

# CISM Exam Registration, CISM Exams Torrent



What's more, part of that Pass4guide CISM dumps now are free: <https://drive.google.com/open?id=1D6mdjcc8gEgaIniOJp5s6xd3h8Z0Rt7a>

The ISACA CISM certification exam is one of the hottest and career-oriented certifications in the market. This Certified Information Security Manager (CISM) certification exam has been inspiring beginners and experienced professionals since its beginning. Over this long time period, countless Certified Information Security Manager (CISM) exam candidates have passed their Certified Information Security Manager (CISM) certification exam, and now they are offering their services to the top world brands.

The CISM certification exam is designed to help professionals demonstrate their expertise and knowledge in information security management to potential employers and clients. Certified Information Security Manager certification provides professionals with a competitive edge in the job market and helps them stand out from other candidates. Furthermore, the CISM Certification is recognized by many organizations, including government agencies, as a standard for information security management professionals.

>> CISM Exam Registration <<

## ISACA CISM Exams Torrent & CISM Latest Test Fee

Our products are the accumulation of professional knowledge worthy practicing and remembering. There are so many specialists who join together and contribute to the success of our CISM guide quiz just for your needs. Our responsible and patient staff who has been trained strictly before get down to business and interact with customers. Once you have practiced and experienced the quality of our CISM Exam Preparation, you will remember the serviceability and usefulness of them. It explains why our CISM practice materials helped over 98 percent of exam candidates get the certificate you dream of successfully. Believe me you can get it too.

ISACA CISM certification is a globally recognized certification for information security professionals. It is designed for individuals who are responsible for managing, designing, and overseeing the information security programs of their organizations. Certified Information Security Manager certification is highly respected in the industry and is considered a benchmark for information security management.

The CISM Exam Tests the knowledge and skills required to manage, design, and oversee an organization's information security program. It covers four domains: information security governance, risk management, information security program development and management, and information security incident management. CISM exam is designed to test the candidate's ability to apply these concepts in real-world situations.

## ISACA Certified Information Security Manager Sample Questions (Q377-Q382):

### NEW QUESTION # 377

Which of the following would be the MOST important goal of an information security governance program?

- A. Effective involvement in business decision making
- B. Review of internal control mechanisms
- C. Ensuring trust in data

- D. Total elimination of risk factors

**Answer: C**

Explanation:

Section: INFORMATION SECURITY GOVERNANCE

Explanation:

The development of trust in the integrity of information among stakeholders should be the primary goal of information security governance. Review of internal control mechanisms relates more to auditing, while the total elimination of risk factors is not practical or possible. Proactive involvement in business decision making implies that security needs dictate business needs when, in fact, just the opposite is true.

Involvement in decision making is important only to ensure business data integrity so that data can be trusted.

### NEW QUESTION # 378

Which of the following is the MOST essential element of an information security program?

- A. Benchmarking the program with global standards for relevance
- B. Applying project management practices used by the business
- **C. Involving functional managers in program development**
- D. Prioritizing program deliverables based on available resources

**Answer: C**

Explanation:

Involving functional managers in program development is the most essential element of an information security program, because they are responsible for ensuring that the information security policies, standards, and procedures are implemented and enforced within their respective business units. They also provide input and feedback on the information security requirements, risks, and controls that affect their operations and objectives.

Reference =

CISM Review Manual, 16th Edition, ISACA, 2020, p. 37: "Functional managers are responsible for ensuring that the information security policies, standards, and procedures are implemented and enforced within their respective business units." CISM Review Manual, 16th Edition, ISACA, 2020, p. 38: "Functional managers should be involved in the development of the information security program to provide input and feedback on the information security requirements, risks, and controls that affect their operations and objectives."

### NEW QUESTION # 379

Of the following, who is accountable for data loss in the event of an information security incident at a third-party provider?

- A. The information security manager
- B. The incident response team
- C. The service provider that hosts the data
- **D. The business data owner**

**Answer: D**

Explanation:

The business data owner is accountable for data loss in the event of an information security incident at a third-party provider because they are ultimately responsible for the protection and use of their data, regardless of where it is stored or processed. The information security manager is not accountable for data loss at a third-party provider, but rather responsible for implementing and enforcing the security policies and standards that govern the relationship with the provider. The service provider that hosts the data is not accountable for data loss at their site, but rather liable for any breach of contract or service level agreement that may result from such an incident. The incident response team is not accountable for data loss at a third-party provider, but rather responsible for responding to and managing the incident according to the incident response plan. Reference: <https://www.isaca.org/resources/isaca-journal/issues/2017/volume-1/data-ownership-and-custodianship-in-the-cloud> <https://www.isaca.org/resources/isaca-journal/issues/2018/volume-3/incident-response-lessons-learned>

### NEW QUESTION # 380

An organization plans to outsource its customer relationship management (CRM) to a third-party service provider. Which of the



id=1D6mdjcc8gEgaIniOJp5s6xd3h8Z0Rt7a