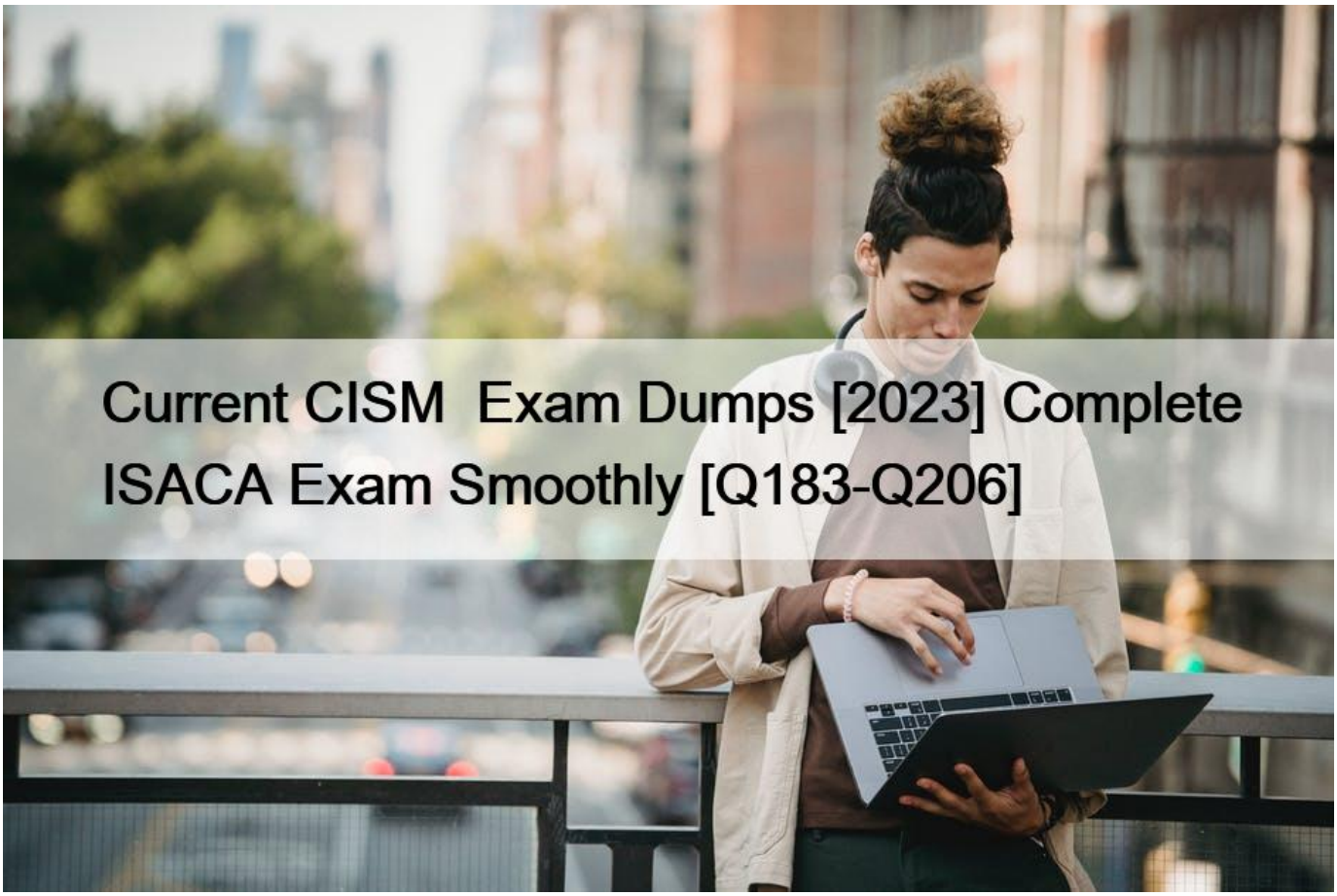
Current CISM Exam Dumps [2023 Complete ISACA Exam Smoothly [Q183-Q206



Current CISM Exam Dumps [2023] Complete ISACA Exam Smoothly
CISM Premium PDF & Test Engine Files with 417 Questions & Answers

NEW QUESTION 183

The impact of losing frame relay network connectivity for 18-24 hours should be calculated using the:
* hourly billing rate charged by the carrier.
* value of the data transmitted over the network.
* aggregate compensation of all affected business users.
* financial losses incurred by affected business units.

Explanation/Reference:

Explanation:

The bottom line on calculating the impact of a loss is what its cost will be to the organization. The other choices are all factors that contribute to the overall monetary impact.

NEW QUESTION 184

In the course of examining a computer system for forensic evidence, data on the suspect media were inadvertently altered. Which of the following should have been the FIRST course of action in the investigative process?
* Perform a backup of the suspect media to new media.
* Perform a bit-by-bit image of the original media source onto new media.
* Make a copy of all files that are relevant to the investigation.
* Run an error-checking program on all logical drives to ensure that there are no disk errors.

Section: INCIDENT MANAGEMENT AND RESPONSE

Explanation:

The original hard drive or suspect media should never be used as the source for analysis. The source or original media should be physically secured and only used as the master to create a bit-by-bit image. The original should be stored using the appropriate procedures, depending on location. The image created for forensic analysis should be used. A backup does not preserve 100 percent of the data, such as erased or deleted files and data in slack space – which may be critical to the investigative process. Once data from the source are altered, they may no longer be admissible in court. Continuing the investigation, documenting the date, time and data altered, are actions that may not be admissible in legal proceedings. The organization would need to know the details of collecting and preserving forensic evidence relevant to their jurisdiction.

NEW QUESTION 185

It is MOST important that information security architecture be aligned with which of the following?
* Industry best practices
* Information technology plans
* Information security best practices
* Business objectives and goals

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.

NEW QUESTION 186

In assessing the degree to which an organization may be affected by new privacy legislation, information security management should FIRST:
* develop an operational plan for achieving compliance with the legislation.
* identify systems and processes that contain privacy components.
* restrict the collection of personal information until compliant.
* identify privacy legislation in other countries that may contain similar requirements.

Identifying the relevant systems and processes is the best first step. Developing an operational plan for achieving compliance with the legislation is incorrect because it is not the first step. Restricting the collection of personal information comes later. Identifying privacy legislation in other countries would not add much value.

NEW QUESTION 187

Which of the following is the PRIMARY responsibility of an information security steering committee?
* Reviewing firewall rules
* Setting up password expiration procedures
* Prioritizing security initiatives
* Drafting security policies

NEW QUESTION 188

Which of the following is the responsibility of a risk owner?
* Performing risk assessments to direct risk response
* Determining the organization’s risk appetite
* Ensuring control effectiveness is monitored
* Implementing controls to mitigate the risk

Explanation

A risk owner is a person or entity that is responsible for ensuring that risk is managed effectively. One of the primary responsibilities of a risk owner is to implement controls that will help mitigate or manage the risk.

While risk assessments, determining the organization’s risk appetite, and monitoring control effectiveness are all important aspects of managing risk, it is the responsibility of the risk owner to take the necessary actions to manage the risk.

NEW QUESTION 189

The MOST complete business case for security solutions is one that.
* includes appropriate justification.
* explains the current risk profile.
* details regulatory requirements.
* identifies incidents and losses.

Explanation

Management is primarily interested in security solutions that can address risks in the most cost-effective way.

To address the needs of an organization, a business case should address appropriate security solutions in line with the organizational strategy.

NEW QUESTION 190

How would an organization know if its new information security program is accomplishing its goals?
* Key metrics indicate a reduction in incident impacts.
* Senior management has approved the program and is supportive of it.
* Employees are receptive to changes that were implemented.
* There is an immediate reduction in reported incidents.

Explanation/Reference:

Explanation:

Option A is correct since an effective security program will show a trend in impact reduction. Options B and C may well derive from a performing program, but are not as significant as option A. Option D may indicate that it is not successful.

NEW QUESTION 191

A risk management program should reduce risk to:
* zero.
* an acceptable level.
* an acceptable percent of revenue.
* an acceptable probability of occurrence.

Section: INFORMATION RISK MANAGEMENT

Explanation:

Risk should be reduced to an acceptable level based on the risk preference of the organization. Reducing risk to zero is impractical and could be cost-prohibitive. Tying risk to a percentage of revenue is inadvisable since there is no direct correlation between the two. Reducing the probability of risk occurrence may not always be possible, as in the ease of natural disasters. The focus should be on reducing the impact to an acceptable level to the organization, not reducing the probability of the risk.

NEW QUESTION 192

In a resource-restricted security program, which of the following approaches will provide the BEST use of the limited resources?
* Cross-training
* Risk avoidance
* Risk prioritization
* Threat management

Section: INFORMATION SECURITY PROGRAM MANAGEMENT

NEW QUESTION 193

When establishing metrics for an information security program, the BEST approach is to identify indicators that:
* demonstrate the effectiveness of the security program.
* reduce information security program spending.
* reflect the corporate risk culture.
* support major information security initiatives.

NEW QUESTION 194

Temporarily deactivating some monitoring processes, even if supported by an acceptance of operational risk, may not be acceptable to the information security manager if:
* it implies compliance risks.
* short-term impact cannot be determined.
* it violates industry security practices.
* changes in the roles matrix cannot be detected.

Explanation/Reference:

Explanation:

Monitoring processes are also required to guarantee fulfillment of laws and regulations of the organization and, therefore, the information security manager will be obligated to comply with the law. Choices B and C are evaluated as part of the operational risk. Choice D is unlikely to be as critical a breach of regulatory legislation. The acceptance of operational risks overrides choices B, C and D.

NEW QUESTION 195

The management staff of an organization that does not have a dedicated security function decides to use its IT manager to perform a security review. The MAIN job requirement in this arrangement is that the IT manager
* report risks in other departments.
* obtain support from other departments.
* report significant security risks.

* have knowledge of security standards.

Explanation

The IT manager needs to report the security risks in the environment pursuant to the security review, including risks in the IT implementation. Choices A, B and D are important, but not the main responsibilities or job requirements.

NEW QUESTION 196

The FIRST step to create an internal culture that focuses on information security is to:

* implement stronger controls.
* conduct periodic awareness training.
* actively monitor operations.
* gain the endorsement of executive management.

Explanation/Reference:

Explanation:

Endorsement of executive management in the form of policies provides direction and awareness. The implementation of stronger controls may lead to circumvention. Awareness training is important, but must be based on policies. Actively monitoring operations will not affect culture at all levels.

NEW QUESTION 197

Which of the following would BEST ensure that security risk assessment is integrated into the life cycle of major IT projects?

* Integrating the risk assessment into the internal audit program
* Applying global security standards to the IT projects
* Training project managers on risk assessment
* Having the information security manager participate on the project setting committees

NEW QUESTION 198

Which of the following would be of GREATEST assistance in determining whether to accept residual risk of a critical security system?

* Cost-benefit analysis of mitigating controls
* Recovery time objective (RTO)
* Available annual budget
* Maximum tolerable outage (MTO)

NEW QUESTION 199

Which of the following is the MOST effective solution for preventing individuals external to the organization from modifying sensitive information on a corporate database?

* Screened subnets
* Information classification policies and procedures
* Role-based access controls
* Intrusion detection system (IDS)

Explanation

Screened subnets are demilitarized zones (DMZs) and are oriented toward preventing attacks on an internal network by external users. The policies and procedures to classify information will ultimately result in better protection but they will not prevent actual

modification. Role-based access controls would help ensure that users only had access to files and systems appropriate for their job role. Intrusion detection systems (IDS) are useful to detect invalid attempts but they will not prevent attempts.

NEW QUESTION 200

Which of the following is MOST important to consider when developing a business case to support the investment in an information security program?
* Senior management support
* Results of a cost-benefit analysis
* Results of a risk assessment
* Impact on the risk profile
Explanation/Reference:

Explanation

The information security manager must understand the business risk profile of the organization. No model provides a complete picture, but logically categorizing the risk areas of an organization facilitates focusing on key risk management strategies and decisions. It also enables the organization to develop and implement risk treatment approaches that are relevant to the business and cost effective.

NEW QUESTION 201

Which of the following is the MOST effective way for senior management to support the integration of information security governance into corporate governance?
* Develop the information security strategy based on the enterprise strategy.
* Appoint a business manager as heard of information security.
* Promote organization-wide information security awareness campaigns.
* Establish a steering committee with representation from across the organization.

NEW QUESTION 202

To ensure IT equipment meets organizational security standards, the MOST efficient approach is to:
* assess security during equipment deployment.
* ensure compliance during user acceptance testing.
* assess the risks of all new equipment.
* develop an approved equipment list.
Section: INFORMATION SECURITY PROGRAM MANAGEMENT

NEW QUESTION 203

An information security manager reviewing firewall rules will be MOST concerned if the firewall allows:
* source routing.
* broadcast propagation.
* unregistered ports.
* nonstandard protocols.
Section: INFORMATION SECURITY PROGRAM MANAGEMENT

Explanation

Explanation:

If the firewall allows source routing, any outsider can carry out spoofing attacks by stealing the internal (private) IP addresses of the organization. Broadcast propagation, unregistered ports and nonstandard protocols do not create a significant security exposure.

NEW QUESTION 204

Which of the following is MOST critical for the successful implementation of an information security strategy?
* Established information security policies
* Sizeable funding for the information security program
* Compliance with regulations
* Ongoing commitment from senior management

NEW QUESTION 205

Vulnerability scanning has detected a critical risk in a vital business application. Which of the following should the information security manager do FIRST?
* Report the business risk to senior management.
* Confirm the risk with the business owner.
* Create an emergency change request
* Update the risk register.

NEW QUESTION 206

Which of the following requirements would have the lowest level of priority in information security?
* Technical
* Regulatory
* Privacy
* Business

Explanation

Information security priorities may, at times, override technical specifications, which then must be rewritten to conform to minimum security standards. Regulatory and privacy requirements are government-mandated and, therefore, not subject to override. The needs of the business should always take precedence in deciding information security priorities.

The CISM certification is an important credential for professionals in the field of information security management. Certified Information Security Manager certification demonstrates an individual's expertise in designing, implementing, and managing an organization's information security program. The CISM exam is a challenging exam that requires candidates to have a deep understanding of information security management principles, best practices, and frameworks. By passing the CISM exam, individuals can enhance their career opportunities and demonstrate their commitment to the field of information security management.

CISM Premium Files Practice Valid Exam Dumps Question: https://www.dumpsmaterials.com/CISM-real-torrent.html]