選擇我們最好的考試認證資料CISM考題套裝: Certified Information Security Manager，復習準備ISACA CISM 很輕松

從Google Drive中免費下載最新的KaoGuTi CISM PDF版考試題庫：https://drive.google.com/open?id=1eDgXo4nMZvARhprhn6uryx_idgaWxniW

通過這幾年IT行業不斷的發展與壯大，CISM考試已經成為ISACA考試裏的里程碑，可以讓你成為IT的專業人士，有數以百計的線上資源，提供ISACA的CISM考試的問題，為什麼大多數選擇KaoGuTi，因為我們KaoGuTi裏有一支龐大的IT精英團隊，專注於ISACA的CISM考試的最新資料。讓你無障礙通過ISACA的CISM考試認證。KaoGuTi保證你第一次嘗試通過ISACA的CISM考試取得認證，KaoGuTi會和你站在一起，與你同甘共苦。

ISACA CISM（信息安全經理認證）考試是為想要展示其信息安全管理知識和專業技能的個人設計的。該認證考試由信息系統審計和控制協會（ISACA）管理，該協會是信息技術治理、安全和保障領域的全球專業人士協會。CISM認證考試在業內享有高度尊重和認可，旨在評估個人管理、設計和監督組織信息安全計劃的能力。

>> CISM考題套裝 <<

最受推薦的CISM考題套裝，免費下載CISM考試題庫得到妳想要的ISACA證書

考古題網站在近幾年激增，這可能是導致你準備 ISACA 的 CISM 考試認證毫無頭緒。ISACA CISM 考試培訓資料是一些專業人士和通過了的考生用實踐證明瞭的有效的培訓資料，它可以幫助你通過考試認證。告訴各考生一個好消息：KaoGuTi CISM 考古題已經更新，解除了考生的擔憂！現在購買考題將得到一定的優惠！每個考生在準備 ISACA 認證考試時，都非常苦惱！希望各位考生順利通過考試！

CISM 證書為資訊安全專業人員提供了眾多好處。它驗證了他們在資訊安全管理方面的專業知識，並在就業市場上提供了競爭優勢。它還表明了對專業發展和持續學習的承諾，因為 CISM 持有人必須獲得繼續教育學分以維持其證書。 CISM 證書獲得全球雇主和客戶的認可，通常是高級資訊安全管理職位的要求。

最新的 Isaca Certification CISM 免費考試真題 (Q775-Q780):

問題 #775
The BEST indication of a change in risk that may negatively impact an organization is an increase in the number of:

- A. security incidents reported by staff to the information security team.
- B. alerts triggered by the security information and event management (SIEM) solution.
- C. malware infections detected by the organization's anti-virus software.
- D. events logged by the intrusion detection system (IDS).

答案：A

問題 #776
Which of the following is the MAJOR advantage of conducting a post-incident review? The review:

- A. provides continuous process improvement.
- B. helps develop business cases for security monitoring tools.
- C. helps identify current and desired level of risk.
- D. facilitates reporting on actions taken during the incident process.

答案：A

問題 #777
Which metric is the BEST indicator that an update to an organization's information security awareness strategy is effective?

- A. An increase in the number of email viruses detected
- B. An increase in the number of incidents reported by staff
- C. A decrease in the number of email viruses detected
- D. A decrease in the number of incidents reported by staff

答案：D

解題說明：
Section: INFORMATION SECURITY PROGRAM DEVELOPMENT

問題 #778
Which of the following is the MOST important action to take when engaging third-party consultants to conduct an attack and penetration test?

- A. Request a list of the software to be used
- B. Establish clear rules of engagement
- C. Provide clear directions to IT staff
- D. Monitor intrusion detection system (IDS) and firewall logs closely

答案：B

解題說明：
It is critical to establish a clear understanding on what is permissible during the engagement. Otherwise, the tester may inadvertently trigger a system outage or inadvertently corrupt files. Not as important, but still useful, is to request a list of what software will be used. As for monitoring the intrusion detection system (IDS) and firewall, and providing directions to IT staff, it is better not to alert those responsible for monitoring (other than at the management level), so that the effectiveness of that monitoring can be accurately assessed.

問題 #779
A security incident has been reported within an organization. When should an inforrnation security manager contact the information owner? After the:

- A. incident has been confirmed.
- B. incident has been mitigated.
- C. potential incident has been logged.
- D. incident has been contained.

答案：A

解題說明：
Explanation
= The information security manager should contact the information owner after the incident has been confirmed, as this is the first step of the incident response process. The information owner is the person who has the authority and responsibility for the information asset that is affected by the incident. The information owner needs to be informed of the incident as soon as possible, as they may have to make decisions or take actions regarding the protection, recovery, or restoration of the information asset. The

information owner may also have to communicate with other stakeholders, such as the business units, customers, regulators, or media, depending on the nature and impact of the incident.
The other options are not the correct time to contact the information owner, as they occur later in the incident response process. Contacting the information owner after the incident has been contained, mitigated, or logged may delay the notification and escalation of the incident, as well as the involvement and collaboration of the information owner. Moreover, contacting the information owner after the incident has been contained or mitigated may imply that the incident response team has already taken actions that may affect the information asset without the consent or approval of the information owner. Contacting the information owner after a potential incident has been logged may cause unnecessary alarm or confusion, as the potential incident may not be a real or significant incident, or it may not affect the information owner's asset. References = CISM Review Manual, 16th Edition, ISACA, 2022, pp. 219-220, 226-227.
CISM Questions, Answers & Explanations Database, ISACA, 2022, QID 1009.

問題 #780
.....