Information Systems Operations, Maintenance and Support I

Radio Frequency Identification(RFID)

1. Which of the following risks is applicable to active RFID?

   the risk of eavesdropping

2. Which of the following reports should an IS auditor verify to determine compliance with the uptime requirement defined in the Service Level Agreement(SLA)?

   the availability report

3. Which of the following is of great help when determining the efficiency of preventive maintenance programs?

   the system downtime report

4. Which of the following activities should not be conducted during peak production hours to avoid unexpected downtime?

   preventive maintenance

5. Which of these is the best method of determining the availability of updated security patches for critical servers?

   use an automated tool to verify the availability of updated patches

IT Asset Management

1. The synchronisation of production source code and object code is best controlled by which of the following?

   Date-and-time stamping source code and object code

2. What is the first step after the replacement of hardware?

   update the IT asset inventory

3. What is the first step in the implementation of access control?

   create an inventory of IT assets

4. What is the first step in developing a risk management program?

   Identify assets

5. Which of the following is the major concern for an IS auditor reviewing desktop software compliance?

   installed software not being approved

Job Scheduling and Production Process

1. Which of the following is most important for an IS audit reviewing the preventive maintenance activity processes of a data center by a third-party service provider?

   maintenance activities being conducted during non-peak hours

2. Which of the following is a major concern for an auditor reviewing the job scheduling process?

   a few jobs having been overridden by the operator

3. Which of the following is the best compensating control for tape management system where some parameters are set to bypass or ignore tape header records?

   staging and job setup

End User Computing

1. Which of the following is the greatest concern for an IS auditor reviewing the end use computing process?

   the lack of a documented end user computing policy

Systems Performance Management

1. Which of the following best describes source code?

   the human-readable instructions written by a programmer.

2. How can the optimal configuration of a server be ensured?

   server utilisation reports

3. An auditor sees certain indications that an organisation is using unlicensed software. What should be the auditor's first step?

   verify the software through testing

4. Which of the following is the greatest concern for the use of open source software?

   an organisation must comply with open source software license terms.

5. Which of the following is the most important consideration when reviewing a hardware maintenance program?

   the maintenance program covers vendor-provided specification

6. Which of the following is most useful for examining the security configuration of an operating system?

   reviewing parameter settings

7. An IS auditor notes that storage resources are continuously added. What should they review?

   the capacity management process

8. An IS auditor notes that some users have installed personal software on their PCs. There is no restriction by security policy. What is the best recommendation for the auditor to make?

   include a clause related to the restriction of unauthorised software in the security policy.

9. An IS auditor notes that it takes a significant amount of time to log on to the system during peak business hours as compared to other times. What should the recommendation of the auditor be?

   establish performance measurement criteria

Problem and Incident Management

1. Which of the following best describes Simple Network Management Protocol(SNMP)?

   a protocol used for monitoring an managing network devices such as routers, switches, and servers by collecting and organising information about their status.

2. Which of the following network diagnostics tools monitors and records network information?

   network protocol analyzer.

3. An IS auditor is reviewing help desk activities. Which of the following is an area of major concern?

   end user not being informed about the closure of resolved incidents.

4. Which of the following does the use of network performance monitoring tools directly affect?

   the availability of a system

5. Which of the following performance indicators is best to include in an Service Level Agreement(SLA) for an outsourced help desk function?

   the percentage of resolution upon the first call

6. What is the best method to prevent the recurrence of IT system failure?

   performing root cause analysis

7. An IS auditor notes that several incidents were assigned the wrong priorities and hence were not able to achieve the defined Service Level Agreement(SLA). Which of the is the most important concern?

   the support model was not properly designed and executed.

8. Which of the following is the first step in the implementation of a problem management mechanism?

   reporting an exception

Change, Configuration, release and patch management

1. Which of the following best describes a roll back process?

   a method used to reverse the changes made by a transaction, restoring the database or system to its previous state.

2. Which of the following is the most important consideration when ensuring system availability during the change management process?

   the change management procedure being followed consistently

3. Which of the following is the best option for patch management to ensure that a new patch will not impact system processing?

   a patch should be tested prior to updating

4. What is the best way to find evidence of unauthorised changes in a production system?

   compliance testing

5. A review of the change management process indicates that the process is not fully documented and also that some migration processes failed. What should the next step for the IS auditor be?

   try to get further information about the findings through root cause analysis

6. Which of the following procedures is used to restore a system to its prior state?

   backout procedure

7. Which of the following is considered a critical component in network management?

   change and configuration management

8. Which of the following is an important aspect of patch management?

   conducting an impact analysis before the installation of a patch

9. Which of the following provides the best evidence regarding the effectiveness of a change control procedure?

   verifying the approvals for the changes conducted

10. An IS auditor reviewing a change management procedure notes that some code that was missed during the production release was subsequently included in production without following the normal change management process. Which of the following is the area of most concern?

    the code was subsequently included without change management approval

11. What is the most effective way to gauge the design effectiveness of a change management process?

    conducting an end-to-end walk-through of the change management process

12. The IS auditor notes that the system malfunctioned after the installation of a security patch. Which of the following is the best control for such an incident?

    the change management procedure should be followed for patch installation

13. What is the objective of code signing?

    ensuring that software has not subsequently modified

14. What is the objective of library control software?

    providing assurance that program changes are authorised

15. Data is copied from a backup server to the production server. Which of the following is the best way to ensure that no unauthorised software moves to the production server?

    reviewing changes in software version control

16. Which of the following is the best control for configuration changes?

    an adequate process of approval and review for critical changes

17. Which of the following is the best compensatory control where developers themselves release emergency changes directly to production?

    changes should be logged and approved on the next business day.

18. An organisation has changed the vendor maintaining critical applications. In the new contract, the incident resolution time has been modified. Which of the following is a major concern?

    the application owners are not aware of the modification

19. Which of the following is a major concern in a change management process?

    the non-availability of a configuration management database

20. Which of the following is a major concern for an in-house-developed application?

    a change request being initiated and approved by the same employee

21. Which of the following is the best process to use to test program changes?

    reviewing samples of change authorisation first and then analysing the supporting change authorisation

22. Which of the following is the best control for emergency changes that bypass the normal change process?

    subsequent review and approval of all emergency changes

23. What is the most important aspect for patch updating for an operating system?

    approval from the owner of the information system asset

24. An IS auditor notes that IT personnel have not yet installed the patches that were released 2 months ago. What should the IS auditor do?

    review the patch management policy and analyse the risks associated with delayed updates.

25. What is the most likely reason for adopting emergency change procedure?

    a change having a significant impact on business operation

26. Which of the following best establishes accountability for personnel when it comes to emergency change?

    granting production access to individual IDs as and when required

27. An IS auditor notes that IT department has not updated a new patch for an application because other security controls are in place. What should the recommendation of the auditor be?

    the overall risk should be analysed before any recommendation is made.

28. An IS auditor notes that users are granted occasional authority to change a system. What should the IS auditor's first step be?

    determine whether this process is allowed by policy

29. An employee is granted authority to change the parameters of a critical file. Which of the following is the most effective control on that employee's activities?

    changes should be approved by supervisor.

30. Which of the following is the fastest technique for determining data-file change management controls?

    transaction logs

Key Points

- Radio Frequency Identification(RFID) tags are exposed to the risk of eavesdropping.
- It is the same as a wireless device.
- Radio Frequency Identification(RFID), by its nature, is not subject to other exposure, such as social engineering, phishing, or malicious code.
- An availability report indicates the time period during which the system is up and available for use.
- An IS auditor can determine downtime with the help of availability reports.

- Utilisation reports determine the level of use of systems.
- A utilisation report is used to predict resource requirements.
- Asset management reports include an inventory of assets.
- Hardware error reports identify system failures and other issues.
- The system downtime log indicates the effectiveness of preventive maintenance programs.
- High downtime indicates that preventive maintenance is not effective.
- Effective preventive maintenance should result in zero or very minimal downtime.
- Preventive maintenance should be conducted during non-peak times to avoid any downtime.
- Date-and-time stamping for both the source code and the object code will help to ensure that the code is in sync.
- CISA aspirants should understand the following sequential activities for the development of a risk management program
    - the identification of assets
    - the identification vulnerabilities and threats
    - impact analysis
    - risk prioritisation
    - control evaluation
    - implementation of appropriate controls
- The installation of unapproved software is a serious violation that carries major legal, financial and security risks.
- The overriding of scheduled jobs should be restricted as this can lead to unauthorised changes to programs or data.
- Staging and job setup is useful in compensating for weaknesses in tape control.
- Through staging, data is stored in an intermediate place(between the data source and the data target) and processing is done.
- End user computing refers to a system wherein a non-programmer can create their own application.
- End user computing is subject to some inherent risks.

- It is important that the documented policy of end user computing should be available to address the risks.
- Server utilisation reports identify underutilised servers and help to monitor overall server utilisation.
- An IS auditor should be more concerned about licensing compliance to avoid any legal consequences.
- A maintenance schedule is not required to be approved by the steering committee.
- Reviewing the parameter settings helps to identify access controls, system usage, and other operating system-related securities.
- Capacity management helps to ensure that IT resources are used effectively and efficiently.
- Effective capacity management processes help in planning and purchasing additional resources.
- Establishing performance criteria for authentication servers would help to monitor performance, and remedial action can be taken where performance is not acceptable.
- Protocol analysers are network diagnostic tools used to monitor the packets flowing along a network.
- Incidents should be regarded as closed only when this is confirmed by the end user.
- Network performance tools help the administrator to take corrective action in the case of network-related issues.
- The root cause analysis determines the key reason why an incident happened.
- Ineffective support models will not be able to prevent or react to potential incidents.
- The most important control for ensuring system availability is a sound change management procedure that is followed consistently.
- Compliance testing will help to determine whether a change management process is applied consistently and whether changes are appropriately approved.
- The Backout procedure is used to restore a system to an earlier state, prior to the state of upgrade.

- The objective of code signing is to provide assurance that code is generated from a reputable source and that the code has not been modified after being signed.
- A program stored in a library can be accessed only by authorised users.
- The best compensatory control is log all such changes and subsequently approve those changes.
- Reviewing a sample of modified programs and then tracing back to relevant supporting change authorisation is the best way to test change management