

CISM: Certified Information Security Manager torrent & Testking CISM guide



What's more, part of that Pass4Test CISM dumps now are free: https://drive.google.com/open?id=1ATZcoK60cdPK7NQ3pP2OfNzM_p3NE-lb

The content system of CISM exam simulation is constructed by experts. After-sales service of our study materials is also provided by professionals. If you encounter some problems when using our CISM study materials, you can also get them at any time. After you choose CISM Preparation questions, professional services will enable you to use it in the way that suits you best, truly making the best use of it, and bringing you the best learning results.

The CISM Certification is widely recognized by employers as a benchmark for measuring the competency of their information security managers. It is also considered as one of the top certifications for security professionals who wish to advance their careers in the field of cybersecurity. Certified Information Security Manager certification exam covers four domains, which are Information Security Governance, Risk Management, Information Security Program Development and Management, and Information Security Incident Management.

>> CISM Certification Questions <<

You Can Never Think About Failure With ISACA CISM Exam Dumps

Pass4Test's promise is to get you a wonderful success in CISM certification exams. Select any certification exam, our dumps and study guides will help you ace it in first attempt. No more cramming from books and note, just prepare our CISM Interactive Questions and answers and learn everything necessary to easily pass the actual CISM exam.

ISACA Certified Information Security Manager Sample Questions (Q293-Q298):

NEW QUESTION # 293

Which of the following is the PRIMARY reason to assign a risk owner in an organization?

- A. To remediate residual risk
- B. To identify emerging risk
- C. To ensure accountability
- D. To define responsibilities

Answer: C

Explanation:

Explanation

The primary reason to assign a risk owner in an organization is to ensure accountability for the risk and its treatment. A risk owner is

a person or entity that has the authority and responsibility to manage a specific risk and to implement the appropriate risk response actions. By assigning a risk owner, the organization can ensure that the risk is monitored, reported, and controlled in accordance with the organization's risk appetite and tolerance.

References: The CISM Review Manual 2023 defines risk owner as "the person or entity with the accountability and authority to manage a risk" and states that "the risk owner is responsible for ensuring that the risk is treated in a manner consistent with the enterprise's risk appetite and tolerance" (p. 93). The CISM Review Questions, Answers & Explanations Manual 2023 also provides the following rationale for this answer: "To ensure accountability is the correct answer because it is the primary reason to assign a risk owner in an organization, as it ensures that the risk and its treatment are managed by a person or entity that has the authority and responsibility to do so" (p. 29). Additionally, the article Risk Ownership: The First Step of Effective Risk Management from the ISACA Journal 2019 states that "risk ownership is the first and most important step of effective risk management" and that "risk ownership ensures that there is clear accountability and responsibility for each risk and that risk owners are empowered to make risk decisions and implement risk responses" (p. 1)

NEW QUESTION # 294

When customer data has been compromised, an organization should contact law enforcement authorities:

- A. in accordance with the corporate communication policy.
- B. when directed by the information security manager.
- C. if the attack comes from an international source.
- D. if there is potential impact to the organization.

Answer: A

Explanation:

Section: INFORMATION SECURITY PROGRAM MANAGEMENT

NEW QUESTION # 295

Who can BEST approve plans to implement an information security governance framework?

- A. Internal auditor
- B. Information security management
- C. Steering committee
- D. Infrastructure management

Answer: C

Explanation:

Senior management that is part of the security steering committee is in the best position to approve plans to implement an information security governance framework. An internal auditor is secondary to the authority and influence of senior management. Information security management should not have the authority to approve the security governance framework. Infrastructure management will not be in the best position since it focuses more on the technologies than on the business.

NEW QUESTION # 296

Which of the following should an information security manager do FIRST when a mandatory security standard hinders the achievement of an identified business objective?

- A. Escalate to senior management.
- B. Recommend risk acceptance.
- C. Revisit the business objective.
- D. Perform a cost-benefit analysis.

Answer: A

Explanation:

Escalate to senior management, because this could help the information security manager to inform the decision-makers of the situation, explain the implications and trade-offs, and seek their guidance and approval for the next steps. However, this answer is not certain, and you might need to consider other factors as well.

NEW QUESTION # 297

The **ULTIMATE** responsibility for ensuring the objectives of an information security framework are being met belongs to:

- A. the internal audit manager.
- B.)the information security officer.
- C. the steering committee.
- D. the board of directors.

Answer: D

Explanation:

The ultimate responsibility for ensuring the objectives of an information security framework are being met belongs to the board of directors, as they are accountable for the governance of the organization and the oversight of the information security strategy. The board of directors should ensure that the information security framework aligns with the business objectives, supports the business processes, and complies with the legal and regulatory requirements. The board of directors should also monitor the performance and effectiveness of the information security framework and provide guidance and direction for its improvement.

Reference = CISM Review Manual, 16th Edition eBook1, Chapter 1: Information Security Governance, Section: Enterprise Governance, Subsection: Board of Directors, Page 18.

NEW QUESTION # 298

With the advent of the era of knowledge-based economy, a man without a sound academic background can hardly accomplish anything. But it is not an uncommon phenomenon that many people become successful without a good education. People can achieve great success without an outstanding education and that the CISM qualifications a successful person needs can be acquired through the study to get some professional certifications. So it cannot be denied that suitable CISM study materials do help you a lot; thus we strongly recommend our CISM study materials for several following reasons.

New CISM Braindumps Files: <https://www.pass4test.com/CISM.html>

BONUS!!! Download part of Pass4Test CISM dumps for free: https://drive.google.com/open?id=1ATZcoK60cdPK7NQ3pP2OfNzM_p3NE-Ib