IS Management Practices

1. From a control perspective, the key element in job descriptions is that they:

A. provide instructions on how to do the job and define authority.

B. are current, documented and readily available to the employee.

C. communicate management's specific job performance expectations.

D. establish responsibility and accountability for the employee's actions.

2. The MOST likely affect of the lack of senior management commitment to IT strategic planning is:

A. a lack of investment in technology.

B. a lack of a methodology for systems development.

C. that the technology will not be aligned with the organization's objectives.

D. an absence of control over technology contracts.

3. Which of the following would BEST provide assurance of the integrity of new staff?

A. Background screening

B. References

C. Bonding

D. Qualifications listed on a resumé

4. Which of the following is the GREATEST risk of an inadequate policy definition for ownership of data and systems?

A. User management coordination does not exist.

B. Specific user accountability cannot be established.

C. Unauthorized users may have access to originate, modify or delete data.

D. Audit recommendations may not be implemented.

5. The PRIMARY objective of an audit of IT security policies is to ensure that:

A. they are distributed and available to all staff.

B. security and control policies support business and IT objectives.

C. there is a published organizational chart with functional descriptions.

D. duties are appropriately segregated.

6. IT control objectives are useful to IS auditors, as they provide the basis for understanding the:

A. desired result or purpose of implementing specific control procedures.

B. best IT security control practices relevant to a specific entity.

C. techniques for securing information.

D. security policy.

7. In reviewing the IS short-range (tactical) plan, the IS auditor should determine whether:

A. there is an integration of IS and business staffs within projects.

B. there is a clear definition of the IS mission and vision.

C. there is a strategic information technology planning methodology in place.

D. the plan correlates business objectives to IS goals and objectives.

8. The rate of change in technology increases the importance of:

A. outsourcing the IS function.

B. implementing and enforcing good processes.

C. hiring personnel willing to make a career within the organization.

D. meeting user requirements.

9. An organization acquiring other businesses continues using its legacy EDI systems and uses three separate value-added network (VAN) providers. No written VAN agreements exist. The IS auditor should recommend that management:

A. obtains independent assurance of the third-party service providers.

B. sets up a process for monitoring the service delivery of the third party.

C. ensures that formal contracts are in place.

D. considers agreements with third-party service providers in the development of continuity plans.

10. Which of the following reports should an IS auditor use to check compliance with a service level agreement's (SLA) requirement for uptime?

A. Utilization reports

B. Hardware error reports

C. System logs

D. Availability reports

11. The implementation of cost-effective controls in an automated system is ultimately the responsibility of the:

A. system administrator.

B. quality assurance function.

C. business unit management.

D. chief of internal audit.

12. An IS auditor finds that not all employees are aware of the enterprise's information security policy. The IS auditor should conclude that:

A. this lack of knowledge may lead to unintentional disclosure of sensitive information

B. information security is not critical to all functions.

C. IS audit should provide security training to the employees.

D. the audit finding will cause management to provide continuous training to staff.

13. An IS auditor reviews an organizational chart PRIMARILY for:

A. an understanding of workflows.

B. investigating various communication channels.

C. understanding the responsibilities and authority of individuals.

D. investigating the network connected to different employees.

14. When an employee is terminated from service, the MOST important action is to:

A. hand over all of the employee's files to another designated employee.

B. complete a back up of the employee's work.

C. notify other employees of the termination.

D. disable the employee's logical access.

15. The initial step in establishing an information security program is the:

A. development and implementation of an information security standards manual.

B. performance of a comprehensive security control review by the IS auditor.

C. adoption of a corporate information security policy statement.

D. purchase of security access control software.

16. Which of the following is the MOST important function to be performed by IS management when a service has been outsourced?

A. Ensuring that invoices are paid to the provider

B. Participating in systems design with the provider

C. Renegotiating the provider's fees

D. Monitoring the outsourcing provider's performance

17. When an information security policy has been designed, it is MOST important that the information security policy be:

A. stored offsite.

B. written by IS management.

C. circulated to users.

D. updated frequently.

18. An IS auditor performing a review of the IS department discovers that formal project approval procedures do not exist. In the absence of these procedures, the IS manager has been arbitrarily approving projects that can be completed in a short duration and referring other, more complicated projects to higher levels of management for approval. The IS auditor should recommend as a FIRST course of action that:

A. users participate in the review and approval process.

B. formal approval procedures be adopted and documented.

C. projects be referred to appropriate levels of management for approval.

D. the IS manager's job description be changed to include approval authority.

19. Which of the following would an IS auditor consider to be the MOST important when evaluating an organization's IS strategy? That it:

A. has been approved by line management.

B. does not vary from the IS department's preliminary budget.

C. complies with procurement procedures.

D. supports the business objectives of the organization.

20. The development of an IS security policy is ultimately the responsibility of the:

A. IS department.

B. security committee.

C. security administrator.

D. board of directors.

21. Many organizations require an employee to take a mandatory vacation (holiday) of a week or more to:

A. ensure the employee maintains a quality of life, which will lead to greater productivity.

B. reduce the opportunity for an employee to commit an improper or illegal act.

C. provide proper cross-training for another employee.

D. eliminate the potential disruption caused when an employee takes vacation one day at a time.

22. A long-term IS employee with a strong technical background and broad managerial experience has applied for a vacant position in the IS audit department. Determining whether to hire this individual for this position should be based on the individual's experience and:

A. the length of service since this will help ensure technical competence.

B. age as training in audit techniques may be impractical.

C. IS knowledge since this will bring enhanced credibility to the audit function.

D. ability, as an IS auditor, to be independent of existing IS relationships.

23. A probable advantage to an organization that has outsourced its data processing services is that:

A. needed IS expertise can be obtained from the outside.

B. greater control can be exercised over processing.

C. processing priorities can be established and enforced internally.

D. greater user involvement is required to communicate user needs.

24. In a small organization, an employee performs computer operations and, when the situation demands, program modifications. Which of the following should the IS auditor recommend?

A. Automated logging of changes to development libraries

B. Additional staff to provide separation of duties

C. Procedures that verify that only approved program changes are implemented

D. Access controls to prevent the operator from making program modifications

25. Which of the following should be included in an organization’s IS security policy?

A. A list of key IT resources to be secured

B. The basis for access authorization

C. Identity of sensitive security features

D. Relevant software security features

26. A comprehensive and effective e-mail policy should address the issues of e-mail structure, policy enforcement, monitoring and:

A. recovery.

B. retention.

C. rebuilding.

D. reuse.

27. An organization has outsourced its software development. Which of the following is the responsibility of the organization's IT management?

A. Paying for provider services

B. Participating in systems design with the provider

C. Managing compliance with the contract for the outsourced services

D. Negotiating contractual agreement with the provider

28. In an organization where an IT security baseline has been defined, the IS auditor should FIRST ensure:

A. implementation.

B. compliance.

C. documentation.

D. sufficiency.

28. An IS auditor performing a general controls review of IS management practices relating to personnel should pay particular attention to:

A. mandatory vacation policies and compliance.

B. staff classifications and fair compensation policies.

C. staff training.

D. the functions assigned to staff.

29. Effective IT governance will ensure that the IT plan is consistent with the organization's:

A. business plan.

B. audit plan.

C. security plan.

D. investment plan.

30. IT governance is PRIMARILY the responsibility of the:

A. chief executive officer.

B. board of directors.

C. IT steering committee.

D. audit committee.

31. From a control perspective, the key element in job descriptions is that they:

A. provide instructions on how to do the job and define authority.

B. are current, documented and readily available to the employee.

C. communicate management's specific job performance expectations.

D. establish responsibility and accountability for the employee's actions.

32. The rate of change in technology increases the importance of:

A. outsourcing the IS function.

B. implementing and enforcing good processes.

C. hiring personnel willing to make a career within the organization.

D. meeting user requirements.

33. An IS auditor finds that not all employees are aware of the enterprise's information security policy. The IS auditor should conclude that:

A. this lack of knowledge may lead to unintentional disclosure of sensitive information

B. information security is not critical to all functions.

C. IS audit should provide security training to the employees.

D. the audit finding will cause management to provide continuous training to staff.

34. When an information security policy has been designed, it is MOST important that the information security policy be:

A. stored offsite.

B. written by IS management.

C. circulated to users.

D. updated frequently.

35. The development of an IS security policy is ultimately the responsibility of the:

A. IS department.

B. security committee.

C. security administrator.

D. board of directors.

36. Which of the following is the MOST critical for the successful implementation and maintenance of a security policy?

A. Assimilation of the framework and intent of a written security policy by all appropriate parties

B. Management support and approval for the implementation and maintenance of a security policy

C. Enforcement of security rules by providing punitive actions for any violation of security rules

D. Stringent implementation, monitoring and enforcing of rules by the security officer through access control software

37. Which of the following is the PRIMARY objective of an IT performance measurement process?

A. Minimize errors.

B. Gather performance data.

C. Establish performance baselines.

D. Optimize performance.

38. A top-down approach to the development of operational policies will help ensure:

A. that they are consistent across the organization.

B. that they are implemented as a part of risk assessment.

C. compliance with all policies.

D. that they are reviewed periodically.

39. An IS auditor reviewing an organization that uses cross-training practices should assess the risk of:

A. dependency on a single person.

B. inadequate succession planning.

C. one person knowing all parts of a system.

D. a disruption of operations.

40. When an organization is outsourcing their information security function, which of the following should be kept in the organization?

A. Accountability for the corporate security policy

B. Defining the corporate security policy

C. Implementing the corporate security policy

D. Defining security procedures and guidelines

41. From a control perspective, the key element in job descriptions is that they:

A. provide instructions on how to do the job and define authority.

B. are current, documented and readily available to the employee.

C. communicate management's specific job performance expectations.

D. establish responsibility and accountability for the employee's actions.

42. Which of the following is the **BEST** performance criterion for evaluating the adequacy of an organization's security awareness training?

A. Senior management is aware of critical information assets and demonstrates an adequate concern for their protection.

B. Job descriptions contain clear statements of accountability for information security.

C. In accordance with the degree of risk and business impact, there is adequate funding for security efforts.

D. No actual incidents have occurred that have caused a loss or a public embarrassment.

43.Which of the following is the **GREATEST** risk of an inadequate policy definition for ownership of data and systems?

A. User management coordination does not exist.

B. Specific user accountability cannot be established.

C. Unauthorized users may have access to originate, modify or delete data.

D. Audit recommendations may not be implemented.

44. The **PRIMARY** objective of an audit of IT security policies is to ensure that:

A. they are distributed and available to all staff.

B. security and control policies support business and IT objectives.

C. there is a published organizational chart with functional descriptions.

D. duties are appropriately segregated.

45. The management of an organization has decided to establish a security awareness program. Which of the following would **MOST** likely be a part of the program?

A. Utilization of an intrusion detection system to report incidents

B. Mandating the use of passwords to access all software

C. Installing an efficient user log system to track the actions of each user

D. Training provided on a regular basis to all current and new employees

46. Which of the following is the **MOST** important function to be performed by IS management when a service has been outsourced?

A. Ensuring that invoices are paid to the provider

B. Participating in systems design with the provider

C. Renegotiating the provider's fees

D. Monitoring the outsourcing provider's performance

47. When an organization is outsourcing their information security function, which of the following should be kept in the organization?

A. Accountability for the corporate security policy

B. Defining the corporate security policy

C. Implementing the corporate security policy

D. Defining security procedures and guidelines

48. With respect to the outsourcing of IT services, which of the following conditions should be of **GREATEST** concern to an IS auditor?

A. Outsourced activities are core and provide a differentiated advantage to the organization.

B. Periodic renegotiation is specified in the outsourcing contract.

C. The outsourcing contract fails to cover every action required by the arrangement.

D. Similar activities are outsourced to more than one vendor.

49. The rate of change in technology increases the importance of:

A. outsourcing the IS function.

B. implementing and enforcing sound processes.

C. hiring qualified personnel.

D. meeting user requirements.

50. To ensure an organization is complying with privacy requirements, an IS auditor should FIRST review:

A. the IT infrastructure.

B. organizational policies, standards and procedures.

C. legal and regulatory requirements.

D. adherence to organizational policies, standards and procedures.