

1. A development team has developed and is currently maintaining a customer-facing web application which is hosted at their regional office versus at the central data center. The GREATEST risk in this scenario is that:
  - a. Additional traffic of the web site would slow down Internet access for the regional office
  - b. Development team may lack the expertise and staffing to manage and maintain a hosted application environment
  - c. Regional office may not have the same level of fire detection and suppression that exists at the main data center
  - d. Regional office may not have a firewall or network that is sufficiently secure for a web server
  
2. Which of the following is the GREATEST risk to the effectiveness of application system controls?
  - a. Removal of manual processing steps
  - b. Inadequate procedure manuals
  - c. Collusion between employees
  - d. Unresolved regulatory compliance issues
  
3. A business application system accesses a corporate database using a single ID and password embedded in a program. Which of the following would provide efficient access control over the organization's data?
  - a. Introduce a secondary authentication method such as a card swipe
  - b. Apply role-based permissions within the application system
  - c. Have users input the ID and password for each database transaction
  - d. Set an expiration period for the database password embedded in the program
  
4. An Information System (IS) auditor finds that a database administrator (DBA) has read and write access to production data. The IS auditor should:
  - a. Accept the DBA access as a common practice
  - b. Assess the controls relevant to the DBA function
  - c. Recommend the immediate revocation of the DBA access to production data
  - d. Review user access authorizations approved by the DBA
  
5. Inadequate programming and coding practices introduce the risk of:
  - a. Phishing
  - b. Buffer overflow exploitation
  - c. Denial of service attack through synchronization (SYN) flood
  - d. Brute force attacks
  
6. Which of the following is a control that can be implemented if application programmers are allowed to move programs into the production environment in a small organization?
  - a. Independent post-implementation testing
  - b. Independent review of the changed program
  - c. Independent review of user requirements
  - d. Independent review of user acceptance

7. Which of the following groups would create MOST concern to an IS auditor if they have direct full access to the production database?
  - a. Application testers
  - b. System administrators
  - c. The database owner
  - d. The data recovery team
  
8. During an audit of an internally developed, web-based purchase approval application, an IS auditor discovers that all business users share a common access profile. Which of the following is the MOST important recommendation for the IS auditor to include in the report?
  - a. Ensure that all user activity is logged and that the logs are reviewed by management
  - b. Develop additional profiles within the application to restrict user access per the job profiles
  - c. Ensure that a policy exists to control what activities users can perform within the application
  - d. Ensure that a virtual private network (VPN) is implemented so that users can log on to the application securely
  
9. Which of the following should an IS auditor be MOST concerned about in a financial application?
  - a. Programmers have access to application source code
  - b. Secondary controls are documented for identified role conflicts
  - c. The information security officer does not authorize all application changes
  - d. Programmers have access to the production database
  
10. Which of the following prevention control BEST helps secure a web application?
  - a. Password masking
  - b. Developer training
  - c. Encryption
  - d. Vulnerability testing
  
11. An organization is developing a new web-based application to process orders from customers. Which of the following security measures should be taken to protect this application from hackers?
  - a. Ensure that ports 80 and 443 are blocked at the firewall
  - b. Inspect file and access permissions on all servers to ensure all files have read-only access
  - c. Perform a web application security review
  - d. Make sure that only IP addresses of existing customers are allowed through the firewall
  
12. Which control is the BEST way to ensure that the data in a file have not been changed during transmission?
  - a. Reasonableness check
  - b. Parity bits
  - c. Hash values
  - d. Check digits