4/23/2014 MIS5205 Quiz #6

1. In a relational database with referential integrity, the use of which of the following keys would prevent deletion of a row from a customer table as long as the customer number of that row is stored with live orders on the orders table?

A. Foreign key

B. Primary key

C. Secondary key

D. Public key

2. The **FIRST** step in managing the risk of a cyberattack is to:

A. assess the vulnerability impact.

B. evaluate the likelihood of threats.

C. identify critical information assets.

D. estimate potential damage.

3. After consulting with senior management, an organization's IT department decided that all IT hardware would be replaced three years from the procurement date. The **MOST** likely reason for doing this is to:

A. manage IT assets in a cost-effective manner.

B. keep pace with new cost-effective technologies.

C. ensure that existing capacity can meet all users' needs.

D. ensure that IT hardware is covered by the manufacturer warranty.

4. Which of the following would be the **BEST** way for an IS auditor to provide assurance on the adequacy and effectiveness of system change control procedures?

A. Observing a system change procedure by the IS staff being audited

B. Sampling source code library changes from the system being audited

C. Interviewing users to inquire whether they were satisfied with the changes

D. Reviewing system documentation to ensure it is complete and up to date

5. IS management has decided to install a level1 Redundant Array of Inexpensive Disks (RAID) system in all servers to compensate for the elimination of offsite backups. The IS auditor should recommend:

A. upgrading to a level 5 RAID.

B. increasing the frequency of onsite backups.

C. reinstating the offsite backups.

D. establishing a cold site in a secure location.

6. Which of the following is the **GREATEST** benefit to implementing open source software (OSS)?

A. Reduction of the total cost of ownership (TCO)

B. Ability to more easily customize program source code

C. Mitigation of the risk of being locked into a single provider

D. Reduction of the effort of performing system upgrades

7. Which of the following is **MOST** important to ensure business continuity?

A. Current contact information for key employees

B. Backup data

C. Access to funds for short-term needs

D. Alternate processing site

8. A database administrator has detected a performance problem with some tables which could be solved through denormalization. This situation will increase the risk of:

A. concurrent access.

B. deadlocks.

C. unauthorized access to data.

D. a loss of data integrity.

9. A lower recovery time objective (RTO) results in:

A. higher disaster tolerance.

B. higher cost.

c. wider interruption windows.

D. more permissive data loss.

10. A review of wide area network (WAN) usage discovers that traffic on one communication line between sites, synchronously linking the master and standby database, peaks at 96 percent of the line capacity. An IS auditor should conclude that:

A. analysis is required to determine if a pattern emerges that results in a service loss for a short period of time.

B. WAN capacity is adequate for the maximum traffic demands since saturation has not been reached.

C. the line should immediately be replaced by one with a larger capacity to provide approximately 85 percent saturation.

D. users should be instructed to reduce their traffic demands or distribute them across all service hours to flatten bandwidth consumption.

11. When reviewing procedures for emergency changes to programs, the IS auditor should verify that the procedures:

A. allow changes, which will be completed using after-the-fact follow-up.

B. allow undocumented changes directly to the production library.

C. do not allow any emergency changes.

D. allow programmers permanent access to production programs.

12. Once an organization has finished the business process reengineering (BPR) of all its critical operations, an IS auditor would **MOST** likely focus on a review of:

A. pre-BPR process flowcharts.

B. post-BPR process flowcharts.

C. BPR project plans.

D. continuous improvement and monitoring plans.

13. An IS auditor discovers that developers have operator access to the command line of a production environment operating system. Which of the following controls would **BEST** mitigate the risk of undetected and unauthorized program changes to the production environment?

A. Commands typed on the command line are logged.

B. Hash keys are calculated periodically for programs and matched against hash keys calculated for the most recent authorized versions of the programs.

C. Access to the operating system command line is granted through an access restriction tool with preapproved rights.

D. Software development tools and compilers have been removed from the production environment.

14. During the audit of a database server, which of the following would be considered the **GREATEST** exposure?

A. The password does not expire on the administrator account.

B. Default global security settings for the database remain unchanged.

C. Old data have not been purged.

D. Database activity is not fully logged.

15. An IS auditor performing an application maintenance audit would review the log of program changes for the:

A. authorization of program changes.

B. creation date of a current object module.

C. number of program changes actually made.

D. creation date of a current source program.

16. An IS auditor observes a weakness in the tape management system at a data center in that some parameters are set to bypass or ignore tape header records. Which of the following is the **MOST** effective compensating control for this weakness?

A. Staging and job setup

B. Supervisory review of logs

C. Regular back-up of tapes

D. Offsite storage of tapes

17. Due to changes in IT, the disaster recovery plan of a large organization has been changed. What is the **PRIMARY** risk if the new plan is not tested?

A. Catastrophic service interruption

B. High consumption of resources

C. Total cost of the recovery may not be minimized

D. Users and recovery teams may face severe difficulties when activating the plan

18. An IS auditor determined that the IT manager recently changed the vendor that is responsible for performing maintenance on critical computer systems to cut costs. While the new vendor is less expensive, the new maintenance contract specifies a change in incident resolution time specified by the original vendor. Which of the following should be the **GREATEST** concern to the IS auditor?

A. Disaster recovery plans (DRPs) may be invalid and need to be revised.

B. Transactional business data may be lost in the event of system failure.

C. The new maintenance vendor is not familiar with the organization's policies.

D. Application owners were not informed of the change.

19. After a full operational contingency test, an IS auditor performs a review of the recovery steps. The IS auditor concludes that the time it took for the technological environment and systems to return to full-functioning exceeded the required critical recovery time. Which of the following should the IS auditor recommend?

A. Perform an integral review of the recovery tasks.

B. Broaden the processing capacity to gain recovery time.

C. Make improvements in the facility's circulation structure.

D. Increase the amount of human resources involved in the recovery.

20. An IS auditor performing an independent classification of systems should consider a situation where functions could be performed manually at a tolerable cost for an extended period of time as:

A. critical.

B. vital.

c. sensitive.

D. noncritical.