Certified Information Systems Auditor

1. An IT balanced scorecard is the MOST effective means of monitoring:

A. governance of enterprise IT.

B. control effectiveness.

C. return on investment (ROI).

D. change management effectiveness.

Answer(s): A

---

2. When reviewing an organization's information security policies, an IS auditor should verify that the policies have been defined PRIMARILY on the basis of:

A. a risk management process.

B. an information security framework.

C. past information security incidents.

D. industry best practices.

Answer(s): B

---

3. Which of the following would be an IS auditor's GREATEST concern when reviewing the early stages of a software development project?

A. The lack of technical documentation to support the program code

B. The lack of completion of all requirements at the end of each sprint

C. The lack of acceptance criteria behind user requirements.

D. The lack of a detailed unit and system test plan

Answer(s): C

---

4. Which of the following is the BEST data integrity check?

A. Counting the transactions processed per day

B. Performing a sequence check

C. Tracing data back to the point of origin

D. Preparing and running test data

Answer(s): C

---

5. Spreadsheets are used to calculate project cost estimates. Totals for each cost category are then keyed into the job-costing system.
What is the BEST control to ensure that data is accurately entered into the system?

A. Reconciliation of total amounts by project

B. Validity checks, preventing entry of character data

C. Reasonableness checks for each cost type

D. Display back of project detail after entry

Answer(s): A

---

6. An incorrect version of source code was amended by a development team. This MOST likely indicates a weakness in:

A. incident management.

B. quality assurance (QA).

C. change management.

D. project management.

Answer(s): C

---

7. An organizations audit charier PRIMARILY:

A. describes the auditors' authority to conduct audits.

B. defines the auditors' code of conduct.

C. formally records the annual and quarterly audit plans.

D. documents the audit process and reporting standards.

Answer(s): A

---

8. The decision to accept an IT control risk related to data quality should be the responsibility of the:

A. information security team.

B. IS audit manager.

C. chief information officer (CIO).

D. business owner.

Answer(s): D

---

9. Which of the following data would be used when performing a business impact analysis (BIA)?

A. Projected impact of current business on future business

B. Cost-benefit analysis of running the current business

C. Cost of regulatory compliance

D. Expected costs for recovering the business

Answer(s): A

---

10. Which of the following is the MOST important consideration for an IS auditor when assessing the adequacy of an organization's information security policy?

A. Alignment with the IT tactical plan

B. IT steering committee minutes

C. Compliance with industry best practice

D. Business objectives

Answer(s): D

---

11. During the evaluation of controls over a major application development project, the MOST effective use of an IS auditor's time would be to review and evaluate:

A. application test cases.

B. acceptance testing.

C. cost-benefit analysis.

D. project plans.

Answer(s): A

---

12. An IS auditor finds that firewalls are outdated and not supported by vendors.
Which of the following should be the auditor's NEXT course of action?

A. Report the mitigating controls.

B. Report the security posture of the organization.

C. Determine the value of the firewall.

D. Determine the risk of not replacing the firewall.

Answer(s): D

---

13. Which of the following is the BEST way to determine whether a test of a disaster recovery plan (DRP) was successful?

A. Analyze whether predetermined test objectives were met.

B. Perform testing at the backup data center.

C. Evaluate participation by key personnel.

D. Test offsite backup files.

Answer(s): A

---

14. An IS auditor found that a company executive is encouraging employee use of social networking sites for business purposes.
Which of the following recommendations would BEST help to reduce the risk of data leakage?

A. Requiring policy acknowledgment and nondisclosure agreements (NDAs) signed by employees

B. Establishing strong access controls on confidential data

C. Providing education and guidelines to employees on use of social networking sites

D. Monitoring employees' social networking usage

Answer(s): C

---

15. An IS auditor notes that several employees are spending an excessive amount of time using social media sites for personal reasons.
Which of the following should the auditor recommend be performed FIRST?

A. Implement a process to actively monitor postings on social networking sites.

B. Adjust budget for network usage to include social media usage.

C. Use data loss prevention (DLP) tools on endpoints.

D. implement policies addressing acceptable usage of social media during working hours.

Answer(s): D

---

16. Which of the following fire suppression systems needs to be combined with an automatic switch to shut down the electricity supply in the event of activation?

A. Carbon dioxide

B. FM-200

C. Dry pipe

D. Halon

Answer(s): C

---

17. Which of the following would MOST likely impair the independence of the IS auditor when performing a post-implementation review of an application system?

A. The IS auditor provided consulting advice concerning application system best practices.

B. The IS auditor participated as a member of the application system project team, but did not have operational responsibilities.

C. The IS auditor designed an embedded audit module exclusively for auditing the application system.

D. The IS auditor implemented a specific control during the development of the application system.

Answer(s): D

---

18. An organization plans to receive an automated data feed into its enterprise data warehouse from a third-party service provider.
Which of the following would be the BEST way to prevent accepting bad data?

A. Obtain error codes indicating failed data feeds.

B. Appoint data quality champions across the organization.

C. Purchase data cleansing tools from a reputable vendor.

D. Implement business rules to reject invalid data.

Answer(s): D

---

19. An IS auditor suspects an organization's computer may have been used to commit a crime. Which of the following is the auditor's BEST course of action?

A. Examine the computer to search for evidence supporting the suspicions.

B. Advise management of the crime after the investigation.

C. Contact the incident response team to conduct an investigation.

D. Notify local law enforcement of the potential crime before further investigation.

Answer(s): C

---

20. Which of the following access rights presents the GREATEST risk when granted to a new member of the system development staff?

A. Write access to production program libraries

B. Write access to development data libraries

C. Execute access to production program libraries

D. Execute access to development program libraries

Answer(s): A
