- Threat Modelling and Threat Landscape- Vulnerability and Control Deficiency Analysis (e.g., root cause analysis)- Risk Scenario Development **B. IT Risk Analysis and Evaluation**- Risk Assessment Concepts, Standards, and Frameworks- Risk Register- Risk Analysis Methodologies- Business Impact Analysis- Inherent and Residual Risk20%Governance**A. Organizational Governance**- Organizational Strategy, Goals, and Objectives- Organizational Structure, Roles, and Responsibilities- Organizational Culture- Policies and Standards- Business Processes- Organizational Assets **B. Risk Governance**- Enterprise Risk Management and Risk Management Framework- Three Lines of Defense- Risk Profile- Risk Appetite and Risk Tolerance- Legal, Regulatory, and Contractual Requirements- Professional Ethics of Risk Management26%Risk Response and Reporting**A. Risk Response**- Risk Treatment / Risk Response Options- Risk and Control Ownership- Third-Party Risk Management - Issue, Finding, and Exception Management- Management of Emerging Risk **B. Control Design and Implementation**-

Control Types, Standards, and Frameworks- Control Design, Selection, and Analysis- Control Implementation- Control Testing and Effectiveness Evaluation **C. Risk Monitoring and Reporting**- Risk Treatment Plans- Data Collection, Aggregation, Analysis, and Validation- Risk and Control Monitoring Techniques- Risk and Control Reporting Techniques (heatmap, scorecards, dashboards)- Key Performance Indicators- Key Risk Indicators (KRIs)- Key Control Indicators (KCIs) 32%Information Technology and Security**A. Information Technology Principles**- Enterprise Architecture- IT Operations Management (e.g., change management, IT assets, problems, incidents)- Project Management- Disaster Recovery Management (DRM)- Data Lifecycle Management- System Development Life Cycle (SDLC)- Emerging Technologies **B. Information Security Principles**- Information Security Concepts, Frameworks, and Standards- Information Security Awareness Training- Business Continuity Management- Data Privacy and Data Protection Principles22%

Isaca CRISC Practice Test Questions, Isaca CRISC Exam Practice Test Questions

It is a known fact that the certified professionals in the field of IT have more career potentials than their non-certified counterparts. If you are looking to get certified, ISACA CRISC is an industry recognized option that validates your knowledge and experience in enterprise risk management. The Certified in Risk and Information Systems Control (CRISC) certification demonstrates one's expertise in identifying and managing corporate IT risks and implementing and maintaining information systems control.

Q123. Which of the following is the GREATEST concern associated with the transmission of healthcare data across the internet?
* Unencrypted data
* Lack of redundant circuits
* Low bandwidth connections
* Data integrity

Q124. You are the project manager of a SGT project. You have been actively communicating and working with the project stakeholders. One of the outputs of the &#8220;manage stakeholder expectations&#8221; process can actually create new risk events for your project. Which output of the manage stakeholder expectations process can create risks?
* Project management plan updates
* An organizational process asset updates
* Change requests
* Project document updates
* Explanation:

The manage stakeholder expectations process can create change requests for the project, which

can cause new risk events to enter into the project.

Change requests are requests to expand or reduce the project scope, modify policies, processes,

plans, or procedures, modify costs or budgets or revise schedules. These requests for a change

can be direct or indirect, externally or internally initiated, and legally or contractually imposed or

optional. A Project Manager needs to ensure that only formally documented requested changes

are processed and

only approved change requests are implemented.
* is incorrect. The project management plan updates do not create new risks.

- is incorrect. The project document updates do not create new risks.

is incorrect. The organizational process assets updates do not create new risks.

Q125. Which of the following considerations should be taken into account while selecting risk indicators that ensures greater buy-in and ownership?

- Lag indicator
- Lead indicator
- Root cause
- Stakeholder
- Explanation:

To ensure greater buy-in and ownership, risk indicators should be selected with the involvement of relevant stakeholders. Risk indicators should be identified for all stakeholders and should not focus solely on the more operational or strategic side of risk.
is incorrect. Lead indicators indicate which capabilities are in place to prevent events from occurring. They do not play any role in ensuring greater buy-in and ownership. Answer: A is incorrect. Role of lag indicators is to ensure that risk after events have occurred is being indicated. Answer: C is incorrect. Root cause is considered while selecting risk indicator but it does not ensure greater buy-in or ownership.

Q126. Which of the following is the BEST way for an organization to enable risk treatment decisions?

- Allocate sufficient funds for risk remediation.
- Promote risk and security awareness.
- Establish clear accountability for risk.
- Develop comprehensive policies and standards.

Q127. Which of the following is the PRIMARY reason to perform ongoing risk assessments?

- The risk environment is subject to change.
- The information security budget must be justified.
- Emerging risk must be continuously reported to management.
- New system vulnerabilities emerge at frequent intervals.

Section: Volume D

Q128. Natural disaster is BEST associated to which of the following types of risk?

- Short-term
- Long-term
- Discontinuous
- Large impact

Explanation/Reference:

Explanation:

Natural disaster can be a long-term or short-term and can have large or small impact on the company.

However, as the natural disasters are unpredictable and infrequent, they are best considered as discontinuous.

Incorrect Answers:

A: Natural disaster can be a short-term, but it is not the best answer.

B: Natural disaster can be a long-term, but it is not the best answer.

D: Natural disaster can be of large impact depending upon its nature, but it is not the best answer.

Q129. Which of the following are risk components of the COSO ERM framework?

Each correct answer represents a complete solution. Choose three.
* Risk response
* Internal environment
* Business continuity
* Control activities
Section: Volume A

Explanation

Explanation:

The risk components defined by the COSO ERM are internal environment, objective settings, event identification, risk assessment, risk response, control objectives, information and communication, and monitoring.

Incorrect Answers:

C: Business continuity is not considered as risk component within the ERM framework.

Q130. Which of the following would present the GREATEST challenge when assigning accountability for control ownership?
* Weak governance structures
* Senior management scrutiny
* Complex regulatory environment
* Unclear reporting relationships

Q131. Which of the following BEST mitigates the risk of violating privacy laws when transferring personal information lo a supplier?
* Encrypt the data while in transit lo the supplier
* Contractually obligate the supplier to follow privacy laws.
* Require independent audits of the supplier&#8217;s control environment
* Utilize blockchain during the data transfer

Q132. You are using Information system. You have chosen a poor password and also sometimes transmits data over unprotected communication lines. What is this poor quality of password and unsafe transmission refers to?
* Probabilities
* Threats
* Vulnerabilities
* Impacts
Section: Volume A

Explanation:

Vulnerabilities represent characteristics of information resources that may be exploited by a threat. The given scenario describes such a situation, hence it is a vulnerability.

Incorrect Answers:

A: Probabilities represent the likelihood of the occurrence of a threat, and this scenario does not describe a probability.

B: Threats are circumstances or events with the potential to cause harm to information resources. This scenario does not describe a threat.

D: Impacts represent the outcome or result of a threat exploiting a vulnerability. The stem does not describe an impact.

Q133. Which of the following is the most accurate definition of a project risk?
* It is an unknown event that can affect the project scope.
* It is an uncertain event or condition within the project execution.
* It is an uncertain event that can affect the project costs.
* It is an uncertain event that can affect at least one project objective.
* Explanation:

Risk is an uncertain event or condition that, if it occurs, has an effect on at least one project objective. Project risk is concerned with the expected value of one or more results of one or more future

events in a project. It is an uncertain condition that, if it occurs, has an effect on at least one

project objective. Objectives can be scope, schedule, cost, and quality. Project risk is always in the

future.
* is incorrect. Risk is not unknown, it is uncertain; in addition, the event can affect at least

one project objective &#8211; not just the project scope.
* is incorrect. This statement is almost true, but the event does not have to happen within

project execution.
is incorrect. Risks can affect time, costs, or scope, rather affecting only cost.

Q134. What is the IMMEDIATE step after defining set of risk scenarios?
* Risk mitigation
* Risk monitoring
* Risk management
* Risk analysis
Section: Volume B

Explanation:

Once the set of risk scenarios is defined, it can be used for risk analysis. In risk analysis, likelihood and impact of the scenarios are assessed. Important components of this assessment are the risk factors.

Incorrect Answers:

A: Risk mitigation is the latter step after analyzing risk.

B: Risk monitoring is the latter step after risk analysis and risk mitigation.

C: Risk analysis comes under risk management, therefore management is a generalized term, and is not the best answer for this question.

Q135. Marie has identified a risk event in her project that needs a mitigation response. Her response actually creates a new risk event that must now be analyzed and planned for. What term is given to this newly created risk event?

* Residual risk
* Secondary risk
* Infinitive risk
* Populated risk

Section: Volume B

Explanation:

Secondary risks are the risks that come about as a result of implementing a risk response. This new risk event must be recorded, analyzed, and planned for management.

Incorrect Answers:

A: A residual risk event is similar to a secondary risk, but is often small in probability and impact, so it may just be accepted.

C: Infinitive risk is not a valid project management term.

D: Populated risk event is not a valid project management term.

Q136. You work as a Project Manager for Company Inc. You have to conduct the risk management activities for a project. Which of the following inputs will you use in the plan risk management process?

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

* Quality management plan
* Schedule management plan
* Cost management plan
* Project scope statement

Section: Volume C

Explanation:

The inputs to the plan risk management process are as follows:

* Project scope statement: It provides a clear sense of the range of possibilities associated with the project and establishes the framework for how significant the risk management effort may become.

* Cost management plan: It describes how risk budgets, contingencies, and management reserves will be reported and accessed.

* Schedule management plan: It describes how the schedule contingencies will be reported and assessed.

* Communication management plan: It describes the interactions, which occurs on the project and determines who will be available to share information on various risks and responses at different times.

* Enterprise environmental factors: It include, but are not limited to, risk attitudes and tolerances that describe the degree of risk that an organization withstand.

* Organizational process assets: It includes, but are not limited to, risk categories, risk statement formats, standard templates, roles

and responsibilities, authority levels for decision-making, lessons learned, and stakeholder registers.

Incorrect Answers:

A: It is not an input for Plan risk management process.

Q137. An IT department has organized training sessions to improve user awareness of organizational information security policies. Which of the following is the BEST key performance indicator (KPI) to reflect effectiveness of the training?
* Number of training sessions completed
* Percentage of staff members who complete the training with a passing score
* Percentage of attendees versus total staff
* Percentage of staff members who attend the training with positive feedback

Q138. You are the project manager for your company and a new change request has been approved for your project. This change request, however, has introduced several new risks to the project. You have communicated these risk events and the project stakeholders understand the possible effects these risks could have on your project. You elect to create a mitigation response for the identified risk events. Where will you record the mitigation response?
* Risk register
* Risk log
* Project management plan
* Risk management plan
* Explanation:

The Identified risks and potential responses are documented in the risk register. A risk register is an inventory of risks and exposure associated with those risks. Risks are commonlyfound in project management practices, and provide information to identify, analyze, and manage risks. Typically a risk register contains: A description of the risk The impact should this event actually occur The probability of its occurrence Risk Score (the multiplication of Probability and Impact) A summary of the planned response should the event occur A summary of the mitigation (the actions taken in advance to reduce the probability and/or impact of the event) Ranking of risks by Risk Score so as to highlight the highest priority risks to all involved.
is incorrect. The risk management plan is an input to the risk response planning, but it is not the best choice for thisquestionoption B is incorrect. This is not a valid choice for thequestionoption C is incorrect. The project management plan is the parent of the risk management plan, but the best choice is the risk register.

Q139. The PRIMARY purpose of vulnerability assessments is to:
* test intrusion detection systems (IDS) and response procedures.
* provide clear evidence that the system is sufficiently secure.
* detect weaknesses that could lead to a system compromise.
* determine the impact of potential threats.

Q140. Which of the following are true for threats?

Each correct answer represents a complete solution. Choose three.
* They can become more imminent as time goes by, or it can diminish
* They can result in risks from external sources
* They are possibility
* They are real
* They will arise and stay in place until they are properly dealt.
Explanation/Reference:

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.

Q141. You are an experienced Project Manager that has been entrusted with a project to develop a machine which produces auto components. You have scheduled meetings with the project team and the key stakeholders to identify the risks for your project. Which of the following is a key output of this process?
* Risk Register
* Risk Management Plan
* Risk Breakdown Structure
* Risk Categories
Section: Volume A

Explanation:

The primary outputs from Identify Risks are the initial entries into the risk register. The risk register ultimately contains the outcomes of other risk management processes as they are conducted, resulting in an increase in the level and type of information contained in the risk register over time.

Incorrect Answers:

B, C, D: All these are outputs from the &#8220;Plan Risk Management&#8221; process, which happens prior to the starting of risk identification.

Q142. While reviewing an organization&#8217;s monthly change management metrics, a risk practitioner notes that the number of emergency changes has increased substantially Which of the following would be the BEST approach for the risk practitioner to take?
* Temporarily suspend emergency changes.
* Document the control deficiency in the risk register.
* Conduct a root cause analysis.
* Continue monitoring change management metrics.

Q143. You are the project manager of a large networking project. During the execution phase the customer requests for a change in the existing project plan. What will be your immediate action?
* Update the risk register.
* Ask for a formal change request.
* Ignore the request as the project is in the execution phase.
* Refuse the change request.
Section: Volume A

Explanation:

Whenever the customer or key stakeholder asks for a change in the existing plan, you should ask him/her to submit a formal change request. Change requests may modify project policies or procedures, project scope, project cost or budget, project schedule, or project quality.

Incorrect Answers:

A, C, D: The first action required is to create a formal change request, if a change is requested in the project.

Q144. You have been assigned as the Project Manager for a new project that involves building of a new roadway between the city airport to a designated point within the city. However, you notice that the transportation permit issuing authority is taking longer than the planned time to issue the permit to begin construction.

What would you classify this as?
* Project Risk
* Status Update
* Risk Update
* Project Issue
Explanation/Reference:

Explanation:

This is a project issue. It is easy to confuse this as a project risk; however, a project risk is always in the future. In this case, the delay by the permitting agency has already happened; hence this is a project issue.

The possible impact of this delay on the project cost, schedule, or performance can be classified as a project risk.

Incorrect Answers:

A: It is easy to confuse this as a project risk; however, a project risk is always in the future. In this case, the delay by the permitting agency has already happened; hence this is a project issue.

B, C: These are options are not valid.

Q145. Which of the following is the FIRST step in risk assessment?
* Review risk governance
* Asset identification
* Identify risk factors
* Inherent risk identification