

# CRISC Exam Questions And Answers, CRISC Latest Exam Review

## CRISC Exam Questions and Answers

How many steps in NIST RMF? -  6

- Name steps of the NIST RMF -  1) Categorize Info Systems
- 2) Select Security Controls
- 3) Implement Security Controls
- 4) Assess Security Controls
- 5) Authorize Info Systems
- 6) Monitor Security Controls

What are the layers of COBIT? -  Governance and Management

- What are the Management layers of COBIT? -  1) Align, Plan, and Organize
- 2) Build, Acquire, and Implement
- 3) Deliver, Service, and Support
- 4) Monitor, Evaluate, and Assess

What are the layers of ISACA Risk IT Framework? -  1) Risk Governance  
2) Risk Evaluation  
3) Risk Response

- What are the levels of SDLC? -  1) Initiation
- 2) Requirements
- 3) Design
- 4) Development/Acquisition
- 5) Implementation
- 6) Operations/Maintenance
- 7) Disposal/Retirement

What does SDLC stand for? -  Software Development Life Cycle

What is the NIST Business Continuity Document? -  800-34 "Contingency Planning Guide for Federal Information Systems"

- What components of risk do Risk Scenarios include? -  1) Asset
- 2) Threat
- 3) Threat Agent
- 4) Vulnerability
- 5) Time/Location

They leave off likelihood and impact

- What elements should a Risk Register include? -  1) Risk factors
- 2) Threat agents, threats, and vulnerabilities

P.S. Free & New CRISC dumps are available on Google Drive shared by ITExamReview: <https://drive.google.com/open?id=1WVsZoN4ObiNxr-hcVmOJDQJ82VJmq6eR>

All these three CRISC exam questions formats are easy to use and compatible with all devices, operating systems, and web browsers. Just choose the best CRISC exam questions format and start ISACA CRISC exam preparation without wasting further time. As far as the price of Certified in Risk and Information Systems Control exam practice test questions is concerned, these exam practice test questions are being offered at a discounted price. Get benefits from CRISC Exam Questions at discounted prices and download them quickly. Best of luck in CRISC exam and career!!!

The CRISC certification exam is designed to test an individual's ability to identify, assess, and evaluate risks related to information and technology systems. CRISC exam covers four domains, which include risk identification, assessment, response, and monitoring. A candidate who passes the exam is considered to have a strong understanding of risk management principles and is capable of developing and implementing risk management strategies in an organization. It is a globally recognized certification that demonstrates a professional's commitment to the field of information and technology risk management.

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. Certified in Risk and Information Systems Control certification provides a comprehensive understanding of risk management and enables professionals to effectively manage risks in their organizations. CRISC 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.

ISACA CRISC (Certified in Risk and Information Systems Control) certification exam is one of the most highly respected and sought-after certifications in the field of risk management and information systems control. CRISC exam is designed to test the

knowledge and skills of professionals who are responsible for managing risks related to information systems and technology in their organizations.

>> CRISC Exam Questions And Answers <<

## ISACA CRISC Latest Exam Review - Dumps CRISC Vce

We offer a money-back guarantee, which means we are obliged to return 100% of your sum (terms and conditions apply) in case of any unsatisfactory results. Even though the ISACA experts who have designed CRISC assure us that anyone who studies properly cannot fail the exam, we still offer a money-back guarantee. This way we prevent pre and post-purchase anxiety.

### ISACA Certified in Risk and Information Systems Control Sample Questions (Q1881-Q1886):

#### NEW QUESTION # 1881

Which of the following would provide the MOST objective assessment of the effectiveness of an organization's security controls?

- A. A third-party audit
- B. Security operations center review
- C. An internal audit
- D. Internal penetration testing

**Answer: A**

#### NEW QUESTION # 1882

During a control review, the control owner states that an existing control has deteriorated over time. What is the BEST recommendation to the control owner?

- A. Certify the control after documenting the concern.
- B. Implement compensating controls to reduce residual risk
- C. Escalate the issue to senior management
- D. Discuss risk mitigation options with the risk owner.

**Answer: D**

Explanation:

The best recommendation to the control owner when an existing control has deteriorated over time is to discuss risk mitigation options with the risk owner. This is because the risk owner is the person or entity who has the authority and accountability to make decisions and take actions regarding the risk, including the selection and implementation of the risk response strategies. The control owner is the person or entity who is responsible for the design, operation, and maintenance of the control, but not for the overall risk management.

By discussing risk mitigation options with the risk owner, the control owner can communicate the current status and performance of the control, and collaborate on finding the most appropriate and effective solution to address the risk and the control deterioration. The other options are not the best recommendation to the control owner, because they do not involve the risk owner, who is the key stakeholder in the risk management process, as explained below:

\* A. Implement compensating controls to reduce residual risk is not the best recommendation, because it may not be feasible, efficient, or sufficient to address the risk and the control deterioration.

Compensating controls are additional or alternative controls that are implemented to mitigate the risk when the primary control is not available, adequate, or effective. However, implementing compensating controls without discussing with the risk owner may result in wasting resources, duplicating efforts, or conflicting objectives, and may not align with the risk appetite or strategy of the organization.

\* B. Escalate the issue to senior management is not the best recommendation, because it may not be necessary, timely, or appropriate to involve senior management in the risk and control deterioration issue. Senior management is the highest level of authority and oversight in the organization, and may not have the detailed or operational knowledge or involvement in the risk and control management.

Escalating the issue to senior management without discussing with the risk owner may create confusion, delay, or misunderstanding, and may not result in the optimal risk mitigation solution.

\* D. Certify the control after documenting the concern is not the best recommendation, because it may not be accurate, honest, or

compliant to certify the control when it has deteriorated over time. Certifying the control is the process of attesting that the control is designed and operating effectively and efficiently, and meets the established criteria and standards. Certifying the control after documenting the concern may not reflect the true status and performance of the control, and may not comply with the internal or external audit or regulatory requirements. References = Risk and Information Systems Control Study Manual, Chapter 4, Section 4.2.1, page 115. Roles and Responsibilities in Risk Management, Risk Owner vs. Control Owner: What's the Difference?, Control Deterioration: How to Avoid It and What to Do About It

#### NEW QUESTION # 1883

Which of the following is the MOST important consideration when prioritizing risk response?

- A. Cost of control implementation.
- B. Effectiveness of risk treatment.
- C. Requirements for regulatory obligations.
- D. Number of risk response options.

#### Answer: B

Explanation:

The effectiveness of risk treatment determines whether the selected response sufficiently mitigates the identified risk. This consideration ensures alignment with risk appetite and reduces residual risk to acceptable levels, reflecting the priorities set out in the Risk Response and Treatment domain of CRISC.

#### NEW QUESTION # 1884

Which of the following is the MOST important key performance indicator (KPI) to monitor the effectiveness of disaster recovery processes?

- A. Percentage of IT systems meeting the recovery time objective (RTO) during the disaster recovery test
- B. Percentage of issues arising from the disaster recovery test resolved on time
- C. Percentage of IT systems included in the disaster recovery test scope
- D. Percentage of IT systems recovered within the mean time to restore (MTTR) during the disaster recovery test

#### Answer: A

Explanation:

The most important key performance indicator (KPI) to monitor the effectiveness of disaster recovery processes is the percentage of IT systems meeting the recovery time objective (RTO) during the disaster recovery test. The RTO is the maximum acceptable time that a system or process can be unavailable after a disruption. The disaster recovery test is a simulation of a disaster scenario to evaluate the readiness and capability of the organization to restore its critical functions and systems. By measuring the percentage of IT systems meeting the RTO during the test, the organization can assess how well the disaster recovery processes meet the predefined objectives and standards. Percentage of IT systems recovered within the mean time to restore (MTTR), percentage of issues arising from the disaster recovery test resolved on time, and percentage of IT systems included in the disaster recovery test scope are other possible KPIs, but they are not as important as the percentage of IT systems meeting the RTO. References = ISACA Certified in Risk and Information Systems Control (CRISC) Certification Exam Question and Answers, question 12; CRISC Review Manual, 6th Edition, page 215.

#### NEW QUESTION # 1885

You are the project manager of the HGT project in Bluewell Inc. The project has an asset valued at \$125,000 and is subjected to an exposure factor of 25 percent. What will be the Single Loss Expectancy of this project?

- A. \$ 125,025
- B. \$ 5,000
- C. \$ 3,125,000
- D. \$ 31,250
- E. Explanation:

The Single Loss Expectancy (SLE) of this project will be \$31,250. Single Loss Expectancy is a term related to Quantitative Risk Assessment. It can be defined as the monetary value expected from the occurrence of a risk on an asset. It is mathematically expressed as follows: Single Loss Expectancy (SLE) = Asset Value (AV) \* Exposure Factor (EF) where the

Exposure Factor represents the impact of the risk over the asset, or percentage of asset lost. As an example, if the Asset Value is reduced two third, the exposure factor value is .66. If the asset is completely lost, the Exposure Factor is 1.0. The result is a monetary value in the same unit as the Single Loss Expectancy is expressed. Therefore,  $SLE = \text{Asset Value} * \text{Exposure Factor}$

$$125,000 * 0.25 = \$31,250$$

**Answer: D**

### Explanation:

C, and A are incorrect. These are not SLEs of this project.

## NEW QUESTION # 1886

• • • • •

According to our information there is a change for CRISC, I advise you to take a look at our latest ISACA CRISC reliable exam guide review rather than pay attention on old-version materials. You can regard old-version materials as practice questions to improve your basic knowledge. If you are searching the valid CRISC Reliable Exam Guide review which includes questions and answer of the real test, our products will be your only choice.

**CRISC Latest Exam Review:** <https://www.itexamreview.com/CRISC-exam-dumps.html>

BTW, DOWNLOAD part of iTEXAMReview CRISC dumps from Cloud Storage: <https://drive.google.com/open?id=1WVsZoN4ObiNxr-hcVmOJDQJ82VJmq6eR>