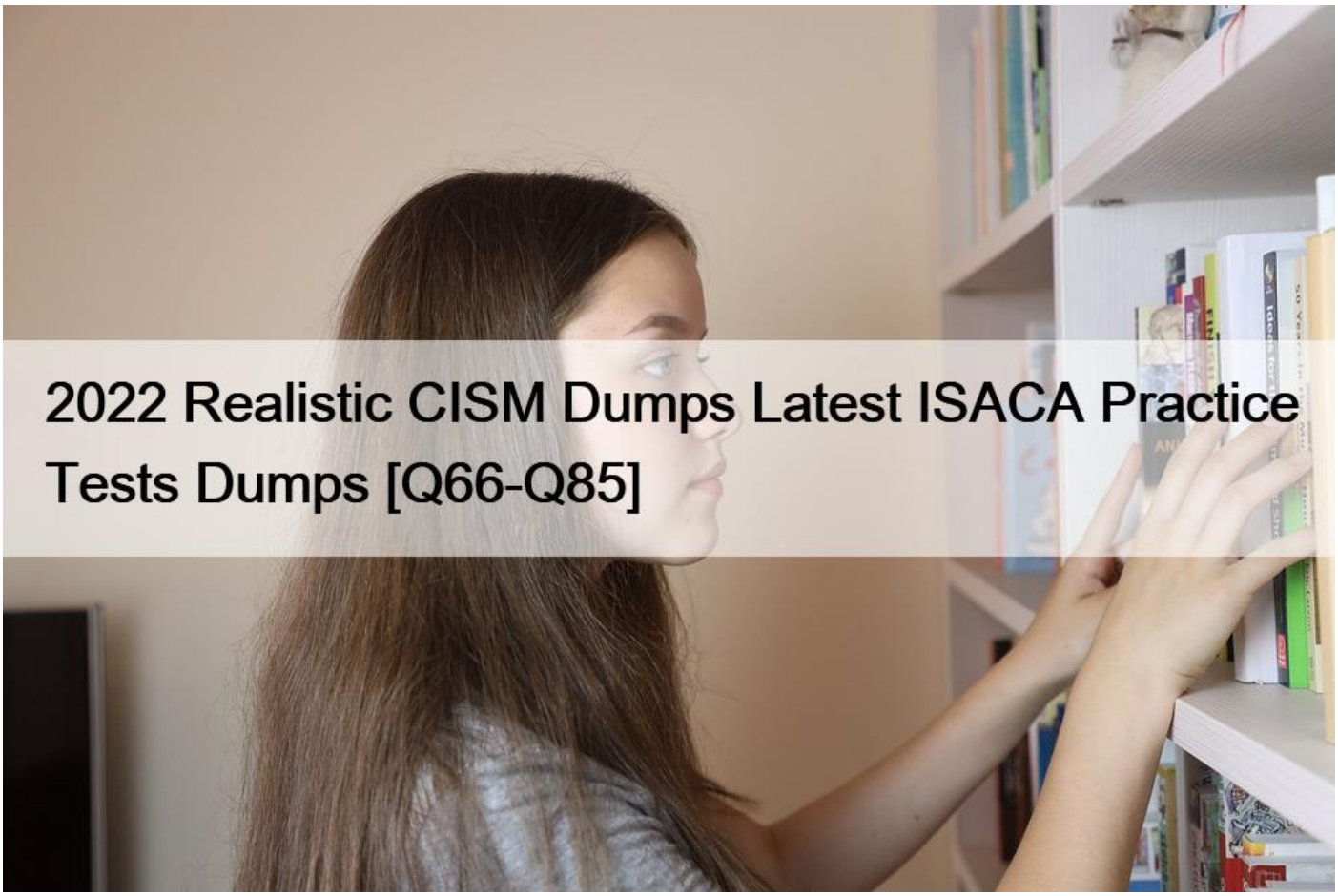
2022 Realistic CISM Dumps Latest ISACA Practice Tests Dumps [Q66-Q85



2022 Realistic CISM Dumps Latest ISACA Practice Tests Dumps
CISM Dumps PDF - CISM Real Exam Questions Answers

Who Is the Target Audience?

Now that you have an idea of the key topics of CISM, it's also relevant to know the main audience of the certification. First and foremost, it is created for individuals who have managerial roles. Their position allows them to design, supervise, and calculate the information security features of the organization. In addition, these professionals must have a minimum of 5 years of industry experience in managing information security. Isaca may allow a waiver of the number of working years for up to 2 years.

ISACA CISM: What exam details should you know?

The CISM certification exam usually lasts about 4 hours and contains 150 questions. The test has the multiple-choice format, and there are no negative points if you choose an incorrect answer. However, the correct ones are nullified within the same question. Thus, you should choose only the answers you are sure about. Each of the questions has a different score, depending on how difficult it is. You need to have the score of more than 450 points out of 800 to pass the exam successfully. The test is available in Simplified Chinese, English, Japanese, and Spanish. The exam voucher will cost you $760 or $575 if you enroll for membership.

Why Is CISM Highly Recommended for Management Positions?

CISM is one of the best certifications needed by professionals in managerial roles in an information security domain. These may be

security managers, IT managers, security administrators, senior system administrators, and so forth. By obtaining this Isaca certificate, you add value to your career because the exam coverage for CISM strategically highlights the entire aspects of IS management.
Therefore, if you want to level up your skills as well as your technical proficiency, this certification can help in reaching your objectives. Another thing that makes CISM famous among tech professionals is the fact that it serves as a salary booster. By having this on your profile, employers can distinguish your skills ahead of time. Thus, CISM certified individuals take home an average salary of more than $123,000+, as stated by PayScale, which is relatively higher than non-certified security professionals earn.
In addition, one can opt for other Isaca certifications. Although there is no further track related to CISM, applicant can choose alternatives such as CISA ? Certified Information Systems Auditor, CSX-P ? Cybersecurity Practitioner Certification, etc.

QUESTION 66

Which of the following is a potential indicator of inappropriate Internet use by staff?
* Increased help desk calls for password resets
* Reduced number of pings on firewalls
* Increased reports of slow system performance
* Increased number of weakness from vulnerability scans

QUESTION 67

Which of the following is the MOST important consideration when selecting members for an information security steering committee?
* Cross-functional composition
* Information security expertise
* Tenure in the organization
* Business expertise
Section: INFORMATION SECURITY PROGRAM MANAGEMENT

QUESTION 68

Documented standards/procedures for the use of cryptography across the enterprise should PRIMARILY:
* define the circumstances where cryptography should be used.
* define cryptographic algorithms and key lengths.
* describe handling procedures of cryptographic keys.
* establish the use of cryptographic solutions.
Section: INFORMATION SECURITY PROGRAM MANAGEMENT

Explanation:

There should be documented standards-procedures for the use of cryptography across the enterprise; they should define the circumstances where cryptography should be used. They should cover the selection of cryptographic algorithms and key lengths, but not define them precisely, and they should address the handling of cryptographic keys. However, this is secondary to how and when cryptography should be used. The use of cryptographic solutions should be addressed but, again, this is a secondary consideration.

QUESTION 69

A multinational organization has developed a bring your own device (BYOD) policy that requires the installation of mobile device management (MDM) software on personally owned devices. Which of the following poses the GREATEST challenge for implementing the policy?

* Differences in mobile OS platforms
* Varying employee data privacy rights
* Differences in corporate cultures
* Translation and communication of policy

QUESTION 70

The PRIMARY reason for using metrics to evaluate information security is to:
* identify security weaknesses.
* justify budgetary expenditures.
* enable steady improvement.
* raise awareness on security issues.

The purpose of a metric is to facilitate and track continuous improvement. It will not permit the identification of all security weaknesses. It will raise awareness and help in justifying certain expenditures, but this is not its main purpose.

QUESTION 71

A core business unit relies on an effective legacy system that does not meet the current security standards and threatens the enterprise network. Which of the following is the BEST course of action to address the situation?
* Document the deficiencies in the risk register.
* Disconnect the legacy system from the rest of the network.
* Require that new systems that can meet the standards be implemented.
* Develop processes to compensate for the deficiencies.

QUESTION 72

Which of the following is the PRIMARY goal of a risk management program?
* Implement preventive controls against threats.
* Manage the business impact of inherent risks.
* Manage compliance with organizational policies.
* Reduce the organization’s risk appetite.

Section: INFORMATION RISK MANAGEMENT

QUESTION 73

When configuring a biometric access control system that protects a high-security data center, the system’s sensitivity level should be set:
* to a higher false reject rate (FRR).
* to a lower crossover error rate.
* to a higher false acceptance rate (FAR).
* exactly to the crossover error rate.

Section: INFORMATION SECURITY PROGRAM DEVELOPMENT

Explanation:

Biometric access control systems are not infallible. When tuning the solution, one has to adjust the sensitivity level to give preference either to false reject rate (type I error rate) where the system will be more prone to err denying access to a valid user or erring and allowing access to an invalid user. As the sensitivity of the biometric system is adjusted, these values change inversely. At one point, the two values intersect and are equal. This condition creates the crossover error rate, which is a measure of the system accuracy. In systems where the possibility of false rejects is a problem, it may be necessary’ to reduce sensitivity and

thereby increase the number of false accepts. This is sometimes referred to as equal error rate (EER). In a very sensitive system, it may be desirable to minimize the number of false accepts – the number of unauthorized persons allowed access. To do this, the system is tuned to be more sensitive, which causes the false rejects the number of authorized persons disallowed access to increase.

QUESTION 74

Which of the following would BEST help to identify vulnerabilities introduced by changes to an organization’s technical infrastructure?
* An intrusion detection system
* Established security baselines
* Penetration testing
* Log aggregation and correlation

QUESTION 75

Which of the following architectures for e-business BEST ensures high availability?
* Availability of an adjacent hot site and a standby server with mirrored copies of critical data
* A single point of entry allowing transactions to be received and processed quickly
* Intelligent middleware to direct transactions from a downed system to an alternative
* Automatic failover to the web site of another e-business that meets the user’s needs

QUESTION 76

An organization has a policy in which all criminal activity is prosecuted. What is MOST important for the information security manager to ensure when an employee is suspected of using a company computer to commit fraud?
* The forensics process is immediately initiated
* The incident response plan is initiated
* The employee’s log files are backed-up
* Senior management is informed of the situation

Section: INFORMATION SECURITY PROGRAM MANAGEMENT

QUESTION 77

The MAIN advantage of implementing automated password synchronization is that it:
* reduces overall administrative workload.
* increases security between multi-tier systems.
* allows passwords to be changed less frequently.
* reduces the need for two-factor authentication.

Explanation

Automated password synchronization reduces the overall administrative workload of resetting passwords. It does not increase security between multi-tier systems, allow passwords to be changed less frequently or reduce the need for two-factor authentication.

QUESTION 78

In the absence of technical controls, what would be the BEST way to reduce unauthorized text messaging on company-supplied mobile devices?
* Conduct a business impact analysis (BIA) and provide the report to management.
* Update the corporate mobile usage policy to prohibit texting.

* Stop providing mobile devices until the organization is able to implement controls.
* Include the topic of prohibited texting in security awareness training.

Section: INFORMATION SECURITY PROGRAM MANAGEMENT

QUESTION 79

Which of the following is an information security manager’s MOST important consideration during the investigative process of analyzing the hard drive of 3 compromises..

* Maintaining chain of custody
* Notifying the relevant stakeholders
* Identifying the relevant strain of malware
* Determining the classification of stored data

QUESTION 80

Which of the following is the MOST appropriate individual to ensure that new exposures have not been introduced into an existing application during the change management process?

* System analyst
* System user
* Operations manager
* Data security officer

Section: INFORMATION SECURITY PROGRAM MANAGEMENT

Explanation:

System users, specifically the user acceptance testers, would be in the best position to note whether new exposures are introduced during the change management process. The system designer or system analyst, data security officer and operations manager would not be as closely involved in testing code changes.

QUESTION 81

Which of the following should be determined FIRST when establishing a business continuity program?

* Cost to rebuild information processing facilities
* Incremental daily cost of the unavailability of systems
* Location and cost of offsite recovery facilities
* Composition and mission of individual recovery teams

Explanation/Reference:

Explanation:

Prior to creating a detailed business continuity plan, it is important to determine the incremental daily cost of losing different systems. This will allow recovery time objectives to be determined which, in turn, affects the location and cost of offsite recovery facilities, and the composition and mission of individual recovery teams. Determining the cost to rebuild information processing facilities would not be the first thing to determine.

QUESTION 82

A risk mitigation report would include recommendations for:

* assessment.
* acceptance

* evaluation.
* quantification.

Explanation/Reference:

Explanation:

Acceptance of a risk is an alternative to be considered in the risk mitigation process. Assessment.

evaluation and risk quantification are components of the risk analysis process that are completed prior to determining risk mitigation solutions.

QUESTION 83

A risk has been formally accepted and documented. Which of the following is the MOST important action for an information security manager?

* Update risk tolerance levels.
* Notify senior management and the board.
* Monitor the environment for changes
* Re-evaluate the organization’s risk appetite

QUESTION 84

The information classification scheme should:

* consider possible impact of a security breach.
* classify personal information in electronic form.
* be performed by the information security manager.
* classify systems according to the data processed.

Explanation

Data classification is determined by the business risk, i.e., the potential impact on the business of the loss, corruption or disclosure of information. It must be applied to information in all forms, both electronic and physical (paper), and should be applied by the data owner, not the security manager. Choice B is an incomplete answer because it addresses only privacy issues, while choice A is a more complete response. Data classification is determined by the business risk, i.e., the potential impact on the business of the loss, corruption or disclosure of information. It must be applied to information in all forms, both electronic and physical (paper), and should be applied by the data owner, not the security manager.

QUESTION 85

When performing an information risk analysis, an information security manager should FIRST:

* establish the ownership of assets.
* evaluate the risks to the assets.
* take an asset inventory.
* categorize the assets.

Explanation

Assets must be inventoried before any of the other choices can be performed.

CISM Premium Exam Engine pdf Download: https://www.topexamcollection.com/CISM-vce-collection.html]