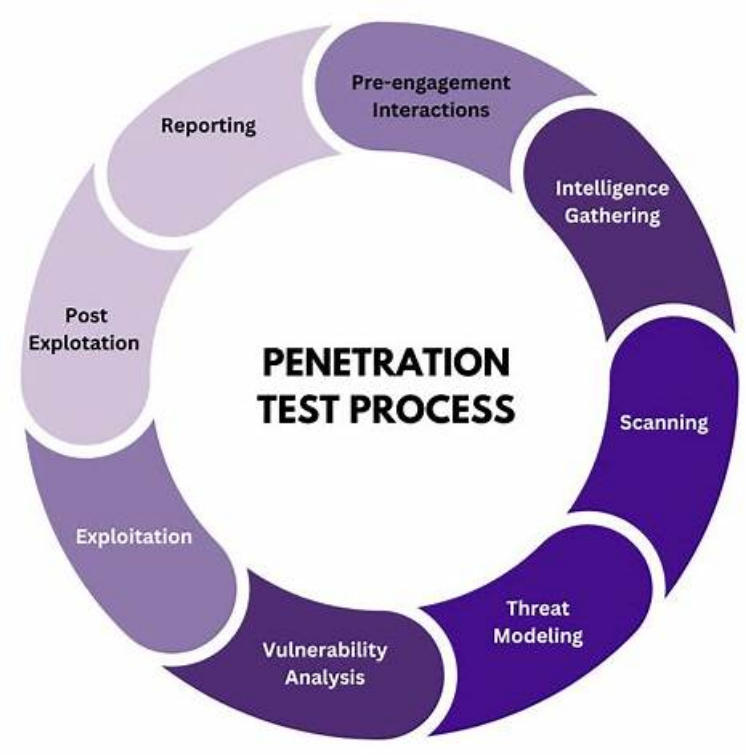
Penetration Testing: CRISC Pre-assessment Test



DOWNLOAD the newest Dumpcollection CRISC PDF dumps from Cloud Storage for free: https://drive.google.com/open?id=1xXTID82JpAcgOQtfPF83LVp0lwmQKTjf

The product Dumpcollection provide with you is compiled by professionals elaborately and boosts varied versions which aimed to help you pass the CRISC exam by the method which is convenient for you. It is not only cheaper than other dumps but also more effective. The high pass rate of our CRISC Study Materials has been approved by thousands of candidates, they recognized our website as only study tool to pass CRISC exam.

ISACA CRISC certification is an essential credential for IT risk management professionals. Certified in Risk and Information Systems Control certification demonstrates an individual's ability to design, implement, monitor and maintain effective risk management programs. The CRISC certification exam is a comprehensive exam that covers four domains and requires a passing score of 450 out of 800 points.

The benefits of obtaining a CRISC certification are numerous. Certified in Risk and Information Systems Control certification demonstrates to employers and clients that you have the necessary skills and knowledge to manage risks related to information technology and information systems. Additionally, CRISC professionals are in high demand and are often paid more than non-certified professionals in the same field. Furthermore, the certification is a globally recognized credential that can open doors to new opportunities and career advancement.

>> CRISC Real Exam Questions <<

Reliable ISACA CRISC Test Vce | CRISC Reliable Exam Registration

After so many years' development, our Isaca Certificaton exam torrent is absolutely the most excellent than other competitors, the content of it is more complete, the language of it is more simply. Believing in our CRISC guide tests will help you get the certificate and embrace a bright future. Time and tide wait for no man. Come to buy our test engine. Dumpcollection have most professional team to compiled and revise CRISC Exam Question. In order to try our best to help you pass the exam and get a better condition of your life and your work, our team worked day and night to complete it. Moreover, only need to spend 20-30 is it enough for you to grasp whole content of our practice materials that you can pass the exam easily, this is simply unimaginable.

Achieving the CRISC certification demonstrates an individual's expertise in risk management and information systems control, which is becoming increasingly important in today's technology-driven world. Certified in Risk and Information Systems Control

certification is recognized globally and is an essential credential for IT professionals looking to advance their careers in the fields of risk management and information systems control. The CRISC Certification helps professionals to identify and assess risks, develop effective risk management strategies, and successfully implement information systems controls to mitigate risks.

ISACA Certified in Risk and Information Systems Control Sample Questions (Q487-Q492):

NEW QUESTION # 487
Which of the following is the BEST evidence that a user account has been properly authorized?

- A. An email from the user accepting the account
- B. Formal approval of the account by the user's manager
- C. Notification from human resources that the account is active
- D. User privileges matching the request form

Answer: D

Explanation:
According to the CRISC Review Manual, formal approval of the account by the user's manager is the best evidence that a user account has been properly authorized, because it ensures that the user's role and access rights are consistent with the business needs and the principle of least privilege. The user's manager is responsible for verifying the user's identity, job function, and access requirements, and for approving or rejecting the account request. The other options are not the best evidence of proper authorization, because they do not involve the user's manager's approval. An email from the user accepting the account is a confirmation of the account creation, but it does not indicate that the account was authorized by the user's manager. Notification from human resources that the account is active is an administrative process that does not verify the user's access rights and role. User privileges matching the request form is a verification of the account configuration, but it does not ensure that the request form was approved by the user's manager. References = CRISC Review Manual, 7th Edition, Chapter 4, Section 4.1.2, page 163.

NEW QUESTION # 488
Management has noticed storage costs have increased exponentially over the last 10 years because most users do not delete their emails. Which of the following can BEST alleviate this issue while not sacrificing security?

- A. Establishing e-discovery and data loss prevention (DLP)
- B. Implementing record retention tools and techniques
- C. Sending notifications when near storage quota
- D. Implementing a bring your own device 1BVOD) policy

Answer: B

Explanation:
According to the Risk and Information Systems Control documents, implementing record retention tools and techniques is the best solution in this scenario. Record retention involves managing the lifecycle of records, including their creation, usage, storage, and disposal. By implementing record retention policies, organizations can define how long emails and other data should be retained before being deleted. This helps in efficiently managing storage space and reducing unnecessary storage costs.
Establishing e-discovery and data loss prevention (DLP) (Option B) focuses more on legal and compliance aspects and may not directly address the issue of reducing storage costs. Sending notifications when near storage quota (Option C) is a reactive approach and may not prevent the exponential increase in storage costs. Implementing a bring your own device (BYOD) policy (Option D) is unrelated to the issue of email storage costs.
References = Risk and Information Systems Control Study Manual

NEW QUESTION # 489
Which of the following role carriers is accounted for analyzing risks, maintaining risk profile, and risk-aware decisions?

- A. Chief information officer (CIO)
- B. Explanation:
  Business management is the business individuals with roles relating to managing a program. They are typically accountable for

analyzing risks, maintaining risk profile, and risk-aware decisions. Other than this, they are also responsible for managing risks, react to events, etc.

- C. Business management
- D. Chief risk officer (CRO)
- E. Business process owner

Answer: C

Explanation:
is incorrect. CIO is the most senior official of the enterprise who is accountable for IT advocacy; aligning IT and business strategies; and planning, resourcing and managing the delivery of IT services and information and the deployment of associated human resources. CIO has some responsibility analyzing risks, maintaining risk profile, and risk-aware decisions but is not accounted for them. Answer: B is incorrect. Business process owner is an individual responsible for identifying process requirements, approving process design and managing process performance. He/she is responsible for analyzing risks, maintaining risk profile, and risk-aware decisions but is not accounted for them. Answer: D is incorrect. CRO is the individual who oversees all aspects of risk management across the enterprise. He/she is responsible for analyzing risks, maintaining risk profile, and risk-aware decisions but is not accounted for them.

NEW QUESTION # 490
Which of the following would BEST facilitate the maintenance of data classification requirements?

- A. Establishing a data loss prevention (DLP) solution
- B. Implementing technical controls over the assets
- C. Scheduling periodic audits
- D. Assigning a data custodian

Answer: C

Explanation:
Scheduling periodic audits is the best way to facilitate the maintenance of data classification requirements, because it helps to verify and validate that the data are classified and handled according to the established policies, standards, and guidelines, and that the data classification requirements are updated and aligned with the changes in the data environment or regulations. Data classification is a process of categorizing data according to their sensitivity, confidentiality, and value to the organization, and specifying the appropriate handling and protection measures for each category. Data classification requirements are the rules or criteria that define how data should be classified and treated. Scheduling periodic audits is the best way to ensure that the data classification requirements are followed and maintained, and that any issues or gaps are identified and addressed. Assigning a data custodian, implementing technical controls over the assets, and establishing a data loss prevention (DLP) solution are all useful ways to facilitate the maintenance of data classification requirements, but they are not the best way, as they do not provide a comprehensive and independent review and assessment of the data classification process and outcomes. References = Risk and Information Systems Control Study Manual, Chapter 4, Section 4.3.2, page 158

NEW QUESTION # 491
Which of the following is the FIRST step in managing the security risk associated with wearable technology in the workplace?

- A. Develop risk awareness training.
- B. Assess the potential risk.
- C. Monitor employee usage.
- D. Identify the potential risk.

Answer: D

Explanation:
The security risk associated with wearable technology in the workplace is the possibility and impact of unauthorized access, disclosure, or use of the data or information that are collected, stored, or transmitted by the wearable devices, such as smartwatches, fitness trackers, or glasses, that are worn or used by the employees12.
The first step in managing the security risk associated with wearable technology in the workplace is to identify the potential risk, which is the process of recognizing and describing the sources,causes, and consequences of the risk, and the potential impacts on the organization's objectives, performance, and value creation34.
Identifying the potential risk is the first step because it provides the basis and input for the subsequent steps of the risk management

process, such as assessing, treating, monitoring, and communicating the risk34.
Identifying the potential risk is also the first step because it enables the organization to understand and prioritize the risk, and to allocate the appropriate resources and controls for the risk management process34.
The other options are not the first step, but rather possible subsequent steps that may depend on or follow the identification of the potential risk. For example:
Monitoring employee usage is a step that involves collecting and analyzing data and information on the frequency, duration, and purpose of the wearable devices that are used by the employees, and detecting and reporting any deviations, anomalies, or issues that may indicate a security risk5 . However, this step is not the first step because it requires theidentification of the potential risk to provide the guidance and standards for the monitoring process5 .
Assessing the potential risk is a step that involves estimating and evaluating the likelihood and impact of the risk, and the level of risk exposure or tolerance for the organization34. However, this step is not the first step because it requires the identification of the potential risk to provide the information and data for the assessment process34.
Developing risk awareness training is a step that involves educating and training the employees and other stakeholders on the security risks and best practices associated with the wearable technology, and informing them of their roles, obligations, and responsibilities for the risk management process . However, this step is not the first step because it requires the identification of the potential risk to provide the content and objectives for the training process . References =
1: Wearable Devices in the Workplace: Security Threats and Protection1
2: 10 security risks of wearables | CSO Online2
3: Risk IT Framework, ISACA, 2009
4: IT Risk Management Framework, University of Toronto, 2017
5: Continuous Monitoring - ISACA3
Continuous Monitoring: A New Approach to Risk Management - ISACA Journal4 What Is Security Awareness Training and Why Is It Important? - Kaspersky5 Security Awareness Training - Cybersecurity Education Online | Proofpoint US

NEW QUESTION # 492
.....

id=1xXTID82JpAcgOQtfPF83LVp0lwmQKTjf