[Jun-2022 Verified CISA dumps Q&As - CISA dumps with Correct Answers [Q91-Q108

[Jun-2022] Verified CISA dumps Q&As - CISA dumps with Correct Answers
The Best Isaca Certification Study Guide for the CISA Exam

NEW QUESTION 91

An IS auditors independence with respect to the audit of an application system is MOST likely to be impaired if the auditor
* designed an embedded audit module for the application
* knows that the application contains the auditors personal transactions
* reports to an individual responsible ta the application
* performed a development review of the application.

NEW QUESTION 92

During an IT operations audit multiple unencrypted backup tapes containing sensitive credit card information cannot be found
Which of the following presents the GREATEST risk to the organization?
* Reputational damage due to potential identity theft
* Business disruption if a data restore cannot be completed

* The cost of recreating the missing backup tapes
* Human resource cost of responding to the incident

NEW QUESTION 93

Which of the following should be the PRIMARY objective of conducting an audit follow-up of management action plans?
* To verify that risks listed in the audit report have been properly mitigated
* To identify new risks and controls for the organization
* To align the management action plans with business requirements
* To ensure senior management is aware of the audit finidings.

NEW QUESTION 94

When reviewing the implementation of a LAN, an IS auditor should FIRST review the:
* node list.
* acceptance test report.
* network diagram.
* user’s list.

To properly review a LAN implementation, an IS auditor should first verify the network diagram and confirm the approval. Verification of nodes from the node list and the network diagram would be next, followed by a review of the acceptance test report and then the user’s list.

NEW QUESTION 95

A sender of an e-mail message applies a digital signature to the digest of the message. This action provides assurance of the:
* date and time stamp of the message.
* identity of the originating computer.
* confidentiality of the message’s content.
* authenticity of the sender.

The signature on the digest can be used to authenticate the sender. It does not provide assurance of the date and time stamp or the identity of the originating computer. Digitally signing an e-mail message does not prevent access to its content and,therefore , does not assure confidentiality.

NEW QUESTION 96

.What is the recommended initial step for an IS auditor to implement continuous-monitoring systems?
* Document existing internal controls
* Perform compliance testing on internal controls
* Establish a controls-monitoring steering committee
* Identify high-risk areas within the organization

When implementing continuous-monitoring systems, an IS auditor’s first step is to identify highrisk areas within the organization.

NEW QUESTION 97

Talking about application system audit, focus should always be placed on:
* performance and controls of the system
* the ability to limit unauthorized access and manipulation
* input of data are processed correctly
* output of data are processed correctly

* changes to the system are properly authorized
* None of the choices.

Talking about application system audit, focus should be placed on the performance and controls of the system, its ability to limit unauthorized access and manipulation, that input and output of data are processed correctly on the system, that any changes to the system are authorized, and that users have access to the system.

NEW QUESTION 98

Which of the following will prevent dangling tuples in a database?

* Cyclic integrity
* Domain integrity
* Relational integrity
* Referential integrity

Referential integrity ensures that a foreign key in one table will equal null or the value of a primary in the other table. For every tuple in a table having a referenced/foreign key, there should be a corresponding tuple in another table, i.e., forexistence of all foreign keys in the original tables, if this condition is not satisfied, then it results in a dangling tuple . Cyclical checking is the control technique for the regular checking of accumulated data on a file against authorized sourcedocumentation . There is no cyclical integrity testing. Domain integrity testing ensures that a

data item has a legitimate value in the correct range or set. Relational integrity is performed at the record level and is ensured by calculating and verifying specific fields.

NEW QUESTION 99

Which of the following is the BEST way to handle obsolete magnetic tapes before disposing of them?

* Overwriting the tapes
* initializing the tape labels
* Degaussing the tapes
* Erasing the tapes

The best way to handle obsolete magnetic tapes is to degauss them. This action leaves a very low residue of magnetic induction, essentially erasing the data from the tapes. Overwriting or erasing the tapes may cause magnetic errors but would not remove the data completely. Initializing the tape labels would not remove the data that follows the label.

NEW QUESTION 100

While executing follow-up activities, an IS auditor is concerned that management has implemented corrective actions that are different from those originally discussed and agreed the audit function. In order to resolve the situation, the IS auditor/, BEST course of action would be to:

* postpone follow-up activities and escalate the alternative controls to senior audit management
* schedule another audit due to the implementation of alternative controls.
* reject the alternative controls and re-prioritize the original issue as high risk.
* determine whether the alternative controls sufficiently mitigate the risk and record the results

NEW QUESTION 101

Receiving an EDI transaction and passing it through the communication’s interface stage usually requires:

* translating and unbundling transactions.
* routing verification procedures.
* passing data to the appropriate application system.
* creating a point of receipt audit log.

The communication’s interface stage requires routing verification procedures. EDI or ANSI X12 is a standard that must be interpreted by an application for transactions to be processed and then to be invoiced, paid and sent, whether they are for merchandise or services. There is no point in sending and receiving EDI transactions if they cannot be processed by an internal system. Unpacking transactions and recording audit logs are important elements that help follow business rules and establish controls, but are not part of the communication’s interface stage.

NEW QUESTION 102

An IS auditor finds that a required security patch was not installed on a critical server for more than 6 months. The NEXT course of action should be to:
* determine the root cause of the delay.
* review patch management procedures.
* request the patch be installed as soon as possible.
* notify senior management of audit findings.
Section: Information System Operations, Maintenance and Support

NEW QUESTION 103

What would be the major purpose of rootkit?
* to hide evidence from system administrators.
* to encrypt files for system administrators.
* to corrupt files for system administrators.
* to hijack system sessions.
* None of the choices.
Section: Protection of Information Assets

Explanation:

rootkit originally describes those recompiled Unix tools that would hide any trace of the intruder.

You can say that the only purpose of rootkit is to hide evidence from system administrators so there is no way to detect malicious special privilege access attempts.

NEW QUESTION 104

Which of the following are the characteristics of a good password?
* It has mixed-case alphabetic characters, numbers, and symbols.
* It has mixed-case alphabetic characters and numbers.
* It has mixed-case alphabetic characters and symbols.
* It has mixed-case alphabetic characters, numbers, and binary codes.
* None of the choices.
Passwords are the first defensive line in protecting your data and information. Your users need to be made aware of what a password provides them and what can be done with their password. They also need to be made aware of the things that make up a good password versus a bad password. A good password has mixed-case alphabetic characters, numbers, and symbols. Do use a password that is at least eight or more characters.

NEW QUESTION 105

The goal of an information system is to achieve integrity, authenticity and non-repudiation of information’s sent across the network. Which of the following statement correctly describe the steps to address all three?

* Encrypt the message digest using symmetric key and then send the encrypted digest to receiver along with original message.
* Encrypt the message digest using receiver’s public key and then send the encrypted digest to receiver along with original message. The receiver can decrypt the message digest using his own private key.
* Encrypt the message digest using sender’s public key and then send the encrypted digest to the receiver along with original message. The receiver can decrypt using his own private key.
* Encrypt message digest using sender’s private key and then send the encrypted digest to the receiver along with original message. Receiver can decrypt the same using sender’s public key.

Section: Protection of Information Assets

Explanation:

The digital signature is used to achieve integrity, authenticity and non-repudiation. In a digital signature, the sender’s private key is used to encrypt the message digest of the message. Encrypting the message digest is the act of Signing the message. The receiver will use the matching public key of the sender to decrypt the Digital Signature using the sender’s public key.

A digital signature (not to be confused with a digital certificate) is an electronic signature that can be used to authenticate the identity of the sender of a message or the signer of a document, and possibly to ensure that the original content of the message or document that has been sent is unchanged. Digital signatures cannot be forged by someone else who does not possess the private key, it can also be automatically time- stamped. The ability to ensure that the original signed message arrived means that the sender cannot easily repudiate it later.

A digital signature can be used with any kind of message, whether it is encrypted or not, simply so that the receiver can be sure of the sender’s identity and that the message arrived intact. A digital certificate contains the digital signature of the certificate-issuing authority so that anyone can verify that the certificate is real and has not been modified since the day it was issued.

How Digital Signature Works

Assume you were going to send the draft of a contract to your lawyer in another town. You want to give your lawyer the assurance that it was unchanged from what you sent and that it is really from you.

You copy-and-paste the contract (it’s a short one!) into an e-mail note.

Using special software, you obtain a message hash (mathematical summary) of the contract.

You then use a private key that you have previously obtained from a public-private key authority to encrypt the hash.

The encrypted hash becomes your digital signature of the message. (Note that it will be different each time you send a message.) At the other end, your lawyer receives the message.

To make sure it’s intact and from you, your lawyer makes a hash of the received message.

Your lawyer then uses your public key to decrypt the message hash or summary.

If the hashes match, the received message is valid.

Below are some common reasons for applying a digital signature to communications:

Authentication

Although messages may often include information about the entity sending a message, that information may not be accurate. Digital signatures can be used to authenticate the source of messages. The importance of high assurance in the sender authenticity is especially obvious in a financial context. For example, suppose a bank’s branch office sends instructions to the central office requesting a change in the balance of an account. If the central office is not convinced that such a message is truly sent from an authorized source, acting on such a request could be a serious mistake.

Integrity

In many scenarios, the sender and receiver of a message may have a need for confidence that the message has not been altered during transmission. Although encryption hides the contents of a message, it may be possible to change an encrypted message without understanding it.(Some encryption algorithms, known as nonmalleable ones, prevent this, but others do not.) However, if a message is digitally signed, any change in the message after the signature has been applied would invalidates the signature.

Furthermore, there is no efficient way to modify a message and its signature to produce a new message with a valid signature, because this is still considered to be computationally infeasible by most cryptographic hash functions (see collision resistance).

Non-repudiation

Non-repudiation, or more specifically non-repudiation of origin, is an important aspect of digital signatures.

By this property, an entity that has signed some information cannot at a later time deny having signed it.

Similarly, access to the public key only does not enable a fraudulent party to fake a valid signature.

Note that authentication, non-repudiation, and other properties rely on the secret key not having been revoked prior to its usage. Public revocation of a key-pair is a required ability, else leaked secret keys would continue to implicate the claimed owner of the key-pair. Checking revocation status requires an

“online” check, e.g. checking a “Certificate Revocation List” or via the “Online Certificate Status Protocol”.

This is analogous to a vendor who receives credit-cards first checking online with the credit-card issuer to find if a given card has been reported lost or stolen.

Tip for the exam

Digital Signature does not provide confidentiality. It provides only authenticity and integrity. The sender’s private key is used to encrypt the message digest to calculate the digital signature Encryption provides only confidentiality. The receiver’s public key or symmetric key is used for encryption The following were incorrect answers:

Encrypt the message digest using symmetric key and then send the encrypted digest to receiver along with original message – Symmetric key encryption does not provide non-repudiation as symmetric key is shared between users Encrypt the message digest using receiver’s public key and then send the encrypted digest to receiver along with original message. The receiver can decrypt the message digest using his own private key – Receiver’s public key is known to everyone. This will not address non-repudiation Encrypt the message digest using sender’s public key and then send the encrypted digest to the receiver along with original message. The receiver can decrypt using his own private key -The sender public key is known to everyone. If sender’s key is used for encryption, then sender’s private key is required to decrypt data. The receiver will not be able to decrypt the digest as receiver will not have sender’s private key.

Reference:

CISA review manual 2014 Page number 331

http://upload.wikimedia.org/wikipedia/commons/2/2b/Digital_Signature_diagram.svg

http://en.wikipedia.org/wiki/Digital_signature

http://searchsecurity.techtarget.com/definition/digital-signature

NEW QUESTION 106

An IS auditor reviewing an accounts payable system discovers that audit logs are not being reviewed.

When this issue is raised with management the response is that additional controls are not necessary

because effective system access controls are in place. The BEST response the auditor can make is to:
* review the integrity of system access controls.
* accept management’s statement that effective access controls are in place.
* stress the importance of having a system control framework in place.
* review the background checks of the accounts payable staff.

Section: Protection of Information Assets

Explanation:

Experience has demonstrated that reliance purely on preventative controls is dangerous. Preventative

controls may not prove to be as strong as anticipated or their effectiveness can deteriorate over time.

Evaluating the cost of controls versus the quantum of risk is a valid management concern. However, in a

high-risk system a comprehensive control framework is needed, intelligent design should permit additional

detective and corrective controls to be established that don’t have high ongoing costs, e.g., automated

interrogation of logs to highlight suspicious individual transactions or data patterns. Effective access

controls are, in themselves, a positive but, for reasons outlined above, may not sufficiently compensate for

other control weaknesses. In this situation the IS auditor needs to be proactive. The IS auditor has a

fundamental obligation to point out control weaknesses that give rise to unacceptable risks to the

organization and work with management to have these corrected. Reviewing background checks on

accounts payable staff does not provide evidence that fraud will not occur.

NEW QUESTION 107

Segregation of duties would be compromised if:
* application programmers moved programs into production.

* application programmers accessed test data.
* database administrators (DBAs) modified the structure of user tables.
* operations staff modified batch schedules.

NEW QUESTION 108

An IS auditor is reviewing the installation of a new server. The IS auditor’s PRIMARY objective is to ensure that
* security parameters are set in accordance with the organizations policies
* security parameters are set in accordance with the manufacturer’s standards
* a detailed business case was formally approved prior to the purchase.
* the procurement project invited tenders from at least three different suppliers.

Exam Details

The exam for the ISACA CISA certification is available in English, French, Italian, Turkish, Korean, German, Japanese, Spanish, Simplified Chinese, and Traditional Chinese. The test is made up of 150 multiple-choice questions covering five domains of the exam content. The time allocated for the completion is 240 minutes. The passing score is 450/800 points. To register, the applicants are expected to pay the fee. For the ISACA members, it is $575, while the non members should pay $760.
The CISA exam is computer-based and administered at the authorized PSI testing centers across the world. You can schedule your appointment for 48 hours after the payment. You can find the complete details of the test-taking process on the certification webpage. You will also find links to different preparation resources, including virtual or in-person training and practice tests. There is no penalty for incorrect answers, and your grades are determined by the number of questions you answered correctly.

CISA certification guide Q&A from Training Expert ExamcollectionPass:
https://www.examcollectionpass.com/ISACA/CISA-practice-exam-dumps.html]