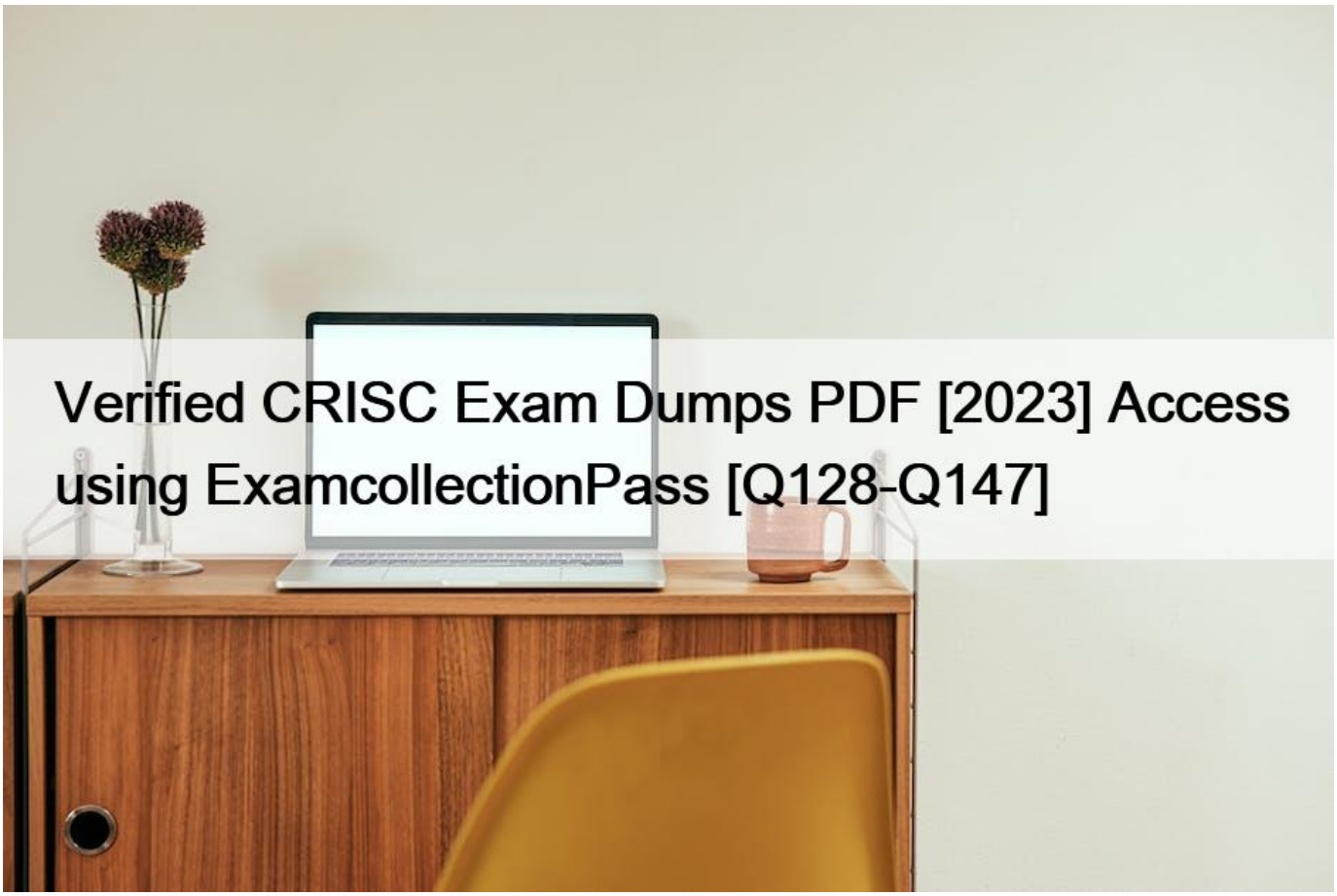
Verified CRISC Exam Dumps PDF [2023 Access using ExamcollectionPass [Q128-Q147



Verified CRISC Exam Dumps PDF [2023] Access using ExamcollectionPass
Try Best CRISC Exam Questions from Training Expert ExamcollectionPass

The CRISC certification is ideal for IT professionals who are responsible for managing risks in their organizations. This includes IT risk professionals, IT managers, business analysts, compliance professionals, and security professionals. The certification provides a comprehensive understanding of risk management and enables professionals to effectively manage risks in their organizations. The exam is challenging and requires extensive preparation, but passing the exam demonstrates a high level of knowledge and expertise in IT risk management. Overall, the CRISC certification is a valuable credential that enhances the professional credibility of IT risk management professionals.

To be eligible to take the exam, candidates must have at least three years of experience in the fields of risk management or information systems control, as well as a solid understanding of the principles and practices of these areas. Additionally, candidates must meet certain educational requirements and agree to abide by the ISACA Code of Professional Ethics.

NO.128 Which of the following should be the PRIMARY objective of a risk awareness training program?
* To promote awareness of the risk governance function.
* To clarify fundamental risk management principles.
* To enable risk-based decision making.
* To ensure sufficient resources are available.

Section: Volume D

NO.129 Establishing ao organizational code of conduct is an example of which type of control?
* Preventive
* Directive
* Detective
* Compensating

NO.130 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.

Section: Volume C

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.

NO.131 Which of the following would be of GREATEST concern to a risk practitioner reviewing current key risk indicators (KRIs)?
* The KRIs’ source data lacks integrity.
* The KRIs are not automated.
* The KRIs are not quantitative.
* The KRIs do not allow for trend analysis.

NO.132 Which of the following is MOST important to compare against the corporate risk profile?
* Industry benchmarks
* Risk tolerance
* Risk appetite
* Regulatory compliance

NO.133 You are the project manager of the QPS project. You and your project team have identified a pure risk.

You along with the key stakeholders, decided to remove the pure risk from the project by changing the project plan altogether. What is a pure risk?

* It is a risk event that only has a negative side and not any positive result.
* It is a risk event that is created by the application of risk response.
* It is a risk event that is generated due to errors or omission in the project work.
* It is a risk event that cannot be avoided because of the order of the work.

Explanation/Reference:

Explanation:

A pure risk has only a negative effect on the project. Pure risks are activities that are dangerous to complete and manage such as construction, electrical work, or manufacturing. It is a class of risk in which loss is the only probable result and there is no positive result.

Pure risk is associated to the events that are outside the risk-taker’s control.

Incorrect Answers:

B: The risk event created by the application of risk response is called secondary risk.

C: A risk event that is generated due to errors or omission in the project work is not necessarily pure risk.

D: This in not valid definition of pure risk.

NO.134 Which of the following is MOST important when developing key risk indicators (KRIs)?
* Alignment with regulatory requirements
* Availability of qualitative data
* Properly set thresholds
* Alignment with industry benchmarks

NO.135 For no apparent reason, the time required to complete daily processing for a legacy application is approaching a risk threshold. Which of the following activities should be performed FIRST?
* Temporarily increase the risk threshold.
* Initiate a feasibility study for a new application.
* Suspend processing to investigate the problem.
* Conduct a root-cause analysis.

NO.136 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.
* 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.
A, and D are incorrect. The first action required is to create a formal change request, if a change is requested in the project.

NO.137 Which of the following events refer to loss of integrity?

Each correct answer represents a complete solution. Choose three.
* Someone sees company’s secret formula
* Someone makes unauthorized changes to a Web site
* An e-mail message is modified in transit
* A virus infects a file
Section: Volume C

Explanation:

Loss of integrity refers to the following types of losses:

* An e-mail message is modified in transit A virus infects a file

* Someone makes unauthorized changes to a Web site

Incorrect Answers:

A: Someone sees company’s secret formula or password comes under loss of confidentiality.

NO.138 Which of the following attributes of a key risk indicator (KRI) is MOST important?
* Repeatable
* Qualitative
* Automated
* Quantitative
Section: Volume D

NO.139 Which of the following events refer to loss of integrity?

Each correct answer represents a complete solution. Choose three.
* Someone sees company’s secret formula
* Someone makes unauthorized changes to a Web site
* An e-mail message is modified in transit
* A virus infects a file
Explanation/Reference:

Explanation:

Loss of integrity refers to the following types of losses:

An e-mail message is modified in transit A virus infects a file

▪

Someone makes unauthorized changes to a Web site

▪

Incorrect Answers:

A: Someone sees company’s secret formula or password comes under loss of confidentiality.

NO.140 The PRIMARY reason for periodically monitoring key risk indicators (KRIs) is to:
* detect changes in the risk profile.
* rectify errors in results of KRIs.
* continually improve risk assessments.
* reduce costs of risk mitigation controls

NO.141 Which of the following is prepared by the business and serves as a starting point for producing the IT Service Continuity Strategy?
* Business Continuity Strategy
* Index of Disaster-Relevant Information
* Disaster Invocation Guideline
* Availability/ ITSCM/ Security Testing Schedule
Section: Volume A

Explanation:

The Business Continuity Strategy is an outline of the approach to ensure the continuity of Vital Business Functions in the case of disaster events. The Business Continuity Strategy is prepared by the business and serves as a starting point for producing the IT Service Continuity Strategy.

Incorrect Answers:

B: Index of Disaster-Relevant Information is a catalog of all information that is relevant in the event of disasters.

This document is maintained and circulated by IT Service Continuity Management to all members of IT staff with responsibilities for fighting disasters.

C: Disaster Invocation Guideline is a document produced by IT Service Continuity Management with detailed instructions on when and how to invoke the procedure for fighting a disaster. Most importantly, the guideline defines the first step to be taken by the Service Desk after learning that a disaster has occurred.

D: Availability/ ITSCM/ Security Testing Schedule is a schedule for the regular testing of all availability, continuity, and security mechanisms jointly maintained by Availability, IT Service Continuity, and IT Security Management.

NO.142 A project team member has just identified a new project risk. The risk event is determined to have significant impact but a low probability in the project. Should the risk event happen it’ll cause the project to be delayed by three weeks, which will cause new risk in the project. What should the project manager do with the risk event?
* Add the identified risk to a quality control management chart.
* Add the identified risk to the issues log.
* Add the identified risk to the risk register.
* Add the identified risk to the low-level risk watch-list.
Section: Volume D

Explanation:

All identified risks, their characteristics, responses, and their status should be added and monitored as part of the risk register. A risk register is an inventory of risks and exposure associated with those risks. Risks are commonly found 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.

Incorrect Answers:

A: Control management charts are not the place where risk events are recorded.

B: This is a risk event and should be recorded in the risk register.

D: Risks that have a low probability and a low impact may go on the low-level risk watch-list.

NO.143 When developing risk treatment alternatives for a Business case, it is MOST helpful to show risk reduction based on:
* cost-benefit analysis.
* risk appetite.
* regulatory guidelines
* control efficiency

NO.144 The number of tickets to rework application code has significantly exceeded the established threshold. Which of the following would be the risk practitioner s BEST recommendation?
* Perform a root cause analysis
* Perform a code review
* Implement version control software.
* Implement training on coding best practices

NO.145 FISMA requires federal agencies to protect IT systems and data. How often should compliance be audited by an external organization?
* Annually
* Quarterly
* Every three years
* Never
Section: Volume B

Explanation

Explanation:

Inspection of FISMA is required to be done annually. Each year, agencies must have an independent evaluation of their program. The objective is to determine the effectiveness of the program. These evaluations include:

* Testing for effectiveness: Policies, procedures, and practices are to be tested. This evaluation does not test every policy, procedure, and practice. Instead, a representative sample is tested.

* An assessment or report: This report identifies the agency’s compliance as well as lists compliance with FISMA. It also lists compliance with other standards and guidelines.

Incorrect Answers:

B, C, D: Auditing of compliance by external organization is done annually, not quarterly or every three years.

NO.146 Which of the following BEST indicates the effectiveness of anti-malware software?
* Number of staff hours lost due to malware attacks
* Number of downtime hours in business critical servers
* Number of patches made to anti-malware software
* Number of successful attacks by malicious software

NO.147 Which of the following will BEST help mitigate the risk associated with malicious functionality in outsourced application development?
* Utilize the change management process.
* Validate functionality by running in a test environment.
* Perform an in-depth code review with an expert.
* Implement a service level agreement.

Section: Volume D