Isaca.Premium.CISA.207q - DEMO

Exam Code: CISA
Exam Name: Certified Information Systems Auditor
Certification Provider: Isaca
Corresponding Certification: CISA

Topic 1, Exam Pool A

Question No: 1

Which of the following system conversion strategies provides the GREATEST redundancy?

A. Pilot study

B. Phased approach

C. Direct cutover

D. Parallel run

Answer: D

Explanation:

Question No: 2

A USB device containing sensitive production data was lost by an employee and its contents were subsequently found published online Which of the following controls is the BEST recommendation to prevent a similar recurrence?

A. Training users on USB device security

B. Monitoring data being downloaded on USB devices

C. Electronically tracking portable devices

D. Using a strong encryption algorithm

Answer: D

Explanation:

Question No: 3

Following significant organizational changes, which of the following is the MOST important consideration when updating the IT policy?

A. The policy is integrated into job descriptions.

B. The policy is endorsed by senior executives.

C. The policy is compliant with relevant laws and regulations.

D. The policy is aligned with industry standards and best practice.

Answer: C

Explanation:

Question No: 4

Which of the following would be the GREATEST risk associated with a new chat feature on a retailer's website?

A. Productivity loss

B. Reputational damage

C. System downtime

D. Data loss

Answer: C

Explanation:

Question No: 5

Which of the following should be the MOST important consideration when prioritizing the funding for competing IT projects?

A. Quality and accuracy of the IT project inventory

B. Senior management preferences

C. Criteria used to determine the benefits of projects

D. Skill and capabilities within the project management team

Answer: B

Explanation:

Question No: 6

Which of the following would an IS auditor consider the GREATEST risk associated with a mobile workforce environment?

A. Lack of compliance with organizational policies

B. Decrease in employee productivity and accountability

C. Loss or damage to the organization's assets

D. Inability to access data remotely

Answer: D

Explanation:

Question No: 7

An organization experienced a domain name system (DNS) attack caused by default user accounts not being removed from one of the servers. Which of the following would have been the BEST way to mitigate the risk of this DNS attack?

A. Configure the servers from an approved standard configuration

B. Require all employees to attend training for secure configuration management

C. Have a third party configure the virtual servers

D. Configure the intrusion prevention system (IPS) to identify DNS attacks

Answer: A

Explanation:

Question No: 8

An organization is running servers with critical business application that are in an area subject to frequent but brief power outages. Knowledge of which of the following would allow the organization’s management to monitor the ongoing adequacy of the uninterruptable power supply

(UPS)?

A. Number of servers supported by the ups

B. Duration and interval of the power outages

C. Business impact of server downtime

D. Mean time to recover servers after failure

Answer: B

Explanation:

Question No: 9

Reconciliations have identified data discrepancies between an enterprise data warehouse and a revenue system for key financial reports. What is the GREATEST risk to the organization in this situation?

A. Financial reports may be delayed.

B. Undetected fraud may occur.

C. The key financial reports may no longer be produced.

D. Decisions may be made based on incorrect information

Answer: D

Explanation:

Question No: 10

Which of the following should be the MOST important consideration when prioritizing the funding for competing IT projects?

A. Quality and accuracy of the IT project inventory

B. Senior management preferences

C. Criteria used to determine the benefits of projects

D. Skill and capabilities within the project management team

Answer: B

Explanation:

Question No: 11

Which of the following is a characteristic of a single mirrored data center used for disaster recovery?

A. The mirrored data center does not require staffing.

B. Real-time data replication occurs from the production site

C. Data replication to the mirrored site should continue after failover

D. The mirrored site may create brief interruptions noticeable to users

Answer: C

Explanation:

Question No: 12

A computer forensic audit is MOST relevant in which of the following situations?

VCEûp

A. Missing server patches

B. Data loss due to hacking of servers

C. Inadequate controls in the IT environment

D. Mismatches in transaction data

Answer: B

Explanation:

Question No: 13

Which of the following is the PRIMARY reason for using a digital signature?

A. Provide confidentiality to the transmission

B. Authenticate the sender of a message

C. Verify the integrity of the data and the identity of the recipient

D. Provide availability to the transmission

Answer: C

Explanation:

Question No: 14

The PRIMARY benefit of information asset classification is that it:

VCEûp

A. facilitates budgeting accuracy.

B. enables risk management decisions.

C. prevents loss of assets.

D. helps to align organizational objectives.

Answer: B

Explanation:

Question No: 15

An organization's information security department has recently created a centralized governance model to ensure that network-related findings are remediated within the service level agreement (SLA). What should the IS auditor use to assess the maturity and capability of this governance model?

A. Key performance indicators (KPIs)

B. Key data elements

C. Key risk indicators (KRIs)

D. Key process controls

Answer: A

Explanation:

VCEûp

Question No: 16

Which of the following observations would an IS auditor consider the GREATEST risk when conducting an audit of a virtual server farm for potential software vulnerabilities?

A. A variety of guest operating systems operate on one virtual server.

B. The hypervisor is updated quarterly.

C. Antivirus software has been implemented on the guest operating system only.

D. Guest operating systems are updated monthly

Answer: C

Explanation:

Question No: 17

Which of the following cloud deployment models would BEST meet the needs of a startup software development organization with limited initial capital?

A. Community

B. Public

C. Hybrid

D. Private

Answer: B

Explanation:

VCEûp

Question No: 18

An organization's software developers need access to personally identifiable information (Pll) stored in a particular data format. Which of the following is the BEST way to protect this sensitive information while allowing the developers to use it in development and test environments?

A. Data encryption

B. Data tokenization

C. Data abstraction

D. Data masking

Answer: D

Explanation:

Question No: 19

Which of the following is MOST likely to ensure that an organization's systems development meets its business objectives?

A. A focus on strategic projects

B. Business owner involvement

C. A project plan with clearly identified requirements

D. Segregation of systems development and testing

Answer: B

Explanation:

Question No: 20

Which of the following is the GREATEST risk associated with the lack of an effective data privacy program?

A. Inability to obtain customer confidence

B. Inability to manage access to private or sensitive data

C. Failure to comply with data-related regulations

D. Failure to prevent fraudulent transactions

Answer: C

Explanation:

Question No: 21

An organization is considering allowing users to conned personal devices to the corporate network.

Which of the following should be done FIRST?

A. Configure users on the mobile device management (MDM) solution.

B. Conduct security awareness training.

C. Implement an acceptable use policy.

D. Create inventory records of personal devices.

Answer: C

Explanation:

Question No: 22

To develop meaningful recommendations for findings, which of the following is MOST important for an IS auditor to determine and understand?

A. Root cause

B. Criteria

C. Responsible party

D. Impact

Answer: A

Explanation:

Question No: 23

Which of the following reports would provide the GREATEST assurance to an IS auditor about the controls of a third party that processes critical data for the organization?

A. Independent control assessment

B. Black box penetration test report

C. Vulnerability scan report

D. The third party's control self-assessment (CSA)

Answer: A

Explanation:

Question No: 24

Which of the following is an IS auditor s GREATEST concern when an organization does not regularly update software on individual workstations in the internal environment?

A. The organization may be more susceptible to cyber-attacks.

B. The organization may not be in compliance with licensing agreement.

C. System functionality may not meet business requirements.

D. The system may have version control issues.

Answer: D

Explanation:

Question No: 25

An IS auditor reviewing a project to acquire an IT-based solution learns the risk associated with project failure has been assessed as high. What is the auditor's BEST course of action?

A. Reassess project costs to ensure they are within the organization's risk tolerance.

B. Review the risk monitoring process during project execution.

C. Review benefits realization against the business case.

D. Inform management about potential losses due to project failure.

Answer: C

Explanation:

Question No: 26

Which of the following is the PRIMARY concern when negotiating a contract for a hot site?

A. Availability of the site in the event of multiple disaster declarations

B. Coordination with the site staff in the event of multiple disaster declarations

C. Reciprocal agreements with other organizations

D. Complete testing of the recovery plan

Answer: A

Explanation:

Question No: 27

Which of the following is the BEST way to ensure that business continuity plans (BCPs) will work effectively in the event of a major disaster?

A. Regularly update business impact assessments

VCEûp

B. Prepare detailed plans for each business function.

C. Involve staff at all levels in periodic paper walk-through exercises

D. Make senior managers responsible for their plan sections.

Answer: A

Explanation:

Question No: 28

An IS auditor is evaluating the risk associated with moving from one database management system

(DBMS) to another. Which of the following would be MOST helpful to ensure the integrity of the system throughout the change?

A. Preserving the same data inputs

B. Preserving the same data interfaces

C. Preserving the same data classifications

D. Preserving the same data structure

Answer: A

Explanation:

Question No: 29

Which audit approach is MOST helpful in optimizing the use of IS audit resources?

VCEûp

A. Outsourced auditing

B. Continuous auditing

C. Agile auditing

D. Risk-based auditing

Answer: D

Explanation:

Question No: 30

Which of the following measures BEST mitigates the risk of exfiltration during a cyber attack?

A. Perimeter firewall

B. Data loss prevention (DLP) system

C. Network access controls (NAC)

D. Hashing of sensitive data

Answer: C

Explanation:

Question No: 31

An IS audit of notes the transaction processing times in an order processing system have significantly increased after a major release Which of the following should the IS auditor review FIRST?

A. Training plans

B. Stress testing results

C. Capacity management plan

D. Database conversion results

Answer: B

Explanation:

Question No: 32

Which of the following controls BEST ensures appropriate segregation of duties within an accounts payable department?

A. Restricting program functionality according to user security profiles

B. Restricting access to update programs to accounts payable staff only

C. Including the creators user ID as a field in every transaction record created

D. Ensuring that audit trails exist for transactions

Answer: A

Explanation:

Question No: 33

Which of the following would be a result of utilizing a top-down maturity model process?

A. Identification of older, more established processes to ensure timely review

B. Identification of processes with the most improvement opportunities

C. A means of comparing the effectiveness of other processes within the enterprise

D. A means of benchmarking the effectiveness of similar processes with peers

Answer: B

Explanation:

Question No: 34

An IS auditor is examining a front-end sub ledger and a main ledger Which of the following would be the GREATEST concern if there are flaws in the mapping of accounts between the two systems?

A. Double-posting of a single journal entry

B. Inaccuracy of financial reporting

C. Unauthorized alteration of account attributes

D. inability to support new business Transactions

Answer: B

Explanation:

VCEup

Question No: 35

An organization has begun using social media to communicate with current and potential clients.

Which of the following should be of PRIMARY concern to the auditor?

A. Reduced productivity of staff using social media

B. Using a third-party provider to host and manage content

C. Lack of guidance on appropriate social media usage and monitoring

D. Negative posts by customers affecting the organization's image

Answer: C

Explanation:

Question No: 36

A client/server configuration will:

A. keep track of all the clients using the IS facilities of a service organization.

B. limit the clients and servers relationship by limiting the IS facilities to a single hardware system.

C. enhance system performance through the separation of front-end and back-end processes.

D. optimize system performance by having a server on a front-end and clients on a host.

Answer: C

VCEup

Explanation:

Question No: 37

Which of the following approaches would utilize data analytics to facilitate the testing of a new account creation process?

A. Review new account applications submitted in the past month for invalid dates of birth

B. Evaluate configuration settings for the date of birth field requirements.

C. Review the business requirements document for date of birth field requirements.

D. Attempt to submit new account applications with invalid dates of birth

Answer: A

Explanation:

Question No: 38

Which of the following is the BEST way for an IS auditor to validate that employees have been made aware of the organization's information security policy?

A. Interview employees to determine their level of understanding of the policy

B. Compare the employee roster against a list of those who attended security training

C. Review HR records for employee violations of the information security policy.

D. Review the training process to determine how policies are explained to employees

VCEûp

Answer: A

Explanation:

Question No: 39

Which of the following should be the PRIMARY objective of conducting an audit follow-up of management action plans?

A. To verify that risks listed in the audit report have been properly mitigated

B. To identify new risks and controls for the organization

C. To align the management action plans with business requirements

D. To ensure senior management is aware of the audit finidings.

Answer: A

Explanation:

Question No: 40

An organization sends daily backup media by courier to an offsite location. Which of the following provides the BEST evidence that the media is transported reliably?

A. Documented backup media transport procedures

B. Signed acknowledgments by offsite manager

C. Certification of the courier company

D. Delivery schedule of the backup media.

VCEûp

Answer: B

Explanation:

Question No: 41

Which of the following findings should be of GREATEST concern to an IS auditor performing a review of IT operations?

A. Operations shift turnover logs are not utilized to coordinate and control the processing environment.

B. Changes to the job scheduler application's parameters are not approved reviewed by an operations supervisor.

C. Access to the job scheduler application has not been restricted to a maximum of two start members

D. The job scheduler application has not been designed to display pop-up error

Answer: B

Explanation:

Question No: 42

Code changes are compiled and placed in a change folder by the developer. An implementation learn migrates changes to production from the change folder. Which of the following BEST indicates separation of duties is in place during the migration process?

A. A second individual performs code review before the change is released to production.

B. The implementation team does not have access to change the source code.

C. The implementation team does not have experience writing code.

D. The developer approves changes prior to moving them to the change folder.

Answer: B

Explanation:

Question No: 43

Which of the following would BEST help to ensure the availability of data stored with a cloud provider?

A. Requiring the provider to conduct daily backups

B. Defining service level agreements (SLAs) in the contract

C. Defining the reporting process and format

D. Confirming the cloud provider has a disaster recovery site

Answer: B

Explanation:

Question No: 44

Which of the following should be done FIRST when planning a penetration test?

A. Execute nondisclosure agreements (NDAs).

B. Define the testing scope.

C. Determine reporting requirements for vulnerabilities

D. Obtain management consent for the testing

Answer: D

Explanation:

Question No: 45

Cross-site scripting (XSS) attacks are BEST prevented through:

A. use of common industry frameworks.

B. secure coding practices.

C. application firewall policy settings.

D. a three-tier web architecture.

Answer: B

Explanation:

Question No: 46

Which of the following is the GREATEST risk associated with conducting penetration testing on a business-critical application production environment?

A. System owners may not be informed in advance

B. Results may differ from those obtained in the test environment

C. Data integrity may become compromised

D. This type of testing may not adhere to audit standards

Answer: C

Explanation:

Question No: 47

Which of the following is an example of a corrective control?

A. Generating automated batch job failure notifications

B. Employing only qualified personnel to execute tasks

C. Restoring system information from data backups

D. Utilizing processes that enforce segregation of duties

Answer: C

Explanation:

Question No: 48

An IS auditor is analysing a sample of assesses recorded on the system log of an application. The auditor intends to launch an intensive investigation if one exception is found. Which sampling method would be appropriate?

A. Stratified sampling

B. Variable sampling

C. Judgemental sampling

D. Discovery sampling

Answer: D

Explanation:

Question No: 49

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?

A. Reputational damage due to potential identity theft

B. Business disruption if a data restore cannot be completed

C. The cost of recreating the missing backup tapes

D. Human resource cost of responding to the incident

Answer: A

Explanation:

Question No: 50

Due to system limitations, segregation of duties (SoD) cannot be enforced in an accounts payable system. Which of the following is the IS auditor s BEST recommendation for a compensating control?

VCEup

A. Restrict payment authorization to senior staff members

B. Review payment transaction history.

C. Require written authorization for all payment transactions.

D. Reconcile payment transactions with invoices.

Answer: D

Explanation:

Question No: 51

An audit has identified that business units have purchased cloud-based applications without ITs support. What is the GREATEST risk associated with this situation?

A. The applications could be modified without advanced notice.

B. The application purchases did not follow procurement policy.

C. The applications are not included in business continuity plans (BCPs).

D. The applications may not reasonably protect data.

Answer: C

Explanation:

Question No: 52

Which of the following provides the MOST comprehensive description of IT's role in an organization?

VCEup

A. IT job description

B. IT organizational chart

C. IT charter

D. IT project portfolio

Answer: C

Explanation:

Question No: 53

An organization is disposing of a system containing sensitive data and has deleted all files from the hard disk. An IS auditor should be concerned because:

A. backup copies of files were not deleted as well.

B. deleting all files separately is not as efferent as formatting the hard disk,

C. deleting the files logically does not overwrite the files' physical data,

D. deleted data cannot easily be retrieved.

Answer: C

Explanation:

Question No: 54

VCEûp

Which of the following would BEST enable an organization to address the security risks associated with a recently implemented bring your own device (BYOD) strategy?

A. Mobile device testing program

B. Mobile device tracking program

C. Mobile device awareness program

D. Mobile device upgrade program

Answer: C

Explanation:

Question No: 55

Which of the following is MOST critical for the effective implementation of IT governance?

A. Documented policies

B. Internal auditor commitment

C. Strong risk management practices

D. Supportive corporate culture

Answer: D

Explanation:

Question No: 56

VCEûp

Which of the following is a corrective control?

A. Reviewing user access rights for segregation of duties

B. Executing emergency response plans

C. Verifying duplicate calculations in data processing

D. Separating equipment development, testing, and production

Answer: B

Explanation:

Question No: 57

The PRIMARY objective of value delivery in reference to IT governance is to:

A. optimize investments

B. ensure compliance,

C. promote best practices.

D. increase efficiency.

Answer: A

Explanation:

Question No: 58

Which of the following is the MOST important consideration for an IS auditor when assessing the adequacy of an organizations information security policy?

A. Business objectives

B. Alignment with the IT tactical plan

C. Compliance with industry best practice

D. IT steering committee minutes

Answer: A

Explanation:

Question No: 59

Which of the following is the BEST indicator of the effectiveness of signature-based intrusion detection systems (IDSs)?

A. An increase in the number of internally reported critical incidents

B. An increase in the number of detected incidents not previously identified

C. An increase in the number of identified false positives

D. An increase in the number of unfamiliar sources of intruders

Answer: D

Explanation:

Question No: 60

The implementation of an IT governance framework requires that the board of directors of an organization:

A. address technical IT issues.

B. be informed of all IT initiatives.

C. approve the IT strategy.

D. have an IT strategy committee.

Answer: B

Explanation:

Question No: 61

Which of the following is the MOST effective control to ensure electronic records beyond their retention periods are deleted from IT systems?

A. Build in system logic to trigger data deletion at predefined times.

B. Perform a sample check of current data against the retention schedule.

C. Review the record retention register regularly to initiate data deletion.

D. Execute all data deletions at a predefined month during the year.

Answer: B

Explanation:

Question No: 62

Which of the following yields the HIGHEST level of system availability?

A. Cloud storage

B. Hot swaps

C. Backups

D. Real-time replication

Answer: D

Explanation:

Question No: 63

Which of the following is the MOST effective way to maintain network integrity when using mobile devices?

A. Perform network reviews

B. Review access control lists.

C. Implement network access control.

D. Implement outbound firewall rules

Answer: C

Explanation:

Question No: 64

Which of the following observations noted during a review of the organization s social media practices should be of MOST concern to the IS auditor?

A. The organization does not require approval for social media posts.

B. Not all employees using social media have attended the security awareness program.

C. The organization does not have a documented social media policy.

D. More than one employee is authorized to publish on social media on behalf of the organization

Answer: A

Explanation:

Question No: 65

Which of the following BEST enables an organization to quantify acceptable data loss in the event of a disaster?

A. Availability of backup software

B. Recovery point objective (RPO)

C. Recovery time objective (RTO)

D. Mean time to recover (MTTR)

Answer: B

Explanation:

Question No: 66

When reviewing a data classification scheme, it is MOST important for an IS auditor to determine if.

A. each information asset is to a assigned to a different classification.

B. the security criteria are clearly documented for each classification

C. Senior IT managers are identified as information owner.

D. the information owner is required to approve access to the asset

Answer: B

Explanation:

Question No: 67

Which of the following would be of GREATEST concern to an IS auditor reviewing backup and recovery controls?

A. Backups are stored in an external hard drive

B. Restores from backups are not periodically tested

C. Backup procedures are not documented

D. Weekly and monthly backups are stored onsite

Answer: A

Explanation:

Question No: 68

Which of the following is MOST important when creating a forensic image of a hard drive?

A. Requiring an independent third-party be present while imaging

B. Choosing an industry-leading forensics software tool

C. Securing a backup copy of the hard drive

D. Generating a content hash of the hard drive

Answer: D

Explanation:

Question No: 69

Which of the following findings should be of GREATEST concern for an IS auditor when auditing the effectiveness of a phishing simulation test administered for staff members?

A. Test results were not communicated to staff members

B. Staff members who failed the test did not receive follow-up education

C. Security awareness training was not provided poor to the test

D. Staff members were not notified about the test beforehand

Answer: B

Explanation:

Question No: 70

During an audit of an organization's financial statements, an IS auditor finds that the IT general controls are deficient. What should the IS auditor recommend?

A. Increase the substantive testing of the financial balances.

B. Place greater reliance on the framework of control.

C. Place greater reliance on the application controls.

D. Increase the compliance testing of the application controls.

Answer: D

Explanation:

Question No: 71

Which of the following is an IS auditor's BEST recommendation to mitigate the risk of eavesdropping associated with an application programming interface (API) integration implementation?

A. Implement Transport Layer Security (TLS)

B. Implement Simple Object Access Protocol (SOAP)

C. Encrypt the extensible markup language (XML) file

D. Mask the API endpoints

Answer: A

Explanation:

Question No: 72

An IS auditor finds that one employee has unauthorized access to confidential dat a. The IS auditor's BEST recommendation should be to:

A. recommend corrective actions to be taken by the security administrator.

B. reclassify the data to a lower level of confidentiality.

C. implement a strong password schema for users,

D. require the business owner to conduct regular access reviews.

Answer: D

Explanation:

Question No: 73

An IS auditor finds that an organization's data toss prevention (DLP) system is configured to use vendor default settings to identify violations. The auditor's MAIN concern should be that:

A. violations may not be categorized according to the organization's risk profile.

B. a significant number of false positive violations may be reported.

C. violation reports may not be retained according to the organization's risk profile.

D. violation reports may not be reviewed in a timely manner.

Answer: A

Explanation:

Question No: 74

Which of the following is MOST important for an organization to complete prior to developing its disaster recovery plan (DRP)?

A. Risk assessment

B. Business impact analysis (BIA)

C. Comprehensive IT inventory

D. Support staff skills gap analysis

Answer: B

Explanation:

Question No: 75

Which of the following metrics would be MOST useful to an IS auditor when assessing the resilience of an application programming interface (API)?

A. Number of patches released within a time interval for the API

B. Number of API calls expected versus actually received within a time interval

C. Number of defects logged during development compared to other APIs

D. Number of developers adopting the API for their applications

Answer: B

Explanation:

Question No: 76

Which of the following is the GREATEST concern associated with control self-assessments (CSAs)?

A. Controls may not be assessed objectively.

B. The assessment may not provide sufficient assurance to stakeholders.

C. Employees may have insufficient awareness of controls.

D. Communication between operational management and senior management may not be effective.

Answer: B

Explanation:

Question No: 77

The practice of periodic secure code reviews is which type of control?

A. Preventive

B. Compensating

C. Corrective

D. Detective

Answer: A

Explanation:

Question No: 78

A data Breach has occurred due to malware. Which of the following should be the FIRST course of action?

A. Notify the cyber insurance company.

B. Notify customers of the breach.

C. Shut down the affected systems.

D. Quarantine the impacted systems.

Answer: D

Explanation:

Question No: 79

Following a recent internal data breach, an IS auditor was asked to evaluate information security practices within the organization. Which of the following findings would be MOST important to report to senior management?

A. Desktop passwords do not require special characters

B. Employees are not required to sign a non-compete agreement.

C. Users lack technical knowledge related to security and data protection

D. Security education and awareness workshops have not been completed

Answer: B

Explanation:

Question No: 80

An IS department is evaluated monthly on its cost-revenue ratio user satisfaction rate, and computer downtime This is BEST zed as an application of.

A. risk framework

B. balanced scorecard

C. value chain analysis

D. control self-assessment (CSA)

Answer: B

Explanation:

Question No: 81

Which of the following Is a challenge in developing a service level agreement (SLA) for network services?

A. Ensuring that network components are not modified by the client

B. Reducing the number of entry points into the network

C. Finding performance metrics that can be measured property

D. Establishing a well-designed framework for network services

Answer: C

Explanation:

Question No: 82

Which of the following is the PRIMARY objective of baselining the IT control environment?

A. Align IT strategy with business strategy.

B. Detect control deviations.

C. Define process and control ownership.

D. Ensure IT security strategy and policies are effective.

Answer: B

Explanation:

Question No: 83

During a follow-up audit, an IS auditor finds that some critical recommendations have not been addressed as management has decided to accept the risk. Which of the following is the IS auditor's BEST course of action?

A. Adjust the annual risk assessment accordingly.

B. Update the audit program based on management's acceptance of risk.

C. Evaluate senior managements acceptance of the risk.

D. Require the auditee to address the recommendations in full.

Answer: A

Explanation:

Question No: 84

An IS auditor has been asked to assess the security of a recently migrated database system that contains personal and financial data for a bank's customers. Which of the following controls is MOST important for the auditor to confirm is in place?

A. The default configurations have been changed.

B. The default administration account is used after changing the account password.

C. The service port used by the database server has been changed.

D. All tables in the database are normalized.

Answer: A

Explanation:

VCEûp

Question No: 85

An IS auditor is conducting a post-implementation review of an enterprise resource planning (ERP) system End users indicated concerns with the accuracy of critical automatic calculations made by the system. The auditor's FIRST course of action should be to:

A. review recent changes to the system

B. verify completeness of user acceptance testing

C. verify results to determine validity of user concerns

D. review initial business requirements

Answer: C

Explanation:

Question No: 86

An IS auditor plans to review all access attempts to a video-monitored and proximity card-controlled communications room. Which of the following would be MOST useful to the auditor?

A. Alarm system with CCTV

B. Security incident log

C. Manual sign-in and sign-out log

D. System electronic log

Answer: B

VCEûp

Explanation:

Question No: 87

What is the PRIMARY reason to adopt a risk-based IS audit strategy?

A. To achieve synergy between audit and other risk management functions

B. To identity key threats, risks, and controls for the organization

C. To reduce the time and effort needed to perform a full audit cycle

D. To prioritize available resources and focus on areas with significant risk

Answer: D

Explanation:

Question No: 88

Which of the following governance functions is responsible for ensuring IT projects have sufficient resources and are prioritized appropriately?

A. Executive management

B. IT management

C. IT steering committee

D. Board of directors

Answer: C

Explanation:

Question No: 89

After the merger of two organizations, which of the following is the MOST important task for an IS auditor to perform?

A. Updating the continuity plan for critical resources

B. Investigating access rights for expiration dates

C. Verifying that access privileges have been reviewed

D. Updating the security policy

Answer: C

Explanation:

Question No: 90

An organization is shifting to a remote workforce. In preparation, the IT department is performing stress and capacity testing of remote access infrastructure and systems. What type of control is being implemented?

A. Directive

B. Preventive

C. Compensating

D. Detective

Answer: B

Explanation:

Question No: 91

During the implementation of a new system, an IS auditor must assess whether certain automated calculations comply with the regulatory requirements. Which of the following is the BEST way to obtain this assurance?

A. Review sign-off documentation.

B. Inspect user acceptance test (UAT) results.

C. Re-perform the calculation with audit software.

D. Review the source code related to the calculation.

Answer: C

Explanation:

Question No: 92

An IS auditor is reviewing an industrial control system (ICS) that uses older unsupported technology in the scope of an upcoming audit. What should the auditor consider the MOST significant concern?

A. There is a greater risk of system exploitation.

B. Technical specifications are not documented.

C. Disaster recovery plans (DRPs) are not in place.

D. Attack vectors are evolving for industrial control systems.

Answer: C

Explanation:

Question No: 93

During a post-implementation review, an IS auditor learns that while benefits were realized according to the business case, complications during implementation added to the cost of the solution. Which of the following is the auditor's BEST course of action?

A. Determine if project deliverables were provided on time

B. Verify that lessons learned were documented for future projects.

C. Ensure costs related to the complications were subtracted from realized benefits.

D. Design controls that will prevent future added costs.

Answer: C

Explanation:

Question No: 94

Which of the following is MOST important for an IS auditor to review when evaluating the accuracy of a spreadsheet that contains several macros?

A. Formulas within macros

B. Reconciliation of key calculations

C. Version history

D. Encryption of the spreadsheet

Answer: B

Explanation:

Question No: 95

Which of the following is the GREATEST risk associated with data conversion and migration during implementation of a new application?

A. Lack of data transformation rules

B. Inadequate audit trails and logging

C. Absence of segregation of duties

D. Obsolescence and data backup compatibility

Answer: B

Explanation:

Question No: 96

An IS auditor discovers that validation controls in a web application have been moved from the server side into the browser to boost performance. This would MOST likely increase the risk of a successful attack by:

A. phishing.

B. buffer overflow.

C. denial of service (DoS).

D. structured query language (SQL) injection.

Answer: B

Explanation:

Question No: 97

Which of the following is MOST important when duties in a small organization cannot be appropriately segregated?

A. Variance reporting

B. Audit trail

C. Exception reporting

D. independent reviews

Answer: D

Explanation:

Question No: 98

An IS auditor has discovered that unauthorized customer management software was installed on a workstation. The auditor determines the software has been uploading customer data to an external party Which of the following is the IS auditor's BEST course of action?

A. Present the issue at the next audit progress meeting.

B. Review other workstations to determine the extent of the incident

C. Determine the number of customer records that were uploaded

D. Notify the incident response team

Answer: D

Explanation:

Question No: 99

Which of the following approaches provides the BEST assurance and user confidence when an organization migrates data to a more complex enterprise resource planning (ERP) system?

A. Pilot testing

B. User acceptance testing

C. Phased changeover

D. Parallel processing

Answer: D

Explanation:

Question No: 100

An IS auditor is planning an audit of an organization's accounts payable processes. Which of the following controls is I to assess m the audit?

A. Segregation of duties between receiving invoices and setting authorization limits

B. Management review and approval of purchase orders

C. Segregation of duties between issuing purchase orders and making payments

D. Management review and approval of authorization tiers

Answer: C

Explanation:

Question No: 101

Which of the following are BEST suited for continuous auditing?

A. Manual transactions

B. Irregular transactions

C. Low-value transactions

D. Real-time transactions

Answer: B

Explanation:

Question No: 102

As part of a recent business-critical initiative, an organization is re- purposing its customer dat a. However, its customers are unaware that their data is being used for another purpose. What is the BEST recommendation to address the associated data privacy risk to the organization?

A. Obtain customer consent for secondary use of the data.

B. Adjust the existing data retention requirements.

C. Ensure the data processing activity remains onshore.

D. Maintain an audit trail of the data analysis activity

Answer: A

Explanation:

Question No: 103

Which type of testing is MOST important to perform during a project audit to help ensure business objectives are met?

A. Functional testing

B. System testing

C. Regression testing

D. Pilot testing

Answer: A

Explanation:

Question No: 104

Which of the following is the BEST point in time to conduct a post-implementation review (PIR)?

A. After a full processing cycle

B. Immediately after deployment

C. To coincide with annual PIR cycle

D. Six weeks after deployment

Answer: B

Explanation:

Question No: 105

An organization plans to implement a virtualization strategy enabling multiple operating systems on a single host. Which of the following should be the GREATEST concern with this strategy?

A. Licensing costs of the host

B. Adequate storage space

C. Application performance

D. Network bandwidth

Answer: C

Explanation:

Question No: 106

An IS auditor is reviewing a recent security incident and is seeking information about the approval of a recent modification to a database system's security settings Where would the auditor MOST likely find this information?

A. System event correlation report

B. Change log

C. Database log

D. Security incident and event management (SIEM) report

Answer: B

Explanation:

Question No: 107

Which of the following is MOST important to ensure when reviewing a global organization's controls to protect data held on its IT infrastructure across all of its locations?

A. Relevant data protection legislation and regulations for each location are adhered to.

B. Technical capabilities exist in each location to manage the data and recovery operations

C. The capacity of underlying communications infrastructure in the host locations is sufficient.

D. The threat of natural disasters in each location hosting infrastructure has been accounted for.

VCEûp

Answer: A

Explanation:

Question No: 108

Which of the following security testing techniques is MOST effective in discovering unknown malicious attacks?

A. Vulnerability testing

B. Reverse engineering

C. Penetration testing

D. Sandboxing

Answer: A

Explanation:

Question No: 109

In a typical system development life cycle (SDLC), which group is PRIMARILY responsible for confirming compliance with requirements?

A. Internal audit

B. Risk management

C. Quality assurance (QA)

D. Steering committee

VCEûp

Answer: D

Explanation:

Question No: 110

What is the BEST way to control updates to the vendor master file in an accounts payable system?

A. Using prenumbered and authorized request forms

B. Having only one person updating the master file

C. Periodically reviewing the entire vendor master file

D. Comparing updates against authorization

Answer: D

Explanation:

Question No: 111

An organization plans to implement a virtualization strategy enabling multiple operating systems on a single host. Which of the following should be the GREATEST concern with this strategy?

A. Licensing costs of the host

B. Adequate storage space

C. Application performance

D. Network bandwidth

Answer: C

Explanation:

Question No: 112

An organization has adopted a backup and recovery strategy that involves copying on-premise virtual machine (VM) images to a cloud service provider Which of the following provides the BEST assurance that VMs can be recovered in the event of a disaster?

A. Periodic on-site restoration of VM images obtained from the cloud provider

B. Inclusion of the right to audit in the cloud service provider contract

C. Procurement of adequate storage for the VM images from the cloud service provider

D. Existence of a disaster recovery plan (DRP) with specified roles for emergencies

Answer: A

Explanation:

Question No: 113

Which of the following would be an appropriate role of internal audit in helping to establish an organization’s privacy program?

A. Analyzing risks posed by new regulations

B. Developing procedures to monitor the use of personal data

C. Defining roles within the organization related to privacy

D. Designing controls to protect personal data

Answer: A

Explanation:

Question No: 114

An IS auditor performs a follow-up audit and learns the approach taken by the auditee to fix the findings differs from the agreed-upon approach confirmed during the last audit. Which of the following should be the auditor's NEXT course of action?

A. Evaluate the appropriateness of the remedial action taken.

B. Conduct a risk analysis incorporating the change.

C. Inform senior management of the change in approach.

D. Report results of the follow-up to the audit committee.

Answer: A

Explanation:

Question No: 115

In the case of a disaster where the data center is no longer available which of the following tasks should be done FIRST?

A. Perform data recovery

B. Activate the call tree

C. Analyze risk

D. Arrange for a secondary site

Answer: B

Explanation:

Question No: 116

During the planning stage of a compliance audit an IS auditor discovers that a bank's Inventory of compliance requirements does not include recent regulatory changes related to managing data risk.

What should the auditor do FIRST?

A. Exclude recent regulatory changes from the audit scope

B. Discuss potential regulatory issues with the legal department.

C. Report the missing regulatory updates to the chief information officer (CIO)

D. Ask management why the regulatory changes have not been included

Answer: D

Explanation:

Question No: 117

Which of the following will MOST likely compromise the control provided by a digital signature created using RSA encryption?

A. Deciphering the receiver's public key

B. Obtaining the sender's private key

C. Altering the plaintext message

D. Reversing the hash function using the digest

Answer: A

Explanation:

Question No: 118

An IS auditor assessing the controls within a newly implemented call center would First

A. gather information from the customers regarding response times and quality of service.

B. review the manual and automated controls in the call center.

C. test the technical infrastructure at the call center.

D. evaluate the operational risk associated with the call center.

Answer: D

Explanation:

Question No: 119

An IS auditor is evaluating an organization's IT strategy and plans. Which of the following would be of GREATEST concern?

A. The business strategy meeting minutes are not distributed.

B. There is not a defined IT security policy.

C. IT is not engaged in business strategic planning.

D. There is inadequate documentation of IT strategic planning

Answer: C

Explanation:

Question No: 120

Which of the following should be done FIRST to develop an effective business continuity plan (BCP)?

A. Secure an alternate processing site

B. Perform a business impact analysis (BIA).

C. Create a disaster recovery plan (DRP).

D. Create a business unit communications plan.

Answer: B

Explanation:

Question No: 121

Which of the following BEST enables system resiliency for an e-commerce organization that requires a low recovery time objective (RTO) and a few recovery point objective (RPO)?

A. Remote backups

B. Redundant arrays

C. Nightly backups

D. Mirrored sites

Answer: D

Explanation:

Question No: 122

Which of the following is the MAIN risk associated with adding a new system functionality during the development phase without following a project change management process?

A. The new functionality may not meet requirements

B. The added functionality has not been documented

C. The project may go over budget.

D. The project may fail to meet the established deadline

Answer: A

Explanation:

Question No: 123

While reviewing an organization s business continuity plan (BCP) an IS auditor observes that a recently developed application is not included. The IS auditor should:

A. ignore the observation as the application is not mission critical.

B. recommend that the application b# incorporated in the BCP.

C. ensure that the criticality of the application is determined

D. include m the audit findings that the BCP is incomplete

Answer: C

Explanation:

Question No: 124

Which type of attack poses the GREATEST risk to an organization's most sensitive data?

A. Insider attack

B. Eavesdropping attack

C. Spear phishing attack

D. Password attack

Answer: A

Explanation:

Question No: 125

A company converted its payroll system from an external service to an internal package Payroll processing in April was run in parallel. To validate the completeness of data after the conversion, which of the following comparisons from the old to the new system would be MOST effective?

A. Turnaround time for payroll processing

B. Employee counts and year-to-date payroll totals

C. Cut-off dates and overwrites for a sample of employees

D. Master file employee data to payroll journals

Answer: B

Explanation:

Question No: 126

When conducting a requirements analysis for a project, the BEST approach would be to:

A. Consult key stakeholders

B. Conduct a control self-assessment (CSA)

C. prototype the requirements

D. test operational deliverables

VCEup

Answer: A

Explanation:

Question No: 127

Which of the following types of environmental equipment will MOST likely be deployed below the floor tiles of a data center?

A. Temperature sensors

B. Humidity sensors

C. Water sensors

D. Air pressure sensors

Answer: C

Explanation:

Question No: 128

Which of the following application input controls would MOST likely detect data input errors in the customer account number field during the processing of an accounts receivable transaction?

A. Reasonableness check

B. Validity check

C. Parity check

D. Limit check

VCEup

Answer: B

Explanation:

Question No: 129

When evaluating the ability of a disaster recovery plan (DRP) to enable the recovery of IT processing capabilities, it is MOST important for the IS auditor to verify the plan is:

A. communicated to department heads,

B. regularly reviewed.

C. stored at an offsite location.

D. periodically tested.

Answer: D

Explanation:

Question No: 130

Which of the following BEST guards against the risk of attack by hackers?

A. Tunneling

B. Message validation

C. Encryption

D. Firewalls

Answer: C

Explanation:

Question No: 131

Which of the following is MOST helpful in preventing a systems failure from occurring when an application is replaced using the abrupt changeover technique?

A. Comprehensive testing

B. Comprehensive documentation

C. Threat and risk assessment

D. Change management

Answer: D

Explanation:

Question No: 132

An IS audit manager finds that data manipulation logic developed by the audit analytics team leads to incorrect conclusions This inaccurate logic is MOST likely an indication of lich of the following?

A. Poor change controls over data sets collected from the business

B. The team's poor understanding of the business process being analyzed

C. Poor security controls that grant inappropriate access to analysis produced

D. Incompatibility between data volume and analytics processing capacity

Answer: B

Explanation:

Question No: 133

An IS auditor learns a server administration team regularly applies workarounds to address repeated failures of critical data processing services. Which of the following would BEST enable the organization to resolve this issue?

A. Service level management

B. Problem management

C. Change management

D. Incident management

Answer: B

Explanation:

Question No: 134

Which of the following is the PRIMARY advantage of using virtualization technology for corporate applications?

A. Increased application performance

B. Improved disaster recovery

C. Stronger data security

D. Better utilization of resources

Answer: D

Explanation:

Question No: 135

After discussing findings with an auditee, an IS auditor is required to obtain approval of the report from the CEO before issuing it to the audit committee. This requirement PRIMARILY affects the IS auditor's:

A. judgment

B. effectiveness

C. independence

D. integrity

Answer: C

Explanation:

Question No: 136

Which of the following is the BEST method to maintain an audit trail of changes made to the source code of a program?

A. Standardize file naming conventions.

B. Embed details within source code.

VCEûp

C. Document details on a change register.

D. Utilize automated version control.

Answer: D

Explanation:

Question No: 137

An IS auditor is asked to provide feedback on the systems options analysis for a new project The BEST course of action for the IS auditor would be to:

A. retain comments as findings for the audit report.

B. comment on the criteria used to assess the alternatives.

C. identify the best alternative.

D. request at least one other alternative.

Answer: B

Explanation:

Question No: 138

Which of the following is the BEST use of a balanced scorecard when evaluating IT performance?

A. Determining compliance with relevant regulatory requirements

B. Monitoring alignment of IT with the rest of the organization

C. Evaluating implementation of the business strategy

D. Monitoring alignment of the IT project portfolio to budget

Answer: C

Explanation:

Question No: 139

Which of the following is the BEST way to ensure payment transaction data is restricted to the appropriate users?

A. Implementing two-factor authentication

B. Using a single menu for sensitive application transactions

C. Implementing role-based access at the application level

D. Restricting access to transactions using network security software

Answer: C

Explanation:

Question No: 140

When auditing the closing stages of a system development project, which of the following should be the MOST important consideration?

A. Rollback procedures

B. Control requirements

C. Functional requirements documentation

D. User acceptance test (UAT) results

Answer: A

Explanation:

Question No: 141

An IS auditor is reviewing the perimeter security design of a network Which of the following provides the GREATEST assurance that both incoming and outgoing Internet traffic is controlled?

A. Load balancer

B. Stateful firewall

C. Security information and event management (SIEM) system

D. Intrusion detection system (IDS)

Answer: B

Explanation:

Question No: 142

The MOST important function of a business continuity plan (BCP) is to.

A. provide procedures for evaluating tests of the BCP

B. provide a schedule of events that has to occur if there is a disaster

C. ensure that the critical business functions can be recovered

D. ensure that all business functions are restored

Answer: C

Explanation:

Question No: 143

Which of the following provides the BEST method for maintaining the security of corporate applications pushed to employee-owned mobile devices?

A. Disabling unnecessary network connectivity options

B. Implementing mobile device management (MDM)

C. Enabling remote data destruction capabilities

D. Requiring security awareness training for mobile users

Answer: B

Explanation:

Question No: 144

During a review, an IS auditor discovers that corporate users are able to access cloud-based applications and data from any Internet-connected web browser. Which of the following is the auditor's BEST recommendation to help prevent unauthorized access?

A. Update security policies and procedures.

B. Implement multi-factor authentication.

C. Utilize strong anti-malware controls on all computing devices.

D. Implement an intrusion detection system (IDS).

Answer: B

Explanation:

Question No: 145

Which of the following is the PRIMARY protocol for protecting outbound content from tampering and eavesdropping?

A. Transport Layer Security (TLS)

B. Secure Shell (SSH)

C. Point-to-Point Protocol (PPP)

D. Internet Key Exchange (IKE)

Answer: A

Explanation:

Question No: 146

Which of the following is the MOST likely reason an organization would use Platform as a Service

(PaaS)?

A. To develop and integrate its applications

B. To install and manage operating systems

C. To establish a network and security architecture

D. To operate third-party hosted applications

Answer: A

Explanation:

Question No: 147

An organization seeks to control costs related to storage media throughout the information life cycle while still meeting business and regulatory requirements. Which of the following is the BEST way to achieve this objective?

A. Perform periodic tape backups.

B. Stream backups to the cloud.

C. Implement a data retention policy.

D. Utilize solid state memory.

Answer: C

Explanation:

Question No: 148

In a 24/7 processing environment, a database contains several privileged application accounts with passwords set to "never expire.' Which of the following recommendations would BEST address the risk with minimal disruption to the business?

A. Modify applications to no longer require direct access to the database.

B. Modify the access management policy to make allowances for application accounts

C. Schedule downtime to implement password changes

D. Introduce database access monitoring into the environment

Answer: B

Explanation:

Question No: 149

IS management has recently disabled certain referential integrity controls in the database management system (DBMS) software to provide users increased query performance Which of the following controls win MOST effectively compensate for the lack of referential integrity?

A. Periodic table link checks

B. Concurrent access controls

C. Performance monitoring tools

VCEûp

D. More frequent data backups

Answer: A

Explanation:

Question No: 150

Which of the following should be of GREATEST concern to an IS auditor conducting an audit of an organization that recently experienced a ransomware attack?

A. Backups were only performed within the local network.

B. Employees were not trained on cybersecurity policies and procedures.

C. The most recent security patches were not tested prior to implementation.

D. Antivirus software was unable to prevent the attack even though it was properly updated.

Answer: A

Explanation:

Question No: 151

Which of the following provides the BEST evidence of the effectiveness of an organization s audit quality management procedures?

A. Quality of independent review scores

B. Number of resources dedicated to quality control procedures

C. Quality of auditor performance reviews

VCEûp

D. Number of audits completed within the annual audit plan

Answer: A

Explanation:

Question No: 152

Invoking a business continuity plan (BCP) is demonstrating which type of control?

A. Preventive

B. Detective

C. Corrective

D. Directive

Answer: C

Explanation:

Question No: 153

Critical processes are not defined in an organization's business continuity plan (BCP). Which of the following would have MOST likely identified this gap?

A. Updating the risk register

B. Testing the incident response plan

C. Reviewing the business impact analysis (BIA)

D. Reviewing the business continuity strategy

Answer: D

Explanation:

Question No: 154

An organization is planning to re-purpose workstations mat were used to handle confidential information. Which of the following would be the IS auditor's BEST recommendation to dispose of this information?

A. Overwrite the disks with random data

B. Erase the disks by degaussing.

C. Delete the disk partitions.

D. Reformat the disks.

Answer: A

Explanation:

Question No: 155

A review of an organization’s IT portfolio revealed several applications that are not in use. The BEST way to prevent this situation from recurring would be to implement.

A. A formal request for proposal (RFP) process

B. Business case development procedures

C. An information asset acquisition policy

D. Asset life cycle management.

Answer: D

Explanation:

Question No: 156

Which of the following is the GREATEST concern associated with a high number of IT policy exceptions approved by management?

A. The exceptions may result in noncompliance.

B. The exceptions may negatively impact process efficiency.

C. The exceptions are likely to continue indefinitely.

D. The exceptions may elevate the level of operational risk.

Answer: A

Explanation:

Question No: 157

During a disaster recovery audit, an IS auditor finds that a business impact analysis (BIA) has not been performed The auditor should FIRST.

A. evaluate the impact on current disaster recovery capability.

VCEûp

B. issue an intermediate report to management

C. conduct additional compliance testing

D. perform business impact analysis

Answer: C

Explanation:

Question No: 158

IT disaster recovery lime objectives (RTOs) should be based on the:

A. maximum tolerable loss of data.

B. business-defined critically of the systems.

C. maximum tolerable downtime (MTD).

D. nature of the outage.

Answer: B

Explanation:

Question No: 159

The use of which of the following would BEST enhance a process improvement program?

A. Capability maturity models

VCEûp

B. Model-based design notations

C. Project management methodologies

D. Balanced scorecard

Answer: A

Explanation:

Question No: 160

Which of the following is the BEST compensating control when segregation of duties is lacking in a small IS department?

A. Mandatory holidays

B. Background checks

C. Transaction log review

D. User awareness training

Answer: C

Explanation:

Question No: 161

Which of the following security risks can be reduced by a property configured network firewall?

A. SQL injection attacks

B. Insider attacks

C. Phishing attacks

D. Denial of service (DoS) attacks

Answer: D

Explanation:

Question No: 162

Which of the following is the BEST indication of the completeness of interface control documents used for the development of a new application?

A. All documents have been reviewed by end users.

B. All inputs and outputs for potential actions are included.

C. Both successful and failed interface data transfers are recorded.

D. Failed interface data transfers prevent subsequent processes.

Answer: D

Explanation:

Question No: 163

When conducting a post-implementation review of a new software application, an IS auditor should be MOST concerned with an increasing number of

A. updates required for the end-user operations manual

B. change requests approved to add new services

C. operational errors impacting service delivery

D. help desk calls requesting future enhancements

Answer: C

Explanation:

Question No: 164

What is the MOST critical finding when reviewing an organization's information security management?

A. No periodic assessments to identify threats and vulnerabilities

B. No dedicated security officer

C. No employee awareness training and education program

D. No official charter for the information security management system

Answer: A

Explanation:

Question No: 165

Stress testing should ideally be carried out under a:

A. production environment with test data.

B. test environment with test data.

C. production environment with production workloads.

D. test environment with production workloads.

Answer: D

Explanation:

Question No: 166

Which of the following should be of GREATEST concern to an IS auditor performing a review of information security controls?

A. The information security policy does not include mobile device provisions.

B. The information security policy has not been approved by the chief audit executive (CAE).

C. The information security policy has not been approved by the policy owner.

D. The information security policy is not frequently reviewed.

Answer: C

Explanation:

Question No: 167

Which of the following provides the MOST reliable audit evidence on the validity of transactions in a financial application?

A. Substantive testing

B. Compliance testing

C. Walk-through reviews

D. Design documentation reviews

Answer: A

Explanation:

Question No: 168

To lest the integrity of the data in the accounts receivable master file, an IS auditor is particularly interested in reviewing customers with balances over $400,000. The selection technique the IS auditor would use to obtain such a sample is called:

A. variable sampling

B. stop-or-go sampling

C. random selection

D. stratification.

Answer: A

Explanation:

Question No: 169

Which of the following is MOST important for an IS auditor to consider when planning an assessment of the organization's end-user computing (EUC) program?

A. The integrity of data processed by end user tools

B. The inclusion of end user tools in the IT balanced scorecard

C. The training program curriculum for key end users

D. Identification of IT owners for each end user tool

Answer: A

Explanation:

Question No: 170

An IS auditor is assigned to review the IS departments quality procedures Upon contacting the IS manager, the auditor finds that there is an informal unwritten set of standards Which of the following should be the auditor's NEXT action?

A. Finalize the audit and report the finding

B. Postpone the audit until IS management implements written standards

C. Make recommendations to IS management as to appropriate quality standards

D. Document and test compliance with the informal standards

Answer: D

Explanation:

Question No: 171

Which of the following should be of GREATEST concern to an IS auditor reviewing project documentation for a client relationship management (CRM) system migration project?

A. Employees are concerned that data representation in the new system is completely different from the old system.

B. Five weeks prior to the target date, there are still numerous defects in the printing functionality.

C. A single implementation phase is planned and the legacy system will be immediately decommissioned.

D. The technical migration is planned for a holiday weekend and end users may not be available.

Answer: C

Explanation:

Question No: 172

What is the MOST difficult aspect of access control in a multiplatform, multiple-site client/server environment?

A. Restricting a local user to necessary resources on a local platform

B. Maintaining consistency throughout all platforms

C. Restricting a local user to necessary resources on the host server

VCEup

D. Creating new user IDs valid only on a few hosts

Answer: B

Explanation:

Question No: 173

A bank's web-hosting provider has just completed an internal IT security audit and provides only a summary of the findings to the bank’s auditor. Which of the following should be the bank's GREATEST concern?

A. The bank’s auditors are not independent of the service provider.

B. The audit may be duplicative of the bank's internal audit procedures.

C. The audit procedures are not provided to the bank.

D. The audit scope may not have addressed critical areas.

Answer: D

Explanation:

Question No: 174

An information systems security officer's PRIMARY responsibility for business process applications is to:

A. ensure access rules agree with policies

B. create role-based rules for each business process

C. authorize secured emergency access.

VCEup

D. approve the organization's security policy.

Answer: B

Explanation:

Question No: 175

Which of the following should be the PRIMARY basis for prioritizing follow-up audits?

A. Complexity of management's action plans

B. Recommendation from executive management

C. Audit cycle defined in the audit plan

D. Residual risk from the findings of previous audits

Answer: D

Explanation:

Question No: 176

An organization considers implementing a system that uses a technology that is not in line with the organization’s IT strategy. Which of the following is the BEST justification for deviating from the IT strategy?

A. The system makes use of state-of-the-art technology

B. The organization has staff familiar with the technology

C. The system has a reduced cost of ownership

D. The business benefits are achieved even with extra costs

Answer: B

Explanation:

Question No: 177

Which of the following should be an IS auditor's GREATEST consideration when scheduling follow-up activities for agreed-upon management responses to remediate audit observations?

A. Business interruption due to remediation

B. IT budgeting constraints

C. Risk rating of original findings

D. Availability of responsible IT personnel

Answer: C

Explanation:

Question No: 178

An organization uses multiple offsite data center facilities Which of the following is MOST important to consider when choosing related backup devices and media?

A. Standardization

B. Backup media capacity

C. Restoration speed

D. Associated costs

Answer: A

Explanation:

Question No: 179

Which of the following would BEST demonstrate that an effective disaster recovery plan (DRP) is in place?

A. Periodic risk assessment

B. Full operational test

C. Frequent testing of backups

D. Annual walk-through testing

Answer: B

Explanation:

Question No: 180

Which of the following is the MOST effective control to mitigate unintentional misuse of authorized access?

A. Security awareness training

B. Regular monitoring of user access logs

C. Formalized disciplinary action

D. Annual sign-off of acceptable use policy

Answer: C

Explanation:

Question No: 181

Which of the following would be the MOST useful metric for management to consider when reviewing a project portfolio?

A. Cost of projects divided by total IT cost

B. Expected return divided by total project cost

C. Net present value (NPV) of the portfolio

D. Total cost of each project

Answer: C

Explanation:

Question No: 182

An IS auditor notes that application super-user activity was not recorded in system logs. What is the auditor’s BEST course of action?

A. Investigate the reason for the lack of logging

B. Recommend a least privilege access model

C. Recommend activation of super user activity logging

D. Report the issue to the audit manager

Answer: A

Explanation:

Question No: 183

An organization has recently implemented a Voice-over IP (VoIP) communication system. Which of the following should be the IS auditor's PRIMARY concern?

A. Lack of integration of voice and data communications

B. A single point of failure for both voice and data communications

C. Voice quality degradation due to packet loss

D. Inability to use virtual private networks (VPNs) for internal traffic

Answer: B

Explanation:

Question No: 184

An organization recently decided to send the backup of its customer relationship management (CRM) system to its cloud provider for recovery. Which of the following should be of GREATEST concern to an IS auditor reviewing this process?

A. Validation of backup data has not been performed.

B. The cloud provider is located in a different country.

C. Testing of restore data has not been performed.

D. Backups are sent and stored in unencrypted format.

Answer: B

Explanation:

Question No: 185

Management has decided to include a compliance manager in the approval process for a new business that may require changes to tie IT infrastructure. Which of the following is the GREATEST benefit of this approach?

A. Process accountabilities to external stakeholders are improved

B. Security breach incidents can be identified in early stages

C. Fewer views are needed when updating the IT compliance process

D. Regulatory risk exposures can be identified before they materialize

Answer: D

Explanation:

Question No: 186

An IS auditor finds the log management system is overwhelmed with false positive alerts. The auditor's BEST recommendation would be to:

A. reduce the firewall rules.

B. establish criteria for reviewing alerts.

C. fine tune the intrusion detection system (IDS).

D. recruit more monitoring personnel.

Answer: C

Explanation:

Question No: 187

An algorithm in an email program analyzes traffic to quarantine emails identified as spam The algorithm in the program is BEST characterized as which type of control?

A. Directive

B. Preventive

C. Corrective

D. Detective

Answer: B

VCEûp

Explanation:

Question No: 188

Which of the following demonstrates the use of data analytics for a loan origination process?

A. Evaluating whether loan records are included in the batch file and are validated by the servicing system

B. Validating whether reconciliations between the two systems are performed and discrepancies are investigated

C. Reviewing error handling controls to notify appropriate personnel in the event of a transmission failure

D. Comparing a population of loans input in the origination system to loans booked on the servicing system

Answer: B

Explanation:

Question No: 189

An organization's security policy mandates that all new employees must receive appropriate security awareness training. Which of the following metrics would BEST assure compliance with this policy?

A. Percentage of new hires who report incidents

B. Number of reported incidents by new hires

C. Percentage of new hires that have completed the training .

D. Number of new hires who have violated enterprise security policies

Answer: B

VCEûp

Explanation:

Question No: 190

An employee has accidentally posted confidential data to the company's social media page. Which of the following is the BEST control to prevent this from recurring?

A. Perform periodic audits of social media updates.

B. Implement a moderator approval process.

C. Require all updates to be made by the marketing director.

D. Establish two-factor access control for social media accounts.

Answer: B

Explanation:

Question No: 191

During an operational audit of a biometric system used to control physical access, which of the following should be of GREATEST concern to an IS auditor?

A. False positives

B. Lack of biometric training

C. False negatives

D. User acceptance of biometrics

VCEûp

Answer: A

Explanation:

Question No: 192

Which of the following is the BEST methodology to use for estimating the complexity of developing a large business application?

A. Work breakdown structure

B. Critical path analysis

C. Software cost estimation

D. Function point analysis

Answer: D

Explanation:

Question No: 193

An IS auditor is performing a follow-up audit for findings identified In an organization's user provisioning process Which of the Mowing is the MOST appropriate population to sample from when testing for remediation?

A. All users provisioned after the final audit report was issued

B. All users provisioned after management resolved the audit issue

C. All users who have followed user provisioning processes provided by management

D. All users provisioned after the finding was originally identified

VCEûp

Answer: B

Explanation:

Question No: 194

A new privacy regulation requires a customer's privacy information to be deleted within 72 hours, if requested. Which of the following would be an IS auditor's GREATEST concern regarding compliance to this regulation?

A. Outdated online privacy policies

B. Incomplete backup and retention policies

C. End user access to applications with customer information

D. Lack of knowledge of where customers' information is saved

Answer: D

Explanation:

Question No: 195

A data analytics team has developed a process automation bot for internal audit that scans user access to all servers in the environment and then randomly selects a sample of new users for testing.

Which of the following presents the GREATEST concern with this approach?

A. Evidence of population completeness is not maintained.

B. The bot can only select samples from the current period.

VCEûp

C. Auditor judgment is removed from the process

D. Data must be validated manually before being loaded into the bot.

Answer: C

Explanation:

Question No: 196

Which of the following testing methods is MOST appropriate for assessing whether system integrity has been maintained after changes have been made?

A. Acceptance testing

B. Unit testing

C. Integration testing

D. Regression testing

Answer: D

Explanation:

Question No: 197

Which of the following should be defined in an audit charter?

A. Audit methodology

B. Audit schedule

C. Audit results

D. Audit authority

VCEûp

Answer: D

Explanation:

Question No: 198

Which of the following is the GREATEST security risk associated with data migration from a legacy human resources (HR) system to a cloud-based system?

A. Data from the source and target system may be intercepted

B. Records past their retention period may not be migrated to the new system

C. System performance may be impacted by the migration

D. Data from the source and target system may have different data formats

Answer: A

Explanation:

Question No: 199

When implementing a new IT maturity model which of the following should occur FIRST?

A. Define the target IT maturity level

VCEûp

B. Develop performance metrics

C. Determine the model elements to be evaluated

D. Benchmark with industry peers

Answer: A

Explanation:

Question No: 200

Malicious program code was found in an application and corrected prior to release into production.

After the release, the same issue was reported. Which of the following is the IS auditor's BEST recommendation?

A. Ensure change management reports are independently reviewed.

B. Ensure the business signs off on end-to-end user acceptance test (UAT) results.

C. Ensure programmers cannot access code after the completion of program edits.

D. Ensure corrected program code is compiled in a dedicated server.

Answer: C

Explanation:

Question No: 201

Coding standards provide which of the following?

VCEûp

A. Field naming conventions

B. Access control tables

C. Data flow diagrams

D. Program documentation

Answer: A

Explanation:

Question No: 202

A warehouse employee of a retail company has been able to conceal the theft of inventory items by entering adjustments of either damaged or lost stock items to the inventory system Which control would have BEST prevented this type of fraud in a retail environment?

A. Statistical sampling of adjustment transactions

B. Unscheduled audits of lost stock lines

C. An edit check for the validity of the inventory transaction

D. Separate authorization for input of transactions

Answer: D

Explanation:

Question No: 203

An organization allows its employees to use personal mobile devices for work. Which of the following would BEST maintain information security without compromising employee privacy?

A. Installing security software on the devices

B. Restricting the use of devices for personal purposes during working hours

C. Preventing users from adding applications

D. Partitioning the work environment from personal space on devices

Answer: D

Explanation:

Question No: 204

During an audit of a financial application, it was determined that many terminated users' accounts were not disabled. Which of the following should be the IS auditors NEXT step?

A. Conclude that IT general controls are ineffective.

B. Perform a review of terminated users' account activity.

C. Communicate risks to the application owner.

D. Perform substantive testing of terminated users' access rights.

Answer: B

Explanation:

Question No: 205

What is the PRIMARY reason for conducting a risk assessment when developing an annual IS audit plan?

A. Decide which audit procedures and techniques to use

B. Determine the existence of controls in audit areas

C. Identify and prioritize audit areas

D. Provide assurance material items will be covered

Answer: C

Explanation:

Question No: 206

The performance, risks, and capabilities of an IT infrastructure are BEST measured using a:

A. service level agreement (SLA).

B. balanced Scorecard.

C. risk management review.

D. control self-assessment (CSA).

Answer: B

VCEûp

Explanation:

Question No: 207

An advantage of object-oriented system development is that it:

A. partitions systems into a client/server architecture.

B. decreases the need for system documentation.

C. is suited to data with complex relationships.

D. is easier to code than procedural languages.

Answer: D

Explanation:

VCEûp