IS Management Practices – 1st June, 2014

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.

The correct answer is:

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

Explanation:

From a control perspective, a job description should establish responsibility and accountability. This will aid in ensuring that users are given system access in accordance with their defined job responsibilities. The other choices are not directly related to controls. Providing instructions on how to do the job and defining authority addresses the managerial and procedural aspects of the job. It is important that job descriptions are current, documented and readily available to the employee, but this in itself is not a control. Communication of management’s specific expectations for job performance outlines the standard of performance and would not necessarily include controls.

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.

The correct answer is:

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

Explanation:

A steering committee should exist to ensure that the IT strategies support the organization’s goals. The absence of an information technology committee or a committee not composed of senior managers would be an indication of a lack of top-level management commitment. This condition would increase the risk that IT would not be aligned with the organization’s strategy.

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

The correct answer is:

A. Background screening

Explanation:

A background screening is the primary method for assuring the integrity of a prospective staff member. References are important and would need to be verified, but they are not as reliable as background screening. Bonding is directed at due-diligence compliance, not at integrity, and qualifications listed on a resumé may not be accurate.

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.

The correct answer is:

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

Explanation:

Without a policy defining who has the responsibility for granting access to specific systems, there is an increased risk that one could gain (be given) system access when they should not have authorization. By assigning authority to grant access to specific users, there is a better chance that business objectives will be properly supported.

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.

The correct answer is:

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

Explanation:

Business orientation should be the main theme in implementing security. Hence, an IS audit of IT security policies should primarily focus on whether the IT and related security and control policies support business and IT objectives. Reviewing whether policies are available to all is an objective, but distribution does not ensure compliance. Availability of organizational charts with functional descriptions and segregation of duties might be included in the review, but are not the primary objective of an audit of security policies.

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.

The correct answer is:

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

Explanation:

An IT control objective is defined as the statement of the desired result or purpose to be achieved by implementing control procedures in a particular IT activity. They provide the actual objectives for implementing controls and may or may not be the best practices. Techniques are the means of achieving an objective, and a security policy is a subset of IT control objectives.

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.

The correct answer is:

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

Explanation:

The integration of IS and business staff in projects is an operational issue and should be considered while reviewing the short-range plan. A strategic plan would provide a framework for the IS short-range plan. Choices B, C and D are areas covered by a strategic plan.

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.

The correct answer is:

B. implementing and enforcing good processes.

Explanation:

Change requires that good change management processes be implemented and enforced. Outsourcing the IS function is not directly related to the rate of technological change. Personnel in a typical IS department are highly qualified and educated, usually they do not feel their jobs are at risk and are prepared to switch jobs frequently. Although meeting user requirements is important, it is not directly related to the rate of technological change in the IS environment.

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.

The correct answer is:

C. ensures that formal contracts are in place.

Explanation:

Written agreements would assist management in ensuring compliance with external requirements. While management should obtain independent assurance of compliance, this cannot be achieved until there is a contract in place. One aspect of managing third-party services is to provide monitoring; however, this cannot be achieved until there is a contract. Ensuring that VAN agreements are available for review may assist in the development of continuity plans, if they are deemed critical IT resources. However, this cannot be achieved until a contract is in place.

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

The correct answer is:

D. Availability reports

Explanation:

IS inactivity, such as downtime, is addressed by availability reports. These reports provide the time periods during which the computer was available for utilization by users or other processes. Utilization reports document the use of computer equipment, and can be used by management to predict how/where/when resources are required. Hardware error reports provide information to aid in detecting hardware failures and initiating corrective action. System logs are a recording of the system’s activities.

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.

The correct answer is:

C. business unit management.

Explanation:

It is the business unit management's responsibility to implement cost-effective controls in an automated system. They are the best group in an organization to know which information assets need to be secured in terms of availability, confidentiality and integrity. System administrators take care of services related to the system requirements of the user management group. The quality assurance function addresses the overall quality of the systems. The audit group will assess or examine the compliance level of the controls with written policies, procedures or practices.

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.

The correct answer is:

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

Explanation:

All employees should be aware of the enterprise's information security policy to prevent unintentional disclosure of sensitive information. Training is a preventive control. Security awareness programs for employees can prevent unintentional disclosure of sensitive information to outsiders.

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.

The correct answer is:

C. understanding the responsibilities and authority of individuals.

Explanation:

An organizational chart provides information about the responsibilities and authority of individuals in the organization. This helps the IS auditor to know if there is a proper segregation of functions. A workflow chart would provide information about the roles of different employees. A network diagram will provide information about the usage of various communication channels and will indicate the connection of users to the network.

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.

The correct answer is:

D. disable the employee's logical access.

Explanation:

There is a probability that a terminated employee may misuse access rights; therefore, disabling the terminated employee's logical access is the most important action to take. All the work of the terminated employee needs to be handed over to a designated employee; however, this should be performed after implementing choice D. All the work of the terminated employee needs to be backed up and the employees need to be notified of the termination of the employee, but this should not precede the action in choice D.

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.

The correct answer is:

C. adoption of a corporate information security policy statement.

Explanation:

A policy statement reflects the intent and support provided by executive management for proper security and establishes a starting point for developing the security program.

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

The correct answer is:

D. Monitoring the outsourcing provider’s performance

Explanation:

In an outsourcing environment, the company is dependent on the performance of the service provider. Therefore, it is critical the outsourcing provider’s performance be monitored to ensure that services are delivered to the company as required. Payment of invoices is a finance function, which would be completed per contractual requirements. Participating in systems design is a by-product of monitoring the outsourcing provider’s performance, while renegotiating fees is usually a one-time activity.

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.

The correct answer is:

C. circulated to users.

Explanation:

To be effective, an information security policy should reach all members of the staff. Storing the security policy offsite or in a safe place may be desirable but of little value if its contents are not known to the organization’s employees. The information security policy should be written by business unit managers including IS, but not exclusively IS managers. Updating the information security policy is important but will not assure its dissemination.

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.

The correct answer is:

B. formal approval procedures be adopted and documented.

Explanation:

It is imperative that formal, written approval procedures be established to set accountability. This is true of the IS manager and higher levels of management. Choices A, C and D would be subsequent recommendations once authority has been established.

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.

The correct answer is:

D. supports the business objectives of the organization.

Explanation:

Strategic planning sets corporate or department objectives into motion. Both long-term and short-term strategic plans should be consistent with the organization’s broader plans and business objectives for attaining these goals. Answer A is incorrect since line management prepared the plans.

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.

The correct answer is:

D. board of directors.

Explanation:

Normally the designing of an information systems security policy is the responsibility of top management or the board of directors. The IS department is responsible for the execution of the policy, having no authority in framing the policy. The security committee also functions within the broad security policy framed by the board of directors. The security administrator is responsible for implementing, monitoring and enforcing the security rules that management has established and authorized.

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.

The correct answer is:

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

Explanation:

Required vacations/holidays of a week or more duration in which someone other than the regular employee performs the job function is often mandatory for sensitive positions. This reduces the opportunity to commit improper or illegal acts, and during this time it may be possible to discover any fraudulent activity that was taking place. Choices A, C and D could all be organizational benefits from a mandatory vacation policy, but they are not the reason why the policy is established.

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.

The correct answer is:

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

Explanation:

Independence should be continually assessed by the auditor and management. This assessment should consider such factors as changes in personal relationships, financial interests, and prior job assignments and responsibilities. The fact that the employee has worked in IS for many years may not in itself ensure credibility. The audit department's needs should be defined and any candidate should be evaluated against those requirements. In addition, the length of service will not ensure technical competency, and evaluating an individual's qualifications based on the age of the individual is not a good criterion and is illegal in many parts of the world.

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.

The correct answer is:

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

Explanation:

Outsourcing is a contractual arrangement whereby the organization relinquishes control over part or all of the information processing to an external party. This is frequently done to acquire additional resources or expertise that is not obtainable from inside the organization.

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

The correct answer is:

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

Explanation:

While it would be preferred that strict separation of duties be adhered to and that additional staff is recruited, as suggested in choice B, this practice is not always possible in small organizations. The IS auditor must look at recommended alternative processes. Of the choices, C is the only practical one that has an impact. The IS auditor should recommend processes that detect changes to production source and object code, such as code comparisons, so the changes can be reviewed on a regular basis by a third party. This would be a compensating control process. Choice A, involving logging of changes to development libraries, would not detect changes to production libraries. Choice D is in effect requiring a third party to do the changes, which may not be practical in a small organization.

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

The correct answer is:

B. The basis for access authorization

Explanation:

The security policy provides the broad framework of security, as laid down and approved by the senior management. It includes a definition of those authorized to grant access and the basis for granting the access. Choices A, B and C are more detailed than that which should be included in a policy.

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.

The correct answer is:

B. retention.

Explanation:

Besides being a good practice, laws and regulations may require that an organization keep information that has an impact on the financial statements. The prevalence of lawsuits in which e-mail communication is held in the same regard as the official form of classic "paper" makes the retention of corporate e-mail a necessity. All e-mail generated on an organization's hardware is the property of the organization, and an e-mail policy should address the retention of messages, considering both known and unforeseen litigation. The policy should also address the destruction of e-mails after a specified time to protect the nature and confidentiality of the messages themselves. Addressing the retention issue in the e-mail policy would facilitate recovery, rebuilding and 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

The correct answer is:

C. Managing compliance with the contract for the outsourced services

Explanation:

Actively managing compliance with the contract terms for the outsourced services is the responsibility of IT management. Payment of invoices is a finance responsibility. Negotiation of the contractual agreement would have already taken place and is usually a shared responsibility of the legal department and other departments, such as IT.

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.

The correct answer is:

D. sufficiency.

Explanation:

The auditor should first evaluate the definition of the minimum baseline level by ensuring the sufficiency of controls. Documentation, implementation and compliance are further steps.

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.

The correct answer is:

D. the functions assigned to staff.

Explanation:

When performing a general controls review it is important for an IS auditor to pay attention to the issue of segregation of duties, which is affected by vacation/holiday practices. Mandatory vacation policies and compliance may vary depending on the country and industry. Staff classifications and fair compensation policies may be a morale issue, not a controls issue. Staff training is desirable, but not as critical as an appropriate segregation of duties.

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.

The correct answer is:

A. business plan.

Explanation:

To govern IT effectively, IT and business should be moving in the same direction, requiring that the IT plans are aligned with an organization's business plans. The audit and investment plans are not part of the IT plan, and the security plan should be at a corporate level.

30. IT governance is PRIMARILY the responsibility of the:

A. chief executive officer.

B. board of directors.

C. IT steering committee.

D. audit committee.

The correct answer is:

B. board of directors.

Explanation:

IT governance is primarily the responsibility of the executives and shareholders (as represented by the board of directors). The chief executive officer is instrumental in implementing IT governance per the directions of the board of directors. The IT steering committee monitors and facilitates deployment of IT resources for specific projects in support of business plans. The audit committee reports to the board of directors and should monitor the implementation of audit recommendations.

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.

The correct answer is:

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

Explanation:

From a control perspective, a job description should establish responsibility and accountability. This will aid in ensuring that users are given system access in accordance with their defined job responsibilities. The other choices are not directly related to controls. Providing instructions on how to do the job and defining authority addresses the managerial and procedural aspects of the job. It is important that job descriptions are current, documented and readily available to the employee, but this in itself is not a control. Communication of management's specific expectations for job performance outlines the standard of performance and would not necessarily include controls.

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.

The correct answer is:

B. implementing and enforcing good processes.

Explanation:

Change requires that good change management processes be implemented and enforced. Outsourcing the IS function is not directly related to the rate of technological change. Personnel in a typical IS department are highly qualified and educated, usually they do not feel their jobs are at risk and are prepared to switch jobs frequently. Although meeting user requirements is important, it is not directly related to the rate of technological change in the IS environment.

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.

The correct answer is:

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

Explanation:

All employees should be aware of the enterprise's information security policy to prevent unintentional disclosure of sensitive information. Training is a preventive control. Security awareness programs for employees can prevent unintentional disclosure of sensitive information to outsiders.

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.

The correct answer is:

C. circulated to users.

Explanation:

To be effective, an information security policy should reach all members of the staff. Storing the security policy offsite or in a safe place may be desirable, but is of little value if its contents are not known to the organization's employees. The information security policy should be written by business unit managers including, but not exclusively, IS managers. Updating the information security policy is important but will not assure its dissemination.

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.

The correct answer is:

D. board of directors.

Explanation:

Normally, the designing of an information systems security policy is the responsibility of top management or the board of directors. The IS department is responsible for the execution of the policy, having no authority in framing the policy. The security committee also functions within the broad security policy framed by the board of directors. The security administrator is responsible for implementing, monitoring and enforcing the security rules that management has established and authorized.

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

The correct answer is:

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

Explanation:

Assimilation of the framework and intent of a written security policy by the users of the system is critical to the successful implementation and maintenance of the security policy. A good password system may exist, but if the users of the system keep passwords written on his/her table, the password is of little value. Management support and commitment is no doubt important, but for successful implementation and maintenance of security policy, educating the users on the importance of security is paramount. The stringent implementation, monitoring and enforcing of rules by the security officer through access control software, and provision for punitive actions for violation of security rules are also required along with the user's education on the importance of security.

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.

The correct answer is:

D. Optimize performance.

Explanation:

An IT performance measurement process can be used to optimize performance, measure and manage products/services, assure accountability, and make budget decisions. Minimizing errors is an aspect of performance, but not the primary objective of performance management. Gathering performance data is a phase of the IT measurement process and would be used to evaluate the performance against previously established performance baselines.

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.

The correct answer is:

A. that they are consistent across the organization.

Explanation:

Deriving lower level policies from corporate policies (a top-down approach) aids in ensuring consistency across the organization and consistency with other policies. The bottom-up approach to the development of operational policies is derived as a result of risk assessment. A top-down approach of itself does not ensure compliance and development does not ensure that policies are reviewed.

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.

The correct answer is:

C. one person knowing all parts of a system.

Explanation:

Cross-training is a process of training more than one individual to perform a specific job or procedure. This practice helps decrease the dependence on a single person and assists in succession planning. This provides for the backup of personnel in the event of an absence and, thereby, provides for the continuity of operations. However, in using this approach, it is prudent to have first assessed the risk of any person knowing all parts of a system and the related potential exposures. Cross-training reduces the risks addressed in choices A, B and D.

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

The correct answer is:

A. Accountability for the corporate security policy

Explanation:

Accountability cannot be transferred to external parties. Choices B, C and D can be performed by outside entities as long as accountability remains within the organization.

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.

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

Explanation

From a control perspective, a job description should establish responsibility and accountability. This will aid in ensuring that users are given system access in accordance with their defined job responsibilities. The other choices are not directly related to controls. Providing instructions on how to do the job and defining authority addresses the managerial and procedural aspects of the job. It is important that job descriptions are current, documented and readily available to the employee, but this in itself is not a control. Communication of management's specific expectations for job performance outlines the standard of performance and would not necessarily include controls.

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.

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

Explanation

Inclusion in job descriptions of security responsibilities is a form of security training and helps ensure that staff and management are aware of their roles with respect to information security. The other three choices are not criterion for evaluating security awareness training. Awareness is a criterion for evaluating the importance that senior management attaches to information assets and their protection. Funding is a criterion that aids in evaluating whether security vulnerabilities are being addressed, and the number of incidents that have occurred is a criterion for evaluating the adequacy of the risk management program.

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.

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

Without a policy defining who has the responsibility for granting access to specific systems, there is an increased risk that one could gain (be given) system access when they should not have authorization. By assigning authority to grant access to specific users, there is a better chance that business objectives will be properly supported.

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.

Answer : **B. security and control policies support business and IT objectives.**

Business orientation should be the main theme in implementing security. Hence, an IS audit of IT security policies should primarily focus on whether the IT and related security and control policies support business and IT objectives. Reviewing whether policies are available to all is an objective, but distribution does not ensure compliance. Availability of organizational charts with functional descriptions and segregation of duties might be included in the review, but are not the primary objective of an audit of security policies.

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

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

Utilizing an intrusion detection system to report on incidents that occur is an implementation of a security program and is not effective in establishing a security awareness program. Choices B and C do not address awareness. Training is the only choice that is directed at security awareness.

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

Answer : **D. Monitoring the outsourcing provider's performance**

In an outsourcing environment, the company is dependent on the performance of the service provider. Therefore, it is critical the outsourcing provider's performance be monitored to ensure that services are delivered to the company as required. Payment of invoices is a finance function, which would be completed per contractual requirements. Participating in systems design is a byproduct of monitoring the outsourcing provider's performance, while renegotiating fees is usually a one-time activity.

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

Answer : **A. Accountability for the corporate security policy**

Accountability cannot be transferred to external parties. Choices B, C and D can be performed by outside entities as long as accountability remains within the organization.

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.

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

An organization's core activities generally should not be outsourced, because they are what the organization does best. An auditor observing that should be concerned. The auditor should not be concerned about the other conditions because specification of periodic renegotiation in the outsourcing contract is a best practice. Outsourcing contracts cannot be expected to cover every action and detail expected of the parties involved, and multisourcing is an acceptable way to reduce risk.

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.

Answer B Change requires that good change management processes be implemented and enforced.
Outsourcing the IS function is not directly related to the rate of technological change. Personnel in a typical IS department are highly qualified and educated; usually they do not feel their jobs are at risk and are prepared to switch jobs frequently.
Although meeting user requirements is important, it is not directly related to the rate of technological change in the IS environment.

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.

Answer C To ensure that the organization is complying with privacy issues, an IS auditor should address legal and regulatory requirements first.

To comply with legal and regulatory requirements, organizations need to adopt the appropriate infrastructure. After understanding the legal and regulatory requirements, an IS auditor should evaluate organizational policies, standards and procedures to determine whether they adequately address the privacy requirements, and then review the adherence to these specific policies, standards and procedures.