



CISM

Certified Information Security Manager

Q&A

DEMO Version

Copyright (c) 2009 Chinatag LLC. All rights reserved.

Important Note Please Read Carefully

For demonstration purpose only, this free version Chinatag study guide contains **10** full length questions selected from our full version products which have more than **200** questions each.

This Study guide has been carefully written and compiled by Chinatag certification experts. It is designed to help you learn the concepts behind the questions rather than be a strict memorization tool. Repeated readings will increase your comprehension.

For promotion purposes, all PDF files are **not** encrypted. Feel free to distribute copies among your friends and let them know Chinatag website.

Study Tips

This product will provide you questions and answers along with detailed explanations carefully compiled and written by our experts. Try to understand the concepts behind the questions instead of cramming the questions. Go through the entire document at least twice so that you make sure that you are not missing anything.

Latest Version

We are constantly reviewing our products. New material is added and old material is revised. Free updates are available for 90 days after the purchase. You should check the products page on the <http://www.chinatag.com> website for an update 3-4 days before the scheduled exam date.

Please tell us what you think of our products. We appreciate both positive and critical comments as your feedback helps us improve future versions. Feedback on specific questions should be send to feedback@chinatag.com.

Thanks for purchasing our products and look forward to supplying you with all your Certification training needs.

Good studying!

Technical and Support Team
Chinatag LLC.

QUESTION NO: 1

Senior management commitment and support for information security can BEST be obtained through presentations that:

- A. use illustrative examples of successful attacks.
- B. explain the technical risks to the organization.
- C. evaluate the organization against best security practices.
- D. tie security risks to key business objectives.

Answer: D

Explanation:

Senior management seeks to understand the business justification for investing in security. This can best be accomplished by tying security to key business objectives.

Senior management will not be as interested in technical risks or examples of successful attacks if they are not tied to the impact on business environment and objectives. Industry best practices are important to senior management but, again, senior management will give them the right level of importance when they are presented in terms of key business objectives.

QUESTION NO: 2

Which of the following is characteristic of centralized information security management?

- A. More expensive to administer
- B. Better adherence to policies
- C. More aligned with business unit needs
- D. Faster turnaround of requests

Answer: B

Explanation:

Centralization of information security management results in greater uniformity and better adherence to security policies. It is generally less expensive to administer due to the economies of scale. However, turnaround can be slower due to the lack of alignment with business units.

QUESTION NO: 3

The MOST important component of a privacy policy is:

- A. notifications
- B. warranties

- C. liabilities
- D. geographic coverage

Answer: A

Explanation:

Privacy policies must contain notifications and opt-out provisions; they are a high-level management statement of direction. They do not necessarily address warranties, liabilities or geographic coverage, which are more specific.

QUESTION NO: 4

It is MOST important that information security architecture be aligned with which of the following?

- A. Industry best practices
- B. Information technology plans
- C. Information security best practices
- D. Business objectives and goals

Answer: D

Explanation:

Information security architecture should always be properly aligned with business goals and objectives. Alignment with IT plans or industry and security best practices is secondary by comparison.

QUESTION NO: 5

Security technologies should be selected PRIMARILY on the basis of their:

- A. ability to mitigate business risks
- B. evaluations in trade publications
- C. use of new and emerging technologies
- D. benefits in comparison to their costs

Answer: A

Explanation:

The most fundamental evaluation criteria for the appropriate selection of any security technology is its ability to reduce or eliminate business risks. Investments in security technologies should be based on their overall value in relation to their cost; the value can be demonstrated in terms of risk mitigation. This should take precedence over whether they use new or exotic technologies or how they are evaluated in trade publications.

QUESTION NO: 6

What will have the HIGHEST impact on standard information security governance models?

- A. Number of employees
- B. Distance between physical locations
- C. Complexity of organizational structure
- D. Organizational budget

Answer: C

Explanation:

Information security governance models are highly dependent on the overall organizational structure. Some of the elements that impact organizational structure are multiple missions and functions across the organization, leadership and lines of communication. Number of employees and distance between physical locations have less impact on information security governance models since well-defined process, technology and people components intermingle to provide the proper governance.

Organizational budget is not a major impact once good governance models are in place, hence governance will help in effective management of the organization's budget.

QUESTION NO: 7

The PRIMARY goal in developing an information security strategy is to:

- A. establish security metrics and performance monitoring.
- B. educate business process owners regarding their duties.
- C. ensure that legal and regulatory requirements are met.
- D. support the business objectives of the organization.

Answer: D

Explanation:

The business objectives of the organization supersede all other factors.

Establishing metrics and measuring performance, meeting legal and regulatory requirements, and educating business process owners are all subordinate to this overall goal.

QUESTION NO: 8

What is the PRIMARY role of the information security manager in the process of information classification within an organization?

- A. Defining and ratifying the classification structure of information assets
- B. Deciding the classification levels applied to the organization's information assets
- C. Securing information assets in accordance with their classification
- D. Checking if information assets have been classified properly

Answer: A

Explanation:

Defining and ratifying the classification structure of information assets is the primary role of the information security manager in the process of information classification within the organization. Choice B is incorrect because the final responsibility for deciding the classification levels rests with the data owners. Choice C is incorrect because the job of securing information assets is the responsibility of the data custodians. Choice D may be a role of an information security manager but is not the key role in this context.

QUESTION NO: 9

An information security manager at a global organization that is subject to regulation by multiple governmental jurisdictions with differing requirements should:

- A. bring all locations into conformity with the aggregate requirements of all governmental jurisdictions.
- B. establish baseline standards for all locations and add supplemental standards as required.
- C. bring all locations into conformity with a generally accepted set of industry best practices.
- D. establish a baseline standard incorporating those requirements that all jurisdictions have in common.

Answer: B

Explanation:

It is more efficient to establish a baseline standard and then develop additional standards for locations that must meet specific requirements. Seeking a lowest common denominator or just using industry best practices may cause certain locations to fail regulatory compliance. The opposite approach-forcing all locations to be in compliance with the regulations-places an undue burden on those locations.

QUESTION NO: 10

Which of the following BEST describes an information security manager's role in a multidisciplinary team that will address a new regulatory requirement regarding operational risk?

- A. Ensure that all IT risks are identified

- B. Evaluate the impact of information security risks
- C. Demonstrate that IT mitigating controls are in place
- D. Suggest new IT controls to mitigate operational risk

Answer: B

Explanation:

The job of the information security officer on such a team is to assess the risks to the business operation. Choice A is incorrect because information security is not limited to IT issues. Choice C is incorrect because at the time a team is formed to assess risk, it is premature to assume that any demonstration of IT controls will mitigate business operations risk. Choice D is incorrect because it is premature at the time of the formation of the team to assume that any suggestion of new IT controls will mitigate business operational risk.