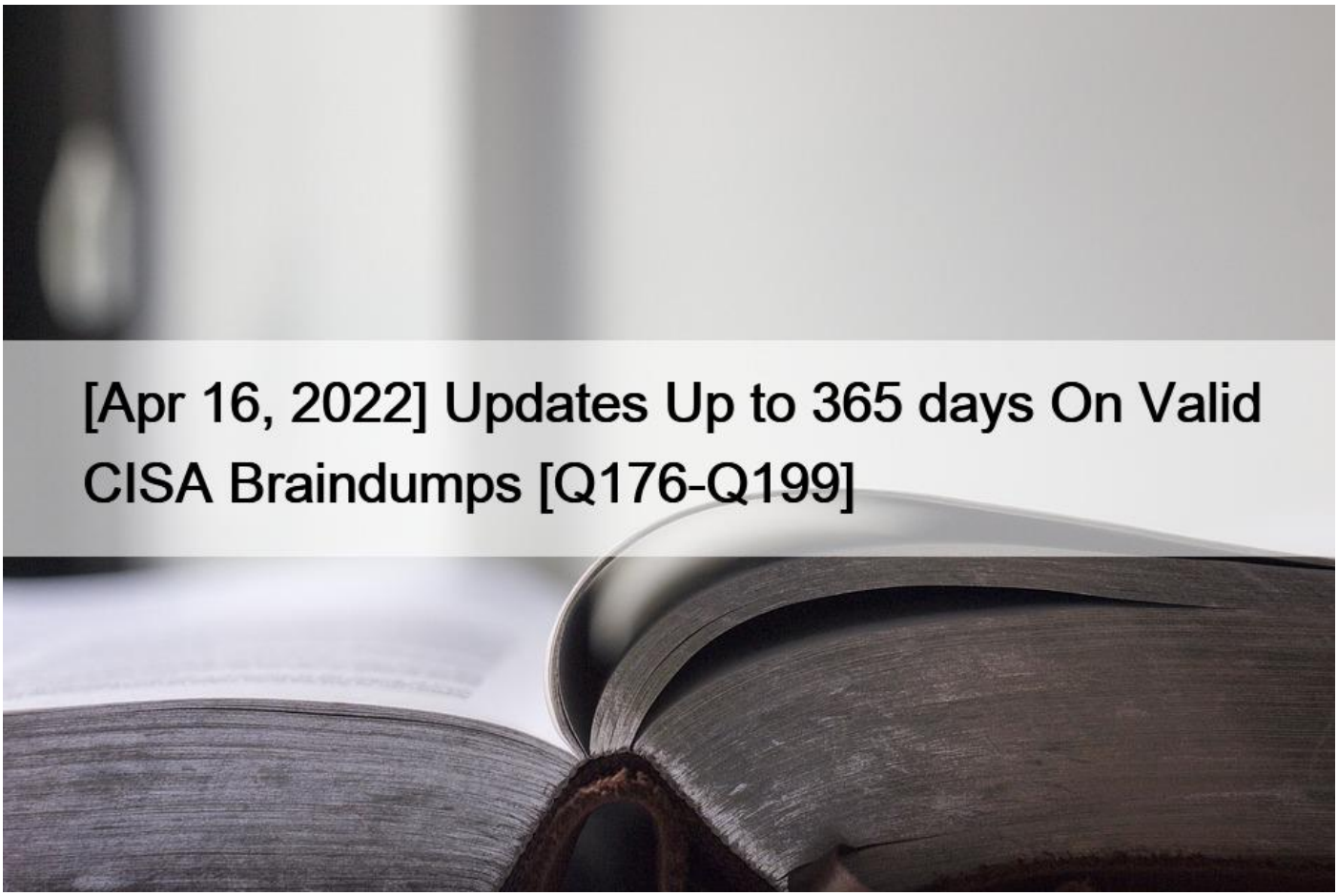
[Apr 16, 2022 Updates Up to 365 days On Valid CISA Braindumps [Q176-Q199



[Apr 16, 2022] Updates Up to 365 days On Valid CISA Braindumps
Best QualityCISA Exam Questions ISACA Test To Gain Brilliante Result

How long is CISA Certification valid?

Validity of CISA certification is for a period of 3 years from the date of issue after that you need to renew certification. ISACA will recharge some amount for this. In case the certification you have achieved is expired, you have to do all the processes from the start.

NO.176 During a review of an insurance company s claims system, the IS auditor learns that claims for specific medical procedures are acceptable only from females This is an example of a:

* logical relationship check
* key verification.
* completeness check.
* reasonableness check

NO.177 Of the three major types of off-site processing facilities, what type is characterized by at least providing for electricity and HVAC?

* Cold site

* Alternate site
* Hot site
* Warm site

Explanation/Reference:

Explanation:

Of the three major types of off-site processing facilities (hot, warm, and cold), a cold site is characterized by at least providing for electricity and HVAC. A warm site improves upon this by providing for redundant equipment and software that can be made operational within a short time.

NO.178 During the audit of an acquired software package, an IS auditor learned that the software purchase was based on information obtained through the Internet, rather than from responses to a request for proposal (RFP). The IS auditor should FIRST:

* test the software for compatibility with existing hardware.
* perform a gap analysis.
* review the licensing policy.
* ensure that the procedure had been approved.

In the case of a deviation from the predefined procedures, an IS auditor should first ensure that the procedure followed for acquiring the software is consistent with the business objectives and has been approved by the appropriate authorities. The other choices are not the first actions an IS auditor should take. They are steps that may or may not be taken after determining that the procedure used to acquire the software had been approved.

NO.179 While planning an audit, an assessment of risk should be made to provide:

* reasonable assurance that the audit will cover material items.
* definite assurance that material items will be covered during the audit work.
* reasonable assurance that all items will be covered by the audit.
* sufficient assurance that all items will be covered during the audit work.

Section: Protection of Information Assets

Explanation:

The ISACA IS Auditing Guideline G15 on planning the IS audit states, ‘An assessment of risk should be

made to provide reasonable assurance that material items will be adequately covered during the audit

work. This assessment should identify areas with a relatively high risk of the existence of material

problems.’ Definite assurance that material items will be covered during the audit work is an impractical

proposition. Reasonable assurance that all items will be covered during the audit work is not the correct

answer, as material items need to be covered, not all items.

NO.180 .Input/output controls should be implemented for which applications in an integrated systems environment?

* The receiving application
* The sending application
* Both the sending and receiving applications
* Output on the sending application and input on the receiving application

Input/output controls should be implemented for both the sending and receiving applications in an integrated systems environment

NO.181 Distributed denial-of-service (DDOS) attacks on Internet sites are typically evoked by hackers using which of the following?
* Logic bombs
* Phishing
* Spyware
* Trojan horses

Explanation/Reference:

Explanation:

Trojan horses are malicious or damaging code hidden within an authorized computer program. Hackers use Trojans to mastermind DDOS attacks that affect computers that access the same Internet site at the same moment, resulting in overloaded site servers that may no longer be able to process legitimate requests. Logic bombs are programs designed to destroy or modify data at a specific time in the future.

Phishing is an attack, normally via e-mail, pretending to be an authorized person or organization requesting information. Spyware is a program that picks up information from PC drives by making copies of their contents.

NO.182 When reviewing the procedures for the disposal of computers, which of the following should be the GREATEST concern for the IS auditor?
* Hard disks are overwritten several times at the sector level, but are not reformatted before leaving the organization.
* All files and folders on hard disks are separately deleted, and the hard disks are formatted before leaving the organization.
* Hard disks are rendered unreadable by hole-punching through the platters at specific positions before leaving the organization.
* The transport of hard disks is escorted by internal security staff to a nearby metal recycling company, where the hard disks are registered and then shredded.

Explanation/Reference:

Explanation:

Deleting and formatting does not completely erase the data but only marks the sectors that contained files as being free. There are tools available over the Internet which allow one to reconstruct most of a hard disk’s contents. Overwriting a hard disk at the sector level would completely erase data, directories, indices and master file tables. Reformatting is not necessary since all contents are destroyed. Overwriting several times makes useless some forensic measures which are able to reconstruct former contents of newly overwritten sectors by analyzing special magnetic features of the platter’s surface. While hole-punching does not delete file contents, the hard disk cannot be used anymore, especially when head parking zones and track zero information are impacted. Reconstructing data would be extremely expensive since all analysis must be performed under a clean room atmosphere and is only possible within a short time frame or until the surface is corroded. Data reconstruction from shredded hard disks is virtually impossible, especially when the scrap is mixed with other metal parts. If the transport can be secured and the destruction be proved as described in the option, this is a valid method of disposal.

NO.183 An organization can ensure that the recipients of e-mails from its employees can authenticate the identity of the sender by:
* digitally signing all e-mail messages.
* encrypting all e-mail messages.
* compressing all e-mail messages.
* password protecting all e-mail messages.

Explanation/Reference:

Explanation:

By digitally signing all e-mail messages, the receiver will be able to validate the authenticity of the sender.

Encrypting all e-mail messages would ensure that only the intended recipient will be able to open the message; however, it would not ensure the authenticity of the sender. Compressing all e-mail messages would reduce the size of the message, but would not ensure the authenticity. Password protecting all e- mail messages would ensure that only those who have the password would be able toopen the message; however, it would not ensure the authenticity of the sender.

NO.184 An IS auditor is reviewing IT policies and found that most policies have not been reviewed in over 3 years. The MOST significant risk is that the policies do not reflect.
* The vision of the CEO
* Current industry best practices
* The mission of the organization
* Current legal requirements

NO.185 Which of the following environment controls is MOST appropriate in an area where power outages lasting up to 8 hours are frequent?
* A power generator
* Data mirroring
* An alternate power supply line
* A surge protector

NO.186 Which of the following measures can protect systems files and data, respectively?
* User account access controls and cryptography
* User account access controls and firewall
* User account access controls and IPS
* IDS and cryptography
* Firewall and cryptography
* None of the choices.

User account access controls and cryptography can protect systems files and data, respectively. On the other hand, firewalls are by far the most common prevention systems from a network security perspective as they can shield access to internal network services, and block certain kinds of attacks through packet filtering.

NO.187 Which of the following types of attack makes use of common consumer devices that can be used to transfer data surreptitiously?
* Direct access attacks
* Indirect access attacks
* Port attack
* Window attack
* Social attack
* None of the choices.

Explanation/Reference:

Explanation:

Direct access attacks make use of common consumer devices that can be used to transfer data surreptitiously. Someone gaining physical access to a computer can install all manner of devices to compromise security, including operating system modifications, software worms, keyboard loggers, and covert listening devices. The attacker can also easily download large quantities of data onto backup media or portable devices.

NO.188 Which of the following are effective controls for detecting duplicate transactions such as payments made or

received?
* Concurrency controls
* Reasonableness checks
* Time stamps
* Referential integrity controls

Section: Protection of Information Assets

Explanation:

Time stamps are an effective control for detecting duplicate transactions such as payments made or

received.

NO.189 A recent audit identified duplicate software licenses and technologies Which of the following would be MOST helpful to prevent this type of duplication in the future?
* Conducting periodic inventory reviews
* Updating IT procurement policies and procedures
* Centralizing IT procurement and approval practices
* Establishing a project management office

NO.190 The MOST significant security concerns when using flash memory (e.g., USB removable disk) is that the:
* contents are highly volatile.
* data cannot be backed up.
* data can be copied.
* device may not be compatible with other peripherals.

Section: Protection of Information Assets

Explanation: Unless properly controlled, flash memory provides an avenue for anyone to copy any content

with ease. The contents stored in flash memory are not volatile. Backing up flash memory data is not a

control concern, as the data are sometimes stored as a backup. Flash memory will be accessed through a

PC rather than any other peripheral; therefore, compatibility is not an issue.

NO.191 Which of the following is the BEST control to mitigate the malware risk associated with an instant messaging (IM) system1?
* Allowing only corporate IM solutions
* Encrypting IM traffic
* Blocking external IM traffic
* Blocking attachments in IM

NO.192 Which of the following Confidentiality, Integrity, Availability (CIA) attribute supports the principle of least privilege by providing access to information only to authorized and intended users?
* Confidentiality
* Integrity
* Availability
* Accuracy

Explanation/Reference:

Confidentiality supports the principle of “least privilege” by providing that only authorized individuals, processes, or systems should have access to information on a need-to-know basis.

The level of access that an authorized individual should have is at the level necessary for them to do their job. In recent years, much press has been dedicated to the privacy of information and the need to protect it from individuals, who may be able to commit crimes by viewing the information.

Identity theft is the act of assuming one’s identity through knowledge of confidential information obtained from various sources.

An important measure to ensure confidentiality of information is data classification. This helps to determine who should have access to the information (public, internal use only, or confidential). Identification, authentication, and authorization through access controls are practices that support maintaining the confidentiality of information.

A sample control for protecting confidentiality is to encrypt information. Encryption of information limits the usability of the information in the event it is accessible to an unauthorized person.

For your exam you should know the information below:

Integrity

Integrity is the principle that information should be protected from intentional, unauthorized, or accidental changes.

Information stored in files, databases, systems, and networks must be relied upon to accurately process transactions and provide accurate information for business decision making. Controls are put in place to ensure that information is modified through accepted practices.

Sample controls include management controls such as segregation of duties, approval checkpoints in the systems development life cycle, and implementation of testing practices that assist in providing information integrity. Well-formed transactions and security of the update programs provide consistent methods of applying changes to systems. Limiting update access to those individuals with a need to access limits the exposure to intentional and unintentional modification.

Availability

Availability is the principle that ensures that information is available and accessible to users when needed.

The two primary areas affecting the availability of systems are:

1. Denial-of-Service attacks and

2. Loss of service due to a disaster, which could be man-made (e.g., poor capacity planning resulting in system crash, outdated hardware, and poor testing resulting in system crash after upgrade) or natural (e.g., earthquake, tornado, blackout, hurricane, fire, and flood).

In either case, the end user does not have access to information needed to conduct business. The criticality of the system to the user and its importance to the survival of the organization will determine how significant the impact of the extended downtime becomes. The lack of appropriate security controls can increase the risk of viruses, destruction of data, external penetrations, or denial-of-service (DOS) attacks.

Such events can prevent the system from being used by normal users.

CIA

The following answers are incorrect:

Integrity- Integrity is the principle that information should be protected from intentional, unauthorized, or accidental changes.

Availability – Availability is the principle that ensures that information is available and accessible to users when needed.

Accuracy – Accuracy is not a valid CIA attribute.

Following reference(s) were/was used to create this question:

CISA review manual 2014 Page number 314

Official ISC2 guide to CISSP CBK 3rd Edition Page number350

NO.193 Which of the following could an IS auditor recommend to improve the estimated resources required in

system development?
* Business areas involvement
* Prototyping
* Function point analysis
* CASE tools

Section: Information System Acquisition, Development and Implementation

NO.194 During a software acquision review, an IS auditor should recommend that there be a software escrow agreement when:
* There is no service level agreement (SLA)
* The product is new in the market
* The estimated life for the product is less than 3 years
* The deliverables do not include the source code

NO.195 An IS auditor observes a weakness in the tape management system at a data center in that some parameters are set to bypass or ignore tape header records. Which of the following is the MOST effective compensating control for this weakness?
* Staging and job set up
* Supervisory review of logs
* Regular back-up of tapes
* Offsite storage of tapes

Section: Protection of Information Assets

Explanation:

If the IS auditor finds that there are effective staging and job set up processes, this can be accepted as a compensating control. Choice B is a detective control while choices C and D are corrective controls, none of which would serve as good compensating controls.

NO.196 Documentation of a business case used in an IT development project should be retained until:
* the end of the system’s life cycle.
* the project is approved.
* user acceptance of the system.
* the system is in production.

Explanation/Reference:

Explanation:

A business case can and should be used throughout the life cycle of the product. It serves as an anchor for new (management) personnel, helps to maintain focus and provides valuable information on estimates vs.

actuals. Questions like, ‘why do we do that,”what was the original intent’ and ‘how did we perform against the plan’ can be answered, and lessons for developing future business cases can be learned. During the development phase of a project one should always validate the business case, as it is a good management instrument. After finishing a project and entering production, the business case and all the completed research are valuable sources of information that should be kept for further reference

NO.197 Which of the following will BEST help to ensure that an in-house application in the production environment is current?
* Version control procedures
* Change management
* Production access control
* Quality assurance

NO.198 An IS auditor is reviewing an organization’s incident management processes and procedures. Which of the following observations should be the auditor’s GREATEST concern?
* Ineffective incident classification
* Ineffective incident prioritization
* Ineffective incident detection
* Ineffective post-incident review

Section: The process of Auditing Information System

NO.199 Which of the following BEST ensures the confidentiality of sensitive data during transmission?
* Sending data through proxy servers
* Restricting the recipient through destination IP addresses
* Password protecting data over virtual local area networks (VLAN)
* Sending data over public networks using Transport Layer Security (TLS)

The benefits of Obtaining the ISACA CISA Exam Certification

ISACA CISA certification is often preferred by employers. You can have many benefits of obtaining the ISACA CISA exam by doing preparation from **ISACA CISA Dumps**.

Candidates who have obtained any of the following certifications are eligible to apply for the CISA credential: Certified Information Systems Auditor (CISA), Certified Information Security Manager (CISM), Certified in the Governance of Enterprise IT (CGEIT), Certified in Risk and Information Systems Control (CRISC), Certified Software Development Asset Manager(CSDAM), International Information Systems Security Certification Consortium's Certified Internet Webmaster.

Focus on CISA All-in-One Exam Guide For Quick Preparation: https://www.topexamcollection.com/CISA-vce-collection.html]