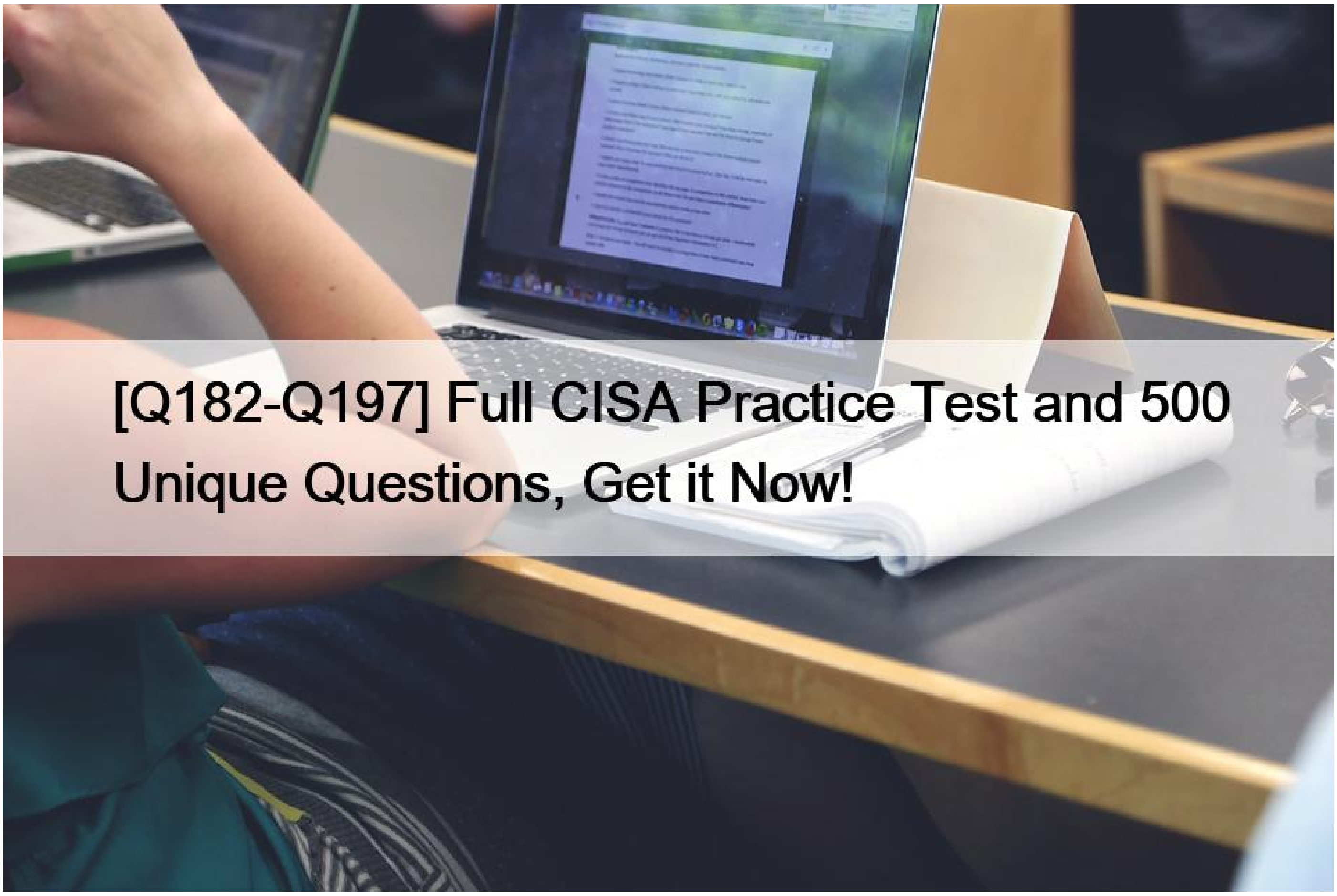
[Q182-Q197 Full CISA Practice Test and 500 Unique Questions, Get it Now!



Full CISA Practice Test and 500 Unique Questions, Get it Now!
The Best CISA Exam Study Material Premium Files and Preparation Tool

NO.182 Which of the following is the MOST effective way to achieve the integration of information security governance into corporate governance?
* Ensure information security aligns with IT strategy.
* Provide periodic IT balanced scorecards to senior management.
* Align information security budget requests to organizational goals.
* Ensure information security efforts support business goals.
Section: Governance and Management of IT

NO.183 Which of the following would BEST help to support an auditor&#8217;s conclusion about the effectiveness of an implemented data classification program?
* Detailed data classification scheme
* Access rights provisioned according to scheme
* Business use cases and scenarios
* Purchase of information management tools
Section: Protection of Information Assets

NO.184 The technique used to ensure security in virtual private networks (VPNs) is:
* encapsulation.
* wrapping.
* transform.
* encryption.
Explanation/Reference:

Explanation:

Encapsulation, or tunneling, is a technique used to carry the traffic of one protocol over a network that does not support that protocol directly. The original packet is wrapped in another packet. The other choices are not security techniques specific to VPNs.

NO.185 Which of the following is the BEST way to ensure enterprise architectural objectives are aligned with business and technology objectives?
* Identify dependencies between current and future state technologies.
* Adopt industry-approved architecture standards and best practices.
* Optimize technology investments with business requirements.
* Identify business stakeholder responsibilities for IT projects.

NO.186 Which of the following is the MOST important privacy consideration for an organization that uses a cloud service provider to process customer data?
* Data privacy must be monitored in accordance with industry standards and best practices.
* All customer data transferred to the service provider must be reported to the regulatory authority.
* No personal information may be transferred to the service provider without the consent of the customer.
* Data privacy must be managed in accordance with the regulations applicable to the organization.
Section: Information System Acquisition, Development and Implementation

NO.187 A small organization is experiencing rapid growth and plans to create a new information security policy.

Which of the following is MOST relevant to creating the policy?
* Industry standards
* The business objectives
* The business impact analysis (BIA)
* Previous audit recommendations

NO.188 Which of the following ensures confidentiality of information sent over the internet?
* Digital signature
* Digital certificate
* Online Certificate Status Protocol
* Private key cryptosystem
Explanation/Reference:

Explanation:

Confidentiality is assured by a private key cryptosystem. Digital signatures assure data integrity, authentication and nonrepudiation, but not confidentially. A digital certificate is a certificate that uses a digital signature to bind together a public key with an identity; therefore, it does not address confidentiality.

Online Certificate Status Protocol (OCSP) is an Internet protocol used for obtaining the revocation status of a digital certificate.

NO.189 During a disaster recovery audit, an IS auditor finds that a business impact analysis (BIA) has not been performed. The auditor should FIRST

* perform a business impact analysis (BIA).
* issue an intermediate report to management.
* evaluate the impact on current disaster recovery capability.
* conduct additional compliance testing.

NO.190 Which of the following is MOST important for an IS auditor to examine when reviewing an organization&#8217;s privacy policy?

* The encryption mechanism selected by the organization for protecting personal data
* Whether there is explicit permission from regulators to collect personal data
* The organization&#8217;s legitimate purpose for collecting personal data
* Whether sharing of personal information with third-party service providers is prohibited

NO.191 An efficient use of public key infrastructure (PKI) should encrypt the:

* entire message.
* private key.
* public key.
* symmetric session key.

Public key (asymmetric) cryptographic systems require larger keys (1,024 bits) and involve intensive and time-consuming computations. In comparison, symmetric encryption is considerably faster, yet relies on the security of the process for exchanging the secret key. To enjoy the benefits of both systems, a symmetric session key is exchanged using public key methods, after which it serves as the secret key for encrypting/decrypting messages sent between two parties.

NO.192 A manufacturing firm wants to automate its invoice payment system. Objectives state that the system should require considerably less time for review and authorization and the system should be capable of identifying errors that require follow up. Which of the following would BEST meet these objectives?

* Establishing an inter-networked system of client servers with suppliers for increased efficiencies
* Outsourcing the function to a firm specializing in automated payments and accounts receivable/invoice processing
* Establishing an EDI system of electronic business documents and transactions with key suppliers, computer to computer, in a standard format
* Reengineering the existing processing and redesigning the existing system

Explanation/Reference:

Explanation:

EDI is the best answer. Properly implemented (e.g., agreements with trading partners transaction standards, controls over network security mechanisms in conjunction with application controls), EDI is best suited to identify and follow up on errors more quickly, given reduced opportunities for review and authorization.

NO.193 Which function in the purchasing module of an enterprise resource planning (ERP) system ensures payments are not issued for incorrect invoices&#8217;

* Sequential payment numbers
* Management workflow approval
* Three-way match
* Purchasing authority levels

NO.194 Which of the following should be the PRIMARY consideration when developing an IT strategy?

* Alignment with the IT investment portfolio

* IT key performance indicators based on business objectives
* Short and long-term plans for the enterprise IT architecture
* Alignment with overall business objectives

NO.195 Which of the following would be MOST useful to an IS auditor confirming that an IS department meets its service level agreements (SLAs)?
* System utilization reports
* System downtime reports
* IS strategic plan
* Capacity planning tools

NO.196 Which of the following is the BEST way to mitigate the risk associated with malicious changes to binary code during the software development life cycle (SDLC)?
* Parity check
* Digital envelope
* Segregation of duties
* Cryptographic hash

NO.197 After discovering a security vulnerability in a third-party application that interfaces with several external systems, a patch is applied to a significant number of modules. Which of the following tests should an IS auditor recommend?
* Stress
* Black box
* Interface
* System
Section: Protection of Information Assets

Explanation:

Given the extensiveness of the patch and its interfaces to external systems, system testing is most appropriate. Interface testing is not enough, and stress or black box testing are inadequate in these circumstances.