Reliable CRISC Exam Blueprint & Certification CRISC Test Answers

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

BTW, DOWNLOAD part of VCEDumps CRISC dumps from Cloud Storage: https://drive.google.com/open?id=1ZqSrdMVYCOJsp7sYs7gN_oWkFebUwQRo

Are you still looking for CRISC exam materials? Don't worry about it, because you find us, which means that you've found a shortcut to pass CRISC certification exam. With research and development of IT certification test software for years, our VCEDumps team had a very good reputation in the world. We provide the most comprehensive and effective help to those who are preparing for the important exams such as CRISC Exam.

ISACA CRISC Exam Syllabus Topics:

Section	Weight	Objectives

IT Risk Assessment	26%	- Assess capability maturity • 1. Risk management maturity models • 2. Control assessment framework - Identify control effectiveness • 1. Root cause analysis • 2. Risk and control gap analysis - Risk analysis methodologies • 1. Qualitative and quantitative analysis • 2. Risk ownership and accountability
Monitoring and Reporting	28%	- Key risk indicator (KRI) development • 1. KRI threshold setting • 2. Performance monitoring - Communicate risk and control status • 1. Risk dashboards and reporting • 2. Senior management reporting • 3. Board reporting - Risk and control monitoring • 1. Incident management • 2. Continuous monitoring • 3. Control testing and validation
Risk Response and Mitigation	20%	- Develop and implement controls • 1. Control design and optimization • 2. Control types and classification - Manage and monitor risk treatment • 1. Risk appetite and tolerance • 2. Risk response strategies • 3. Third-party risk management
IT Risk Identification	26%	- Collect and process information • 1. Business continuity and disaster recovery • 2. Risk aggregation and reporting • 3. Risk taxonomy and terminology - Communicate risk analysis • 1. Risk register management • 2. Risk reporting and escalation - Analyze and classify information • 1. Threat landscape and vulnerability assessment • 2. Risk scenarios and events

>> Reliable CRISC Exam Blueprint <<

Pass Guaranteed Quiz ISACA - CRISC - Certified in Risk and Information

Systems Control Useful Reliable Exam Blueprint

The price for CRISC learning materials is quite reasonable, and no matter you are a student or you are an employee, you can afford them. Besides, we offer you free demo to have a try, and through free demo, you can know some detailed information of CRISC Exam Dumps. With experienced experts to compile and verify, CRISC learning materials are high quality. Besides, CRISC exam dumps contain both questions and answers, and you check your answers quickly after practicing.

ISACA Certified in Risk and Information Systems Control Sample Questions (Q726-Q731):

NEW QUESTION # 726
Which of the following are the principles of risk management?
Each correct answer represents a complete solution. Choose three.

- A. Risk management should be an integral part of the organization
- B. Risk management is the responsibility of executive management
- C. Risk management should be transparent and inclusive
- D. Risk management should be a part of decision-making

Answer: A,C,D

Explanation:
The International Organization for Standardization (ISO) identifies the following principles of risk management. Risk management should: create value be an integral part of organizational processes be part of decision making explicitly address uncertainty be systematic and structured be based on the best available information be tailored take into account human factors be transparent and inclusive be dynamic, iterative, and responsive to change be capable of continual improvement and enhancement

NEW QUESTION # 727
A risk assessment has identified that departments have installed their own WiFi access points on the enterprise network. Which of the following would be MOST important to include in a report to senior management?

- A. Planned remediation actions
- B. The network security policy
- C. Potential business impact
- D. The WiFi access point configuration

Answer: C

Explanation:
A risk assessment is a process of identifying, analyzing, and evaluating the risks that may affect the enterprise' s objectives and operations. It involves determining the likelihood and impact of various risk scenarios, and prioritizing them based on their significance and urgency.
A WiFi access point is a device that allows wireless devices to connect to a wired network using radio signals.
It can provide convenience and flexibility for users, but it can also introduce security risks, such as unauthorized access, data leakage, malware infection, or denial of service attacks.
If departments have installed their own WiFi access points on the enterprise network, without proper authorization, configuration, or monitoring, it means that they have bypassed the network security policy and controls, and created potential vulnerabilities and exposures for the enterprise.
The most important information to include in a report to senior management is the potential business impact of this risk, which is the estimated loss or damage that the enterprise may suffer if the risk materializes. The potential business impact can be expressed in terms of financial, operational, reputational, or legal consequences, and it can help senior management to understand the severity and urgency of the risk, and to decide on the appropriate risk response and allocation of resources.
The other options are not the most important information to include in a report to senior management, because they do not convey the magnitude and significance of the risk, and they may not be relevant or actionable for senior management.
The network security policy is the set of rules and guidelines that define the security objectives, requirements, and responsibilities for the enterprise network. It is important to have a clear and comprehensive network security policy, and to ensure that it is communicated, enforced, and monitored across the enterprise, but it is not the most important information to include in a report to senior management, because it does not indicate the actual or potential impact of the risk, and it may not reflect the current or desired state of the network security.

The WiFi access point configuration is the set of parameters and settings that define the functionality, performance, and security of the WiFi access point. It is important to have a secure and consistent WiFi access point configuration, and to follow the best practices and standards for wireless network security, but it is not the most important information to include in a report to senior management, because it does not indicate the actual or potential impact of the risk, and it may not be relevant or understandable for senior management.
The planned remediation actions are the steps and measures that are intended to mitigate, transfer, avoid, or accept the risk, and to restore the normal operation and security of the enterprise network. It is important to have a feasible and effective plan for remediation actions, and to implement and monitor them in a timely and efficient manner, but it is not the most important information to include in a report to senior management, because it does not indicate the actual or potential impact of the risk, and it may not be feasible or appropriate without senior management's approval or support. References = ISACA, CRISC Review Manual, 7th Edition, 2022, pp. 19-20, 23-24, 27-28, 31-32, 40-41, 47-48 ISACA, CRISC Review Questions, Answers & Explanations Database, 2022, QID 146

NEW QUESTION # 728
The objective of aligning mitigating controls to risk appetite is to ensure that:

- A. the cost of controls does not exceed the expected loss.
- B. exposures are reduced to the fullest extent
- C. insurance costs are minimized
- D. exposures are reduced only for critical business systems

Answer: A

Explanation:
The objective of aligning mitigating controls to risk appetite is to ensure that the cost of controls does not exceed the expected loss. The cost of controls is the amount of resources and efforts required to implement and maintain the controls that are designed to reduce the risk exposure. The expected loss is the estimated amount of loss or harm that may result from a risk event. Therisk appetite is the amount and type of risk that an organization is willing to accept in pursuit of its objectives. By aligning mitigating controls to risk appetite, the organization can optimize the balance between the cost of controls and the expected loss, and avoid over- or under-investing in controls. Exposures being reduced to the fullest extent,exposures being reduced only for critical business systems, and insurance costs being minimized are other possible objectives, but they are not as relevant as the cost of controls not exceeding the expected loss. References = ISACA Certified in Risk and Information Systems Control (CRISC) Certification Exam Question and Answers, question 8; CRISC Review Manual, 6th Edition, page 97.

NEW QUESTION # 729
Which of the following is the BEST key performance indicator (KPI) to measure the ability to deliver uninterrupted IT services?

- A. Mean time between failures (MTBF)
- B. Planned downtime
- C. Mean time to recover (MTTR)
- D. Unplanned downtime

Answer: A

Explanation:
Mean time between failures (MTBF) is a key performance indicator (KPI) that measures the average time that a system or component operates without interruption or failure. MTBF is a common metric for reliability and availability of IT services. A higher MTBF indicates a lower frequency of failures and a higher ability to deliver uninterrupted IT services. According to the CRISC Review Manual 2022, MTBF is one of the KPIs for IT service delivery1. According to the CRISC Review Questions, Answers & Explanations Manual 2022, MTBF is the correct answer to this question2.
Mean time to recover (MTTR), planned downtime, and unplanned downtime are not the best KPIs to measure the ability to deliver uninterrupted IT services. MTTR measures the average time that it takes to restore a system or component to normal operation after a failure. Planned downtime measures the scheduled time that a system or component is not available for use due to maintenance or upgrades. Unplanned downtime measures the unscheduled time that a system or component is not available for use due to failures or incidents.

These KPIs are useful for measuring the impact and duration of service interruptions, but they do not directly reflect the ability to prevent or avoid service interruptions.

NEW QUESTION # 730
The PRIMARY purpose of vulnerability assessments is to:

- A. detect weaknesses that could lead to system compromise.
- B. test intrusion detection systems (IDS) and response procedures.
- C. determine the impact of potential threats.
- D. provide clear evidence that the system is sufficiently secure.

Answer: A

Explanation:
The primary purpose of vulnerability assessments is to detect weaknesses that could lead to system compromise. A vulnerability assessment is a systematic review of security weaknesses in an information system. It evaluates if the system is susceptible to any known vulnerabilities, assigns severity levels to those vulnerabilities, and recommends remediation or mitigation, if and whenever needed1. By identifying and prioritizing the vulnerabilities, a vulnerability assessment helps to prevent or reduce the risk of cyberattacks that could exploit the vulnerabilities and compromise the system. The other options are not the primary purpose, but they may be secondary or tertiary outcomes or benefits of a vulnerability assessment. Providing clear evidence that the system is sufficiently secure is a result of a successful vulnerability assessment and remediation process, but it is not the main objective. Determining the impact of potential threats is a part of the risk assessment process, which complements the vulnerability assessment process, but it is not the same as detecting the vulnerabilities. Testing intrusion detection systems (IDS) and response procedures is a part of the penetration testing process, which simulates a real-world attack on the system to evaluate its security posture, but it is not the same as scanning the system for vulnerabilities. References = What is Vulnerability Assessment | VA Tools and Best Practices - Imperva

NEW QUESTION # 731
.....

VCEDumps has built customizable ISACA CRISC practice exams (desktop software & web-based) for our customers. Users can customize the time and Certified in Risk and Information Systems Control (CRISC) questions of ISACA CRISC Practice Tests according to their needs. You can give more than one test and track the progress of your previous attempts to improve your marks on the next try.

Certification CRISC Test Answers: https://www.vcedumps.com/CRISC-examcollection.html

- Free PDF CRISC - Marvelous Reliable Certified in Risk and Information Systems Control Exam Blueprint □ Enter □ www.torrentvce.com □ and search for ▹ CRISC ◃ to download for free □Reliable CRISC Cram Materials
- CRISC Prep Exam - CRISC Latest Torrent - CRISC Training Guide □ Search for □ CRISC □ and download it for free on 【 www.pdfvce.com 】 website □CRISC Exam Questions Fee
- CRISC Valid Braindumps Free □ Practice CRISC Online □ Valid CRISC Vce □ Search on { www.dumpsquestion.com } for □ CRISC □ to obtain exam materials for free download □Practice CRISC Online
- Real CRISC Torrent □ CRISC Valid Test Camp □ Sure CRISC Pass □ Go to website 【 www.pdfvce.com 】 open and search for 《 CRISC 》 to download for free □CRISC Valid Braindumps Free
- Practice CRISC Online □ Real CRISC Torrent □ Exam CRISC Preparation □ Open website ➥ www.pdfdumps.com □ and search for ➤ CRISC □ for free download ⤴New CRISC Test Cram
- Prepare with Confidence Using ISACA's Updated CRISC Dumps and Receive Free Updates for 1 Year □ Open 「 www.pdfvce.com 」 enter ➥ CRISC □ and obtain a free download □CRISC Valid Test Book
- Download Certified in Risk and Information Systems Control actual test dumps, and start your CRISC exam preparation □ Open [www.pdfdumps.com] enter ▹ CRISC ◃ and obtain a free download ☢Real CRISC Torrent
- Download Certified in Risk and Information Systems Control actual test dumps, and start your CRISC exam preparation □ Download □ CRISC □ for free by simply entering { www.pdfvce.com } website □New CRISC Practice Questions
- CRISC Prep Exam - CRISC Latest Torrent - CRISC Training Guide □ Download □ CRISC □ for free by simply entering { www.prep4sures.top } website □Reliable CRISC Cram Materials
- Latest Reliable CRISC Exam Blueprint - Free Demo Certification CRISC Test Answers: Certified in Risk and Information Systems Control □ Download □ CRISC □ for free by simply searching on 《 www.pdfvce.com 》 □Sure CRISC Pass
- Latest Reliable CRISC Exam Blueprint - Free Demo Certification CRISC Test Answers: Certified in Risk and Information Systems Control □ Go to website ➡ www.exam4labs.com □□□ open and search for 《 CRISC 》 to download for free

Exam CRISC Preparation

- www.scener.com, scalar.usc.edu, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.slideshare.net, github.com, www.fanart-central.net, learn.csisafety.com.au, learn.csisafety.com.au, www.stes.tyc.edu.tw, Disposable vapes

BTW, DOWNLOAD part of VCEDumps CRISC dumps from Cloud Storage: https://drive.google.com/open?id=1ZqSrdMVYCOJsp7sYs7gN_oWkFebUwQRo