01. A financial enterprise has had difficulties establishing clear responsibilities between its IT strategy committee and its IT steering committee. Which of the following responsibilities would **MOST** likely be assigned to its IT steering committee?

A. Approving IT project plans and budgets
B. Aligning IT to business objectives
C. Advising on IT compliance risk
D. Promoting IT governance practices

An IT steering committee typically has a variety of responsibilities, including approving IT project plans and budgets. Choices B, C and D are responsibilities that are generally assigned to an IT strategy committee because it provides insight and advice to the board.

02. After implementation of a disaster recovery plan, predisaster and postdisaster operational costs for an organization will:

A. decrease.
B. not change (remain the same).
C. increase.
D. increase or decrease depending upon the nature of the business.

There are costs associated with all activities and a disaster recovery plan is not an exception. Although there are costs associated with a disaster recovery plan, there are unknown costs that are incurred if a disaster recovery plan is not implemented.

02. An enterprise hosts its data center onsite and has outsourced the management of its key financial applications. Which of the following controls **BEST** ensures that the outsourced company's employees adhere to the security policies?

A. Sign-off is required on the enterprise's security policies for all users.
B. An indemnity clause is included in the contract with the service provider.
C. Mandatory security awareness training is implemented for all users.
D. Security policies should be modified to address compliance by third-party users.

Having the service provider sign an indemnity clause will ensure compliance to the enterprise's security policies because any violations discovered would lead to a financial liability for the service provider. This will also prompt the enterprise to monitor security violations closely. Choices A and C are good practices; however, they put the onus of compliance on the individual user. Choice D does not ensure compliance by users unless the policies are appropriately communicated to users and awareness training is provided.

03. An IS auditor finds that, in accordance with IS policy, IDs of terminated users are deactivated within 90 days of termination. The IS auditor should:

A. report that the control is operating effectively since deactivation happens within the time frame stated in the IS policy.
B. verify that user access rights have been granted on a need-to-have basis.
C. recommend changes to the IS policy to ensure deactivation of user IDs upon termination.
D. recommend that activity logs of terminated users be reviewed on a regular basis.

Although a policy provides a reference for performing IS audit assignments, an IS auditor needs to review the adequacy and the appropriateness of the policy. If, in the opinion of the IS auditor, the time frame defined for deactivation is inappropriate, the auditor needs to communicate this to management and recommend changes to the policy. Although the deactivation happens as stated in the policy, it cannot be concluded that the control is effective. Best practice would require that the ID of a terminated user be deactivated immediately. Verifying that user access rights have been granted on a need-to-have basis is necessary when permissions are granted. Recommending that activity logs of terminated users be reviewed on a regular basis is a good practice, but not as effective as deactivation upon termination.

04. 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.

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.

05. An IS auditor has been assigned to review an organization's information security policy. Which of the following issues represents the **HIGHEST** potential risk?
    A. The policy has not been updated in more than one year.
    B. The policy includes no revision history.
    C. The policy is approved by the security administrator.
    D. The company does not have an information security policy committee.

    The information security policy should have an owner who has approved management responsibility for the development, review and evaluation of the security policy. The position of security administrator is typically a staff-level position (not management), and therefore would not have the authority to approve the policy. Without proper management approval, enforcing the policy may be problematic, leading to compliance or security issues. While the information security policy should be updated on a regular basis, the specific time period may vary based on the organization. Although reviewing policies annually is a best practice, the policy could be updated less frequently and still be relevant and effective. An outdated policy is still enforceable, whereas a policy without proper approval is not enforceable. The lack of a revision history with respect to the IS policy document is an issue, but not as significant as not having it approved by management. An IS policy committee is not required to develop and enforce a good information security policy. The policy could be written by one person, as long as the person who approves the policy has the proper authority and knowledge to review and approve the policy. Although a policy committee drawn from across the company is a best practice and may help write better policies, a good policy can be written by a single person, and the lack of a committee is not a problem by itself.

06. An IS auditor is performing an audit in the data center when the fire alarm begins sounding. The audit scope includes disaster recovery, so the auditor observes the data center staff response to the alarm. Which of the following is the **MOST** important action for the data center staff to complete in this scenario?
    A. Notify the local fire department of the alarm condition.
    B. Prepare to activate the fire suppression system.
    C. Ensure that all persons in the data center are evacuated.
    D. Remove all backup tapes from the data center.

    In an emergency, safety of life is always the first priority; therefore, the complete and orderly evacuation of the facility staff would be the most important activity. Notifying the fire department of the alarm is not typically necessary since most data center alarms are configured to automatically report to the local authorities. Fire suppression systems also are designed to operate automatically, and activating the system when staff are not yet evacuated could create confusion and panic, leading to injuries or even fatalities. Manual triggering of the system could be necessary under certain conditions, but only after all other data center personnel are safely evacuated. Removal of backup tapes from the data center is not an appropriate action since it could delay the evacuation of personnel. Most companies would have copies of backup tapes in offsite storage to mitigate the risk of data loss for this type of disaster.

07. An IS auditor noted that an organization had adequate business continuity plans for each individual process, but no comprehensive business continuity plan. Which would be the **BEST** course of action for the IS auditor?
    A. Recommend that an additional comprehensive BCP be developed.
    B. Determine whether the BCPs are consistent.
    C. Accept the BCPs as written.
    D. Recommend the creation of a single BCP.

    Depending on the complexity of the organization, there could be more than one plan to address various aspects of business continuity and disaster recovery. These do not necessarily have to be integrated into one single plan; however, each plan should be consistent with other plans to have a viable business continuity planning (BCP) strategy.

08. An IS auditor performing an audit of the risk assessment process should **FIRST** confirm that:
    A. reasonable threats to the information assets are identified.
    B. technical and organizational vulnerabilities have been analyzed.
    C. assets have been identified and ranked.
    D. the effects of potential security breaches have been evaluated.

    Identification and ranking of information assets—e.g., data criticality, locations of assets—will set the tone or scope of how to assess risk in relation to the organizational value of the asset. Second, the threats facing each of the organization's assets should be analyzed according to their value to the organization. Third, weakness should be identified so that controls can be evaluated to determine if they mitigate the weaknesses. Fourth, analyze how these weaknesses, in absence of given controls, would impact the organization information assets.

09. An IS auditor reviewing the IT organization would be **MOST** concerned if the IT steering committee:
    A. is responsible for project approval and prioritization.
    B. is responsible for developing the long-term IT plan.
    C. advises the board of directors on the relevance of developments in IT.
    D. is responsible for determining business goals.
    Determining the business goals is the responsibility of senior management and not of the IT steering committee. The other choices are all appropriate responsibilities of the IT steering committee.

10. An IT steering committee should review information systems **PRIMARILY** to assess:
    A. whether IT processes support business requirements
    B. whether proposed system functionality is adequate
    C. the stability of existing software
    D. the complexity of installed technology
    The role of an IT steering committee is to ensure that the IS department is in harmony with the organization's mission and objectives. To ensure this, the committee must determine whether IS processes support the business requirements. Assessing proposed additional functionality and evaluating software stability and the complexity of technology are too narrow in scope to ensure that IT processes are, in fact, supporting the organization's goals.

11. An organization has outsourced its help desk activities. An IS auditor's **GREATEST** concern when reviewing the contract and associated service level agreement (SLA) between the organization and vendor should be the provisions for:
    A. documentation of staff background checks.
    B. independent audit reports or full audit access.
    C. reporting the year-to-year incremental cost reductions.
    D. reporting staff turnover, development or training.
    When the functions of an IS department are outsourced, an IS auditor should ensure that a provision is made for independent audit reports that cover all essential areas, or that the outsourcer has full audit access. Although it is necessary to document the fact that background checks are performed, this is not as important as provisions for audits. Financial measures such as year-to-year incremental cost reductions are desirable to have in an SLA; however, cost reductions are not as important as the availability of independent audit reports or full audit access. An SLA might include human relationship measures such as resource planning, staff turnover, development or training, but this is not as important as the requirements for independent reports or full audit access by the outsourcing organization.

12. A financial services enterprise has a small IT department, and individuals perform more than one role. Which of the following practices represents the **GREATEST** risk?
    A. The developers promote code into the production environment.
    B. The business analyst writes the requirements and performs functional testing.
    C. The IT manager also performs systems administration.
    D. The database administrator (DBA) also performs data backups.
    If developers have access to the production environment, there is a risk that untested code can be migrated into the production environment. In situations in which there is no dedicated testing group, the business analyst is often the one to perform testing because the analyst has detailed knowledge of how the system must function as a result of writing the requirements. It is acceptable in a small team for the IT manager to perform system administration, as long as the manager does not also develop code. Choice D is not correct because it may be part of the DBA's duties to perform backups.

13. An IS auditor reviewing an organization's IT strategic plan should **FIRST** review:
    A. the existing IT environment.
    B. the business plan.
    C. the present IT budget.
    D. current technology trends.
    The IT strategic plan exists to support the organization's business plan. To evaluate the IT strategic plan, an IS auditor would first need to familiarize themselves with the business plan.

14. An IS auditor can verify that an organization's business continuity plan (BCP) is effective by reviewing the:
    A. alignment of the BCP with industry best practices.
    B. results of business continuity tests performed by IS and end-user personnel.
    C. offsite facility, its contents, security and environmental controls.
    D. annual financial cost of the BCP activities versus the expected benefit of implementation of the plan.
    The effectiveness of the BCP can best be evaluated by reviewing the results from previous business continuity tests for thoroughness and accuracy in accomplishing their stated objectives. All other choices do not provide the assurance of the effectiveness of the BCP.

15. An organization completed a business impact analysis (BIA) as part of business continuity planning. The **NEXT** step in the process is to develop:
    A. a business continuity strategy.
    B. a test and exercise plan.
    C. a user training program.
    D. the business continuity plan (BCP).
    A business continuity strategy is the next phase because it identifies the best way to recover. The criticality of the business process, the cost, the time required to recover and security must be considered during this phase. The recovery strategy and plan development precede the test plan. Training can only be developed once the BCP is in place. A strategy must be determined before the BCP is developed.

16. An IS auditor is reviewing changes to a company's disaster recovery (DR) strategy. The IS auditor notices that the recovery point objective (RPO) has been shortened for the company's mission-critical application. What is the **MOST** significant risk of this change?
    A. The existing DR plan is not updated to achieve the new RPO.
    B. The DR team has not been trained on the new RPO.
    C. Backups are not done frequently enough to achieve the new RPO.
    D. The plan has not been tested with the new RPO.
    The RPO is defined in the glossary of the CISA Review Manual as "the earliest point in time to which it is acceptable to recover the data." If backups are not performed frequently enough to meet the new RPO, a risk is created that the company will not have adequate backup data in the event of a disaster. This is the most significant risk because, without data, all other DR considerations are not useful. If the plan is not updated to reflect the new strategic goals of recovery time objective (RTO) and RPO, then the plan may not achieve those new goals. This is a less significant problem than not having the appropriate data available. The lack of training on the new DR strategy, as well as the lack of testing of the revised plan, both create risk in the team's ability to execute the plan; but, again, this risk is not as significant as not having data available due to the frequency of backups.

17. An IS auditor is reviewing an IT security risk management program. Measures of security risk should:
    A. address all of the network risk.
    B. be tracked over time against the IT strategic plan.
    C. take into account the entire IT environment.
    D. result in the identification of vulnerability tolerances.
    When assessing IT security risk, it is important to take into account the entire IT environment. Measures of security risk should focus on those areas with the highest criticality so as to achieve maximum risk reduction at the lowest possible cost. IT strategic plans are not granular enough to provide appropriate measures. Objective metrics must be tracked over time against measurable goals, thus the management of risk is enhanced by comparing today's results against last week, last month, last quarter. Risk measures will profile assets on a network to objectively measure vulnerability risk. They do not identify tolerances.

18. An IS auditor reviewing an outsourcing contract of IT facilities would expect it to define the:
    A. hardware configuration.
    B. access control software.
    C. ownership of intellectual property.
    D. application development methodology.
    Of the choices, the hardware and access control software is generally irrelevant as long as the functionality, availability and security can be affected, which are specific contractual obligations. Similarly, the development methodology should be of no real concern. The contract must, however, specify who owns the intellectual property (i.e., information being processed, application programs). Ownership of intellectual property will have a significant cost and is a key aspect to be defined in an outsourcing contract.

19. An IS auditor is reviewing a contract management process to determine the financial viability of a software vendor for a critical business application. An IS auditor should determine whether the vendor being considered:
    A. can deliver on the immediate contract.
    B. is of similar financial standing as the organization.
    C. has significant financial obligations that can impose liability to the organization.
    D. can support the organization in the long term.
    The long-term financial viability of a vendor is essential for deriving maximum value for the organization—it is more likely that a financially sound vendor would be in business for a long period of time. The capability of the organization to support the enterprise should extend beyond the time of execution of the contract. The objective of financial evaluation should not be confined to the immediate contract, but to provide assurance over a longer time frame. The specific financial condition of the vendor would not be of primary concern.

20. An organization has just completed their annual risk assessment. Regarding the business continuity plan, what should an IS auditor recommend as the next step for the organization?
    A. Review and evaluate the business continuity plan for adequacy
    B. Perform a full simulation of the business continuity plan
    C. Train and educate employees regarding the business continuity plan
    D. Notify critical contacts in the business continuity plan

    The business continuity plan should be reviewed every time a risk assessment is completed for the organization. Training of the employees and a simulation should be performed after the business continuity plan has been deemed adequate for the organization. There is no reason to notify the business continuity plan contacts at this time.
21. As a driver of IT governance, transparency of IT's cost, value and risk is primarily achieved through:
    A. performance measurement.
    B. strategic alignment.
    C. value delivery.
    D. resource management.

    Performance measurement includes setting and monitoring measurable objectives of what the IT processes need to deliver (process outcome) and how they deliver it (process capability and performance). Strategic alignment primarily focuses on ensuring linkage of business and IT plans. Value delivery is about executing the value proposition throughout the delivery cycle. Resource management is about the optimal investment in and proper management of critical IT resources. Transparency is primarily achieved through performance measurement as it provides information to the stakeholders on how well the enterprise is performing when compared to objectives.
22. Before implementing an IT balanced scorecard (BSC), an organization must:
    A. deliver effective and efficient services.
    B. define key performance indicators.
    C. provide business value to IT projects.
    D. control IT expenses.

    A definition of key performance indicators is required before implementing an IT BSC. Choices A, C and D are objectives.
23. During an audit, an IS auditor notices that the IT department of a medium-sized organization has no separate risk management function, and the organization's operational risk documentation only contains a few broadly described types of IT risk. What is the **MOST** appropriate recommendation in this situation?
    A. Create an IT risk management department and establish an IT risk framework with the aid of external risk management experts.
    B. Use common industry standard aids to divide the existing risk documentation into several individual types of risk which will be easier to handle.
    C. No recommendation is necessary since the current approach is appropriate for a medium-sized organization.
    D. Establish regular IT risk management meetings to identify and assess risk, and create a mitigation plan as input to the organization's risk management.

    Establishing regular IT risk management meetings is the best way to identify and assess IT-related risk in a medium-sized organization, to address responsibilities to the respective management and to keep the risk list and mitigation plans up to date. A medium-sized organization would normally not have a separate IT risk management department. Moreover, the risk is usually manageable enough so that external help would not be needed. While common risk may be covered by common industry standards, they cannot address the specific situation of an organization. Individual types of risk will not be discovered without a detailed assessment from within the organization. Splitting the one risk position into several is not sufficient.

24. During an audit of a business continuity plan (BCP), an IS auditor found that, although all departments were housed in the same building, each department had a separate BCP. The IS auditor recommended that the BCPs be reconciled. Which of the following areas should be reconciled **FIRST**?
    A. Evacuation plan
    B. Recovery priorities
    C. Backup storages
    D. Call tree

    Protecting human resources during a disaster-related event should be addressed first. Having separate BCPs could result in conflicting evacuation plans, thus jeopardizing the safety of staff and clients. Choices B, C and D may be unique to each department and could be addressed separately, but still should be reviewed for possible conflicts and/or the possibility of cost reduction, but only after the issue of human safety has been analyzed.

25. Effective IT governance requires organizational structures and processes to ensure that:
    A. the organization's strategies and objectives extend the IT strategy.
    B. the business strategy is derived from an IT strategy.
    C. IT governance is separate and distinct from the overall governance.
    D. the IT strategy extends the organization's strategies and objectives.
    Effective IT governance requires that board and executive management extend governance to IT and provide the leadership, organizational structures and processes that ensure that the organization's IT sustains and extends the organization's strategies and objectives, and that the strategy is aligned with business strategy. Choice A is incorrect because it is the IT strategy that extends the organizational objectives, not the opposite. IT governance is not an isolated discipline; it must become an integral part of the overall enterprise governance.

26. 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.
    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, while the security plan should be at a corporate level.

27. In determining the acceptable time period for the resumption of critical business processes:
    A. only downtime costs need to be considered.
    B. recovery operations should be analyzed.
    C. both downtime costs and recovery costs need to be evaluated.
    D. indirect downtime costs should be ignored.
    Both downtime costs and recovery costs need to be evaluated in determining the acceptable time period before the resumption of critical business processes. The outcome of the business impact analysis (BIA) should be a recovery strategy that represents the optimal balance. Downtime costs cannot be looked at in isolation. The quicker information assets can be restored and business processing resumed, the smaller the downtime costs. However, the expenditure needed to have the redundant capability required to recover information resources might be prohibitive for nonessential business processes. Recovery operations do not determine the acceptable time period for the resumption of critical business processes, and indirect downtime costs should be considered in addition to the direct cash outflows incurred due to business disruption. The indirect costs of a serious disruption to normal business activity, e.g., loss of customer and supplier goodwill and loss of market share, may actually be more significant than direct costs over time, thus reaching the point where business viability is threatened.

28. In a small manufacturing business, an IT employee is doing both manufacturing work as well as all the programming activities. Which of the following is the **BEST** control to mitigate risk in the given scenario?
    A. Access restrictions to prevent the clerk from accessing the production environment
    B. Segregation of duties implemented by hiring additional staff
    C. Automated logging of all program changes in the production environment
    D. Procedures to verify that only approved program changes are implemented
    Procedures to verify and review that only approved changes are implemented would be an effective control in this scenario. Segregation of duties will prevent a combination of conflicting functions, but choice B is not correct because it may not be practical in a small business to hire and maintain additional staff in order to achieve the desired segregation of duties. Choice A is not correct because denying the clerk access to the production environment would prevent work from being performed unless additional staff were retained, which is not a realistic solution and may not be economically viable for a small organization. Choice C is not correct because logging of program changes in the production environment will detect changes after they have been implemented but will not prevent unauthorized changes.

29. Many organizations require employees to take a mandatory one-week (or two-week) vacation each year **PRIMARILY** because the organization wants to ensure that:
    A. adequate cross-training exists between all functions of the organization.
    B. employee morale and satisfaction is maintained to help ensure an effective internal control environment.
    C. potential irregularities in processing are identified by temporarily replacing an employee in the job function.
    D. employee satisfaction is maintained to reduce the risk of processing errors.
    Employees who perform critical and sensitive functions within an organization should be required to take some time off in order to help ensure that irregularities and fraud are detected. Cross-training is a good practice to follow, but can be achieved without the requirement for mandatory vacation. Good employee morale and high levels of employee satisfaction are worthwhile objectives, but they should not be considered a means to achieve an

effective internal control system. Although high levels of employee satisfaction could contribute to fewer processing errors, this is not typically a reason to require a mandatory vacation policy.

30. Many organizations require an employee to take a mandatory vacation (holiday) of a week or more to:
    A. ensure the employee maintains a good 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.

    Required vacations/holidays of a week or more in duration in which someone other than the regular employee performs the job function is often mandatory for sensitive positions, as this reduces the opportunity to commit improper or illegal acts. 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.

31. Responsibility for the governance of IT should rest with the:
    A. IT strategy committee.
    B. chief information officer (CIO).
    C. audit committee.
    D. board of directors.

    Governance is the set of responsibilities and practices exercised by the board and executive management with the goal of providing strategic direction, ensuring that objectives are achieved, ascertaining that risk is managed appropriately and verifying that the enterprise's resources are used responsibly. The audit committee, the CIO and the IT strategy committee all play a significant role in the successful implementation of IT governance within an organization, but the ultimate accountability resides with the board of directors.

32. 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.

    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.

32 The IT balanced scorecard (BSC) is a business governance tool intended to monitor IT performance evaluation indicators other than:
    A. financial results.
    B. customer satisfaction.
    C. internal process efficiency.
    D. innovation capacity.

    Financial results have traditionally been the sole overall performance metric. The IT balanced scorecard (BSC) is an IT business governance tool aimed at monitoring IT performance evaluation indicators other than financial results. The IT BSC considers other key success factors, such as customer satisfaction, innovation capacity and processing.

33. When auditing the IT governance framework and IT risk management practices that exist within an organization, the IS auditor identified some undefined responsibilities regarding IT management and governance roles. Which of the following recommendations is the **MOST** appropriate?
    A. Review the strategic alignment of IT with the business.
    B. Implement accountability rules within the organization.
    C. Ensure that independent IT audits are conducted periodically.
    D. Create a chief risk officer (CRO) role in the organization

    IT risk is managed by embedding accountability into the enterprise. The IS auditor should recommend the implementation of accountability rules to ensure that all responsibilities are defined within the organization. While the strategic alignment of IT with business is important, it is not directly related to the gap identified in this scenario. Similarly, performing more frequent IS audits or recommending the creation of a new role (CRO) is not helpful if the accountability rules are not clearly defined and implemented.

34. When developing a formal enterprise security program, the **MOST** critical success factor (CSF) would be the:
    A. establishment of a review board
    B. creation of a security unit
    C. effective support of an executive sponsor
    D. selection of a security process owner

    The executive sponsor would be in charge of supporting the organization's strategic security program, and would aid in directing the organization's overall security management activities. Therefore, support by the executive level

of management is the most CSF. None of the other choices are effective without visible sponsorship of top management.

35. When developing a risk management program, what is the **FIRST** activity to be performed?
    A. Threat assessment
    B. Classification of data
    C. Inventory of assets
    D. Criticality analysis
    Identification of the assets to be protected is the first step in the development of a risk management program. A listing of the threats that can affect the performance of these assets and criticality analysis are later steps in the process. Data classification is required for defining access controls and in criticality analysis.

36. Which of the following activities performed by a database administrator (DBA) should be performed by a different person?
    A. Deleting database activity logs
    B. Implementing database optimization tools
    C. Monitoring database usage
    D. Defining backup and recovery procedures
    Since database activity logs record activities performed by the database administrator (DBA), deleting them should be performed by an individual other than the DBA. This is a compensating control to aid in ensuring an appropriate segregation of duties and is associated with the DBA's role. A DBA should perform the other activities as part of the normal operations.

37. Which of the following **BEST** supports the prioritization of new IT projects?
    A. Internal control self-assessment (CSA)
    B. Information systems audit
    C. Investment portfolio analysis
    D. Business risk assessment
    It is most desirable to conduct an investment portfolio analysis, which will present not only a clear focus on investment strategy, but will provide the rationale for terminating nonperforming IT projects. Internal CSA may highlight noncompliance to the current policy, but may not necessarily be the best source for driving the prioritization of IT projects. Like internal CSA, IS audits may provide only part of the picture for the prioritization of IT projects. Business risk analysis is part of the investment portfolio analysis but, by itself, is not the best method for prioritizing new IT projects.

38. Which of the following does a lack of adequate security controls represent?
    A. Threat
    B. Asset
    C. Impact
    D. Vulnerability
    The lack of adequate security controls represents a vulnerability, exposing sensitive information and data to the risk of malicious damage, attack or unauthorized access by hackers. This could result in a loss of sensitive information and lead to the loss of goodwill for the organization. A succinct definition of risk is provided by the Guidelines for the Management of IT Security published by the International Organization for Standardization (ISO), which defines risk as the “potential that a given threat will exploit the vulnerability of an asset or group of assets to cause loss or damage to the assets.” The various elements of the definition are vulnerability, threat, asset and impact. Lack of adequate security functionality in this context is a vulnerability.

39. Which of the following goals would you expect to find in an organization's strategic plan?
    A. Test a new accounting package.
    B. Perform an evaluation of information technology needs.
    C. Implement a new project planning system within the next 12 months.
    D. Become the supplier of choice for the product offered.
    Strategic planning sets corporate or departmental objectives into motion. Comprehensive planning helps ensure an effective and efficient organization. Strategic planning is time- and project-oriented, but also must address and help determine priorities to meet business needs. Long- and short-range plans should be consistent with the organization's broader plans for attaining their goals. Choice D represents a business objective that is intended to focus the overall direction of the business and would thus be a part of the organization's strategic plan. The other choices are project-oriented and do not address business objectives.

40. Which of the following IT governance best practices improves strategic alignment?
    A. Supplier and partner risk is managed.
    B. A knowledge base on customers, products, markets and processes is in place.
    C. A structure is provided that facilitates the creation and sharing of business information.
    D. Top management mediate between the imperatives of business and technology.
    Top management mediating between the imperatives of business and technology is an IT strategic alignment best practice. Supplier and partner risk being managed is a risk management best practice. A knowledge base on customers, products, markets and processes being in place is an IT value delivery best practice. An infrastructure being provided to facilitate the creation and sharing of business information is an IT value delivery and risk management best practice.

41. Which of the following is the **BEST** method to ensure that the business continuity plan (BCP) remains up to date?
    A. The group walks through the different scenarios of the plan, from beginning to end.
    B. The group ensures that specific systems can actually perform adequately at the alternate offsite facility.
    C. The group is aware of full-interruption test procedures.
    D. Interdepartmental communication is promoted to better respond in the case of a disaster.
    A structured walk-through test gathers representatives from each department who will review the plan and identify weaknesses. The ability of the group to ensure that specific systems can actually perform adequately at the alternate offsite facility is a parallel test and does not involve group meetings. Group awareness of full-interruption test procedures is the most intrusive test to regular operations and the business. While improving communication is important, it is not the most valued method.

42. Which of the following is the initial step in creating a firewall policy?
    A. A cost-benefit analysis of methods for securing the applications
    B. Identification of network applications to be externally accessed
    C. Identification of vulnerabilities associated with network applications to be externally accessed
    D. Creation of an applications traffic matrix showing protection methods
    Identification of the applications required across the network should be identified first. After identification, depending on the physical location of these applications in the network and the network model, the person in charge will be able to understand the need for, and possible methods of, controlling access to these applications. Identifying methods to protect against identified vulnerabilities and their comparative cost-benefit analysis is the third step. Having identified the applications, the next step is to identify vulnerabilities (weaknesses) associated with the network applications. The next step is to analyze the application traffic and create a matrix showing how each type of traffic will be protected.

43. Which of the following is the **MOST** important element for the successful implementation of IT governance?
    A. Implementing an IT scorecard
    B. Identifying organizational strategies
    C. Performing a risk assessment
    D. Creating a formal security policy
    The key objective of an IT governance program is to support the business, thus the identification of organizational strategies is necessary to ensure alignment between IT and corporate governance. Without identification of organizational strategies, the remaining choices—even if implemented—would be ineffective.

44. 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.
    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.

45. Which of the following provides the best evidence of the adequacy of a security awareness program?
    A. The number of stakeholders including employees trained at various levels
    B. Coverage of training at all locations across the enterprise
    C. The implementation of security devices from different vendors
    D. Periodic reviews and comparison with best practices
    The adequacy of security awareness content can best be assessed by determining whether it is periodically reviewed and compared to industry best practices. Choices A, B and C provide metrics for measuring various aspects of a security awareness program, but do not help assess the content.

46. Which of the following should be a **MAJOR** concern for an IS auditor reviewing a business continuity plan (BCP)?
    A. The plan is approved by the chief information officer (CIO).
    B. The plan contact lists have not been updated.
    C. Test results are not adequately documented.
    D. The training schedule for recovery personnel is not included.
    A. Ideally, the board of directors should approve the plan to ensure acceptability, but it is possible to delegate approval authority to the CIO. Pragmatically, lack of documenting test results could have more significant consequences.
    B. The contact lists are an important part of the BCP; however, they are not as important as documenting the test results.
    C. The effectiveness of a BCP can best be determined through tests. If results of tests are not documented, then there is no basis for feedback, updates, etc.
    D. If test results are documented, a need for training will be identified and the BCP will be updated.

47. 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.
    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. Choice A is incorrect since line management prepared the plans.

48. Which of the following would contribute **MOST** to an effective business continuity plan (BCP)?
    A. The document is circulated to all interested parties.
    B. Planning involves all user departments.
    C. The plan is approved by senior management.
    D. An audit is performed by an external IS auditor.
    The involvement of user departments in the BCP is crucial for the identification of the business processing priorities. The BCP circulation will ensure that the BCP document is received by all users. Although essential, this does not contribute significantly to the success of the BCP. A BCP approved by senior management would not ensure the quality of the BCP, nor would an audit necessarily improve the quality of the BCP.

49. Which of the following would **MOST** likely indicate that a customer data warehouse should remain in-house rather than be outsourced to an offshore operation?
    A. Time zone differences could impede communications between IT teams.
    B. Telecommunications cost could be much higher in the first year.
    C. Privacy laws could prevent cross-border flow of information.
    D. Software development may require more detailed specifications.
    Privacy laws prohibiting the cross-border flow of personally identifiable information would make it impossible to locate a data warehouse containing customer information in another country. Time zone differences and higher telecommunications costs are more manageable. Software development typically requires more detailed specifications when dealing with offshore operations.

50. While conducting an IS audit of a service provider for a governmental program involving confidential information, an IS auditor noted that the service provider delegated a part of the IS work to another subcontractor. Which of the following provides the **MOST** assurance that the requirements for protecting confidentiality of information are met?
    A. Monthly committee meetings include the subcontractor's IS manager
    B. Management reviews weekly reports from the subcontractor
    C. Permission is obtained from the government agent regarding the contract
    D. Periodic independent audit of the work is delegated to the subcontractor
    Periodic independent audits provide reasonable assurance that the requirements for protecting confidentiality of information are not compromised. Regular committee meetings are a good monitoring tool for delegated operations; however, independent reviews provide better assurance. Management should not just rely on self-reported information from the subcontractor. Obtaining permission from the government agent is not related to ensuring the confidentiality of information.

51. With respect to business continuity strategies, an IS auditor interviews key stakeholders in an organization to determine whether they understand their roles and responsibilities. The IS auditor is attempting to evaluate the:
    A. clarity and simplicity of the business continuity plans.
    B. adequacy of the business continuity plans.
    C. effectiveness of the business continuity plans.
    D. ability of IS and end-user personnel to respond effectively in emergencies.

    The IS auditor should interview key stakeholders to evaluate how well they understand their roles and responsibilities. When all stakeholders have a detailed understanding of their roles and responsibilities in the event of a disaster, an IS auditor can deem the business continuity plan to be clear and simple. To evaluate adequacy, the IS auditor should review the plans and compare them to appropriate standards. To evaluate effectiveness, the IS auditor should review the results from previous tests. This is the best determination for the evaluation of effectiveness. An understanding of roles and responsibilities by key stakeholders will assist in ensuring the business continuity plan is effective. To evaluate the response, the IS auditor should review results of continuity tests. This will provide the IS auditor with assurance that target and recovery times are met. Emergency procedures and employee training need to be reviewed to determine whether the organization had implemented plans to allow for the effective response.

52. Which of the following reasons **BEST** describes the purpose of a mandatory vacation policy?
    A. To ensure that employees are properly cross-trained in multiple functions
    B. To improve employee morale
    C. To identify potential errors or inconsistencies in business processes
    D. To be used as a cost-saving measure

    Mandatory vacations help uncover potential fraud or inconsistencies. Ensuring that people who have access to sensitive internal controls or processes take a mandatory vacation annually is most important. Ensuring that employees are properly cross-trained in multiple functions improves the skills of employees. Improving employee morale helps in reducing employee burnout. Mandatory vacations may or may not be a cost-saving measure, depending on the enterprise.

53. When auditing a disaster recovery plan for a critical business area, an IS auditor finds that it does not cover all the systems. Which of the following is the **MOST** appropriate action for the IS auditor?
    A. Alert management and evaluate the impact of not covering all systems.
    B. Cancel the audit.
    C. Complete the audit of the systems covered by the existing disaster recovery plan.
    D. Postpone the audit until the systems are added to the disaster recovery plan.

    An IS auditor should make management aware that some systems are omitted from the disaster recovery plan. An IS auditor should continue the audit and include an evaluation of the impact of not including all systems in the disaster recovery plan. Cancelling the audit, ignoring the fact that some systems are not covered or postponing the audit are inappropriate actions to take.

54. While observing a full simulation of the business continuity plan, an IS auditor notices that the notification systems within the organizational facilities could be severely impacted by infrastructural damage. The **BEST** recommendation the IS auditor can provide to the organization is to ensure:
    A. the salvage team is trained to use the notification system.
    B. the notification system provides for the recovery of the backup.
    C. redundancies are built into the notification system.
    D. the notification systems are stored in a vault.

    If the notification system has been severely impacted by the damage, redundancy would be the best control. The salvage team would not be able to use a severely damaged notification system, even if they are trained to use it. The recovery of the backups has no bearing on the notification system and storing the notification system in a vault would be of little value if the building is damaged.

55. Which of the following is **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

    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 their desk, the password is of little value. Management support and commitment is, no doubt, important, but for successful implementation and maintenance of a 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, is also required, along with the user's education on the importance of security.

56. Which of the following is responsible for the development of an information security policy?
    A. The IS department
    B. The security committee
    C. The security administrator
    D. The board of directors

    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.

57 Which of the following is **MOST** important to ensure that effective application controls are maintained?
    A. Exception reporting
    B. Manager involvement
    C. Control self-assessment (CSA)
    D. Peer review

    CSA is the review of business objectives and internal controls in a formal and documented collaborative process. It includes testing the design of automated application controls. Exception reporting only looks at what has not been achieved. Manager involvement is important, but may not be a consistent or well-defined process compared to CSA. Peer review lacks the direct involvement of audit specialists and management.

58. Which of the following is a function of an IS steering committee?
    A. Monitoring vendor-controlled change control and testing
    B. Ensuring a separation of duties within the information's processing environment
    C. Approving and monitoring major projects, the status of IS plans and budgets
    D. Liaising between the IS department and the end users

    The IS steering committee typically serves as a general review board for major IS projects and should not become involved in routine operations; therefore, one of its functions is to approve and monitor major projects, the status of IS plans and budgets. Vendor change control is an outsourcing issue and should be monitored by IS management. Ensuring a separation of duties within the information's processing environment is an IS management responsibility. Liaising between the IS department and the end users is a function of the individual parties and not a committee.

59. 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 résumé

    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 résumé may not be accurate.

60. Which of the following should be considered **FIRST** when implementing a risk management program?
    A. An understanding of the organization's threat, vulnerability and risk profile
    B. An understanding of the risk exposures and the potential consequences of compromise
    C. A determination of risk management priorities based on potential consequences
    D. A risk mitigation strategy sufficient to keep risk consequences at an acceptable level

    Implementing risk management, as one of the outcomes of effective information security governance, would require a collective understanding of the organization's threat, vulnerability and risk profile as a first step. Based on this, an understanding of risk exposure and potential consequences of compromise could be determined. Risk management priorities based on potential consequences could then be developed. This would provide a basis for the formulation of strategies for risk mitigation sufficient to keep the consequences from risk at an acceptable level.

61. Which of the following statements is valid while drafting a business continuity plan (BCP)?
    A. Downtime costs decrease as the recovery point objective (RPO) increases.
    B. Downtime costs increase with time.
    C. Recovery costs are independent of time.
    D. Recovery costs can only be controlled on a short-term basis.

Downtime costs—such as loss of sales, idle resources, salaries, etc.—increase with time. A BCP should be drawn to achieve the lowest downtime costs possible. Downtime costs are not related to the RPO. The RPO defines the data backup strategy, which is related to recovery costs rather than to downtime costs. Recovery costs decrease with the time allowed for recovery. For example, recovery costs to recover business operations within two days will be higher than the cost to recover business within seven days. The essence of an effective BCP is to minimize uncertainty and increase predictability. With good planning, recovery costs can be contained.

62. When conducting an IT security risk assessment, the IS auditor asked the IT security officer to participate in a risk identification workshop with users and business unit representatives. What is the **MOST** important recommendation that the IS auditor should make to obtain successful results and avoid future conflicts?
    A. Ensure that the IT security risk assessment has a clearly defined scope.
    B. Require the IT security officer to approve each risk rating during the workshop.
    C. Suggest that the IT security officer accept the business unit risk and rating.
    D. Select only commonly accepted risk with the highest submitted rating.
    The IT risk assessment should have a clearly defined scope in order to be efficient and meet the objectives of risk identification. The IT risk assessment should include relationships with risk assessments in other areas, if appropriate. The other choices involve how risk is ranked and rated, but the success of the entire assessment process depends on making sure that the scope is broad enough to capture all significant risk that is still achievable. If the scope is too broad, the risk assessment process will be too difficult, and this can cause future conflicts.

63. When evaluating IT outsourcing strategies, an IS auditor should be **MOST** concerned if which of the following elements is part of the strategy?
    A. Transfer of legal compliance responsibility
    B. Promoting long-term contracts rather than short-term contracts
    C. Use of only subsidiary companies for outsourcing
    D. Not forming a cross-functional contract management team
    The ultimate responsibility to comply with all applicable laws and regulations lies with the company that is outsourcing or contracting the service, not with the external service provider. Therefore, transferring such responsibility is neither feasible nor in the best interest of the company. While each of the choices may be an issue, an IS auditor should be most concerned if the strategy is to transfer an organization's legal compliance responsibility.

64. Which of the following should be of **MOST** concern to an IS auditor reviewing the business continuity plan (BCP)?
    A. The disaster levels are based on scopes of damaged functions, but not on duration.
    B. The difference between low-level disaster and software incidents is not clear.
    C. The overall BCP is documented, but detailed recovery steps are not specified.
    D. The responsibility for declaring a disaster is not identified.
    If nobody declares the disaster, the response and recovery plan would not be invoked, making all other concerns mute. Although failure to consider duration could be a problem, it is not as significant as scope, and neither is as critical as the need to have someone invoke the plan. The difference between incidents and low-level disasters is always unclear and frequently revolves around the amount of time required to correct the damage. The lack of detailed steps should be documented, but their absence does not mean a lack of recovery, if in fact someone has invoked the plan.

65. Which of the following must exist to ensure the viability of a duplicate information processing facility?
    A. The site is near the primary site to ensure quick and efficient recovery.
    B. The site contains the most advanced hardware available.
    C. The workload of the primary site is monitored to ensure adequate backup is available.
    D. The hardware is tested when it is installed to ensure it is working properly.
    Resource availability must be assured. The workload of the site must be monitored to ensure that availability for emergency backup use is not impaired. The site chosen should not be subject to the same natural disaster as the primary site. In addition, a reasonable compatibility of hardware/software must exist to serve as a basis for backup. The latest or newest hardware may not adequately serve this need. Testing the hardware when the site is established is essential, but regular testing of the actual backup data is necessary to ensure the operation will continue to perform as planned.

66. Which of the following is normally a responsibility of the chief security officer (CSO)?
    A. Periodically reviewing and evaluating the security policy
    B. Executing user application and software testing and evaluation
    C. Granting and revoking user access to IT resources
    D. Approving access to data and applications
    The role of a CSO is to ensure that the corporate security policy and controls are adequate to prevent unauthorized access to the company assets, including data, programs and equipment. User application and other software

testing and evaluation normally are the responsibility of the staff assigned to development and maintenance. Granting and revoking access to IT resources is usually a function of network or database administrators. Approval of access to data and applications is the duty of the data owner.

67. Which of the following is the **BEST** type of program for an organization in order to aggregate, correlate and store different log and event files, and then produce weekly and monthly reports for IS auditors?
    A. A security information event management (SIEM) product
    B. An open-source correlation engine
    C. A log management tool
    D. An extract, transform, load (ETL) system

    A log management tool is a product designed to aggregate events from many log files (with distinct formats and from different sources), store them and typically correlate them offline to produce many reports (e.g., exception reports showing different statistics including anomalies and suspicious activities) and to answer time-based queries (e.g., how many users have entered the system between 2 a.m. and 4 a.m. over the past three weeks). A SIEM product has some similar features. It correlates events from log files, but does it online and normally is not oriented to storing many weeks of historical information and producing audit reports. A correlation engine is part of a SIEM product. It is oriented to making an online correlation of events. An ETL is part of a business intelligence system, dedicated to extracting operational or production data, transforming that data and loading them to a central repository (data warehouse or data mart); an ETL does not correlate data or produce reports, and normally it does not have extractors to read log file formats.

68. Involvement of senior management is **MOST** important in the development of:
    A. strategic plans.
    B. IS policies.
    C. IS procedures.
    D. standards and guidelines.

    Strategic plans provide the basis for ensuring that the enterprise meets its goals and objectives. Involvement of senior management is critical to ensuring that the plan adequately addresses the established goals and objectives. IS policies, IS procedures, standards and guidelines are all structured to support the overall strategic plan.

69. Which of the following represents an example of a preventive control with respect to IT personnel?
    A. Review of visitor logs for the data center
    B. A log server that tracks logon IP addresses of users
    C. Implementation of a badge entry system for the IT facility
    D. An accounting system that tracks employee telephone calls

    Preventive controls are used to reduce the probability of an adverse event occurring. A badge entry system would prevent unauthorized entry to the facility. Review of visitor logs, log servers or telephone call accounting systems are detective controls in most circumstances.

70. A key IT systems developer has suddenly resigned from an enterprise. Which of the following will be the **MOST** important action?
    A. Set up an exit interview with human resources (HR).
    B. Initiate the handover process to ensure continuity of the project.
    C. Terminate the developer's logical access to IT resources.
    D. Ensure that management signs off on the termination paperwork.

    In order to protect IT assets, terminating logical access to IT resources is the first and most important action to take once management has confirmed the employee's clear intention to leave the enterprise. The interview with HR is also an important process if it is conducted by the last date of employment, but it is of secondary importance. As long as the handover process to a designated employee is conducted by the last date of employment, there should be no problems. Ensuring that management signs off on termination paperwork is important, but not as critical as terminating access to the IT systems.

71. Overall business risk for a particular threat can be expressed as:
    A. a product of the likelihood and magnitude of the impact should a threat successfully exploit a vulnerability.
    B. the magnitude of the impact should a threat source successfully exploit the vulnerability.
    C. the likelihood of a given threat source exploiting a given vulnerability.
    D. the collective judgment of the risk assessment team.

    Choice A takes into consideration the likelihood and magnitude of the impact and provides the best measure of the risk to an asset. Choice B provides only the likelihood of a threat exploiting a vulnerability in the asset but does not provide the magnitude of the possible damage to the asset. Similarly, choice C considers only the magnitude of the damage and not the possibility of a threat exploiting a vulnerability. Choice D defines the risk on an arbitrary basis and is not suitable for a scientific risk management process, but is often used and sometimes quite sensible.

72. The output of the risk management process is an input for making:
    A. business plans.
    B. audit charters.
    C. security policy decisions.
    D. software design decisions.

    The risk management process is about making specific, security-related decisions, such as the level of acceptable risk. Choices A, B and D are not ultimate goals of the risk management process.

73. When auditing the IT governance framework and IT risk management practices that exist within an organization, the IS auditor identified some undefined responsibilities regarding IT management and governance roles. Which of the following recommendations is the **MOST** appropriate?
    A. Review the strategic alignment of IT with the business.
    B. Implement accountability rules within the organization.
    C. Ensure that independent IT audits are conducted periodically.
    D. Create a chief risk officer (CRO) role in the organization

    IT risk is managed by embedding accountability into the enterprise. The IS auditor should recommend the implementation of accountability rules to ensure that all responsibilities are defined within the organization. While the strategic alignment of IT with business is important, it is not directly related to the gap identified in this scenario. Similarly, performing more frequent IS audits or recommending the creation of a new role (CRO) is not helpful if the accountability rules are not clearly defined and implemented.

74. A medium-sized organization, whose IT disaster recovery measures have been in place and regularly tested for years, has just developed a formal business continuity plan (BCP). A basic BCP tabletop exercise has been performed successfully. Which testing should an IS auditor recommend be performed **NEXT** to verify the adequacy of the new BCP?
    A. Full-scale test with relocation of all departments, including IT, to the contingency site
    B. Walk-through test of a series of predefined scenarios with all critical personnel involved
    C. IT disaster recovery test with business departments involved in testing the critical applications
    D. Functional test of a scenario with limited IT involvement

    After a tabletop exercise has been performed, the next step would be a functional test, which includes the mobilization of staff to exercise the administrative and organizational functions of a recovery. Since the IT part of the recovery has been tested for years, it would be more efficient to verify and optimize the BCP before actually involving IT in a full-scale test. The full-scale test would be the last step of the verification process before entering into a regular annual testing schedule. A full-scale test in the situation described might fail because it would be the first time that the plan is actually exercised, and a number of resources (including IT) and time would be wasted. The walk-through test is the most basic type of testing. Its intention is to make key staff familiar with the plan and discuss critical plan elements, rather than verifying its adequacy. The recovery of applications should always be verified and approved by the business instead of being purely IT-driven. A disaster recovery test would not help in verifying the administrative and organizational parts of the BCP which are not IT-related.

75. An organization's disaster recovery plan should address early recovery of:
    A. all information systems processes.
    B. all financial processing applications.
    C. only those applications designated by the IS manager.
    D. processing in priority order, as defined by business management.

    Business management should know which systems are critical and when they need to process well in advance of a disaster. It is management's responsibility to develop and maintain the plan. Adequate time will not be available for this determination once the disaster occurs. IS and the information processing facility are service organizations that exist for the purpose of assisting the general user management in successfully performing their jobs.

76. A poor choice of passwords and data transmission over unprotected communications lines are examples of:
    A. vulnerabilities.
    B. threats.
    C. probabilities.
    D. impacts.

    Vulnerabilities represent characteristics of information resources that may be exploited by a threat. Threats are circumstances or events with the potential to cause harm to information resources. Probabilities represent the likelihood of the occurrence of a threat. Impacts represent the outcome or result of a threat exploiting a vulnerability.

77. 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.

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.

78. An IS auditor is evaluating the IT governance framework of an organization. Which of the following would be the **GREATEST** concern?
    A. Senior management has limited involvement.
    B. Return on investment (ROI) is not measured.
    C. Chargeback of IT cost is not consistent.
    D. Risk appetite is not quantified.

    A. To ensure that the IT governance framework is effectively in place, senior management must be involved and aware of roles and responsibilities. Therefore, it is most essential to ensure the role of senior management when evaluating the soundness of IT governance.

    B. Ensuring revenue is a part of the objectives in the IT governance framework. Therefore, it is not effective in verifying the soundness of IT governance.

    C. Introduction of a cost allocation system is part of the objectives in an IT governance framework. Therefore, it is not effective in verifying the soundness of IT governance.

    D. Estimation of risk appetite is important; however, at the same time, management should ensure that controls are in place. Therefore, checking only on risk appetite does not verify soundness of IT governance.

79. 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. Utilizing of 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

    Training is the only choice that is directed at security awareness. 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.

80. An IS auditor reviewing an outsourcing contract of IT facilities would expect it to define the:
    A. hardware configuration.
    B. access control software.
    C. ownership of intellectual property.
    D. application development methodology.

    Of the choices, the hardware and access control software is generally irrelevant as long as the functionality, availability and security can be affected, which are specific contractual obligations. Similarly, the development methodology should be of no real concern. The contract must, however, specify who owns the intellectual property (i.e., information being processed, application programs). Ownership of intellectual property will have a significant cost and is a key aspect to be defined in an outsourcing contract.

81. The optimal business continuity strategy for an entity is determined by the:
    A. lowest downtime cost.
    B. lowest sum of downtime cost and recovery cost.
    C. lowest recovery cost.
    D. average of the combined downtime and recovery cost.

    A. The strategy with the lowest downtime cost is not the optimal strategy. Recovery cost must also be considered.

    B. Both costs have to be minimized, and the strategy for which the sum of the costs is the lowest is the optimal strategy.

    C. The strategy with the lowest recovery cost is not the optimal strategy. Downtime cost must also be considered.

    D. The average of the combined downtime and recovery cost will be higher than the lowest combined cost of downtime and recovery.

82. The cost of ongoing operations when a disaster recovery plan is in place, compared to not having a disaster recovery plan, will **MOST** likely:
    A. increase.
    B. decrease.
    C. remain the same.
    D. be unpredictable.

    Due to the additional cost of disaster recovery plan measures, the cost of normal operations for any organization will always increase after a disaster recovery plan implementation, i.e., the cost of normal operations during a nondisaster period will be more than the cost of operations during a nondisaster period when no disaster recovery plan was in place.

83. Which of the following is the **BEST** way to ensure that organizational policies comply with legal requirements?
    A. Inclusion of a blanket legal statement in each policy
    B. Periodic review by subject matter experts
    C. Annual sign-off by senior management on organizational policies
    D. Policy alignment to the most restrictive regulations

    A. A blanket legal statement in each policy to adhere to all applicable laws and regulations is ineffective because the readers of the policy (internal personnel) will not know which statements are applicable or the specific nature of their requirements. As a result, personnel may lack the knowledge to perform the required activities for legal compliance.

    B. Periodic review of policies by personnel with specific knowledge of regulatory and legal requirements best ensures that organizational policies are aligned with legal requirements.

    C. Annual sign-off by senior management on an organization's policies helps set the tone at the top, but does not ensure that the policies comply with regulatory and legal requirements.

    D. Aligning policies to the most restrictive regulations may create an unacceptable financial burden for the organization. This could then lead to securing minimal risk systems to the same degree as those containing sensitive customer data and other information protected by legislation.

84. Which of the following would be of **MOST** concern to an IS auditor performing an audit of a disaster recovery plan (DRP)?
    A. The DRP has not been tested.
    B. New team members have not read the DRP.
    C. The manager responsible for the DRP recently resigned.
    D. The DRP manual is not updated regularly.

    If the DRP has not been tested, it is very likely that the plan is incomplete or inadequate. This situation would be of concern to an IS auditor because the organization would have no way to accurately assess whether the plan is workable. If new team members are unfamiliar with the plan, current members would be able to assist them, so this would not be a significant issue. While the loss of experienced personnel can create some issues, if the plan was proven to be adequate, less experienced personnel would likely to be able to perform the required job functions in the case of a disaster. A DRP manual which is not updated regularly is a secondary concern to having a DRP which has not been tested.

85. IT governance is **PRIMARILY** the responsibility of the:
    A. chief executive officer (CEO).
    B. board of directors.
    C. IT steering committee.
    D. audit committee.

    IT governance is primarily the responsibility of the executives and shareholders (as represented by the board of directors). The CEO 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.

86. The development of an application has been outsourced to an offshore vendor. Which of the following should be of **GREATEST** concern to an IS auditor?
    A. The right to audit clause was not included in the contract.
    B. The business case was not established.
    C. There was no source code escrow agreement.
    D. The contract does not cover change management procedures.

    Because the business case was not established, it is likely that the business rationale, risk and risk mitigation strategies for outsourcing the application development were not fully evaluated and formally approved by senior management. This situation presents the biggest risk to the organization. The lack of the right to audit clause, source code escrow or change management procedures each present risk to the organization; however, the risk is not as consequential as the lack of a business case.

87. For effective implementation after a business continuity plan (BCP) has been developed, it is **MOST** important that the BCP be:
    A. stored in a secure, offsite facility.
    B. approved by senior management
    C. communicated to appropriate personnel.
    D. made available through the enterprise's intranet.

    The implementation of a BCP will be effective only if appropriate personnel are informed and aware of all the aspects of the BCP6. The BCP, if kept in a safe place, will not reach the users; users will never implement the BCP and, thus, the BCP will be ineffective. Senior management approval is a prerequisite for designing the BCP. Making a BCP available on an enterprise's intranet does not guarantee that personnel will read or understand it.

88. An IS auditor should be concerned when a telecommunication analyst:
    A. monitors systems performance and tracks problems resulting from program changes.
    B. reviews network load requirements in terms of current and future transaction volumes.
    C. assesses the impact of the network load on terminal response times and network data transfer rates.
    D. recommends network balancing procedures and improvements.

    The responsibilities of a telecommunications analyst include reviewing network load requirements in terms of current and future transaction volumes (choice B), assessing the impact of network load or terminal response times and network data transfer rates (choice C), and recommending network balancing procedures and improvements (choice D). Monitoring systems performance and tracking problems as a result of program changes (choice A) would put the analyst in a self-monitoring role.

89. When reviewing the development of information security policies, the **PRIMARY** focus of an IS auditor should be on assuring that these policies:
    A. are aligned with globally accepted industry best practices.
    B. are approved by the board of directors and senior management.
    C. strike a balance between business and security requirements.
    D. provide direction for implementing security procedures.

    Information security policies must be first aligned with an organization's objectives. Best practices are adopted based on the business objectives. It is essential that policies be approved; however, that is not the primary focus during development. Policies cannot provide direction if they are not aligned with business requirements.

90. Which of the following insurance types provide for a loss arising from fraudulent acts by employees?
    A. Business interruption
    B. Fidelity coverage
    C. Errors and omissions
    D. Extra expense

    Fidelity insurance covers the loss arising from dishonest or fraudulent acts by employees. Business interruption insurance covers the loss of profit due to the disruption in the operations of an organization. Errors and omissions insurance provides legal liability protection in the event that the professional practitioner commits an act that results in financial loss to a client. Extra expense insurance is designed to cover the extra costs of continuing operations following a disaster/disruption within an organization.

91. To support an organization's goals, an IS department should have:
    A. a low-cost philosophy.
    B. long- and short-range plans.
    C. leading-edge technology.
    D. plans to acquire new hardware and software.

    To ensure its contribution to the realization of an organization's overall goals, the IS department should have long- and short-range plans that are consistent with the organization's broader plans for attaining its goals. Choices A and C are objectives, and plans would be needed to delineate how each of the objectives would be achieved. Choice D could be a part of the overall plan but would be required only if hardware or software is needed to achieve the organizational goals.

92. Which of the following is the **MOST** important IS audit consideration when an organization outsources a customer credit review system to a third-party service provider? The provider:
    A. meets or exceeds industry security standards.
    B. agrees to be subject to external security reviews.
    C. has a good market reputation for service and experience.
    D. complies with security policies of the organization.

    It is critical that an independent security review of an outsourcing vendor be obtained because customer credit information will be kept there. Compliance with security standards or organization policies is important, but there is no way to verify or prove that that is the case without an independent review. Though long experience in business and good reputation is an important factor to assess service quality, the business cannot outsource to a provider whose security control is weak.

93. 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.

    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.

94. Which of the following should be the **MOST** important consideration when deciding on areas of priority for IT governance implementations?
    A. Process maturity
    B. Performance indicators
    C. Business risk
    D. Assurance reports

    Priority should be given to those areas which represent a known risk to the enterprise's operations. The level of process maturity, process performance and audit reports will feed into the decision making process. Those areas that represent real risk to the business should be given priority.
95. An enterprise's risk appetite is **BEST** established by:
    A. the chief legal officer.
    B. security management.
    C. the audit committee.
    D. the steering committee.

    The steering committee is best suited to determine the enterprise's risk appetite because the committee draws its representation from senior management. Although chief legal officers can give guidance regarding legal issues on the policy, they cannot determine the risk appetite. The security management team is concerned with managing the security posture, but not with determining the posture. The audit committee is not responsible for setting the risk tolerance or appetite of the enterprise.
96. A local area network (LAN) administrator normally would be restricted from:
    A. having end-user responsibilities.
    B. reporting to the end-user manager.
    C. having programming responsibilities.
    D. being responsible for LAN security administration.

    A LAN administrator should not have programming responsibilities but may have end-user responsibilities. The LAN administrator may report to the director of the IPF or, in a decentralized operation, to the end-user manager. In small organizations, the LAN administrator may also be responsible for security administration over the LAN.
97. Establishing the level of acceptable risk is the responsibility of:
    A. quality assurance management.
    B. senior business management.
    C. the chief information officer.
    D. the chief security officer.

    Senior management should establish the acceptable risk level, since they have the ultimate or final responsibility for the effective and efficient operation of the organization. Choices A, C and D should act as advisors to senior management in determining an acceptable risk level.
98. During the design of a business continuity plan, the business impact analysis (BIA) identifies critical processes and supporting applications. This will **PRIMARILY** influence the:
    A. responsibility for maintaining the business continuity plan.
    B. criteria for selecting a recovery site provider.
    C. recovery strategy.
    D. responsibilities of key personnel.

    The most appropriate strategy is selected based on the relative risk level and criticality identified in the BIA. The other choices are made after the selection or design of the appropriate recovery strategy.
99. 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.

    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.
100. In an organization where an IT security baseline has been defined, an IS auditor should **FIRST** ensure:
    A. implementation.
    B. compliance.
    C. documentation.
    D. sufficiency.

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

101. In reviewing the IS short-range (tactical) plan, an IS auditor should determine whether:
   A. there is an integration of IS and business personnel within projects.
   B. there is a clear definition of the IS mission and vision.
   C. a strategic information technology planning methodology is in place.
   D. the plan correlates business objectives to IS goals and objectives.

   The integration of IS and business personnel 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.

102. As part of the business continuity planning (BCP) process, which of the following should be identified **FIRST** in the business impact analysis (BIA)?
   A. Organizational risk such as single point-of-failure and infrastructure risk
   B. Threats to critical business processes
   C. Critical business processes for ascertaining the priority for recovery
   D. Resources required for resumption of business

   The identification of the priority for recovering critical business processes should be addressed first. Organizational risk should be identified next, followed by the identification of threats to critical business processes. Identification of resources for business resumption will occur after the tasks mentioned.

103. As an outcome of information security governance, strategic alignment provides:
   A. security requirements driven by enterprise requirements.
   B. baseline security following best practices.
   C. institutionalized and commoditized solutions.
   D. an understanding of risk exposure.

   Information security governance, when properly implemented, should provide four basic outcomes: strategic alignment, value delivery, risk management and performance measurement. Strategic alignment provides input for security requirements driven by enterprise requirements. Value delivery provides a standard set of security practices, i.e., baseline security following best practices or institutionalized and commoditized solutions. Risk management provides an understanding of risk exposure.

104. An IS auditor identifies that reports on product profitability produced by an organization's finance and marketing departments give different results. Further investigation reveals that the product definition being used by the two departments is different. What should the IS auditor recommend?
   A. User acceptance testing (UAT) occur for all reports before release into production
   B. Organizational data governance practices be put in place
   C. Standard software tools be used for report development
   D. Management sign-off on requirements for new reports

   This choice directly addresses the problem. An organizationwide approach is needed to achieve effective management of data assets. This includes enforcing standard definitions of data elements, which is part of a data governance initiative. The other choices, while sound development practices, do not address the root cause of the problem described.

105. Which of the following distinguishes a business impact analysis (BIA) from a risk assessment?
   A. An inventory of critical assets
   B. An identification of vulnerabilities
   C. A listing of threats
   D. A determination of acceptable downtime

   A. An inventory of critical assets is completed in both a risk assessment and a BIA.
   B. An identification of vulnerabilities is relevant in both a risk assessment and a BIA.
   C. A listing of threats is relevant both in a risk assessment and a BIA.
   D. A determination of acceptable downtime is made only in a BIA.

106. Which of the following is the **MOST** important aspect of effective business continuity management?
   A. The recovery site is secure and located an appropriate distance from the primary site.
   B. The recovery plans are periodically tested.
   C. Fully tested backup hardware is available at the recovery site.
   D. Network links are available from multiple service providers.

   Periodic testing of the recovery plan is critical to ensure that whatever has been planned and documented is feasible. The other options are more tactical considerations that are secondary to the need for testing. If a disaster occurs, choices A, C and D would be more important.

107. The **PRIMARY** objective of testing a business continuity plan is to:
   A. familiarize employees with the business continuity plan.
   B. ensure that all residual risk is addressed.
   C. exercise all possible disaster scenarios.
   D. identify limitations of the business continuity plan.

Testing the business continuity plan provides the best evidence of any limitations that may exist. Familiarizing employees with the business continuity plan is a secondary benefit of a test. It is not cost effective to address residual risk in a business continuity plan, and it is not practical to test all possible disaster scenarios.

108. When developing a security architecture, which of the following steps should be executed **FIRST**?
    A. Developing security procedures
    B. Defining a security policy
    C. Specifying an access control methodology
    D. Defining roles and responsibilities

    Defining a security policy for information and related technology is the first step toward building a security architecture. A security policy communicates a coherent security standard to users, management and technical staff. Security policies will often set the stage in terms of what tools and procedures are needed for an organization. The other choices should be executed only after defining a security policy.

109. When an organization's disaster recovery plan (DRP) has a reciprocal agreement, which of the following risk treatment approaches is being applied?
    A. Transfer
    B. Mitigation
    C. Avoidance
    D. Acceptance

    A reciprocal agreement in which two organizations agree to provide computing resources to each other in the event of a disaster is a form of risk mitigation. This usually works well if both organizations have similar information processing facilities. Because the intended effect of reciprocal agreements is to have a functional DRP, it is a risk mitigation strategy. Risk transfer is the transference of risk to a third party, e.g., buying insurance for activities that pose a risk. Risk avoidance is the decision to cease operations or activities that give rise to a risk. For example, a company may stop accepting credit card payments to avoid the risk of credit card information disclosure. When an organization decides to accept the risk as is and do nothing to mitigate or transfer it, that is risk acceptance.

110. When developing a business continuity plan (BCP), which of the following tools should be used to gain an understanding of the organization's business processes?
    A. Business continuity self-audit
    B. Resource recovery analysis
    C. Risk assessment
    D. Gap analysis

    Risk assessment and business impact assessment are tools for understanding business-for-business continuity planning. Business continuity self-audit is a tool for evaluating the adequacy of the BCP, resource recovery analysis is a tool for identifying a business resumption strategy, while the role gap analysis can play in business continuity planning is to identify deficiencies in a plan. Neither of these is used for gaining an understanding of the business.

111. After an organization completed a threat and vulnerability analysis as part of a risk assessment, the final report suggested that an intrusion prevention system (IPS) should be installed at the main Internet gateways, and that all business units should be separated via a proxy firewall. Which of the following is the **BEST** method to determine whether the controls should be implemented?
    A. A cost-benefit analysis
    B. An annualized loss expectancy (ALE) calculation
    C. A comparison of the cost of the IPS and firewall and the cost of the business systems
    D. A business impact analysis (BIA)

    In a cost-benefit analysis, the total expected purchase and operational/support costs and a qualitative value for all actions are weighted against the total expected benefits in order to choose the best technical, most profitable, least expensive, or acceptable risk option. The ALE is the expected monetary loss that is estimated for an asset over a one-year period. It is a useful calculation that should be included in determining the necessity of controls, but is not sufficient alone. The cost of the hardware assets should be compared to the total value of the information that the asset protects, including the cost of the systems where the data reside and across which data are transmitted. Potential business impact is only one part of the cost-benefit analysis.

112. The risk associated with electronic evidence gathering would **MOST** likely be reduced by an email:
    A. destruction policy.
    B. security policy.
    C. archive policy.
    D. audit policy.

    With a policy of well-archived email records, access to or retrieval of specific email records is possible without disclosing other confidential email records. Security and/or audit policies would not address the efficiency of record retrieval, and destroying emails may be an illegal act.

113. Which of the following is the **MOST** important for an IS auditor to consider when reviewing a service level agreement (SLA) with an external IT service provider?
    A. Payment terms
    B. Uptime guarantee
    C. Indemnification clause
    D. Default resolution

    The most important element of an SLA is the measurable terms of performance, such as uptime agreements. While all of the choices are important, payment terms, indemnification and default resolution are typically included in the master agreement rather than in the SLA.
114. 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.

    An organization's core activities generally should not be outsourced, because they are what the organization does best; an IS auditor observing that should be concerned. An IS 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, while multisourcing is an acceptable way to reduce risk.
115. An IS auditor conducting a review of disaster recovery planning (DRP) at a financial processing organization has discovered the following:
    - The existing disaster recovery plan was compiled two years earlier by a systems analyst in the organization's IT department using transaction flow projections from the operations department.
    - The plan was presented to the deputy chief executive officer (CEO) for approval and formal issue, but it is still awaiting their attention.
    - The plan has never been updated, tested or circulated to key management and staff, though interviews show that each would know what action to take for its area in the event of a disruptive incident.

    The IS auditor's report should recommend that:
    A. the deputy CEO be censured for their failure to approve the plan.
    B. a board of senior managers is set up to review the existing plan.
    C. the existing plan is approved and circulated to all key management and staff.
    D. a manager coordinates the creation of a new or revised plan within a defined time limit.

    The primary concern is to establish a workable disaster recovery plan, which reflects current processing volumes to protect the organization from any disruptive incident. Censuring the deputy CEO will not achieve this and is generally not within the scope of an IS auditor to recommend. Establishing a board to review the plan, which is two years out of date, may achieve an updated plan, but is not likely to be a speedy operation, and issuing the existing plan would be folly without first ensuring that it is workable. The best way to achieve a disaster recovery plan in a short time is to make an experienced manager responsible for coordinating the knowledge of other managers into a single, formal document within a defined time limit.
116. 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.

    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.
117. The **PRIMARY** benefit of implementing a security program as part of a security governance framework is the:
    A. alignment of the IT activities with IS audit recommendations.
    B. enforcement of the management of security risk.
    C. implementation of the chief information security officer's (CISO) recommendations.
    D. reduction of the cost for IT security.

    The major benefit of implementing a security program is management's assessment of risk and its mitigation to an appropriate level of risk, and the monitoring of the remaining residual risk. Recommendations, visions and objectives of the auditor and the CISO are usually included within a security program, but they would not be the major benefit. The cost of IT security may or may not be reduced.

118. Which of the following is the **MOST** important requirement for the successful testing of a disaster recovery plan (DRP)?
    A. Participation by all of the identified resources
    B. Management approval of the testing scenario
    C. Advance notice for all of the impacted employees
    D. IT management approval of the testing scenario

    Management approval of the testing scenario would help to ensure both that the test exercise was relevant and in alignment with business requirements. Obtaining management buy-in for the testing is critical to the success of the disaster recovery testing. Choice A is not correct because a DRP should be flexible enough to adapt to use of whatever personnel are available. Choice C is not correct because advance notice for the impacted employees is not necessarily required if the testing exercise is not expected to create service disruptions or other issues. Choice D is not correct because a testing scenario approved by business management approval is more likely to reflect the needs of the business. IT management may select a testing scenario more focused on IT priorities, which may be less effective.
119. 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.

    The inclusion of security responsibilities in job descriptions 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 criteria for evaluating security awareness training. Senior management's level of awareness and concern for information assets is a criterion for evaluating the importance that they attach to those assets and their protection. Funding is a criterion that aids in evaluating whether security vulnerabilities are being addressed. The number of incidents that have occurred is a criterion for evaluating the adequacy of the risk management program.
120. When reviewing the IT strategy, an IS auditor can **BEST** assess whether the strategy supports the organizations' business objectives by determining whether IS:
    A. has all the personnel and equipment it needs.
    B. plans are consistent with management strategy.
    C. uses its equipment and personnel efficiently and effectively.
    D. has sufficient excess capacity to respond to changing directions.

    Determining if the IT plan is consistent with management strategy relates IS/IT planning to business plans. Choices A, C and D are effective methods for determining the alignment of IS plans with business objectives and the organization's strategies.
121 An IS auditor was hired to review e-business security. The IS auditor's first task was to examine each existing e-business application, looking for vulnerabilities. What would be the next task?
    A. Immediately report the risk to the chief information officer (CIO) and chief executive officer (CEO).
    B. Examine the e-business application in development.
    C. Identify threats and the likelihood of occurrence.
    D. Check the budget available for risk management.

    An IS auditor must identify the assets, look for vulnerabilities, and then identify the threats and the likelihood of occurrence. Choices A, B and D should be discussed with the CIO, and a report should be delivered to the CEO. The report should include the findings along with priorities and costs.
122. The **PRIMARY** objective of business continuity and disaster recovery plans should be to:
    A. safeguard critical IS assets.
    B. provide for continuity of operations.
    C. minimize the loss to an organization.
    D. protect human life.

    Since human life is invaluable, the main priority of any business continuity and disaster recovery plan should be to protect people. All other priorities are important but are secondary objectives of a business continuity and disaster recovery plan.
123. The **PRIMARY** objective of implementing corporate governance is to:
    A. provide strategic direction.
    B. control business operations.
    C. align IT with business.
    D. implement best practices.

    Corporate governance is a set of management practices to provide strategic direction, thereby ensuring that goals are achievable, risk is properly addressed and organizational resources are properly utilized. Hence, the primary

objective of corporate governance is to provide strategic direction. Based on the strategic direction, business operations are directed and controlled.

124. The **MOST** important point of consideration for an IS auditor while reviewing an enterprise's project portfolio is that it:
    A. does not exceed the existing IT budget.
    B. is aligned with the investment strategy.
    C. has been approved by the IT steering committee.
    D. is aligned with the business plan.

    Portfolio management takes a holistic view of an enterprise's overall IT strategy, which, in turn, should be aligned with the business strategy. A business plan provides the justification for each of the projects in the project portfolio, and that is the major consideration for an IS auditor.

125. Not every enterprise has an I In a review of the human resources policies and procedures within an organization, an IS auditor would be **MOST** concerned with the absence of a:
    A. requirement for job rotation on a periodic basis.
    B. process for formalized exit interviews.
    C. termination checklist requiring that keys and company property be returned and all access permissions revoked upon termination.
    D. requirement for employees to sign a form signifying that they have read the organization's policies.

    A termination checklist is critical to ensure the logical and physical security of an enterprise. In addition to preventing the loss of company property issued to the employee, there is the risk of unauthorized access, intellectual property theft and even sabotage by a disgruntled former employee. While the other choices are best practices, they do not present a significant risk to the organization.

126. Which of the following is an appropriate test method to apply to a business continuity plan (BCP)?
    A. Pilot
    B. Paper
    C. Unit
    D. System

    A paper test is appropriate for testing a BCP. It is a walk-through of the entire plan, or part of the plan, involving major players in the plan's execution, who reason out what may happen in a particular disaster. Choices A, C and D are not appropriate for a BCP.

127. Which of the following should an IS auditor recommend to **BEST** enforce alignment of an IT project portfolio with strategic organizational priorities?
    A. Define a balanced scorecard (BSC) for measuring performance.
    B. Consider user satisfaction in the key performance indicators (KPIs).
    C. Select projects according to business benefits and risk.
    D. Modify the yearly process of defining the project portfolio.

    Prioritization of projects on the basis of their expected benefit(s) to business, and the related risk, is the **BEST** measure for achieving alignment of the project portfolio to an organization's strategic priorities. Modifying the yearly process of the projects portfolio definition might improve the situation, but only if the portfolio definition process is currently not tied to the definition of corporate strategies; however, this is unlikely since the difficulties are in maintaining the alignment, and not in setting it up initially. Measures such as BSC and KPIs are helpful, but they do not guarantee that the projects are aligned with business strategy.

128. For a health care organization, which one of the following reasons would **MOST** likely indicate that the patient benefit data warehouse should remain in-house rather than be outsourced to an offshore operation?
    A. There are regulations regarding data privacy.
    B. Member service representative training cost will be much higher.
    C. It is harder to monitor remote databases.
    D. Time zone differences could impede customer service.

    Regulations prohibiting the cross-border flow of personally identifiable information (PII) may make it impossible to locate a data warehouse containing customer/member information in another county. Training cost, remote database monitoring and time zone difference issues are common and manageable regardless of where the data warehouse resides.

129. In the context of effective information security governance, the primary objective of value delivery is to:
    A. optimize security investments in support of business objectives.
    B. implement a standard set of security practices.
    C. institute a standards-based solution.
    D. implement a continuous improvement culture.

    In the context of effective information security governance, value delivery is implemented to ensure optimization of security investments in support of business objectives. The tools and techniques for implementing value delivery include implementation of a standard set of security practices, institutionalization and commoditization of

standards-based solutions, and implementation of a continuous improvement culture considering security as a process, not an event.

130. An organization has outsourced its wide area network (WAN) to a third-party service provider. Under these circumstances, which of the following is the **PRIMARY** task the IS auditor should perform during an audit of business continuity (BCP) and disaster recovery planning (DRP)?
    A. Review whether the service provider's BCP process is aligned with the organization's BCP and contractual obligations.
    B. Review whether the service level agreement (SLA) contains a penalty clause in case of failure to meet the level of service in case of a disaster.
    C. Review the methodology adopted by the organization in choosing the service provider.
    D. Review the accreditation of the third-party service provider's staff.

    Reviewing whether the service provider's BCP process is aligned with the organization's BCP and contractual obligations is the correct answer since an adverse effect or disruption to the business of the service provider has a direct bearing on the organization and its customers. Reviewing whether the SLA contains a penalty clause in case of failure to meet the level of service in case of a disaster is not the correct answer since the presence of penalty clauses, although an essential element of an SLA, is not a primary concern. Choices C and D are possible concerns, but of lesser importance.

131. Depending on the complexity of an organization's business continuity plan (BCP), the plan may be developed as a set of more than one plan to address various aspects of business continuity and disaster recovery. In such an environment, it is essential that:
    A. each plan is consistent with one another.
    B. all plans are integrated into a single plan.
    C. each plan is dependent on one another.
    D. the sequence for implementation of all plans is defined.

    Depending on the complexity of an organization, there could be more than one plan to address various aspects of business continuity and disaster recovery. These do not necessarily have to be integrated into one single plan. However, each plan has to be consistent with other plans to have a viable business continuity planning strategy. It may not be possible to define a sequence in which plans have to be implemented, as it may be dependent on the nature of disaster, criticality, recovery time, etc.

132. Rotating job responsibilities is a good security practice **PRIMARILY** because it:
    A. ensures that personnel are cross-trained.
    B. improves employee morale.
    C. maximizes employee performance.
    D. reduces the opportunity for fraud.

    A. While cross-training is useful, it is not typically a security issue.
    B. Improving morale is important, but it is not a security concern.
    C. Job rotation may affect employee performance either positively or negatively.
    D. When individuals become familiar with systems and processes, they gain an understanding of the weaknesses of those systems and processes. If the individual is then motivated in some way to take advantage of the situation, various forms of fraud might occur. Job rotation reduces the opportunity and increases the likelihood of exposure of the fraud.

133. Corporate IS policy for a call center requires that all users be assigned unique user accounts. On discovering that this is not the case for all current users, what is the **MOST** appropriate recommendation?
    A. Have the current configuration approved by operations management.
    B. Ensure that there is an audit trail for all existing accounts.
    C. Implement individual user accounts for all staff.
    D. Amend the IS policy to allow shared accounts.

    Individual user accounts allow for accountability of transactions and should be the most important recommendation, given the current scenario. Choices A and B are recommendations that are not in compliance with the enterprise's own policy. Shared user IDs do not allow for accountability of transactions.

134. An IS auditor has been assigned to review IT structures and activities recently outsourced to various providers. Which of the following should the IS auditor determine **FIRST**?
    A. An audit clause is present in all contracts.
    B. The service level agreement (SLA) of each contract is substantiated by appropriate key performance indicators (KPIs).
    C. The contractual warranties of the providers support the business needs of the organization.
    D. At contract termination, support is guaranteed by each outsourcer for new outsourcers.

    The complexity of IT structures matched by the complexity and interplay of responsibilities and warranties may affect or void the effectiveness of those warranties and the reasonable certainty that the business needs will be

met. All other choices are important, but not as potentially dangerous as the interplay of the diverse and critical areas of the contractual responsibilities of the outsourcers.

135 An organization having a number of offices across a wide geographical area has developed a disaster recovery plan. Using actual resources, which of the following is the **MOST** cost-effective test of the disaster recovery plan?

A. Full operational test
B. Preparedness test
C. Paper test
D. Regression test

A preparedness test is performed by each local office/area to test the adequacy of the preparedness of local operations for disaster recovery. A paper test is a structured walk-through of the disaster recovery plan and should be conducted before a preparedness test. A full operational test is conducted after the paper and preparedness test. A regression test is not a disaster recovery plan test and is used in software maintenance.

136. Which of the following reduces the potential impact of social engineering attacks?

A. Compliance with regulatory requirements
B. Promoting ethical understanding
C. Security awareness programs
D. Effective performance incentives

Because social engineering is based on deception of the user, the best countermeasure or defense is a security awareness program. The other choices are not user-focused.

137. During a feasibility study regarding outsourcing IS processing, the relevance for the IS auditor of reviewing the vendor's business continuity plan (BCP) is to:

A. evaluate the adequacy of the service levels that the vendor can provide in a contingency.
B. evaluate the financial stability of the service bureau and its ability to fulfill the contract.
C. review the experience of the vendor's staff.
D. test the BCP.

A key factor in a successful outsourcing environment is the capability of the vendor to face a contingency. Choices B and C are incorrect because neither financial stability nor experience is related to the vendor's BCP. Choice D is incorrect because the IS auditor does not require a substantive test to evaluate the BCP.

138. When reviewing an organization's strategic IT plan an IS auditor should expect to find:

A. an assessment of the fit of the organization's application portfolio with business objectives.
B. actions to reduce hardware procurement cost.
C. a listing of approved suppliers of IT contract resources.
D. a description of the technical architecture for the organization's network perimeter security.

An assessment of how well an organization's application portfolio supports the organization's business objectives is a key component of the overall IT strategic planning process. This drives the demand side of IT planning and should convert into a set of strategic IT intentions. Further assessment can then be made of how well the overall IT organization, encompassing applications, infrastructure, services, management processes, etc., can support the business objectives. Operational efficiency initiatives belong to tactical planning, not strategic planning. The purpose of an IT strategic plan is to set out how IT will be used to achieve or support an organization's business objectives. A listing of approved suppliers of IT contract resources is a tactical rather than a strategic concern. An IT strategic plan would not normally include detail of a specific technical architecture.

139. Which of the following is the **PRIMARY** objective of the business continuity plan (BCP) process?

A. To provide assurance to stakeholders that business operations will continue in the event of disaster
B. To establish an alternate site for IT services to meet predefined recovery time objectives (RTOs)
C. To manage risk while recovering from an event that adversely affected operations
D. To meet the regulatory compliance requirements in the event of natural disaster

A. The BCP in itself does not provide assurance of continuing operations; however, it helps the organization to respond to disruptions to critical business processes.

B. Establishment of an alternate site is more relevant to disaster recovery than the BCP.

C. The BCP process primarily focuses on managing and mitigating risk during recovery of operations due to an event that affected operations.

D. The regulatory compliance requirements may help establish the RTO requirements.

140. When segregation of duties concerns exist between IT support staff and end users, what would be a suitable compensating control?

A. Restricting physical access to computing equipment
B. Reviewing transaction and application logs
C. Performing background checks prior to hiring IT staff
D. Locking user sessions after a specified period of inactivity

Only reviewing transaction and application logs directly addresses the threat posed by poor segregation of duties. The review is a means of detecting inappropriate behavior and also discourages abuse because people who may

otherwise be tempted to exploit the situation are aware of the likelihood of being caught. Inadequate segregation of duties is more likely to be exploited via logical access to data and computing resources rather than physical access. Choice C is a useful control to ensure IT staff are trustworthy and competent but does not directly address the lack of an optimal segregation of duties. Choice D acts to prevent unauthorized users from gaining system access, but the issue of a lack of segregation of duties is more the misuse (deliberately or inadvertently) of access privileges that have officially been granted.

141. Assessing IT risk is **BEST** achieved by:
    A. evaluating threats associated with existing IT assets and IT projects.
    B. using the firm's past actual loss experience to determine current exposure.
    C. reviewing published loss statistics from comparable organizations.
    D. reviewing IT control weaknesses identified in audit reports.

    To assess IT risk, threats and vulnerabilities need to be evaluated using qualitative or quantitative risk assessment approaches. Choices B, C and D are potentially useful inputs to the risk assessment process, but by themselves are not sufficient. Basing an assessment on past losses will not adequately reflect inevitable changes to the firm's IT assets, projects, controls and strategic environment. There are also likely to be problems with the scope and quality of the loss data available to be assessed. Comparable organizations will have differences in their IT assets, control environment and strategic circumstances. Therefore, their loss experience cannot be used to directly assess organizational IT risk. Control weaknesses identified during audits will be relevant in assessing threat exposure and further analysis may be needed to assess threat probability. Depending on the scope of the audit coverage, it is possible that not all of the critical IT assets and projects will have recently been audited, and there may not be a sufficient assessment of strategic IT risk.

142. Which of the following is an attribute of the control self-assessment (CSA) approach?
    A. Broad stakeholder involvement
    B. Auditors are the primary control analysts
    C. Limited employee participation
    D. Policy driven

    The CSA approach emphasizes management of and accountability for developing and monitoring the controls of an organization's business processes. The attributes of CSA include empowered employees, continuous improvement, extensive employee participation and training, all of which are representations of broad stakeholder involvement. Choices B, C and D are attributes of a traditional audit approach.

143. An organization has a well-established risk management process. Which of the following risk management practices would **MOST** likely expose the organization to the greatest amount of compliance risk?
    A. Risk reduction
    B. Risk transfer
    C. Risk avoidance
    D. Risk mitigation

    A. Risk reduction is a term synonymous with risk mitigation. Risk reduction lowers risk to a level commensurate with the organization's risk appetite. However, choice B is the best answer because risk reduction treats the risk, while risk transfer does not always address compliance risk.

    B. Risk transfer typically addresses financial risk. For instance, an insurance policy is commonly used to transfer financial risk, while compliance risk continues to exist.

    C. Risk avoidance does not expose the organization to compliance risk because the business practice that caused the inherent risk to exist is no longer being pursued.

    D. Mitigating risk will still expose the organization to a certain amount of risk. Risk mitigation lowers risk to a level commensurate with the organization's risk appetite. However, choice B is the best answer because risk mitigation treats the risk, while risk transfer does not necessarily address compliance risk.

144. A comprehensive and effective email policy should address the issues of email structure, policy enforcement, monitoring and:
    A. recovery.
    B. retention.
    C. rebuilding.
    D. reuse.

    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 email communication is held in the same regard as the official form of classic “paper” makes the retention of corporate email a necessity. All email generated on an organization's hardware is the property of the organization, and an email policy should address the retention of messages, considering both known and unforeseen litigation. The policy should also address the destruction of emails after a specified time to protect the nature and confidentiality of the messages themselves. Addressing the retention issue in the email policy would facilitate recovery, rebuilding and reuse.

145. 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

    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.

146. The activation of an enterprise's business continuity plan should be based on predetermined criteria that address the:
    A. duration of the outage.
    B. type of outage.
    C. probability of the outage.
    D. cause of the outage.

    The initiation of a business continuity plan (action) should primarily be based on the maximum period for which a business function can be disrupted before the disruption threatens the achievement of organizational objectives.

147. When reviewing the IT strategic planning process, an IS auditor should ensure that the plan:
    A. incorporates state of the art technology.
    B. addresses the required operational controls.
    C. articulates the IT mission and vision.
    D. specifies project management practices.

    The IT strategic plan must include a clear articulation of the IT mission and vision. The plan need not address the technology, operational controls or project management practices.

148. After the merger of two organizations, multiple self-developed legacy applications from both organizations are to be replaced by a new common platform. Which of the following would be the **GREATEST** risk?
    A. Project management and progress reporting is combined in a project management office which is driven by external consultants.
    B. The replacement effort consists of several independent projects without integrating the resource allocation in a portfolio management approach.
    C. The resources of each of the organizations are inefficiently allocated while they are being familiarized with the other company's legacy systems.
    D. The new platform will force the business areas of both organizations to change their work processes, which will result in extensive training needs.

    The efforts should be consolidated to ensure alignment with the overall strategy of the postmerger organization. If resource allocation is not centralized, the separate projects are at risk of overestimating the availability of key knowledge resources for the in-house developed legacy applications. In postmerger integration programs, it is common to form project management offices to ensure standardized and comparable information levels in the planning and reporting structures, and to centralize dependencies of project deliverables or resources. The experience of external consultants can be valuable since project management practices do not require in-depth knowledge of the legacy systems. This can free up resources for functional tasks. It is a good idea to first get familiar with the old systems, to understand what needs to be done in a migration and to evaluate the implications of technical decisions. In most cases, mergers result in application changes and thus in training needs as organizations and processes change to leverage the intended synergy effects of the merger.

149. Which of the following is the **BEST** enabler for strategic alignment between business and IT?
    A. A maturity model
    B. Goals and metrics
    C. Control objectives
    D. A responsible, accountable, consulted and informed (RACI) chart

    Goals and metrics ensure that IT goals are set based on business goals, and they are the best enablers of strategic alignment. Maturity models enable assessment of current process capability and could be used for process improvement, but they do not directly enable strategic alignment. Control objectives facilitate the implementation of controls in the related processes according to business requirements. RACI charts enable the assignment of responsibility to key functionaries, but do not ensure strategic alignment.

150. 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 **MOST** based on the individual's experience and:
   A. length of service, since this will help ensure technical competence.
   B. age since 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.

   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 IS audit department's needs should be defined and any candidate should be evaluated against those requirements. The length of service will not ensure technical competency. 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.
151. Which of the following would impair the independence of a quality assurance team?
   A. Ensuring compliance with development methods
   B. Checking the testing assumptions
   C. Correcting coding errors during the testing process
   D. Checking the code to ensure proper documentation

   Correction of code should not be a responsibility of the quality assurance team as it would not ensure segregation of duties and would impair the team's independence. The other choices are valid quality assurance functions.
152. Which of the following is the **MOST** important criterion for selecting an alternate processing site?
   A. Total geographic distance between the two sites
   B. Likelihood of the same natural event occurring at both sites
   C. Matching processing capacity at both sites
   D. Proximity of the alternate site to local fire, emergency response and hospital facilities

   A. The alternate location should be at a sufficient geographic distance from the main processing facility, but this is not the main objective. Geographic distance is important; however, the same event such as an earthquake could affect two geographically diverse processing facilities.

   B. The likelihood of the occurrence of a natural disaster is a consideration in overall business continuity planning and in whether there is a business case to set up an alternate site. The alternate site should be at a location that does not expose it to the same natural threats as the main processing facility.

   C. The alternate site must sustain operations so that normal business activities are disrupted for only a reasonable duration. This does not mandate that capacity of the alternate site be identical to the main site. Focus must be on critical business services receiving adequate support and resources to prevent disruption.

   D. Proximity to local fire and other emergency response facilities is an advantage, but not a criterion for choosing the alternate location.
153. An IS auditor observes that an enterprise has outsourced software development to a third party that is a startup company. To ensure that the enterprise's investment in software is protected, which of the following should be recommended by the IS auditor?
   A. Due diligence should be performed on the software vendor.
   B. A quarterly audit of the vendor facilities should be performed.
   C. There should be a source code escrow agreement in place.
   D. A high penalty clause should be included in the contract.

   A source code escrow agreement is primarily recommended to help protect the enterprise's investment in software because the source code will be available with a trusted third party and can be retrieved if the third party goes out of business or if the software company goes out of business. While due diligence, quarterly audits of vendor facilities and penalty clauses are best practices, they do not ensure availability of the source code.
154. While reviewing the IT governance processes of an organization, an auditor discovers that the firm has recently implemented an IT balanced scorecard (BSC). The implementation is complete; however, the IS auditor notices that performance indicators are not objectively measurable. What is the **PRIMARY** risk presented by this situation?
   A. Key performance indicators (KPIs) are not reported to management and management cannot determine the effectiveness of the BSC.
   B. IT projects could suffer from cost overruns.
   C. Misleading indications of IT performance may be presented to management.
   D. IT service level agreements (SLAs) may not be accurate.

   The IT BSC is designed to measure IT performance. In order to measure performance, a sufficient number of “performance drivers” or KPIs must be defined and measured over time. If the performance indicators are not objectively measurable, the most significant risk would be the presentation of misleading performance results to management. This could result in a false sense of assurance and, as a result, IT resources may be misallocated or strategic decisions may be based on incorrect information. Whether or not the performance indicators are correctly

defined, the results would be reported to management. Therefore, choice A is not the correct answer. Although project management and performance management issues could arise from performance indicators that were not correctly defined, the presentation of misleading performance to management is a much more significant risk. Therefore, choices B and D are not correct.

155. An IS auditor is reviewing an organization's recovery from a disaster in which not all the critical data needed to resume business operations were retained. Which of the following was incorrectly defined?
    A. The interruption window
    B. The recovery time objective (RTO)
    C. The service delivery objective
    D. The recovery point objective (RPO)

    The RPO is determined based on the acceptable data loss in the case of a disruption of operations. RPO defines the point in time from which it is necessary to recover the data and quantifies, in terms of time, the permissible amount of data loss in the case of interruption. The interruption window is defined as the amount of time during which the organization can maintain operations from the point of failure to the time that the critical services/applications are restored. RTO is determined based on the acceptable downtime in the case of a disruption of operations. The service delivery objective relates to the business needs and service levels and is not applicable to the scenario.

156. Which of the following disaster recovery/continuity plan components provides the **GREATEST** assurance of recovery after a disaster?
    A. The alternate facility will be available until the original information processing facility is restored.
    B. User management is involved in the identification of critical systems and their associated critical recovery times.
    C. Copies of the plan are kept at the homes of key decision-making personnel.
    D. Feedback is provided to management assuring them that the business continuity plans are indeed workable and that the procedures are current.

    The alternate facility should be made available until the original site is restored to provide the greatest assurance of recovery after a disaster. Without this assurance, the plan will not be successful. All other choices ensure prioritization or the execution of the plan.

157. A structured walk-through of a disaster recovery plan involves:
    A. representatives from each of the functional areas coming together to go over the plan.
    B. all employees who participate in the day-to-day operations coming together to practice executing the plan.
    C. moving the systems to the alternate processing site and performing processing operations.
    D. distributing copies of the plan to the various functional areas for review.

    A structured walk-through test of a disaster recovery plan involves representatives from each of the functional areas coming together to review the plan to determine if the plan pertaining to their area is accurate and complete, and can be implemented when required. Choice B is a simulation test to prepare and train the personnel who will be required to respond to disasters and disruptions. Choice C is a form of parallel testing to ensure that critical systems will perform satisfactorily in the alternate site. Choice D is a checklist test.

158. An IS audit department is planning to minimize its dependency on key individuals. Activities that contribute to this objective are documented procedures, knowledge sharing, cross-training, and:
    A. succession planning.
    B. staff job evaluation.
    C. responsibilities definition.
    D. employee award programs.

    Succession planning ensures that internal personnel with the potential to fill key positions in the company are identified and developed. Job evaluation is the process of determining the worth of one job in relation to that of the other jobs in a company so that a fair and equitable wage and salary system can be established. Staff responsibilities definition provides for well-defined roles and responsibilities, and employee award programs provide motivation; however, they do not minimize dependency on key individuals.

159. An IS auditor is verifying IT policies and found that some of the policies have not been approved by management (as required by policy), but the employees strictly follow the policies. What should the IS auditor do **FIRST?**
    A. Ignore the absence of management approval because employees follow the policies.
    B. Recommend immediate management approval of the policies.
    C. Emphasize the importance of approval to management.
    D. Report the absence of documented approval.

    The IS auditor must report the finding. Unapproved policies may present a potential risk to the organization, even if they are being followed, since this technicality may prevent management from enforcing the policies in some cases and may present legal issues. For example, if an employee were terminated as a result of violating a company policy and it was discovered that the policies had not been approved, the company could be faced with an expensive lawsuit. While the IS auditor would likely recommend that the policies should be approved as soon as possible, and

may also remind management of the critical nature of this issue, the first step would be to report this issue to the relevant stakeholders.

160. The ultimate purpose of IT governance is to:
   A. encourage optimal use of IT.
   B. reduce IT costs.
   C. decentralize IT resources across the organization.
   D. centralize control of IT.

   IT governance is intended to specify the combination of decision rights and accountability that is best for the enterprise. It is different for every enterprise. Reducing IT costs may not be the best IT governance outcome for an enterprise. Decentralizing IT resources across the organization is not always desired, although it may be desired in a decentralized environment. Centralizing control of IT is not always desired. An example of where it might be desired is an enterprise desiring a single point of customer contact.

161. An IS steering committee should:
   A. include a mix of members from different departments and staff levels.
   B. ensure that IS security policies and procedures have been executed properly.
   C. maintain minutes of its meetings and keep the board of directors informed.
   D. be briefed about new trends and products at each meeting by a vendor.

   It is important to keep detailed steering committee minutes to document the decisions and activities of the IS steering committee, and the board of directors should be informed about those decisions on a timely basis. Choice A is incorrect because only senior management or high-level staff members should be on this committee because of its strategic mission. Choice B is not a responsibility of this committee, but the responsibility of the security administrator. Choice D is incorrect because a vendor should be invited to meetings only when appropriate.

162. An IS auditor is reviewing the risk management process. Which of the following is the **MOST** important consideration during this review?
   A. Controls are implemented based on cost-benefit analysis.
   B. The risk management framework is based on global standards.
   C. The approval process for risk response is in place.
   D. IT risk is presented in business terms.

   A. Controls to mitigate risk must be implemented based on cost-benefit analysis; however, the cost-benefit analysis is effective only if risk is presented in business terms.

   B. A risk management framework based on global standards helps in ensuring completeness; however, organizations must adapt it to suit specific business requirements.

   C. Approvals for risk response come later in the process.

   D. In order for risk management to be effective, it is necessary to align IT risk with business objectives. This can be done by adopting acceptable terminology that is understood by all, and the best way to achieve this is to present IT risk in business terms.

163. A financial institution has recently developed and installed a new deposit system which interfaces with their customer web site and their automated teller machines (ATMs). During the project, the development team and the business continuity team maintained good communication and the business continuity plan (BCP) has been updated to include the new system. A suitable BCP test to perform at this point in time would be:
   A. using actual resources to simulate a system crash.
   B. a detailed paper walk-through of the plan.
   C. a penetration test for the web site interface application.
   D. performing a failover of the system at the designated secondary site.

   The expectation is that the basic mechanics of recovery for the new system are understood and the recovery infrastructure has been put into place. An appropriate test now would be to involve actual resources in a simulated recovery exercise. This exercise would test the new recovery infrastructure under controlled conditions. Assuming that recovery options have been actively considered during development (as they would need to be for a mission-critical system), a paper walk-through would be of limited value. A security assessment or penetration test is vital for any application exposed to the Internet, but should have been performed much earlier in the process. Choice D is not correct because performing a failover test is not adequate to assess the degree to which the organization is prepared to recover from a wider range of problems.

164. Which of the following is **MOST** indicative of the effectiveness of an information security awareness program?
   A. Employees report more information regarding security incidents.
   B. All employees have signed the information security policy.
   C. Most employees have attended an awareness session.
   D. Information security responsibilities have been included in job descriptions.

   Although the promotion of security awareness is a preventive control, it can also be a detective measure because it encourages people to identify and report possible security violations. Choice A is the correct answer because the reporting of incidents implies that employees are taking action as a consequence of the awareness program. The

existence of evidence that all employees have signed the security policy does not ensure that security responsibilities have been understood and applied. One of the objectives of the security awareness program is to inform the employees of what is expected of them and what their responsibilities are, but this knowledge does not ensure that employees will perform their activities in a secure manner. The documentation of roles and responsibilities in job descriptions is not an indicator of the effectiveness of the awareness program.

165. An IS auditor found that the enterprise architecture (EA) recently adopted by an organization has an adequate current-state representation. However, the organization has started a separate project to develop a future-state representation. The IS auditor should:
    A. recommend that this separate project be completed as soon as possible.
    B. report this issue as a finding in the audit report.
    C. recommend the adoption of the Zachmann framework.
    D. re-scope the audit to include the separate project as part of the current audit.
    It is critical for the EA to include the future state because the gap between the current state and the future state will determine IT strategic and tactical plans. If the EA does not include a future-state representation, it is not complete, and this issue should be reported as a finding. Choice A is not correct because the IS auditor would not ordinarily provide input on the timing of projects, but rather provide an assessment of the current environment. The most critical issue in this scenario is that the EA is not yet complete, so the auditor should be most concerned with reporting this issue. Choice C is not correct because the company is free to choose any EA framework and the IS auditor should not recommend a specific framework. Choice D is not correct because changing the scope of an audit to include the secondary project is not a realistic option.

166. The **PRIMARY** outcome of a business impact analysis (BIA) is:
    A. a plan for resuming operations after a disaster.
    B. a commitment of the organization to physical and logical security.
    C. a framework for an effective disaster recovery plan (DRP).
    D. an understanding of the cost of an interruption.
    A. A BIA does establish a starting point for planning how to resume operations after a disaster. This is, however, not the primary purpose of a BIA.
    B. The public's perception of an organization's physical and logical security is not the primary objective of a BIA.
    C. The BIA provides an important input into business continuity planning, but not a framework for effective disaster recovery planning (DRP).
    D. A BIA helps one understand the cost of an interruption and identify which applications and processes are most critical to the continued functioning of the organization.

167. Which of the following situations is addressed by a software escrow agreement?
    A. The system administrator requires access to software in order to recover from a disaster.
    B. A user requests to have software reloaded onto a replacement hard drive.
    C. The vendor of custom-written software goes out of business.
    D. An IT auditor requires access to software code written by the organization.
    A software escrow is a legal agreement between a software vendor and a customer, to guarantee access to source code. The application source code is held by a trusted third party, according to the contract. This agreement is necessary in the event that the software vendor goes out of business, there is a contractual dispute with the customer or the software vendor fails to maintain an update of the software as promised in the software license agreement. The other choices are not correct because access to software in the other situations should be provided by an internally managed software library.

168. The success of control self-assessment (CSA) depends highly on:
    A. having line managers assume a portion of the responsibility for control monitoring.
    B. assigning staff managers the responsibility for building, but not monitoring, controls.
    C. the implementation of a stringent control policy and rule-driven controls.
    D. the implementation of supervision and the monitoring of controls of assigned duties.
    The primary objective of a CSA program is to leverage the internal audit function by shifting some of the control monitoring responsibilities to the functional area line managers. The success of a CSA program depends on the degree to which line managers assume responsibility for controls. Choices B, C and D are characteristics of a traditional audit approach, not a CSA approach.
169. A subsidiary in another country is forced to depart from the parent organization's IT policies to conform to the local law. The **BEST** approach for the parent organization is to:
    A. create a provision to allow local policies to take precedence where required by law.
    B. have the subsidiary revise its policies to conform to the parent organization's policies.
    C. revise the parent organization's policies so that they match the subsidiary's policies.
    D. track the issue as a violation of policy with a note of the extenuating circumstances.

A. Creating a provision to allow local policies to take precedence where required by local authorities allows the organization to implement the optimal level of control subject to legal limitations.
B. This is not acceptable because it subjects the subsidiary to local fines and penalties.
C. This is a less desirable alternative because the policy in question may provide a superior level of control and risk reduction from which the remainder of the organization should continue to benefit.
D. Tracking the issue as a policy violation fails to satisfactorily resolve the issue and recognize the need for flexibility.

170. An IS auditor is reviewing IT projects for a large company and wants to determine whether the IT projects undertaken in a given year are those which have been assigned the highest priority by the business and which will generate the greatest business value. Which of the following would be **MOST** relevant?
    A. A capability maturity model (CMM)
    B. Portfolio management
    C. Configuration management
    D. Project management body of knowledge (PMBOK)
    Portfolio management is designed to assist in the definition, prioritization, approval and running of a set of projects within a given organization. These tools offer data capture, workflow and scenario planning functionality, which can help identify the optimum set of projects (from the full set of ideas) to take forward within a given budget. A CMM would not help determine the optimum portfolio of capital projects since it is a means of assessing the relative maturity of the IT processes within an organization: running from Level 0 (Incomplete—Processes are not implemented or fail to achieve their purpose) to Level 5 (Optimizing—Metrics are defined and measured, and continuous improvement techniques are in place). A configuration management database (which stores the configuration details for an organization's IT systems) is an important tool for IT service delivery and, in particular, change management. It may provide information that would influence the prioritization of projects, but is not designed for that purpose. PMBOK is a methodology for the management and delivery of projects. It offers no specific guidance or assistance in optimizing a project portfolio.

171. Which of the following is the **BEST** reason to implement a policy which addresses secondary employment for IT employees?
    A. To ensure that employees are not misusing corporate resources
    B. To prevent conflicts of interest
    C. To prevent employee performance issues
    D. To prevent theft of IT assets
    The best reason to implement and enforce a policy governing secondary employment is to prevent conflicts of interest. Conflicts of interest could result in serious risk such as fraud, theft of intellectual property or other improprieties. The other options are not correct because issues such as the misuse of corporate resources, poor performance and theft of IT assets are not as severe as the possible ramifications of a conflict of interest.

172. A top-down approach to the development of operational policies helps 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.
    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.

173. Which of the following business continuity plan (BCP) tests involves participation of relevant members of the crisis management/response team, in order to practice proper coordination?
    A. Table-top
    B. Functional
    C. Full-scale
    D. Walk-through
    The primary purpose of table-top testing is to practice proper coordination since it involves all or some of the crisis team members and is focused more on coordination and communications issues than on technical process details. Functional testing involves mobilization of personnel and resources at various geographic sites. Full-scale testing involves enterprisewide participation and full involvement of external organizations. Walk-through testing requires the least effort of the options given. Its aim is to promote familiarity of the BCP to critical personnel from all areas.

174. 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.
    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.

175. During a review of a business continuity plan, an IS auditor noticed that the point at which a situation is declared to be a crisis has not been defined. The **MAJOR** risk associated with this is that:
    A. assessment of the situation may be delayed.
    B. execution of the disaster recovery plan could be impacted.
    C. notification of the teams might not occur.
    D. potential crisis recognition might be ineffective.
    Execution of the business continuity plan would be impacted if the organization does not know when to declare a crisis. Choices A, C and D are steps that must be performed to know whether to declare a crisis. Problem and severity assessment would provide information necessary in declaring a disaster. Once a potential crisis is recognized, the teams responsible for crisis management need to be notified. Delaying this step until a disaster has been declared would negate the effect of having response teams. Potential crisis recognition is the first step in responding to a disaster.

176. Which of the following would an IS auditor consider the **MOST** relevant to short-term planning for an IS department?
    A. Allocating resources
    B. Keeping current with technology advances
    C. Conducting control self-assessment
    D. Evaluating hardware needs
    The IS department should specifically consider the manner in which resources are allocated in the short term. Investments in IT need to be aligned with top management strategies, rather than focusing on technology for technology's sake. Conducting control self-assessments and evaluating hardware needs are not as critical as allocating resources during short-term planning for the IS department.

177. An IS auditor of a large organization is reviewing the roles and responsibilities for the IS function and has found some individuals serving multiple roles. Which one of the following combinations of roles should be of **GREATEST** concern for the IS auditor?
    A. Network administrators are responsible for quality assurance.
    B. Security administrators are system programmers.
    C. End users are security administrators for critical applications.
    D. Systems analysts are database administrators.
    When individuals serve multiple roles this represents a separation of duties problem with associated risk. Security administrators should not be system programmers, due to the associated rights of both functions. The other combinations of roles are valid from a separation of duties perspective.

178. An IS auditor is reviewing a project to implement a payment system between a parent bank and a subsidiary. The IS auditor should **FIRST** verify that the:
    A. technical platforms between the two companies are interoperable.
    B. parent bank is authorized to serve as a service provider.
    C. security features are in place to segregate subsidiary trades.
    D. subsidiary can join as a co-owner of this payment system.
    Even between parent and subsidiary companies, contractual agreement(s) should be in place to conduct shared services. This is particularly important in highly regulated organizations such as banking. Unless granted to serve as a service provider, it may not be legal for the bank to extend business to the subsidiary companies. Technical aspects should always be considered; however, this can be initiated after confirming that the parent bank can serve as a service provider. Security aspects are another important factor; however, this should be considered after confirming that the parent bank can serve as a service provider. The ownership of the payment system is not as important as the legal authorization to operate the system.

179. The **MOST** likely effect 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. technology not aligning with the organization's objectives.
    D. an absence of control over technology contracts.

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.

180. Which of the following should be included in an organization's information security policy?
    A. A list of key IT resources to be secured
    B. The basis for control access authorization
    C. Identity of sensitive security features
    D. Relevant software security features

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

181. An IS auditor is reviewing an organization's business continuity plan (BCP) to determine the impact of a disruption in an industry where regulatory requirements demand high availability. Which of the following findings should be of **MOST** concern to the auditor?
    A. The organization does not have an original copy of the agreement for the alternate processing site.
    B. The backup tapes are not encrypted for offsite storage.
    C. Data restoration tests for the backups of production data are not performed.
    D. Backup tapes that exceed their lifetime usage are not disposed of securely.

    A. While an original copy of the agreement is important, many third parties will send a duplicate original copy of an agreement so that each party has an original.

    B. Encrypted backups are important to ensure the confidentiality of information; however, if they are not encrypted, it does not impact the organization's ability to continue operations.

    C. Backup tapes should be periodically tested to ensure that data are available when needed and to minimize the impact of a disruption. If the backups are not tested, there could be a delay because the production data may not be available or must be moved to the alternate processing site. In addition, there could be a delay if manual processing is needed.

    D. Secure disposal of backup tapes is important to ensure the confidentiality of information; however, it does not impact the organization's ability to continue operations.

182. Which of the following is a risk of cross-training?
    A. Increases the dependence on one employee
    B. Does not assist in succession planning
    C. One employee may know all parts of a system
    D. Does not help in achieving a continuity of operations

    When cross-training, it would be prudent to first assess the risk of any person knowing all parts of a system and what exposures this may cause. Cross-training has the advantage of decreasing dependence on one employee and, hence, can be part of succession planning. It also provides backup for personnel in the event of absence for any reason and thereby facilitates the continuity of operations.

183. 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.

    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.

184. Which of the following should be of **GREATEST** concern to an IS auditor when reviewing an information security policy? The policy:
    A. is driven by an IT department's objectives.
    B. is published, but users are not required to read the policy.
    C. does not include information security procedures.
    D. has not been updated in over a year.

    Business objectives drive the information security policy, and an IT department's objectives are driven by the business objectives. Policies should be written so that users can understand each policy, and employees should be able to easily access the policies. Policies should not contain procedures. Procedures are established to assist with

policy compliance. Policies should be reviewed annually, but might not necessarily be updated annually unless there are significant changes in the environment such as new laws, rules or regulations.

185. To gain an understanding of the effectiveness of an organization's planning and management of investments in IT assets, an IS auditor should review the:
   A. enterprise data model.
   B. IT balanced scorecard (BSC).
   C. IT organizational structure.
   D. historical financial statements.
   The IT BSC is a tool that provides the bridge between IT objectives and business objectives by supplementing the traditional financial evaluation with measures to evaluate customer satisfaction, internal processes and the ability to innovate. An enterprise data model is a document defining the data structure of an organization and how data interrelate. It is useful, but it does not provide information on investments. The IT organizational structure provides an overview of the functional and reporting relationships in an IT entity. Historical financial statements do not provide information about planning and lack sufficient detail to enable one to fully understand management's activities regarding IT assets. Past costs do not necessarily reflect value, and assets such as data are not represented on the books of accounts.

186. A team conducting a risk analysis is having difficulty projecting the financial losses that could result from a risk. To evaluate the potential losses, the team should:
   A. compute the amortization of the related assets.
   B. calculate a return on investment (ROI).
   C. apply a qualitative approach.
   D. spend the time needed to define exactly the loss amount.
   The common practice, when it is difficult to calculate the financial losses, is to take a qualitative approach, in which the manager affected by the risk defines the financial loss in terms of a weighted factor (e.g., one is a very low impact to the business and five is a very high impact). An ROI is computed when there is predictable savings or revenues that can be compared to the investment needed to realize the revenues. Amortization is used in a profit and loss statement, not in computing potential losses. Spending the time needed to define exactly the total amount is normally a wrong approach. If it has been difficult to estimate potential losses (e.g., losses derived from erosion of public image due to a hack attack), that situation is not likely to change, and at the end of the day, the result will be a not well-supported evaluation.

187. To address the risk of operations staff's failure to perform the daily backup, management requires that the systems administrator sign off on the daily backup. This is an example of risk:
   A. avoidance.
   B. transfer.
   C. mitigation.
   D. acceptance.
   Risk mitigation is the strategy that provides for the definition and implementation of controls to address the risk described. Risk avoidance is a strategy that provides for not implementing certain activities or processes that would incur risk. Risk transfer is the strategy that provides for sharing risk with partners or taking insurance coverage. Risk acceptance is a strategy that provides for formal acknowledgment of the existence of a risk and the monitoring of that risk.

188. The **BEST** method for assessing the effectiveness of a business continuity plan is to review the:
   A. plans and compare them to appropriate standards.
   B. results from previous tests.
   C. emergency procedures and employee training.
   D. offsite storage and environmental controls.
   Previous test results will provide evidence of the effectiveness of the business continuity plan. Comparisons to standards will give some assurance that the plan addresses the critical aspects of a business continuity plan but will not reveal anything about its effectiveness. Reviewing emergency procedures, offsite storage and environmental controls would provide insight into some aspects of the plan but would fall short of providing assurance of the plan's overall effectiveness.

189. The **PRIMARY** control purpose of required vacations or job rotations is to:
   A. allow cross-training for development.
   B. help preserve employee morale.
   C. detect improper or illegal employee acts.
   D. provide a competitive employee benefit.
   The practice of having another individual perform a job function is a control used to detect possible irregularities or fraud. While cross-training is a good practice for business continuity, it is not achieved through mandatory

vacations. It is a best practice to maintain good employee morale, but this is not a primary reason to have a required vacation policy. Vacation time is a competitive benefit, but that is not a control.

190. When implementing an IT governance framework in an organization the **MOST** important objective is:
   A. IT alignment with the business.
   B. accountability.
   C. value realization with IT.
   D. enhancing the return on IT investments.
   The goals of IT governance are to improve IT performance, to deliver optimum business value and to ensure regulatory compliance. The key practice in support of these goals is the strategic alignment of IT with the business (choice A). To achieve alignment, all other choices need to be tied to business practices and strategies.

191. When auditing a role-based access control system (RBAC), the IS auditor noticed that some IT security employees have system administrator privileges on some servers which allows them to modify or delete transaction logs. Which would be the **BEST** recommendation that the IS auditor should make?
   A. Ensure that these employees are adequately supervised.
   B. Ensure that backups of the transaction logs are retained.
   C. Implement controls to detect the changes.
   D. Ensure that transaction logs are written in real time to Write Once and Read Many (WORM) drives.
   Allowing IT security employees access to transaction logs is often unavoidable because having system administrator privileges is required for them to do their job. The best control in this case, to avoid unauthorized modifications of transaction logs, is to write the transaction logs to WORM drive media in real time. It is important to note that simply backing up the transaction logs to tape is not adequate since data could be modified prior (typically at night) to the daily backup job execution. Choice A is not correct because IT security employees cannot be supervised in the traditional sense unless the supervisor were to monitor each keystroke entered on a workstation, which is obviously not a realistic option. Choice B is not correct because retaining backups of the transaction logs does not prevent the files from unauthorized modification prior to backup. Choice C is not correct because the log files themselves are the main evidence that an unauthorized change was made, which is a sufficient detective control. Protecting the log files from modification requires preventive controls such as securely writing the logs.

192. An IS auditor is performing a review of an organization's governance model. Which of the following should be of **MOST** concern to the auditor?
   A. The organization's information security policy is not periodically reviewed by senior management.
   B. A policy to ensure that systems are patched in a timely manner does not exist.
   C. The audit committee did not review the global mission statement.
   D. An organizational policy related to malware protection does not exist.
   A. Data security policies should be reviewed/refreshed once every year to reflect changes in the organization's environment. Policies are fundamental to the organization's governance structure, and therefore this is the greatest concern.
   B. While it is a concern that there is no policy related to system patching, the greater concern is that the information security policy is not reviewed periodically by senior management.
   C. Mission statements tend to be long term because they are strategic in nature and are established by the board of directors and management. This is not the IS auditor's greatest concern because proper governance oversight could lead to meeting the objectives of the organization's mission statement.
   D. While it is a concern that there is no policy related to malware protection, the greater concern is that the security policy is not reviewed periodically by senior management.

193. Disaster recovery planning (DRP) addresses the:
   A. technological aspect of business continuity planning (BCP).
   B. operational part of business continuity planning.
   C. functional aspect of business continuity planning.
   D. overall coordination of business continuity planning.
   DRP is the technological aspect of BCP. Business resumption planning addresses the operational part of BCP.

194. When auditing the archiving of the company's email communications, the IS auditor should pay the **MOST** attention to:
   A. the existence of a data retention policy.
   B. the storage capacity of the archiving solution.
   C. the level of user awareness concerning email use.
   D. the support and stability of the archiving solution manufacturer.
   Without a data retention policy that is aligned to the company's business and compliance requirements, the email archive may not preserve and reproduce the correct information when required. Choice B is not correct because the storage capacity of the archiving solution would be irrelevant if the proper email messages have not been

properly preserved and others have been deleted. Choices C and D are not correct because the level of user awareness concerning email use and the support and stability of the archiving solution manufacturer would not directly affect the completeness and accuracy of the archived email.

195. 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.

   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 risk addressed in choices A, B and D.

196. Which of the following is the key benefit of control self-assessment (CSA)?
   A. Management ownership of the internal controls supporting business objectives is reinforced.
   B. Audit expenses are reduced when the assessment results are an input to external audit work.
   C. Fraud detection will be improved since internal business staff are engaged in testing controls.
   D. Internal auditors can shift to a consultative approach by using the results of the assessment.

   The objective of control self-assessment is to have business management become more aware of the importance of internal control and their responsibility in terms of corporate governance. Reducing audit expenses is not a key benefit of CSA. Improved fraud detection is important, but not as important as ownership, and is not a principal objective of CSA. CSA may give more insights to internal auditors, allowing them to take a more consultative role; however, this is an additional benefit, not the key benefit.

197. A benefit of open system architecture is that it:
   A. facilitates interoperability.
   B. facilitates the integration of proprietary components.
   C. will be a basis for volume discounts from equipment vendors.
   D. allows for the achievement of more economies of scale for equipment.

   Open systems are those for which suppliers provide components whose interfaces are defined by public standards, thus facilitating interoperability between systems made by different vendors. In contrast, closed system components are built to proprietary standards so that other suppliers' systems cannot or will not interface with existing systems. Choices C and D are not correct.

198. Which of the following controls would an IS auditor look for in an environment where duties cannot be appropriately segregated?
   A. Overlapping controls
   B. Boundary controls
   C. Access controls
   D. Compensating controls

   Compensating controls are internal controls that are intended to reduce the risk of an existing or potential control weakness that may arise when duties cannot be appropriately segregated. Overlapping controls are two controls addressing the same control objective or exposure. Since primary controls cannot be achieved when duties cannot or are not appropriately segregated, it is difficult to install overlapping controls. Boundary controls establish the interface between the would-be user of a computer system and the computer system itself, and are individual-based, not role-based, controls. Access controls for resources are based on individuals and not on roles.

199. A financial services organization is developing and documenting business continuity measures. In which of the following cases would an IS auditor **MOST** likely raise an issue?
   A. The organization uses good practice guidelines instead of industry standards and relies on external advisors to ensure the adequacy of the methodology.
   B. The business continuity capabilities are planned around a carefully selected set of scenarios which describe events that might happen with a reasonable probability.
   C. The recovery time objectives (RTOs) do not take IT disaster recovery constraints into account, such as personnel or system dependencies during the recovery phase.
   D. The organization plans to rent a shared alternate site with emergency workplaces that has only enough room for half of the normal staff.

   It is a common mistake to use scenario planning for business continuity. The problem is that it is impossible to plan and document actions for every possible scenario. Planning for just selected scenarios denies the fact that even improbable events can cause an organization to break down. Best practice planning addresses the four possible areas of impact in a disaster: premises, people, systems and suppliers and other dependencies. All scenarios can be

reduced to these four categories and can be handled simultaneously. There are very few special scenarios which justify an additional separate analysis. It is a good idea to use best practices and external advice for such an important topic, especially since knowledge of the right level of preparedness and the judgment about adequacy of the measures taken is not available in every organization. The RTOs are based on the essential business processes required to ensure the organization's survival; therefore, it would be inappropriate for them to be based on IT capabilities. Best practice guidelines recommend having 20–40 percent of normal capacity available at an emergency site; therefore, a value of 50 percent would not be a problem if there are no additional factors.

200. Which of the following would be **MOST** important for an IS auditor to verify while conducting a business continuity audit?

A. Data backups are performed on a timely basis.
B. A recovery site is contracted for and available as needed.
C. Human safety procedures are in place.
D. Insurance coverage is adequate and premiums are current.

The most important element in any business continuity process is the protection of human life. This takes precedence over all other aspects of the plan.

201. To optimize an organization's business contingency plan (BCP), an IS auditor should recommend a business impact analysis (BIA) in order to determine:

A. the business processes that generate the most financial value for the organization and, therefore, must be recovered first.
B. the priorities and order for recovery to ensure alignment with the organization's business strategy.
C. the business processes that must be recovered following a disaster to ensure the organization's survival.
D. the priorities and order of recovery which will recover the greatest number of systems in the shortest time frame.

To ensure the organization's survival following a disaster, it is important to recover the most critical business processes first. It is a common mistake to overemphasize value (A) rather than urgency. For example, while the processing of incoming mortgage loan payments is important from a financial perspective, it could be delayed for a few days in the event of a disaster. On the other hand, wiring funds to close on a loan, while not generating direct revenue, is far more critical because of the possibility of regulatory problems, customer complaints and reputation issues. Choices B and D are not correct because neither the long-term business strategy nor the mere number of recovered systems has a direct impact at this point in time.

202. An IS auditor is performing a review of the software quality management process in an organization. The **FIRST** step should be to:

A. verify how the organization follows the standards.
B. identify and report the controls currently in place.
C. review the metrics for quality evaluation.
D. request all standards that have been adopted by the organization.

The first step of the review of the software quality management process should be to determine the evaluation criteria in the form of standards adopted by the organization. The evaluation of how well the organization follows their own standards cannot be performed until the IS auditor has determined what standards exist. The other items listed—verifying how well standards are being followed, identifying relevant controls and reviewing the quality metrics—are secondary to the identification of standards.

203. While conducting an audit of a service provider, an IS auditor observes that the service provider has outsourced a part of the work to another provider. Since the work involves confidential information, the IS auditor's **PRIMARY** concern should be that the:

A. requirement for protecting confidentiality of information could be compromised.
B. contract may be terminated because prior permission from the outsourcer was not obtained.
C. other service provider to whom work has been outsourced is not subject to audit.
D. outsourcer will approach the other service provider directly for further work.

Many countries have enacted regulations to protect the confidentiality of information maintained in their countries and/or exchanged with other countries. Where a service provider outsources part of its services to another service provider, there is a potential risk that the confidentiality of the information will be compromised. Choices B and C could be concerns but are not related to ensuring the confidentiality of information. There is no reason why an IS auditor should be concerned with choice D.

204. Overall business risk for a particular threat can be expressed as:

A. a product of the likelihood and magnitude of the impact should a threat successfully exploit a vulnerability.
B. the magnitude of the impact should a threat source successfully exploit the vulnerability.
C. the likelihood of a given threat source exploiting a given vulnerability.

D. the collective judgment of the risk assessment team.

Choice A takes into consideration the likelihood and magnitude of the impact and provides the best measure of the risk to an asset. Choice B provides only the likelihood of a threat exploiting a vulnerability in the asset but does not provide the magnitude of the possible damage to the asset. Similarly, choice C considers only the magnitude of the damage and not the possibility of a threat exploiting a vulnerability. Choice D defines the risk on an arbitrary basis and is not suitable for a scientific risk management process, but is often used and sometimes quite sensible.

205. The **MOST** important point of consideration for an IS auditor while reviewing an enterprise's project portfolio is that it:
   A. does not exceed the existing IT budget.
   B. is aligned with the investment strategy.
   C. has been approved by the IT steering committee.
   D. is aligned with the business plan.

   Portfolio management takes a holistic view of an enterprise's overall IT strategy, which, in turn, should be aligned with the business strategy. A business plan provides the justification for each of the projects in the project portfolio, and that is the major consideration for an IS auditor. Not every enterprise has an IT steering committee.

206. Which of the following tasks should be performed **FIRST** when preparing a disaster recovery plan?
   A. Develop a recovery strategy.
   B. Perform a business impact analysis (BIA).
   C. Map software systems, hardware and network components.
   D. Appoint recovery teams with defined personnel, roles and hierarchy.

   The first step in any disaster recovery plan is to perform a BIA. All other tasks come afterwards.

207. After completing the business impact analysis (BIA), what is the **NEXT** step in the business continuity planning (BCP) process?
   A. Test and maintain the plan.
   B. Develop a specific plan.
   C. Develop recovery strategies.
   D. Implement the plan.

   The next phase in the continuity plan development is to identify the various recovery strategies and select the most appropriate strategy for recovering from a disaster. After selecting a strategy, a specific plan can be developed, tested and implemented.

208. Integrating business continuity planning (BCP) into IT project management aids in:
   A. the retrofitting of the business continuity requirements.
   B. the development of a more comprehensive set of requirements.
   C. the development of a transaction flowchart.
   D. ensuring the application meets the user's needs.

   Integrating BCP into the development process ensures complete coverage of the requirements through each phase of the project. Retrofitting of the business continuity plan's requirements occurs when BCP is not integrating into the development methodology. Transaction flowcharts aid in analyzing an application's controls. A business continuity plan will not directly address the detailed processing needs of the users.

209. 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 backup of the employee's work.
   C. notify other employees of the termination.
   D. **disable the employee's logical access**.

   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.

210. To aid management in achieving IT and business alignment, an IS auditor should recommend the use of:
   A. control self-assessments.
   B. a business impact analysis (BIA).
   C. an IT balanced scorecard (BSC).
   D. business process reengineering (BPR).

   An IT BSC provides the bridge between IT objectives and business objectives by supplementing the traditional financial evaluation with measures to evaluate customer satisfaction, internal processes and the ability to innovate. CSA, BIA and BPR are insufficient to align IT with organizational objectives.

211. After initial investigation, an IS auditor has reasons to believe that fraud may be present. The IS auditor should:

A. Expand activities to determine whether an investigation is warranted

B. Report the matter to the audit committee

C. Report the possibility of fraud to management

D. Consult with external legal counsel to determine the course of action to be taken

Explanation: An IS auditor's responsibility is to gather sufficient and appropriate evidence before making conclusions. If fraud is suspected, the auditor should first expand their activities to validate whether an investigation is necessary. Reporting prematurely to management or the audit committee might be inappropriate if evidence is insufficient.

212. An IS auditor discovers several IT-based projects were implement and not approved by the steering committee. What is the GREATEST concern for the IS audit?

A. The IT department's projects will not be adequately funded

B. IT projects are not following the system development life cycle process

C. IT projects are not consistently formally approved

D. The IT department may not be working toward a common goal

Explanation: The lack of steering committee approval for projects indicates a governance issue. The greatest concern is that IT projects might not align with the organization's strategic objectives, leading to inefficiency and resource misalignment.

213. Which of the following should be developed during the requirements definition phase of a software development project to address aspects of software testing?

A. Test data covering critical applications

B. Detailed test plans

C. Quality assurance test specifications

D. User acceptance test specifications

Explanation: During the requirements definition phase, it is crucial to define how the software will be tested for end-user acceptance. This ensures that the software meets user needs and business requirements before deployment.

214. Which of the following is the BEST method for an IS auditor to verify that critical production servers are running the latest security updates released by the vendor?

A. Ensure that automatic updates are enabled on critical production servers

B. Verify manually that the patches are applied on a sample of production servers

C. Review tle change management log for critical production severs

D. Run an automated tool to verify the security patches on production servers

Explanation: Running an automated tool provides the most reliable and efficient method for verifying the application of security patches on critical servers, as it minimizes human error and ensures comprehensive coverage.

215. The implementation of access controls FIRST requires:

A. A classification of IS resources

B. The labeling of IS resources

C. The creation of an access control list

D. An inventory of IS resources

Explanation: Before implementing access controls, the organization must first identify and document all IS resources through an inventory. Without knowing what resources exist, it is impossible to classify, label, or control access effectively.

216. Which of the following is MOST effective for monitoring transactions exceeding predetermined thresholds?

A. Generalized audit software

B. An integrated test facility

C. Regression tests

D. Transaction snapshots

Explanation: Generalized audit software can be programmed to monitor transactions exceeding thresholds, making it the most effective tool for this purpose due to its ability to handle large datasets and generate exception reports.

217. Which of the following types of audit risk assumes an absence of compensating controls in the area being reviewed?

A. Control Risk

B. Detection Risk

C. Inherent Risk

D. Sampling Risk

Explanation: Inherent risk refers to the risk that exists in an area due to its nature, assuming no compensating controls are in place. It represents the baseline risk level before considering controls.

218. Which of the following should an IS auditor review to gain an understanding of the effectiveness of controls over the management of multiple projects?

A. Project database

B. Policy documents

C. Project portfolio database

D. Program organization

Explanation: A project portfolio database provides a consolidated view of all projects, allowing the IS auditor to review how projects are being managed collectively and to assess the effectiveness of controls over project management.

219. An enterprise uses privileged accounts to process configuration changes for mission-critical applications. Which of the following would be the BEST and appropriate control to limit the risk in such a situation?

A. Ensure that audit trails are accurate and specific

B. Ensure that personnel have adequate training

C. Ensure that personnel background checks are performed for critical personnel

D. Ensure that supervisory approval and review are performed for critical changes

Explanation: The best and most appropriate control in this context is to ensure that personnel background checks are performed for critical personnel. Privileged accounts are high-risk because they grant significant access to systems and applications. Ensuring that the individuals entrusted with these accounts have undergone thorough background checks minimizes the risk of insider threats

220. An IS auditor reviewing the configuration of a signature-based intrusion detection system (IDS) would be MOST concerned if which of the following were discovered?

A. Auto-update is turned off.

B. Scanning for application vulnerabilities is disabled.

C. Analysis of encrypted data packets is disabled.

D. The IDS is placed between the demilitarized zone (DMZ) and the firewall.

Explanation: A signature-based IDS relies on frequent updates to recognize new threats. If auto-update is disabled, the IDS may not detect recent threats, which undermines its effectiveness.