I'm not a robot

Cisa exam practice test

QUESTION 4 - (Topic 3)An IS auditor reviewing the threat assessment tor a data center would be MOST concerned if: Correct Answer: C An IS auditor reviewing the threat assessment for a data center would be most concerned if the exercise was completed by local management, because this could introduce bias, conflict of interest, or lack of expertise in the assessment process. A threat assessment is a systematic method of identifying and evaluating the potential threats that could affect the availability, integrity, or confidentiality of the data center and its assets. A threat assessment should be conducted by an independent and qualified team that has the necessary skills, knowledge, and experience to perform a comprehensive and objective analysis of the data center's environment, vulnerabilities, and risks1.The other options are not as concerning as option C for an IS auditor reviewing the threat assessment for a data center. Option A, some of the identified threats are unlikely to occur, is not a problem as long as the likelihood and impact of each threat are properly estimated and prioritized. A threat assessment should consider all possible scenarios, even if they have a low probability of occurrence, to ensure that the data center is prepared for any eventuality2. Option B, all identified threats relate to external entities, is not a flaw as long as the assessment also considers internal threats, such as human errors, malicious insiders, or equipment failures. External threats are often more visible and severe than internal threats, but they are not the only source of risk for a data center3. Option D, neighboring organizations' operations have been included, is not a mistake as long as the assessment also focuses on the data center's own operations. Neighboring organizations' operations may have an impact on the data center's security and availability, especially if they share physical or network infrastructure or resources. A threat assessment should take into account the interdependencies and interactions between the data center and its external environment4.References:➾ ISACA, CISA Review Manual, 27th Edition, 2019➾ ISACA, CISA Review Questions, Answers & Explanations Database - 12 Month Subscription➾ Data Center Threats and Vulnerabilities1➾ Datacenter threat, vulnerability, and risk assessment2➾ Data Centre Risk Assessment3 An audit charter should: be dynamic and change to coincide with the changing nature of technology and the audit profession. The audit charter should not be subject to changes in technology and should not significantly change over time. The charter should be approved at the highest level of management. clearly state audit objectives for, and the delegation of, authority to the maintenance and review of internal controls. An audit charter will state the authority and reporting requirements for the audit but not the details of maintenance of internal controls. document the audit procedures designed to achieve the planned audit objectives. An audit charter would not be at a detailed level and, therefore, would not include specific audit objectives or procedures. outline the overall authority, scope and responsibilities of the audit function. An audit charter should state management's objectives for and delegation of authority to IS auditors. An IS auditor finds a small number of user access requests that had not been authorized by managers through the normal predefined workflow steps and escalation rules. The IS auditor should: perform an additional analysis. The IS auditor needs to perform substantive testing and additional analysis to determine why the approval and workflow processes are not working as intended. Before making any recommendation, the IS auditor should gain a good understanding of the scope of the problem and what factors caused this incident. The IS auditor should identify whether the issue was caused by managers not following procedures, by a problem with the workflow of the automated system or a combination of the two. report the problem to the audit committee. The IS auditor does not yet have enough information to report the problem. conduct a security risk assessment. Changing the scope of the IS audit or conducting a security risk assessment would require more detailed information about the processes and violations being reviewed. recommend that the owner of the identity management (IDM) system fix the workflow issues. The IS auditor must first determine the root cause and impact of the findings and does not have enough information to recommend fixing the workflow issues. An IS auditor observes that an enterprise has outsourced software development to a third party that is a startup company. To ensure that the enterprise's investment in software is protected, which of the following should be recommended by the IS auditor? Due diligence should be performed on the software vendor. While due diligence is a good practice, it does not ensure availability of the source code in the event of vendor failure. A quarterly audit of the vendor facilities should be performed. While a quarterly audit of vendor facilities is a good practice, it does not ensure availability of the source code in the event of failure of the start-up vendor. There should be a source code escrow agreement in place. A source code escrow agreement is primarily recommended to help protect the enterprise's investment in software because the source code will be available through a trusted third party and can be retrieved if the start-up vendor goes out of business. A high penalty clause should be included in the contract. While a penalty clause is a good practice, it does not provide protection or ensure availability of the source code in the event of vendor bankruptcy. An enterprise's risk appetite is BEST established by: the chief legal officer. Although chief legal officers can give guidance regarding legal issues on the policy, they cannot determine the risk appetite. security management. The security management team is concerned with managing the security posture but not with determining the posture. the audit committee. The audit committee is not responsible for setting the risk tolerance or appetite of the enterprise. the steering committee. The steering committee is best suited to determine the enterprise's risk appetite because the committee draws its representation from senior management. When identifying an earlier project completion time, which is to be obtained by paying a premium for early completion, the activities that should be selected are those: whose sum of activity time is the shortest. Attention should focus on the tasks within the critical path that have no slack time. that have zero slack time. A critical path's activity time is longer than that for any other path through the network. This path is important because if everything goes as scheduled, its length gives the shortest possible completion time for the overall project. Activities on the critical path become candidates for crashing (i.e., for reduction in their time by payment of a premium for early completion). Activities on the critical path have zero slack time and conversely, activities with zero slack time are on a critical path. By successively relaxing activities on a critical path, a curve showing total project costs versus time can be obtained. that give the longest possible completion time. The critical path is the longest time length of the activities, but is not based on the longest time of any individual activity. whose sum of slack time is the shortest. A task on the critical path has no slack time. An IS auditor is assigned to audit a software development project, which is more than 80 percent complete, but has already overrun time by 10 percent and costs by 25 percent. Which of the following actions should the IS auditor take? Report that the organization does not have effective project management. The organization may have effective project management practices and still be behind schedule or over budget. Recommend the project manager be changed. There is no indication that the project manager should be changed without looking into the reasons for the overrun. Review the IT governance structure. The organization may have sound IT governance and still be behind schedule or over budget. Review the conduct of the project and the business case. Before making any recommendations, an IS auditor needs to understand the project and the factors that have contributed to bringing the project over budget and over schedule. A programmer maliciously modified a production program to change data and then restored the original code. Which of the following would MOST effectively detect the malicious activity? Comparing source code Source code comparisons are ineffective because the original programs were restored and the changed program does not exist. Reviewing system log files Reviewing system log files is the only trail that may provide information about the unauthorized activities in the production library. Comparing object code Object code comparisons are ineffective because the original programs were restored and the changed program does not exist. Reviewing executable and source code integrity Reviewing executable and source code integrity is an ineffective control, because the source code was changed back to the original and will agree with the current executable. Which of the following would BEST ensure continuity of a wide area network (WAN) across the organization? Built-in alternative routing Alternative routing would ensure that the network would continue if a communication device fails or if a link is severed because message rerouting could be automatic. Complete full system backup daily System backup will not afford protection for a networking failure. A repair contract with a service provider The repair contract will almost always result in some lost time and is not as effective as permanent alternative routing. A duplicate machine alongside each server. Standby servers will not provide continuity if a link is severed. An IS auditor is reviewing the physical security controls of a data center and notices several areas for concern. Which of the following areas is the MOST important? The emergency power off button cover is missing. The emergency power off button issue is a significant concern, but life safety is the highest priority. Scheduled maintenance of the fire suppression system was not performed. The primary purpose of the fire suppression system is to protect the equipment and building. The lack of scheduled maintenance is a concern; however, this does not indicate that the system would not function as required. The more critical issue is the emergency exit because life safety is the highest priority. There are no security cameras inside the data center. The lack of security cameras inside the data center may be a significant concern; however, the more significant issue is the emergency exit door being blocked. The emergency exit door is blocked. Life safety is always the highest priority; therefore, the blocking of the emergency exit is the most serious problem. Which of the following choices BEST helps information owners to properly classify data? Understanding of technical controls that protect data While understanding how the data are protected is important, these controls might not be applied properly if the data classification schema is not well understood. Training on organizational policies and standards RWhile implementing data classification, it is most essential that organizational policies and standards, including the data classification schema, are understood by the owner or custodian of the data so they can be properly classified. Use of an automated data leak prevention (DLP) tool While an automated data leak prevention (DLP) tool may enhance productivity, the users of the application would still need to understand what classification schema was in place. Understanding which people need to access the data In terms of protecting the data, the data requirements of end users are critical, but if the data owner does not understand what data classification schema is in place, it would be likely that inappropriate access to sensitive data might be granted by the data owner. Great job! Your knowledge of IS/IT auditing, control and information security is off to a strong start. Scroll down for your detailed results. Remember: these questions are a small preview of what you can expect on exam day. The official CISA exam has 150 questions. You're just a few steps away from obtaining your CISA certification: Register and pay for your exam. Schedule your exam. Prep for your exam. Ace the CISA exam. Whether you are seeking a new career opportunity or striving to grow within your current organization, the Certified Information Systems Auditor® (CISA®)certification proves your skills and expertise. You've Got This! Now take the CISA exam. Register Today Your knowledge of IS/IT auditing, control and information security is off to a good start. Scroll down for your detailed results. Remember: these questions are a small preview of what you can expect on exam day. The official CISA exam has 150 questions. You're just a few steps away from obtaining your CISA certification: Prep for your exam. Register and pay for your exam. Schedule your exam. Ace the CISA exam. To set yourself up for success on your CISA certification exam, take a look at ISACA's suite of test prep solutions. There's something for every learning style and schedule. Our team of CISA-certified IS/IT audit and control experts have combined cutting-edge industry practices with proven training formats that maximize learning. Choose the Exam Prep that Best Fits Your Needs. Explore CISA Prep Ready for your CISA? Take the exam now. Register Today Great effort! No matter your score, the right preparation from ISACA® will help you excel on your CISA® exam and move your career forward. Scroll down for your detailed results. Remember: these questions are a small preview of what you can expect on exam day. The official CISA exam has 150 questions. You're just a few steps away from obtaining your CISA certification: Prep for your exam. Register and pay for your exam. Schedule your exam. Ace the CISA exam. Choose the Exam Prep that Best Fits Your Needs. Explore CISA Prep Master the CISA material Quickly expand your skillset Become better at your job Make the most of exam day Founded2004HeadquartersFarmington, UtahCountry/TerritoryUnited StatesCEOAaron SkonnardRelated People & CompaniesView ProfileView Profile