DOMAIN 2—GOVERNANCE AND MANAGEMENT OF IT (17%)

A2-1 Organizations requiring employees to take a mandatory vacation each year **PRIMARILY** want to ensure:

A. adequate cross-training exists between functions.
B. an effective internal control environment is in place by increasing morale.
C. potential irregularities in processing are identified by a temporary replacement.
D. the risk of processing errors is reduced.

C is the correct answer.

Justification:
A. Cross-training is a good practice to follow but can be achieved without the requirement for mandatory vacation.
B. 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.
C. **Employees who perform critical and sensitive functions within an organization should be required to take some time off to help ensure that irregularities and fraud are detected.**
D. Although rotating employees could contribute to fewer processing errors, this is not typically a reason to require a mandatory vacation policy.

A2-2 An IS auditor is verifying IT policies and finds 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.

D is the correct answer.

Justification:
A. Absence of management approval is an important (material) finding and, although it is not currently an issue with relation to compliance because the employees are following the policy without approval, it may be a problem at a later time and should be resolved.
B. Although 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 is to report this issue to the relevant stakeholders.
C. The first step is to report the finding and provide recommendations later.
D. **The IS auditor must report the finding. Unapproved policies may present a potential risk to the organization, even if they are being followed, because this technicality may prevent management from enforcing the policies in some cases and may present legal issues. For example, if an employee was terminated as a result of violating an organization policy, and it was discovered that the policies had not been approved, the organization may face an expensive lawsuit.**

A2-3 What is the **PRIMARY** consideration for an IS auditor reviewing the prioritization and coordination of IT projects and program management?

A. Projects are aligned with the organization's strategy.
B. Identified project risk is monitored and mitigated.
C. Controls related to project planning and budgeting are appropriate.
D. IT project metrics are reported accurately.

A is the correct answer.

Justification:

A. The primary goal of IT projects is to add value to the business, so they must be aligned with the business strategy to achieve the intended results. Therefore, the IS auditor should first focus on ensuring this alignment.
B. An adequate process for monitoring and mitigating identified project risk is important; however, strategic alignment helps in assessing identified risk in business terms.
C. Completion of projects within a predefined time and budget is important; however, the focus of project management should be on achieving the desired outcome of the project, which is aligned with the business strategy.
D. Adequate reporting of project status is important but may or may not help in providing the strategic perspective of project deliverables.

A2-4 In a review of the human resources policies and procedures within an organization, an IS auditor is **MOST** concerned with the absence of a:

A. requirement for periodic job rotations.
B. process for formalized exit interviews.
C. termination checklist.
D. requirement for new employees to sign a nondisclosure agreement.

C is the correct answer.

Justification:

A. Job rotation is a valuable control to ensure continuity of operations, but not the most serious human resources policy risk.
B. Holding an exit interview is desirable when possible to gain feedback but is not a serious risk.
C. A termination checklist is critical to ensure the logical and physical security of an enterprise. In addition to preventing the loss of enterprise property that was issued to the employee, there is the risk of unauthorized access, intellectual property theft and even sabotage by a disgruntled former employee.
D. Signing a nondisclosure agreement (NDA) is a recommended human resources practice, but a lack of an NDA is not the most serious risk listed.

A2-5 Which of the following factors is **MOST** critical when evaluating the effectiveness of an IT governance implementation?

A. Ensure that assurance objectives are defined.
B. Determine stakeholder requirements and involvement.
C. Identify relevant risk and related opportunities.
D. Determine relevant enablers and their applicability.

B is the correct answer.

Justification:
A. Stakeholders' needs and their involvement form the basis for scoping the IT governance implementation. This will be used to define assurance objectives.
B. The most critical factor to be considered in auditing an IT governance implementation is to determine stakeholder requirements and involvement. This drives the success of the project. Based on this, the assurance scope and objectives are determined.
C. The relevant risk and related opportunities are identified and driven by the assurance objectives.
D. The relevant enablers and their applicability for the IT governance implementation are considered based on assurance objectives.

A2-6 Which of the following is the **BEST** reason to implement a policy that places conditions on secondary employment for IT employees?

A. To prevent the misuse of corporate resources
B. To prevent conflicts of interest
C. To prevent employee performance issues
D. To prevent theft of IT assets

B is the correct answer.

Justification:
A. The misuse of corporate resources is an issue that must be addressed but is not necessarily related to secondary employment.
B. The best reason to implement and enforce a policy governing secondary employment is to prevent conflicts of interest. Policies should be in place to control IT employees seeking secondary employment from releasing sensitive information or working for a competing otganization. Conflicts of interest can result in serious risk such as fraud, theft of intellectual property or other improprieties.
C. Employee performance can certainly be an issue if an employee is overworked or has insufficient time off, but that should be dealt with as a management function and not the primary reason to have a policy on secondary employment.
D. Theft of assets is a problem but not necessarily related to secondary employment.

A2-7 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.

C is the correct answer.

Justification:

A. Although 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 good practice, the policy may 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.
B. 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. A new policy, for example, may not have been subject to any revisions yet.
C. **The information security policy should have an owner who has management responsibility for the development, review, approval and evaluation of the security policy. The position of security administrator is typically a staff-level position (not management), and therefore does not have the authority to approve the policy. In addition, an individual in a more independent position should also review the policy. Without proper management approval, enforcing the policy may be problematic, leading to compliance or security issues.**
D. Although a policy committee drawn from across the company is a good 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.

A2-8 When performing a review of a business process reengineering (BPR) effort, which of the following is of **PRIMARY** concern?

A. Controls are eliminated as part of the streamlining BPR effort.
B. Resources are not adequate to support the BPR process.
C. The audit department does not have a consulting role in the BPR effort.
D. The BPR effort includes employees with limited knowledge of the process area.

A is the correct answer.

Justification:

A. **A primary risk of business process reengineering (BPR) is that controls are eliminated as part of the reengineering effort. This is the primary concern.**
B. The BPR process can be a resource-intensive initiative; however, the more important issue is whether critical controls are eliminated as a result of the BPR effort.
C. Although BPR efforts often involve many different business functions, it is not a significant concern if audit is not involved, and, in most cases, it is not appropriate for audit to be involved in such an effort.
D. A recommended good practice for BPR is to include individuals from all parts of the enterprise, even those with limited knowledge of the process area. Therefore, this is not a concern.

A2-9 When auditing the IT governance framework and IT risk management practices existing 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 IS audits are conducted periodically.
D. Create a chief risk officer role in the organization.

B is the correct answer.

Justification:

A. While the strategic alignment of IT with the business is important, it is not directly related to the gap identified in this scenario.
B. 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. Note that this question asks for the best recommendation—not about the finding itself.
C. Performing more frequent IS audits is not helpful if the accountability rules are not clearly defined and implemented.
D. Recommending the creation of a new role (e.g., chief risk officer) is not helpful if the accountability rules are not clearly defined and implemented.

A2-10 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 complies the standards.
B. Identify and report the existing controls.
C. Review the metrics for quality evaluation.
D. Request all standards adopted by the organization.

D is the correct answer.

Justification:

A. The auditor needs to know what standards the organization has adopted and then measure compliance with those standards. Determining how the organization follows the standards is secondary to knowing what the standards are. 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.
B. The first step is to know the standards and what policies and procedures are mandated for the organization, then to document the controls and measure compliance.
C. The metrics cannot be reviewed until the auditor has a copy of the standards that describe or require the metrics.
D. Because an audit measures compliance with the standards of 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.

A2-11 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. Rescope the audit to include the separate project as part of the current audit.

B is the correct answer.

Justification:

A. The IS auditor does not ordinarily provide input on the timing of projects, but rather provides an assessment of the current environment. The most critical issue in this scenario is that the enterprise architecture (EA) is undergoing change, so the IS auditor should be most concerned with reporting this issue.
B. 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.
C. The organization is free to choose any EA framework, and the IS auditor should not recommend a specific framework.
D. Changing the scope of an audit to include the secondary project is not required, although a follow-up audit may be desired.

A2-12 An IS auditor is evaluating management's risk assessment of information systems. The IS auditor should **FIRST** review:

A. Controls in place.
B. Effectiveness of the controls.
C. Mechanism for monitoring the risk.
D. Threats/vulnerabilities affecting the assets.

D is the correct answer.

Justification:

A. The controls are irrelevant until the IS auditor knows the threats and risk that the controls are intended to address.
B. The effectiveness of the controls must be measured in relation to the risk (based on assets, threats and vulnerabilities) that the controls are intended to address.
C. The first step must be to determine the risk that is being managed before reviewing the mechanism of monitoring risk.
D. One of the key factors to be considered while assessing the information systems risk is the value of the systems (the assets) and the threats and vulnerabilities affecting the assets. The risk related to the use of information assets should be evaluated in isolation from the installed controls.

A2-13 The **PRIMARY** benefit of an enterprise architecture initiative is to:

A. Enable the organization to invest in the most appropriate technology.
B. Ensure security controls are implemented on critical platforms.
C. Allow development teams to be more responsive to business requirements.
D. Provide business units with greater autonomy to select it solutions that fit their needs.

A is the correct answer.

Justification:

A. **The primary focus of the enterprise architecture (EA) is to ensure that technology investments are consistent with the platform, data and development standards of the IT organization; therefore, the goal of the EA is to help the organization to implement the technology that is most effective.**
B. Ensuring that security controls are implemented on critical platforms is important, but this is not the function of the EA. The EA may be concerned with the design of security controls; however, the EA would not help to ensure that they were implemented. The primary focus of the EA is to ensure that technology investments are consistent with the platform, data and development standards of the IT organization.
C. While the EA process may enable development teams to be more efficient, because they are creating solutions based on standard platforms using standard programming languages and methods, the more critical benefit of the EA is to provide guidance for IT investments of all types, which encompasses much more than software development.
D. A primary focus of the EA is to define standard platforms, databases and interfaces. Business units that invest in technology would need to select IT solutions that meet their business needs and are compatible with the EA of the enterprise. There may be instances when a proposed solution works better for a business unit but is not at all consistent with the EA of the enterprise, so there would be a need to compromise to ensure that the application can be supported by IT. Overall, the EA would restrict the ability of business units in terms of the potential IT systems that they may wish to implement. The support requirements would not be affected in this case.

A2-14 Which of the following situations is addressed by a software escrow agreement?

A. The system administrator requires access to software 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 IS auditor requires access to software code written by the organization.

C is the correct answer.

Justification:

A. Access to software should be managed by an internally managed software library. Escrow refers to the storage of software with a third party—not the internal libraries.
B. Providing the user with a backup copy of software is not escrow. Escrow requires that a copy be kept with a trusted third party.
C. **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.**
D. Software escrow is used to protect the intellectual property of software developed by one organization and sold to another organization. This is not used for software being reviewed by an auditor of the organization that wrote the software.

A2-15 An IS auditor reviews an organizational chart **PRIMARILY** for:

A. Understanding of the complexity of the organizational structure.
B. Investigating various communication channels.
C. Understanding the responsibilities and authority of individuals.
D. Investigating the network connected to different employees.

C is the correct answer.

Justification:
A. Understanding the complexity of the organizational structure is not the primary reason to review an organizational chart because the chart will not necessarily depict the complexity.
B. The organizational chart is a key tool for an auditor to understand roles and responsibilities and reporting lines but is not used for examining communications channels.
C. **An organizational chart provides information about the responsibilities and authority of individuals in the organization. This helps an IS auditor to know if there is a proper segregation of functions.**
D. A network diagram will provide information about the usage of various communication channels and will indicate the connection of users to the network.

A2-16 Sharing risk is a key factor in which of the following methods of managing risk?

A. Transferring risk
B. Tolerating risk
C. Terminating risk
D. Treating risk

A is the correct answer.

Justification:
A. **Transferring risk (e.g., by taking an insurance policy) is a way to share risk.**
B. Tolerating risk means that the risk is accepted, but not shared.
C. Terminating risk would not involve sharing the risk because the organization has chosen to terminate the process associated with the risk.
D. There are several ways of treating or controlling the risk, which may involve reducing or sharing the risk, but this is not as precise an answer as transferring the risk.

A2-17 A team conducting a risk analysis is having difficulty projecting the financial losses that could result from a risk. To evaluate the potential impact, the team should:

A. Compute the amortization of the related assets.
B. Calculate a return on investment.
C. Apply a qualitative approach.
D. Spend the time needed to define the loss amount exactly.

C is the correct answer.

Justification:
A. Amortization is used in a profit and loss statement, not in computing potential losses.
B. A return on investment (ROI) is computed when there is predictable savings or revenues that can be compared to the investment needed to realize the revenues.
C. **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 impact in terms of a weighted factor (e.g., one is a very low impact to the business and five is a very high impact).**
D. 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 the result will be a not well-supported evaluation.

A2-18 While reviewing a quality management system, the IS auditor should **PRIMARILY** focus on collecting evidence to show that:

A. Quality management systems comply with good practices.
B. Continuous improvement targets are being monitored.
C. Standard operating procedures of it are updated annually.
D. Key performance indicators are defined.

B is the correct answer.

Justification:
A. Generally, good practices are adopted according to business requirements. Therefore, conforming to good practices may or may not be a requirement of the business.
B. Continuous and measurable improvement of quality is the primary requirement to achieve the business objective for the quality management system (QMS).
C. Updating operating procedures is part of implementing the QMS; however, it must be part of change management and not an annual activity.
D. Key performance indicators may be defined in a QMS, but they are of little value if they are not being monitored.

A2-19 An IS auditor discovers several IT-based projects were implemented and not approved by the steering committee. What is the **GREATEST** concern for the IS auditor?

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.

D is the correct answer.

Justification:
A. Funding for the projects may be addressed through various budgets and may not require steering committee approval. The primary concern would be to ensure that the project is working toward meeting the goals of the company.
B. Although requiring steering committee approval may be part of the system development life cycle process, the greater concern would be whether the projects are working toward the corporate goals. Without steering committee approval, it would be difficult to determine whether these projects are following the direction of the corporate goals.
C. Although having a formal approval process is important, the greatest concern would be for the steering committee to provide corporate direction for the projects.
D. The steering committee provides direction and control over projects to ensure that the company is making appropriate investments. Without approval, the project may or may not be working toward the company's goals.

A2-20 Value delivery from IT to the business is **MOST** effectively achieved by:

A. Aligning the IT strategy with the enterprise strategy
B. Embedding accountability in the enterprise
C. Providing a positive return on investment
D. Establishing an enterprisewide risk management process

A is the correct answer.

Justification:
A. IT's value delivery to the business is driven by aligning IT with the enterprise's strategy.
B. Embedding accountability in the enterprise promotes risk management (another element of corporate governance).
C. While return on investment is important, it is not the only criterion by which the value of IT is assessed.
D. Enterprisewide risk management is critical to IT governance; however, by itself, it will not guarantee that IT delivers value to the business unless the IT strategy is aligned with the enterprise strategy.

A2-21 During a feasibility study regarding outsourcing IT processing, the relevance for the IS auditor of reviewing the vendor's business continuity plan 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 business continuity plan.

A is the correct answer.

Justification:
A. A key factor in a successful outsourcing environment is the capability of the vendor to face a contingency and continue to support the organization's processing requirements.
B. Financial stability is not related to the vendor's business continuity plan (BCP).
C. Experience of the vendor's staff is not related to the vendor's BCP.
D. The review of the vendor's BCP during a feasibility study is not a way to test the vendor's BCP.

A2-22 An IS auditor is evaluating a newly developed IT policy for an organization. Which of the following factors does the IS auditor consider **MOST** important to facilitate compliance with the policy upon its implementation?

A. Existing IT mechanisms enabling compliance
B. Alignment of the policy to the business strategy
C. Current and future technology initiatives
D. Regulatory compliance objectives defined in the policy

A is the correct answer.

Justification:
A. The organization should be able to comply with a policy when it is implemented. The most important consideration when evaluating the new policy should be the existing mechanisms in place that enable the organization and its employees to comply with the policy.
B. Policies should be aligned with the business strategy, but this does not affect an organization's ability to comply with the policy upon implementation.
C. Current and future technology initiatives should be driven by the needs of the business and would not affect an organization's ability to comply with the policy.
D. Regulatory compliance objectives may be defined in the IT policy, but that would not facilitate compliance with the policy. Defining objectives would only result in the organization knowing the desired state and would not aid in achieving compliance.

A2-23 The **MOST** likely effect of the lack of senior management commitment to IT strategic planning is:

A. Lack of investment in technology
B. Lack of a methodology for systems development
C. Technology not aligning with organization objectives
D. Absence of control over technology contracts

C is the correct answer.

Justification:

A. Lack of management commitment will almost certainly affect investment, but the primary loss will be the lack of alignment of IT strategy with the strategy of the business.
B. Systems development methodology is a process-related function and not a key concern of management.
C. **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 is an indication of a lack of top-level management commitment. This condition increases the risk that IT is aligned with organization strategy.**
D. Approval for contracts is a business process and would be controlled through financial process controls. This is not applicable here.

A2-24 Which of the following is a function of an IT 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 the status of IT plans and budgets
D. Liaising between the IT department and end users

C is the correct answer.

Justification:

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

A2-25 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 information security policy is not periodically reviewed by senior management.
B. A policy ensuring systems are patched in a timely manner does not exist.
C. The audit committee did not review the organization's mission statement.
D. An organizational policy related to information asset protection does not exist.

A is the correct answer.

Justification:

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 the protection of information assets, the greater concern is that the security policy is not reviewed periodically by senior management because top level support is fundamental to information security governance.

A2-26 Involvement of senior management is **MOST** important in the development of:

A. Strategic plans.
B. IT policies.
C. IT procedures.
D. Standards and guidelines.

A is the correct answer.

Justification:

A. **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.**
B. IT policies are created and enforced by IT management and information security. They are structured to support the overall strategic plan.
C. IT procedures are developed to support IT policies. Senior management is not involved in the development of procedures.
D. Standards and guidelines are developed to support IT policies. Senior management is not involved in the development of standards, baselines and guidelines.

A2-27 Effective IT governance ensures that the IT plan is consistent with the organization's:

A. Business plan.
B. Audit plan.
C. Security plan.
D. Investment plan.

A is the correct answer.

Justification:

A. 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.
B. The audit plan is not part of the IT plan.
C. The security plan is not a responsibility of IT and does not need to be consistent with the IT plan.
D. The investment plan is not part of the IT plan.

A2-28 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.

B is the correct answer.

Justification:

A. Quality assurance (QA) is concerned with reliability and consistency of processes. The QA team is not responsible for determining an acceptable risk level.
B. Senior management should establish the acceptable risk level because they have the ultimate or final responsibility for the effective and efficient operation of the organization as a senior manager of the business process. The person can be the QA, chief information officer (CIO), or the chief security officer (CSO), but the responsibility rests with the business manager.
C. The establishment of acceptable risk levels is a senior business management responsibility. The CIO is the most senior official of the enterprise who is accountable for IT advocacy; aligning IT and business strategies; and planning, resourcing and managing the delivery of IT services, information and the deployment of associated human resources. The CIO is rarely the person that determines acceptable risk levels because this could be a conflict of interest unless the CIO is the senior business process owner.
D. The establishment of acceptable risk levels is a senior business management responsibility. The CSO is responsible for enforcing the decisions of the senior management team unless the CIO is the business process manager.

A2-29 IT governance is **PRIMARILY** the responsibility of the:

A. chief executive officer.
B. board of directors.
C. IT steering committee.
D. audit committee.

B is the correct answer.

Justification:

A. The chief executive officer is instrumental in implementing IT governance according to the directions of the board of directors.
B. IT governance is primarily the responsibility of the executives and shareholders (as represented by the board of directors).
C. The IT steering committee monitors and facilitates deployment of IT resources for specific projects "in support of business plans. The IT steering committee enforces governance on behalf of the board of directors.
D. The audit committee reports to the board of directors and executes governance-related audits. The audit committee should monitor the implementation of audit recommendations.

A2-30 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.

D is the correct answer.

Justification:

A. Providing instructions on how to do the job and defining authority addresses the managerial and procedural aspects of the job and is a management responsibility. Job descriptions, which are a human resources (HR)-related function, are primarily used to establish job requirements and accountability.
B. It is important that job descriptions are current, documented and readily available to the employee, but this, in itself, is not the key element of the job description. Job descriptions, which are an HR-related function, are primarily used to establish job requirements and accountability.
C. Communication of management's specific expectations for job performance would not necessarily be included in job descriptions.
D. From a control perspective, a job description should establish responsibility and accountability. This aids in ensuring that users are given system access in accordance with their defined job responsibilities and are accountable for how they use that access.

A2-31 Which of the following **BEST** provides assurance of the integrity of new staff?

A. Background screening
B. References
C. Bonding
D. Qualifications listed on a resume

A is the correct answer.

Justification:

A. **A background screening is the primary method for assuring the integrity of a prospective staff member. This may include criminal history checks, driver's license abstracts, financial status checks, verification of education, etc.**
B. References are important and would need to be verified, but they are not as reliable as background screening because the references themselves may not be validated as trustworthy.
C. Bonding is directed at due-diligence compliance and does not ensure integrity.
D. Qualifications listed on a résumé may be used to demonstrate proficiency but will not indicate the integrity of the candidate employee.

A2-32 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.

D is the correct answer.

Justification:

A. All the work of the terminated employee needs to be handed over to a designated employee; however, this is not as critical as removing terminated employee access.
B. All the work of the terminated employee needs to be backed up, but this is not as critical as removing terminated employee access.
C. The employees need to be notified of the termination, but this is not as critical as removing terminated employee access.
D. **There is a probability that a terminated employee may misuse access rights; therefore, disabling the terminated employee's logical access is the most important and immediate action to take.**

A2-33 A business unit has selected a new accounting application and did not consult with IT early in the selection process. The **PRIMARY** risk is that:

A. The security controls of the application may not meet requirements.
B. The application may not meet the requirements of the business users.
C. The application technology may be inconsistent with the enterprise architecture.
D. The application may create unanticipated support issues for IT.

C is the correct answer.

Justification:

A. Although security controls should be a requirement for any application, the primary focus of the enterprise architecture (EA) is to ensure that new applications are consistent with enterprise standards. Although the use of standard supported technology may be more secure, this is not the primary benefit of the EA.
B. When selecting an application, the business requirements and the suitability of the application for the IT environment must be considered. If the business units selected their application without IT involvement, they are more likely to choose a solution that fits their business process the best with less emphasis on how compatible and supportable the solution will be in the enterprise, and this is not a concern.
C. **The primary focus of the EA is to ensure that technology investments are consistent with the platform, data and development standards of the IT organization. The EA defines both a current and future state in areas such as the use of standard platforms, databases or programming languages. If a business unit selected an application using a database or operating system that is not part of the EA for the business, this increases the cost and complexity of the solution and ultimately delivers less value to the business.**
D. Although any new software implementation may create support issues, the primary benefit of the EA is ensuring that the IT solutions deliver value to the business. Decreased support costs may be a benefit of the EA, but the lack of IT involvement in this case would not affect the support requirements.

A2-34 Many organizations require an employee to take a mandatory vacation (holiday) of a week or more to:

A. Ensure that 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.

B is the correct answer.

Justification:

A. Maintaining a good quality of life is important, but the primary reason for a mandatory vacation is to catch fraud or errors.
B. **Required vacations/holidays of a week or more in duration in which someone other than the regular employee performs the job function of the employee on vacation is often mandatory for sensitive positions because this reduces the opportunity to commit improper or illegal acts. During this time off, it may be possible to discover any fraudulent activity that was taking place.**
C. Providing cross-training is an important management function, but the primary reason for mandatory vacations is to detect fraud or errors.
D. Enforcing a rule that all vacations must be taken a week at a time is a management decision but not related to a mandatory vacation policy. The primary reason for mandatory vacations is to detect fraud or errors.

A2-35 A local area network (LAN) administrator normally is 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.

C is the correct answer.

Justification:
A. Although not ideal, a local area network (LAN) administrator may have end-user responsibilities.
B. The LAN administrator may report to the director of the information processing facility (IPF) or, in a decentralized operation, to the end-user manager.
C. **A LAN administrator should not have programming responsibilities because that could allow modification of production programs without proper separation of duties, but the LAN administrator may have end-user responsibilities.**
D. In small organizations, the LAN administrator may also be responsible for security administration over the LAN.

A2-36 A decision support system is used to help high-level management:

A. Solve highly structured problems.
B. Combine the use of decision models with predetermined criteria.
C. Make decisions based on data analysis and interactive models.
D. Support only structured decision-making tasks.

C is the correct answer.

Justification:
A. A decision support system (DSS) is aimed at solving less structured problems.
B. A DSS combines the use of models and analytic techniques with traditional data access and retrieval functions but is not limited by predetermined criteria.
C. **A DSS emphasizes flexibility in the decision-making approach of management through data analysis and the use of interactive models, not fixed criteria.**
D. A DSS supports semistructured decision-making tasks.

A2-37 During an audit, the IS auditor discovers that the human resources (HR) department uses a cloud-based application to manage employee records. The HR department engaged in a contract outside of the normal vendor management process and manages the application on its own. Which of the following is of **GREATEST** concern?

A. Maximum acceptable downtime metrics have not been defined in the contract.
B. The IT department does not manage the relationship with the cloud vendor.
C. The help desk call center is in a different country, with different privacy requirements.
D. Organization-defined security policies are not applied to the cloud application.

D is the correct answer.

Justification:

A. Maximum acceptable downtime is a good metric to have in the contract to ensure application availability; however, human resources (HR) applications are usually not mission-critical, and therefore, maximum acceptable downtime is not the most significant concern in this scenario.
B. The responsibility for managing the relationship with a third party should be assigned to a designated individual or service management team; however, it is not essential that the individual or team belong to the IT department.
C. An organization-defined security policy ensures that help desk personnel do not have access to personnel data, and this is covered under the security policy. The more critical issue is that the application complied with the security policy.
D. Cloud applications should adhere to the organization-defined security policies to ensure that the data in the cloud are protected in a manner consistent with internal applications. These include, but are not limited to, the password policy, user access management policy and data classification policy.

A2-38 Before implementing an IT balanced scorecard, 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.

B is the correct answer.

Justification:

A. A balanced scorecard (BSC) is a method of specifying and measuring the attainment of strategic results. It will measure the delivery of effective and efficient services, but an organization may not have those in place prior to using a BSC.
B. Because a BSC is a way to measure performance, a definition of key performance indicators is required before implementing an IT BSC.
C. A BSC will measure the value of IT to business, not the other way around.
D. A BSC will measure the performance of IT, but the control over IT expenses is not a key requirement for implementing a BSC.

A2-39 To support an organization's goals, an IT department should have:

A. A low-cost philosophy.
B. Long- and short-term plans.
C. Leading-edge technology.
D. Plans to acquire new hardware and software.

B is the correct answer.

Justification:
A. A low-cost philosophy is one objective, but more important is the cost-benefit and the relation of IT investment cost to business strategy.
B. To ensure its contribution to the realization of an organization's overall goals, the IT department should have long- and short-range plans that are consistent with the organization's broader and strategic plans for attaining its goals.
C. Leading-edge technology is an objective, but IT plans would be needed to ensure that those plans are aligned with organizational goals.
D. Plans to acquire new hardware and software could be a part of the overall plan but would be required only if hardware or software is needed to achieve the organizational goals.

A2-40 In reviewing the IT short-range (tactical) plan, an IS auditor should determine whether:

A. There is an integration of IT and business personnel within projects.
B. There is a clear definition of the IT mission and vision.
C. A strategic information technology planning scorecard is in place.
D. The plan correlates business objectives to IT goals and objectives.

A is the correct answer.

Justification:
A. The integration of IT and business personnel in projects is an operational issue and should be considered while reviewing the short-range plan. A strategic plan provides a framework for the IT short-range plan.
B. A clear definition of the IT mission and vision would be covered by a strategic plan.
C. A strategic information technology planning scorecard would be covered by a strategic plan.
D. Business objectives correlating to IT goals and objectives would be covered by a strategic plan.

A2-41 Which of the following does an IS auditor consider the **MOST** relevant to short-term planning for an IT department?

A. Allocating resources
B. Adapting to changing technologies
C. Conducting control self-assessments
D. Evaluating hardware needs

A is the correct answer.

Justification:
A. The IT department should specifically consider the manner in which resources are allocated in the short term. The IS auditor ensures that the resources are being managed adequately.
B. Investments in IT need to be aligned with top management strategies rather than be relevant to short-term planning and focus on technology for technology's sake.
C. Conducting control self-assessments is not as critical as allocating resources during short-term planning for the IT department.
D. Evaluating hardware needs is not as critical as allocating resources during short-term planning for the IT department.

A2-42 Which of the following goals do you expect to find in an organization's strategic plan?

A. Results of new software testing
B. An evaluation of information technology needs
C. Short-term project plans for a new planning system
D. Approved suppliers for products offered by the company

D is the correct answer.

Justification:

A. Results of a new accounting package is a tactical or short-term goal and would not be included in a strategic plan.
B. An evaluation of information technology needs is a way to measure performance, but not a goal to be found in a strategic plan.
C. Short-term project plans is project-oriented and is a method of implementing a goal but not the goal in itself. The goal would be to have better project management—the new system is how to achieve that goal.
D. Approved suppliers of choice for the product is a strategic business objective that is intended to focus the overall direction of the business and, thus, is a part of the organization's strategic plan.

A2-43 Which of the following does an IS auditor consider to be **MOST** important when evaluating an organization's IT strategy? That it:

A. Was approved by line management.
B. Does not vary from the IT department's preliminary budget.
C. Complies with procurement procedures.
D. Supports the business objectives of the organization.

D is the correct answer.

Justification:

A. A strategic plan is a senior management responsibility and would receive input from line managers but would not be approved by them.
B. The budget should not vary from the plan.
C. Procurement procedures are organizational controls, but not a part of strategic planning.
D. 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.

A2-44 An organization has contracted with a vendor for a turnkey solution for their electronic toll collection system (ETCS). The vendor has provided its proprietary application software as part of the solution. The contract should require that:

A. A backup server is available to run ETCS operations with up-to-date data.
B. A backup server is loaded with all relevant software and data.
C. The systems staff of the organization is trained to handle any event.
D. Source code of the ETCS application is placed in escrow.

D is the correct answer.

Justification:

A. Having a backup server with current data is critical but not as critical as ensuring the availability of the source code.
B. Having a backup server with relevant software is critical but not as critical as ensuring the availability of the source code.
C. Having staff training is critical but not as critical as ensuring the availability of the source code.
D. Whenever proprietary application software is purchased, the contract should provide for a source code escrow agreement. This agreement ensures that the purchasing organization has the opportunity to modify the software should the vendor cease to be in business.

A2-45 When reviewing the IT strategy, an IS auditor can **BEST** assess whether the strategy supports the organizations' business objectives by determining whether IT:

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.

B is the correct answer.

Justification:

A. Having personnel and equipment is an important requirement to meet the IT strategy but will not ensure that the IT strategy supports business objectives.
B. The only way to know if IT strategy will meet business objectives is to determine if the IT plan is consistent with management strategy and that it relates IT planning to business plans.
C. Using equipment and personnel efficiently and effectively is an effective method for determining the proper management of the IT function but does not ensure that the IT strategy is aligned with business objectives.
D. Having sufficient excess capacity to respond to changing directions is important to show flexibility to meet organizational changes but is not in itself a way to ensure that IT is aligned with business goals.

A2-46 An IS auditor of a large organization is reviewing the roles and responsibilities of the IT function and finds 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. System administrators are application programmers.
C. End users are security administrators for critical applications.
D. Systems analysts are database administrators.

B is the correct answer.

Justification:

A. Ideally, network administrators should not be responsible for quality assurance because they could approve their own work. However, that is not as serious as the combination of system administrator and application programmer, which would allow nearly unlimited abuse of privilege.
B. When individuals serve multiple roles, this represents a separation-of-duties problem with associated risk. System administrators should not be application programmers, due to the associated rights of both functions. A person with both system and programming rights can do almost anything on a system, including creating a back door. The other combinations of roles are valid from a separation of duties perspective.
C. In some distributed environments, especially with small staffing levels, users may also manage security.
D. While a database administrator is a very privileged position it would not be in conflict with the role of a systems analyst.

A2-47 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 modify data.
D. Audit recommendations may not be implemented.

C is the correct answer.

Justification:

A. The greatest risk is from unauthorized users being able to modify data. User management is important but not the greatest risk.
B. User accountability is important but not as great a risk as the actions of unauthorized users.
C. Without a policy defining who has the responsibility for granting access to specific systems, there is an increased risk that individuals can gain (be given) system access when they should not have authorization. The ability of unauthorized users to modify data is greater than the risk of authorized user accounts not being controlled properly.
D. The failure to implement audit recommendations is a management problem but not as serious as the ability of unauthorized users making modifications.

A2-48 An IS audit department is planning to minimize the risk of short-term employees. Activities contributing to this objective are documented procedures, knowledge sharing, cross-training and:

A. Succession planning.
B. Staff job evaluation.
C. Responsibilities definitions.
D. Employee award programs.

A is the correct answer.

Justification:

A. **Succession planning ensures that internal personnel with the potential to fill key positions in the organization are identified and developed.**
B. 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.
C. Staff responsibilities definitions provide for well-defined roles and responsibilities; however, they do not minimize dependency on key individuals.
D. Employee award programs provide motivation; however, they do not minimize dependency on key individuals.

A2-49 The rate of change in technology increases the importance of:

A. Outsourcing the IT function.
B. Implementing and enforcing sound processes.
C. Hiring qualified personnel.
D. Meeting user requirement.

B is the correct answer.

Justification:

A. Outsourcing the IT function is a business decision and not directly related to the rate of technological change, nor does the rate of change increase the importance of outsourcing.
B. **Change control requires that good change management processes be implemented and enforced.**
C. Personnel in a typical IT department can often be trained in new technologies to meet organizational requirements.
D. Although meeting user requirements is important, it is not directly related to the rate of technological change in the IT environment.

A2-50 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.

A is the correct answer.

Justification:

A. **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.**
B. Information security is everybody's business, and all staff should be trained in how to handle information correctly.
C. Providing security awareness training is not an IS audit function.
D. Management may agree to or reject an audit finding. The IS auditor cannot be assured that management will act upon an audit finding unless they are aware of its impact; therefore, the auditor must report the risk associated with lack of security awareness.

A2-51 Which of the following is responsible for the approval of an information security policy?

A. IT department
B. Security committee
C. Security administrator
D. Board of directors

D is the correct answer.

Justification:

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

A2-52 While reviewing the IT governance processes of an organization, an IS auditor discovers 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 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 may not be accurate.

C is the correct answer.

Justification:

A. 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.
B. Although project 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.
C. The IT balanced scorecard is designed to measure IT performance. To measure performance, a sufficient number of performance drivers (key performance indicators [KPIs]) must be defined and measured over time. Failure to have objective KPIs may result in arbitrary, subjective measures that may be misleading and lead to unsound decisions.
D. Although performance management issues related to service level agreements could arise from performance indicators that were not correctly defined, the presentation of misleading performance to management is a much more significant risk.

A2-53 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 access control authorization
C. Identity of sensitive security assets
D. Relevant software security features

B is the correct answer.

Justification:

A. A list of key IT resources to be secured is more detailed than that which should be included in a policy.
B. 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.
C. The identity of sensitive security assets is more detailed than that which should be included in a policy.
D. A list of the relevant software security features is more detailed than that which should be included in a policy.

A2-54 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 application traffic matrix showing protection methods

B is the correct answer.

Justification:

A. Identifying methods to protect against identified vulnerabilities and their comparative cost-benefit analysis is the third step.
B. Identification of the applications required across the network should be the initial step. 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.
C. Having identified the externally accessed applications, the second step is to identify vulnerabilities (weaknesses) associated with the network applications.
D. The fourth step is to analyze the application traffic and create a matrix showing how each type of traffic will be protected.

A2-55 Which of the following is an implementation risk within the process of decision support systems?

A. Management control
B. Semistructured dimensions
C. Inability to specify purpose and usage patterns
D. Changes in decision processes

C is the correct answer.

Justification:

A. Management control is not a type of risk, but a characteristic of a decision support system (DSS).
B. Semistructured dimensions is not a type of risk, but a characteristic of a DSS.
C. The inability to specify purpose and usage patterns is a risk that developers need to anticipate while implementing a DSS.
D. Changes in decision processes are not a type of risk, but a characteristic of a DSS.

A2-56 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

A is the correct answer.

Justification:

A. **Assimilation of the framework and intent of a written security policy by all levels of management and users of the system is critical to the successful implementation and maintenance of the security policy. If a policy is not assimilated into daily actions, it will not be effective.**
B. 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.
C. Punitive actions are needed to enforce the policy but are not the key to successful implementation.
D. 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 important, but it is dependent on the support and education of management and users on the importance of security.

A2-57 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.

B is the correct answer.

Justification:

A. Email policy should address the business and legal requirements of email retention. Addressing the retention issue in the email policy would facilitate recovery.
B. **Besides being a good practice, laws and regulations may require an organization to 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 policy 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.**
C. Email policy should address the business and legal requirements of email retention. Addressing the retention issue in the email policy would facilitate rebuilding.
D. Email policy should address the business and legal requirements of email retention. Reuse of email is not a policy matter.

A2-58 An organization is considering making a major investment to upgrade technology. Which of the following choices is the **MOST** important to consider?

A. A cost analysis
B. The security risk of the current technology
C. Compatibility with existing systems
D. A risk analysis

D is the correct answer.

Justification:
A. The information system solution should be cost-effective, but this is not the most important aspect.
B. The security risk of the current technology is one of the components of the risk analysis, and alone is not the most important factor.
C. Compatibility with existing systems is one consideration; however, the new system may be a major upgrade that is not compatible with existing systems, so this is not the most important consideration.
D. Prior to implementing new technology, an organization should perform a risk assessment, which is then presented to business unit management for review and acceptance.

A2-59 Which of the following choices is the **PRIMARY** benefit of requiring a steering committee to oversee IT investment?

A. To conduct a feasibility study to demonstrate IT value
B. To ensure that investments are made according to business requirements
C. To ensure that proper security controls are enforced
D. To ensure that a standard development methodology is implemented

B is the correct answer.

Justification:
A. A steering committee may use a feasibility study in its reviews; however, it is not responsible for performing/conducting the study.
B. A steering committee consists of representatives from the business and IT and ensures that IT investment is based on business objectives rather than on IT priorities.
C. The steering committee is not responsible for enforcing security controls.
D. The steering committee is not responsible for implementing development methodologies.

A2-60 IS control objectives are useful to IS auditors because they provide the basis for understanding the:

A. Desired result or purpose of implementing specific control procedures
B. Best IS security control practices relevant to a specific entity.
C. Techniques for securing information
D. Security policy

A is the correct answer.

Justification:
A. An IS control objective is defined as the statement of the desired result or purpose to be achieved by implementing control procedures in a particular IS activity.
B. Control objectives provide the actual objectives for implementing controls and may or may not be based on good practices.
C. Techniques are the means of achieving an objective, but it is more important to know the reason and objective for the control than to understand the technique itself.
D. A security policy mandates the use of IS controls, but the controls are not used to understand policy.

A2-61 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

C is the correct answer.

Justification:

A. The security program is driven by policy and the standards are driven by the program. The initial step is to have a policy and ensure that the program is based on the policy.
B. Audit and monitoring of controls related to the program can only come after the program is set up.
C. **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.**
D. Access control software is an important security control but only after the policy and program are defined.

A2-62 Which of the following is the **MOST** important function to be performed by IT 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

D is the correct answer.

Justification:

A. Payment of invoices is a finance function, which would be completed per contractual requirements.
B. Participating in systems design is a by-product of monitoring the outsourcing provider's performance.
C. Renegotiating fees is usually a one-time activity and is not as important as monitoring the vendor's performance.
D. **In an outsourcing environment, the enterprise is dependent on the performance of the service provider. Therefore, it is critical that the outsourcing provider's performance bis monitored to ensure that services are delivered to the enterprise as required.**

A2-63 An organization purchased a third-party application and made significant modifications. While auditing the development process for this critical, customer-facing application, the IS auditor noted that the vendor has been in business for only one year. Which of the following helps to mitigate the risk relating to continued application support?

A. A viability study on the vendor
B. A software escrow agreement
C. Financial evaluation of the vendor
D. A contractual agreement for future enhancements

B is the correct answer.

Justification:

A. Although a viability study on the vendor may provide some assurance on the long-term availability of the vendor's services to the entity, in this case, it is more important that the company has the rights to the source code.
B. Considering that the vendor has been in the business for only one year, the biggest concern is financial stability or viability of the vendor and the risk of the vendor going out of business. The best way that this risk can be addressed is to have a software escrow agreement for the source code of the application, which provides the entity access to the source code if the vendor goes out of business.
C. Considering that the vendor has been in business for only one year, financial evaluation of the vendor would not be of much value and cannot provide assurance on the long-term availability of the vendor's services to the entity. In this case, it is more important that the company has rights to the source code.
D. A contractual agreement, while binding, is not enforceable or only has limited value in the event of bankruptcy.

A2-64 An IS auditor reviewing an outsourcing contract of IT facilities expects it to define the:

A. Hardware configuration.
B. Access control software.
C. Ownership of intellectual property.
D. Application development methodology.

C is the correct answer.

Justification:

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

A2-65 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. Because the work involves confidential information, the IS auditor's **PRIMARY** concern should be that the:

A. Requirement for securely protecting of information can 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.

A is the correct answer.

Justification:

A. **Many countries have enacted regulations to protect the confidentiality of information maintained in their countries and/or exchanged with other countries. When 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.**
B. Terminating the contract for a violation of the terms of the contract could be a concern but is not related to ensuring the security of information.
C. The outsourcer not being subject to an audit could be a concern but is not related to ensuring the security of information.
D. There is no reason why an IS auditor should be concerned with the outsourcer approaching the other service providers directly for further work.

A2-66 A benefit of open system architecture is that it:

A. Facilitates interoperability within different systems.
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.

A is the correct answer.

Justification:

A. **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.**
B. Closed system components are built to proprietary standards so that other suppliers' systems cannot or will not interface with existing systems.
C. The ability to obtain volume discounts is achieved through the use of bulk purchasing or a primary vendor, not through open system architecture.
D. Open systems may be less expensive than proprietary systems depending on the supplier, but the primary benefit of open system architecture is its interoperability between vendors.

A2-67 The risk associated with electronic evidence gathering is **MOST** likely reduced by an email:

A. Destruction policy.
B. Security policy.
C. Archive policy.
D. Audit policy.

C is the correct answer.

Justification:
A. The email retention policy would include the destruction or deletion of emails. This must be compliant with legal requirements to retain emails.
B. A security policy is too high level and would not address the risk of inadequate retention of emails or the ability to provide access to emails when required.
C. **With a policy of well-archived email records, access to or retrieval of specific email records to comply with legal requirements is possible.**
D. An audit policy would not address the legal requirement to provide emails as electronic evidence.

A2-68 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.

C is the correct answer.

Justification:
A. Making a business plan is not the ultimate goal of the risk management process.
B. Risk management can help create the audit plan, but not the audit charter.
C. **The risk management process is about making specific, security-related decisions, such as the level of acceptable risk.**
D. Risk management will drive the design of security controls in software but influencing security policy is more important.

A2-69 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 and chief executive officer.
B. Examine the e-business application in development.
C. Identify threats and the likelihood of occurrence.
D. Check the budget available for risk management.

C is the correct answer.

Justification:
A. The risk can only be determined after the threats, likelihood and vulnerabilities are all documented.
B. The first step is to identify the risk levels to existing applications and then to apply those to applications in development. Risk can only be identified after the threats and likelihood have also been determined.
C. **To determine the risk associated with e-business, an IS auditor must identify the assets, look for vulnerabilities, and then identify the threats and the likelihood of occurrence.**
D. The budget available for risk management is not relevant at this point because the risk has not yet been determined.

A2-70 An IS auditor reviewing the IT organization is **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. Reports the status of IT projects to the board of directors.
D. Is responsible for determining business goals.

D is the correct answer.

Justification:
A. The IT steering committee is responsible for project approval and prioritization.
B. The IT steering committee is responsible for oversight of the development of the long-term IT plan.
C. The IT steering committee advises the board of directors on the status of developments in IT.
D. Determining the business goals is the responsibility of senior management and not of the IT steering committee. IT should support business goals and be driven by the business—not the other way around.

A2-71 An IS auditor was asked to review a contract for a vendor being considered to provide data center services. Which is the **BEST** way to determine whether the terms of the contract are adhered to after the contract is signed?

A. Require the vendor to provide monthly status reports.
B. Have periodic meetings with the client IT manager.
C. Conduct periodic audit reviews of the vendor.
D. Require that performance parameters be stated within the contract.

C is the correct answer.

Justification:
A. Although providing monthly status reports may show that the vendor is meeting contract terms, without independent verification these data may not be reliable.
B. Having periodic meetings with the client IT manager will assist with understanding the current relationship with the vendor, but meetings may not include vendor audit reports, status reports and other information that a periodic audit review would take into consideration.
C. Conducting periodic reviews of the vendor ensures that the agreements within the contract are completed in a satisfactory manner. Without future audit reviews after the contract is signed, service level agreements and the client's requirements for security controls may become less of a focus for the vendor, and the results may slip. Periodic audit reviews allow the client to take a look at the vendor's current state to ensure that the vendor is one with which they want to continue to work.
D. Requiring that performance parameters be stated within the contract is important, but only if periodic reviews are performed to determine that performance parameters are met.

A2-72 Which of the following inputs adds the **MOST** value to the strategic IT initiative decision-making process?

A. The maturity of the project management process
B. The regulatory environment
C. Past audit findings
D. The IT project portfolio analysis

D is the correct answer.

Justification:

A. The maturity of the project management process is more important with respect to managing the day-to-day operations of IT versus performing strategic planning.
B. Regulatory requirements may drive investment in certain technologies and initiatives; however, having to meet regulatory requirements is not typically the main focus of the IT and business strategy.
C. Past audit findings may drive investment in certain technologies and initiatives; however, having to remediate past audit findings is not the main focus of the IT and business strategy.
D. Portfolio analysis provides the best input into the decision-making process relating to planning strategic IT initiatives. An analysis of the IT portfolio provides comparable information of planned initiatives, projects and ongoing IT services, which allows the IT strategy to be aligned with the business strategy.

A2-73 Which of the following does a lack of adequate security controls represent?

A. Threat
B. Asset
C. Impact
D. Vulnerability

D is the correct answer.

Justification:

A. A threat is anything (e.g., object, substance, human) that is capable of acting against an asset in a manner that can result in harm. A threat exists regardless of controls or a lack of controls.
B. An asset is something of either tangible or intangible value that is worth protecting, including people, information, infrastructure, finances and reputation. The asset value is not affected by a lack of controls.
C. Impact represents the outcome or result of a threat exploiting a vulnerability. A lack of controls would lead to a higher impact, but the lack of controls is defined as a vulnerability, not an impact.
D. 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 can 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.

A2-74 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

D is the correct answer.

Justification:
A. Minimizing errors is an aspect of performance but not the primary objective of performance management.
B. Gathering performance data is necessary to measure IT performance but is not the objective of the process.
C. The performance measurement process compares actual performance with baselines but is not the objective of the process.
D. An IT performance measurement process can be used to optimize performance, measure and manage products/services, assure accountability and make budget decisions.

A2-75 As an outcome of information security governance, strategic alignment provides:

A. Security requirements driven by enterprise requirements.
B. Baseline security following good practices.
C. Institutionalized and commoditized solutions.
D. An understanding of risk exposure.

A is the correct answer.

Justification:
A. 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.
B. Strategic alignment ensures that security aligns with business goals. Providing a standard set of security practices (i.e., baseline security following good practices or institutionalized and commoditized solutions) is a part of value delivery.
C. Value delivery addresses the effectiveness and efficiency of solutions but is not a result of strategic alignment.
D. Risk management is a primary goal of IT governance, but strategic alignment is not focused on understanding risk exposure.

A2-76 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.

A is the correct answer.

Justification:

A. **Business objectives drive the information security policy, and the information security policy drives the selection of IT department objectives. A policy driven by IT objectives is at risk of not being aligned with business goals.**
B. Policies should be written so that users can understand each policy, and employees should be able to easily access the policies. The fact that users have not read the policy is not the greatest concern because they still may be compliant with the policy.
C. Policies should not contain procedures. Procedures are established to assist with policy implementation and compliance.
D. Policies should be reviewed annually, but they might not necessarily be updated annually unless there are significant changes in the environment such as new laws, rules or regulations.

A2-77 Which of the following IT governance good 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 mediates between the imperatives of business and technology.

D is the correct answer.

Justification:

A. Supplier and partner risk being managed is a risk management good practice but not a strategic function.
B. A knowledge base on customers, products, markets and processes being in place is an IT value delivery good practice but does not ensure strategic alignment.
C. An infrastructure being provided to facilitate the creation and sharing of business information is an IT value delivery and risk management good practice but is not as effective as top management involvement in business and technology alignment.
D. **Top management mediating between the imperatives of business and technology is an IT strategic alignment good practice.**

A2-78 Effective IT governance requires organizational structures and processes to ensure that:

A. Risk is maintained at a level acceptable for IT management.
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.

D is the correct answer.

Justification:
A. Risk acceptance levels are set by senior management, not by IT management.
B. The business strategy drives the IT strategy, not the other way around.
C. IT governance is not an isolated discipline; it must become an integral part of the overall enterprise governance.
D. 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.

A2-79 Assessing IT risk is **BEST** achieved by:

A. Evaluating threats and vulnerabilities associated with existing IT assets and IT projects
B. Using the organization'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

A is the correct answer.

Justification:
A. To assess IT risk, threats and vulnerabilities need to be evaluated using qualitative or quantitative risk assessment approaches.
B. Basing an assessment on past losses will not adequately reflect new threats or 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.
C. 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.
D. 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.

A2-80 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

B is the correct answer.

Justification:
A. IT support staff usually require physical access to computing equipment to perform their job functions. It would not be reasonable to take this away.
B. 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.
C. Performing background checks 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.
D. Locking user sessions after a specified period of inactivity 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.

A2-81 A top-down approach to the development of operational policies helps to 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.

A is the correct answer.

Justification:
A. Deriving lower-level policies from corporate policies (a top-down approach) aids in ensuring consistency across the organization and consistency with other policies.
B. Policies should be influenced by risk assessment, but the primary reason for a top-down approach is to ensure that the policies are consistent across the organization.
C. A top-down approach, of itself, does not ensure compliance.
D. A top-down approach, of itself, does not ensure that policies are reviewed.

A2-82 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.

C is the correct answer.

Justification:
A. Cross-training helps decrease dependence on a single person.
B. Cross-training assists in succession planning.
C. Cross-training is a process of training more than one individual to perform a specific job or procedure. However, before using this approach, it is prudent to assess the risk of any person knowing all parts of a system and the related potential exposures related to abuse of privilege.
D. Cross-training provides for the backup of personnel in the event of an absence and, thereby, provides for the continuity of operations.

A2-83 Which of the following should be of **PRIMARY** concern to an IS auditor reviewing the management of external IT service providers?

A. Minimizing costs for the services provided
B. Prohibiting the provider from subcontracting services
C. Evaluating the process for transferring knowledge to the IT department
D. Determining if the services were provided as contracted

D is the correct answer.

Justification:

A. Minimizing costs, if applicable and achievable (depending on the customer's need), is traditionally not part of an IS auditor's job. This would normally be done by a line management function within the IT department. Furthermore, during an audit, it is too late to minimize the costs for existing provider arrangements.
B. Subcontracting providers could be a concern but would not be the primary concern. This should be addressed in the contract.
C. Transferring knowledge to the internal IT department might be desirable under certain circumstances but should not be the primary concern of an IS auditor when auditing IT service providers and the management thereof.
D. From an IS auditor's perspective, the primary objective of auditing the management of service providers should be to determine if the services that were requested were provided in a way that is acceptable, seamless and in line with contractual agreements.

A2-84 Which of the following **MOST** likely indicates that a customer data warehouse should remain in-house rather than be outsourced to an offshore operation?

A. Time-zone differences can impede communications between IT teams.
B. Telecommunications cost can be much higher in the first year.
C. Privacy laws can prevent cross-border flow of information.
D. Software development may require more detailed specifications.

C is the correct answer.

Justification:

A. Time-zone differences are usually manageable issues for outsourcing solutions.
B. Higher telecommunications costs are a part of the cost-benefit analysis and not usually a reason to retain data in-house.
C. Privacy laws prohibiting the cross-border flow of personally identifiable information make it impossible to locate a data warehouse containing customer information in another country.
D. Software development typically requires more detailed specifications when dealing with offshore operations, but that is not a factor that should prohibit the outsourcing solution.

A2-85 When reviewing an organization's approved software product list, which of the following is the **MOST** important thing to verify?

A. The risk associated with the use of the products is periodically assessed.
B. The latest version of software is listed for each product.
C. Due to licensing issues, the list does not contain open source software.
D. After-hours support is offered.

A is the correct answer.

Justification:

A. Because the business conditions surrounding vendors may change, it is important for an organization to conduct periodic risk assessments of the vendor software list. This may be best incorporated into the IT risk management process.
B. The organization may not be using the latest version of a product.
C. The list may contain open source software depending on the business requirements and associated risk.
D. Support may be provided internally or externally, and technical support should be arranged depending on the criticality of the software.

A2-86 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 good 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.

C is the correct answer.

Justification:

A. An organization is not required to base its IT policies on industry good practices. Policies must be based on the culture and business requirements of the organization.
B. It is essential that policies be approved; however, that is not the primary focus during the development of the policies.
C. Because information security policies must be aligned with an organization's business and security objectives, this is the primary focus of the IS auditor when reviewing the development of information security policies.
D. Policies cannot provide direction if they are not aligned with business requirements.

A2-87 On which of the following factors should an IS auditor **PRIMARILY** focus when determining the appropriate level of protection for an information asset?

A. Results of a risk assessment
B. Relative value to the business
C. Results of a vulnerability assessment
D. Cost of security controls

A is the correct answer.

Justification:

A. **The appropriate level of protection for an asset is determined based on the risk associated with the asset. The results of the risk assessment are, therefore, the primary information that the IS auditor should review.**
B. The relative value of an asset to the business is one element considered in the risk assessment; this alone does not determine the level of protection required.
C. The results of a vulnerability assessment would be useful when creating the risk assessment; however, this would not be the primary focus.
D. The cost of security controls is not a primary factor to consider because the expenditures on these controls are determined by the value of the information assets being protected.

A2-88 From an IT governance perspective, what is the **PRIMARY** responsibility of the board of directors? To ensure that the IT strategy:

A. Is cost-effective.
B. Is future thinking and innovative.
C. Is aligned with the business strategy.
D. Has the appropriate priority level assigned.

C is the correct answer.

Justification:

A. The IT strategy should be cost-effective, but it must align with the business strategy for the strategy to be effective.
B. The IT strategy should be forward thinking and innovative, but it must align with the business strategy to be effective.
C. **The board of directors is responsible for ensuring that the IT strategy is aligned with the business strategy.**
D. The IT strategy should be appropriately prioritized; however, it must align with the business strategy first and then it will be prioritized.

A2-89 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

B is the correct answer.

Justification:

A. A scorecard is an excellent tool to implement a program based on good governance, but the most important factor in implementing governance is alignment with organizational strategies.
B. The key objective of an IT governance program is to support the business; therefore, 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.
C. A risk assessment is important to ensure that the security program is based on areas of highest risk, but risk assessment must be based on organizational strategies.
D. A policy is a key part of security program implementation, but even the policy must be based on organizational strategies.

A2-90 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.
C. an IT balanced scorecard.
D. business process reengineering.

C is the correct answer.

Justification:

A. Control self-assessments are used to improve monitoring of security controls but are not used to align IT with organizational objectives.
B. A business impact analysis is used to calculate the impact on the business in the event of an incident that affects business operations, but it is not used to align IT with organizational objectives.
C. An IT balanced scorecard 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.
D. Business process reengineering is an excellent tool to review and improve business processes but is not focused on aligning IT with organizational objectives.

A2-91 Which of the following is the **BEST** reference for an IS auditor to determine a vendor's ability to meet service level agreement requirements for a critical IT security service?

A. Compliance with the master contract
B. Agreed-on key performance indicators
C. Results of business continuity tests
D. Results of independent audit reports

B is the correct answer.

Justification:

A. The master contract typically includes terms, conditions and costs but does not typically include service levels.
B. Key performance indicators are metrics that allow for a means to measure performance. Service level agreements (SLAs) are statements related to expected service levels. For example, an Internet service provider (ISP) may guarantee that their service will be available 99.99 percent of the time.
C. If applicable to the service, results of business continuity tests are typically included as part of the due diligence review.
D. Independent audits report on the financial condition of an organization or the control environment. Reviewing audit reports is typically part of the due diligence review. Even audits must be performed against a set of standards or metrics to validate compliance.

A2-92 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.

C is the correct answer.

Justification:

A. Risk avoidance is a strategy that provides for not implementing certain activities or processes that would incur risk.
B. Risk transfer is the strategy that provides for sharing risk with partners or purchasing insurance coverage.
C. Risk mitigation is the strategy that provides for the definition and implementation of controls to address the risk described. By requiring the system's administrator to sign off on the completion of the backups, this is an administrative control that can be validated for compliance.
D. Risk acceptance is a strategy that provides for formal acknowledgment of the existence of a risk but not taking any action to reduce the risk, and the monitoring of that risk.

A2-93 A poor choice of passwords and unencrypted data transmissions over unprotected communications lines are examples of:

A. vulnerabilities.
B. threats.
C. probabilities.
D. impacts.

A is the correct answer.

Justification:

A. Vulnerabilities represent weaknesses of information resources that may be exploited by a threat. Because these are weaknesses that can be addressed by the security specialist, they are examples of vulnerabilities.
B. Threats are circumstances or events with the potential to cause harm to information resources. Threats are usually outside the control of the security specialist.
C. Probabilities represent the likelihood of the occurrence of a threat.
D. Impacts represent the outcome or result of a threat exploiting a vulnerability.

A2-94 An IS auditor is 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 of each contract is substantiated by appropriate key performance indicators.
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.

C is the correct answer.

Justification:

A. All other choices are important, but the first step is to ensure that the contracts support the business—only then can an audit process be valuable.
B. All service level agreements should be measurable and reinforced through key performance indicators—but the first step is to ensure that the SLAs are aligned with business requirements.
C. The primary requirement is for the services provided by the outsource supplier to meet the needs of the business.
D. Having appropriate controls in place for contract termination are important, but first the IS auditor must be focused on the requirement of the supplier to meet business needs.

A2-95 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.
C. IT organizational structure.
D. historical financial statements.

B is the correct answer.

Justification:

A. 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 in IT assets.
B. The IT balanced scorecard 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. In this way, the auditor can measure the success of the IT investment and strategy.
C. The IT organizational structure provides an overview of the functional and reporting relationships in an IT entity but does not ensure effectiveness of IT investment.
D. 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.

A2-96 Regarding the outsourcing of IT services, which of the following conditions should be of **GREATEST** concern to an IS auditor?

A. Core activities that provide a differentiated advantage to the organization have been outsourced.
B. Periodic renegotiation is not specified in the outsourcing contract.
C. The outsourcing contract fails to cover every action required by the business.
D. Similar activities are outsourced to more than one vendor.

A is the correct answer.

Justification:

A. An organization's core activities generally should not be outsourced because they are what the organization does best; an IS auditor observing that condition should be concerned.
B. An IS auditor should not be concerned about periodic renegotiation in the outsourcing contract because that is dependent on the term of the contract.
C. Outsourcing contracts cannot be expected to cover every action and detail expected of the parties involved but should cover business requirements.
D. Multisourcing is an acceptable way to reduce risk associated with a single point of failure.

A2-97 For a health care organization, which one of the following reasons **MOST** likely indicates 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.

A is the correct answer.

Justification:
A. Regulations prohibiting the cross-border flow of personally identifiable information may make it impossible to locate a data warehouse containing customer/member information in another country.
B. Training cost is common and manageable regardless of where the data warehouse resides.
C. Remote database monitoring is manageable regardless of where the data warehouse resides.
D. Time zone difference issues are manageable through contract provisions regardless of where the data warehouse resides.

A2-98 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.

C is the correct answer.

Justification:
A. Although cross-training is a good practice for business continuity, it is not achieved through mandatory vacations.
B. It is a good practice to maintain good employee morale, but this is not a primary reason to have a required vacation policy.
C. The practice of having another individual perform a job function is a control used to detect possible irregularities or fraud.
D. Vacation time is a competitive benefit, but that is not a control.

A2-99 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.

C is the correct answer.

Justification:
A. The plan does not need to address state of the art technology; the decision to implement new technology is dependent on the approach to risk and management strategy.
B. The plan does not need to address operational controls because those are too granular for strategic planning.
C. The IT strategic plan must include a clear articulation of the IT mission and vision.
D. The plan should be implemented with proper project management, but the plan does not need to address project management practices.

A2-100 A small organization has only one database administrator (DBA) and one system administrator. The DBA has root access to the UNIX server, which hosts the database application. How should segregation of duties be enforced in this scenario?

A. Hire a second DBA and split the duties between the two individuals.
B. Remove the DBA's root access on all UNIX servers.
C. Ensure that all actions of the DBA are logged and that all logs are backed up to tape.
D. Ensure that database logs are forwarded to a UNIX server where the DBA does not have root access.

D is the correct answer.

Justification:
A. Hiring additional staff is a costly way to ensure segregation of duties.
B. The database administrator (DBA) needs root access to the database servers to install upgrades or patches.
C. The administrator can modify or erase logs prior to the tape backup event.
D. By creating logs that the DBA cannot erase or modify, segregation of duties is enforced.

A2-101 Which of the following user profiles should be of **MOST** concern to an IS auditor when performing an audit of an electronic funds transfer system?

A. Three users with the ability to capture and verify their own messages
B. Five users with the ability to capture and send their own messages
C. Five users with the ability to verify other users and to send their own messages
D. Three users with the ability to capture and verify the messages of other users and to send their own messages

A is the correct answer.

Justification:
A. The ability of one individual to capture and verify their own messages represents an inadequate segregation because messages can be taken as correct and as if they had already been verified. The verification of messages should not be allowed by the person who sent the message.
B. Users may have the ability to send messages but should not be able to verify their own messages.
C. This is an example of separation of duties. A person can send their own message but only verify the messages of other users.
D. The ability to capture and verify the messages of others but only send their own messages is acceptable.

A2-102 Which of the following does an IS auditor **FIRST** reference when performing an IS audit?

A. Implemented procedures
B. Approved policies
C. Internal standards
D. Documented practices

B is the correct answer.

Justification:
A. Procedures are implemented in accordance with policy.
B. Policies are high-level documents that represent the corporate philosophy of an organization. Internal standards, procedures and practices are subordinate to policy.
C. Standards are subordinate to policy.
D. Practices are subordinate to policy.

A2-103 An enterprise selected a vendor to develop and implement a new software system. To ensure that the enterprise's investment in software is protected, which of the following security clauses is **MOST** important to include in the master services agreement?

A. Limitation of liability
B. Service level requirements
C. Software escrow
D. Version control

C is the correct answer.

Justification:

A. A limitation of liability clause protects the financial exposure of the organization but not its software investment.
B. Service level requirements specify financial penalties for not meeting standards, but these do not address issues of vendor insolvency.
C. **Software escrow clauses in a contract ensure that the software source code will still be available to the organization in the event of a vendor issue, such as insolvency and copyright issues.**
D. Version control is related to the software development life cycle and not the software investment.

A2-104 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

A is the correct answer.

Justification:

A. **The goals of IT governance are to improve IT performance, deliver optimum business value and ensure regulatory compliance. The key practice in support of these goals is the strategic alignment of IT with the business. To achieve alignment, all other choices need to be tied to business practices and strategies.**
B. Accountability is important, but the most important objective of IT governance is to ensure that IT investment and oversight is aligned with business requirements.
C. IT must demonstrate value to the organization, but this value is dependent on the ability of IT to align with, and support, business requirements.
D. Enhancing return is a requirement of the IT governance framework, but this requirement is only demonstrated through aligning IT with business requirements.

A2-105 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. consider the entire IT environment.
D. result in the identification of vulnerability tolerances.

C is the correct answer.

Justification:
A. Measures of security risk should not be limited to network risk, but rather focus on those areas with the highest criticality so as to achieve maximum risk reduction at the lowest possible cost.
B. 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 results from last week, last month and last quarter. Risk measures will profile assets on a network to objectively measure vulnerability risk.
C. **When assessing IT security risk, it is important to consider the entire IT environment.**
D. Measures of security risk do not identify tolerances.

A2-106 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.

A is the correct answer.

Justification:
A. **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.**
B. Reducing IT costs may not be the best IT governance outcome for an enterprise.
C. Decentralizing IT resources across the organization is not always desired, although it may be desired in a decentralized environment.
D. Centralizing control of IT is not always desired. An example of where it might be desired is an enterprise wanting a single point of customer contact.

A2-107 Which of the following is the **MOST** important for an IS auditor to consider when reviewing a service level agreement with an external IT service provider?

A. Payment terms
B. Uptime guarantee
C. Indemnification clause
D. Default resolution

B is the correct answer.

Justification:
A. Payment terms are typically included in the master agreement rather than in the service level agreement (SLA).
B. **The most important element of an SLA is the measurable terms of performance, such as uptime agreements.**
C. The indemnification clause is typically included in the master agreement rather than in the SLA.
D. The default resolution would only apply in case of a default of the SLA; therefore, it is more important to review the performance conditions of the SLA.

A2-108 The **PRIMARY** objective of implementing corporate governance is to:

A. provide strategic direction.
B. control business operations.
C. align IT with business.
D. implement good practices.

A is the correct answer.

Justification:

A. **Corporate governance is a set of management practices to provide strategic direction to the organization as a whole, thereby ensuring that goals are achievable, risk is properly addressed and organizational resources are properly used. Hence, the primary objective of corporate governance is to provide strategic direction.**
B. Business operations are directed and controlled based on the strategic direction.
C. Corporate governance applies strategic planning, monitoring and accountability to the entire organization, not just to IT.
D. Governance is applied through the use of good practices, but this is not the objective of corporate governance.

A2-109 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 that are based on potential consequences
D. A risk mitigation strategy sufficient to keep risk consequences at an acceptable level

A is the correct answer.

Justification:

A. **Implementing risk management, as one of the outcomes of effective information security governance, requires a collective understanding of the organization's threat, vulnerability and risk profile as a first step.**
B. An understanding of risk exposure and potential consequences of compromise can be determined only after there is an understanding the organization's threat, vulnerability and risk profile.
C. Risk management priorities that are based on potential consequences can only be developed after the organization's threat, vulnerability and risk profile is determined.
D. Risk mitigation priorities are based on the risk profile, risk acceptance levels and potential mitigating controls. These elements provide a basis for the formulation of strategies for risk mitigation sufficient to keep the consequences from risk at an acceptable level.

A2-110 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.

A is the correct answer.

Justification:

A. **In the context of effective information security governance, value delivery is implemented to ensure optimization of security investments in support of business objectives.**
B. The tools and techniques for implementing value delivery include implementation of a standard set of security practices; however, implementation of standards is a means to achieve the objective of supporting value delivery, not the objective itself.
C. Value delivery may be supported through the use of standards-based solutions, but the use of standards-based solutions is not the goal of value delivery.
D. Continuous improvement culture in relation to a security program is a process, not an objective.

A2-111 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.

A is the correct answer.

Justification:

A. **Performance measurement includes setting and monitoring measurable objectives of that which the IT processes need to deliver (process outcome), and how they deliver it (process capability and performance). Transparency is primarily achieved through performance measurement, because it provides information to the stakeholders on how well the enterprise is performing when compared to objectives.**
B. Strategic alignment primarily focuses on ensuring linkage of business and IT plans, not on transparency.
C. Value delivery is about executing the value proposition throughout the delivery cycle. Value delivery ensures that IT investments deliver on promised values but does not ensure transparency of investment.
D. Resource management is about the optimal investment in and proper management of critical IT resources but does not ensure transparency of IT investments.

A2-112 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

C is the correct answer.

Justification:

A. The level of process maturity will evolve as the implementation of the IT governance program occurs and may feed into the decision-making process. Those areas that represent real risk to the business should be given priority.
B. The level of process performance will demonstrate the effectiveness of the program but will not be the means to establish priorities for governance. Those areas that represent real risk to the business should be given priority.
C. Priority should be given to those areas that represent a known risk to the enterprise operations.
D. Audit reports will provide assurance of the effectiveness of the implementation of governance but will not determine the priorities for program. Those areas that represent real risk to the business should be given priority.

A2-113 Responsibility for the governance of IT should rest with the:

A. IT strategy committee.
B. Chief information officer.
C. Audit committee.
D. Board of directors.

D is the correct answer.

Justification:

A. The IT strategy committee plays a significant role in the successful implementation of IT governance within an organization, but the ultimate responsibility resides with the board of directors.
B. The chief information officer plays a significant role in the successful implementation of IT governance within an organization, but the ultimate responsibility resides with the board of directors.
C. The audit committee plays a significant role in monitoring and overseeing the successful implementation of IT governance within an organization, but the ultimate responsibility resides with the board of directors.
D. 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.

A2-114 Which of the following is normally a responsibility of the chief information security officer?

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

A is the correct answer.

Justification:

A. **The role of the chief information security officer is to ensure that the corporate security policy and controls are adequate to prevent unauthorized access to the enterprise assets, including data, programs and equipment.**
B. User application and other software testing and evaluation normally are the responsibility of the staff assigned to development and maintenance.
C. Granting and revoking access to IT resources is usually a function of system, network or database administrators.
D. Approval of access to data and applications is the duty of the data or application owner.

A2-115 When developing a formal enterprise security program, the **MOST** critical success factor is 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.

C is the correct answer.

Justification:

A. Establishment of a review board is not effective without visible sponsorship of top management.
B. The creation of a security unit is not effective without visible sponsorship of top management.
C. **The executive sponsor is in charge of supporting the organization's strategic security program and aids in directing the organization's overall security management activities. Therefore, support by the executive level of management is the most critical success factor.**
D. The selection of a security process owner is not effective without visible sponsorship of top management.

A2-116 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.

A is the correct answer.

Justification:

A. **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 assessment 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. 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.**
B. Operational efficiency initiatives, including cost reduction of purchasing and maintenance activities of systems, belong to tactical planning, not strategic planning.
C. A list of approved suppliers of IT contract resources is a tactical rather than a strategic concern.
D. An IT strategic plan would not normally include detail of a specific technical architecture.

A2-117 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

B is the correct answer.

Justification:

A. Policy is used to provide direction for procedures, standards and baselines. Therefore, developing security procedures should be executed only after defining a security policy.
B. **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 often set the stage in terms of the tools and procedures that are needed for an organization.**
C. Specifying an access control methodology is an implementation concern and should be executed only after defining a security policy.
D. Defining roles and responsibilities should be executed only after defining a security policy.

A2-118 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 for measuring performance.
B. Consider user satisfaction in the key performance indicators.
C. Select projects according to business benefits and risk.
D. Modify the yearly process of defining the project portfolio.

C is the correct answer.

Justification:
A. Measures such as a balanced scorecard are helpful, but do not guarantee that the projects are aligned with business strategy.
B. Key performance indicators are helpful to monitor and measure IT performance, but they do not guarantee that the projects are aligned with business strategy.
C. **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.**
D. Modifying the yearly process of the project portfolio definition might improve the situation, but only if the portfolio definition process is closely tied to organizational strategies.

A2-119 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 recommendations
D. Reduction of the cost for IT security

B is the correct answer.

Justification:
A. Recommendations, visions and objectives of the IS auditor are usually addressed within a security program, but they would not be the major benefit.
B. **The major benefit of implementing a security program is management's assessment of risk and its mitigation to an appropriate level, and monitoring of the residual risk.**
C. Recommendations, visions and objectives of the chief information security officer are usually included within a security program, but they would not be the major benefit.
D. The cost of IT security may or may not be reduced.

A2-120 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

B is the correct answer.

Justification:

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

A2-121 An employee who has access to highly confidential information resigned. Upon departure, which of the following should be done **FIRST**?

A. Conduct an exit interview with the employee.
B. Ensure succession plans are in place.
C. Revoke the employee's access to all systems.
D. Review the employee's job history.

C is the correct answer.

Justification:

A. It is important to have an exit interview with any employee; however, this would not be the first step to take upon the employee's departure to protect the confidentiality of information.
B. Succession plans are important to prevent disruption of operations. This would address availability and not confidentiality of information.
C. If an employee has dealt with highly classified information, the first step is to revoke their access to all systems, to prevent exfiltration of data and restrict access to the information.
D. Keeping a record of the job history is important; however, its effectiveness may be limited.

A2-122 An organization has outsourced its help desk activities. An IS auditor's **GREATEST** concern when reviewing the contract and associated service level agreement 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.

B is the correct answer.

Justification:
A. Although it is necessary to document the fact that background checks are performed, this is only one of the provisions that should be in place for audits.
B. When the functions of an IT 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.
C. Financial measures such as year-to-year incremental cost reductions are desirable to have in a service level agreement (SLA); however, cost reductions are not as important as the availability of independent audit reports or full audit access.
D. 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.

A2-123 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 occurs for all reports before release into production
B. Organizational data governance practices are put in place
C. Standard software tools are used for report development
D. Management signs off on requirements for new reports

B is the correct answer.

Justification:
A. Recommending that user acceptance testing occur for all reports before release into production does not address the root cause of the problem described.
B. This choice directly addresses the problem. An organization-wide approach is needed to achieve effective management of data assets and reporting standards. This includes enforcing standard definitions of data elements, which is part of a data governance initiative.
C. Recommending standard software tools be used for report development does not address the root cause of the problem described.
D. Recommending that management sign off on requirements for new reports does not address the root cause of the problem described.

A2-124 Which of the following **BEST** supports the prioritization of new IT projects?

A. Internal control self-assessment
B. Information systems audit
C. Investment portfolio analysis
D. Business risk assessment

C is the correct answer.

Justification:

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

A2-125 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. Claims to meet or exceed 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.

B is the correct answer.

Justification:

A. Compliance with security standards is important, but there is no way to verify or prove that is the case without an independent review.
B. It is critical that an independent security review of an outsourcing vendor be obtained, because customer credit information will be kept with the vendor.
C. 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.
D. Compliance with organizational security policies is important, but there is no way to verify or prove that that is the case without an independent review.

A2-126 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 is the **GREATEST** risk?

A. Project management and progress reporting is combined in a project management office that 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 organization'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.

B is the correct answer.

Justification:

A. In postmerger integration programs, it is common to form project management offices (often staffed with external experts) to ensure standardized and comparable information levels in the planning and reporting structures, and to centralize dependencies of project deliverables or resources.
B. 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.
C. The development of new integrated systems can require some knowledge of the legacy systems to gain an understanding of each business process.
D. 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.

A2-127 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 because 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.

D is the correct answer.

Justification:

A. 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.
B. While common risk may be covered by 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 to manage IT risk.
C. The auditor should recommend a formal IT risk management effort because the failure to demonstrate responsible IT risk management may be a liability for the organization.
D. 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 register and mitigation plans up to date.

A2-128 Overall quantitative business risk for a particular threat can be expressed as:

A. A product of the likelihood and magnitude of the impact if a threat successfully exploits a vulnerability.
B. The magnitude of the impact if a threat source successfully exploits the vulnerability.
C. The likelihood of a given threat source exploiting a given vulnerability.
D. The collective judgment of the risk assessment team.

A is the correct answer.

Justification:

A. **Overall business risk takes into consideration the likelihood and magnitude of the impact when a threat exploits a vulnerability, and provides the best measure of the risk to an asset.**
B. The calculation of risk must consider impact and likelihood of a threat (not a threat source) exploiting a vulnerability.
C. Considering only the likelihood of an exploit and not the impact or damage caused is not sufficient to determine the overall risk.
D. The collective judgment of the risk assessment team is a part of qualitative risk assessment but must be combined with calculations of the impact on the business to determine overall risk.

A2-129 While conducting an IS audit of a service provider for a government 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 delegated to the subcontractor.

D is the correct answer.

Justification:

A. Regular committee meetings are a good monitoring tool for delegated operations; however, independent reviews provide better assurance.
B. Management should not only rely on self-reported information from the subcontractor.
C. Obtaining permission from the government agent is not related to ensuring the confidentiality of information.
D. **Periodic independent audits provide reasonable assurance that the requirements for protecting confidentiality of information are not compromised.**

A2-130 During an audit, which of the following situations are **MOST** concerning for an organization that significantly outsources IS processing to a private network?

A. The contract does not contain a right-to-audit clause for the third party.
B. The contract was not reviewed by an information security subject matter expert prior to signing.
C. The IS outsourcing guidelines are not approved by the board of directors.
D. There is a lack of well-defined IS performance evaluation procedures.

A is the correct answer.

Justification:

A. **Lack of a right-to-audit clause in the contract impacts the IS auditor's ability to perform the IS audit. Hence, the IS auditor is most concerned with such a situation. In the case of outsourcing to a private network, the organization should ensure that the third party has a minimum set of IT security controls in place and that they are operating effectively.**
B. Having an information security subject matter expert review a contract is a good practice, but it is not a requirement in all industries.
C. Approval of the IS outsourcing guidelines by the board is a good practice of governance, and lack of approval is an audit issue. However, it does not impact the IS auditor's ability to perform IS audit.
D. Lack of well-defined procedures does not enable objective evaluation of IS performance and is an audit issue. However, it does not result into major risk or repercussions and also does not impact the IS auditor's ability to perform an IS audit.

A2-131 The **MOST** important element for the effective design of an information security policy is the:

A. threat landscape.
B. prior security incidents.
C. emerging technologies.
D. enterprise risk appetite.

D is the correct answer.

Justification:

A. The threat landscape is dynamic. It should be considered when developing policy, but it is not the primary factor as policy is not meant to change as often as the threat landscape.
B. Prior security incidents may provide insight into the risk appetite statement; however, they are more likely to affect security standards and procedures.
C. Emerging technologies are continually evolving. They should be considered when developing policy, but they are not the primary factor as policy is not meant to change as often as technology.
D. **The risk appetite is the amount of risk on a broad level that an entity is willing to accept in pursuit of its mission to meet its strategic objectives. The purpose of the information security policy is to manage information risk to an acceptable level, so that the policy is principally aligned with the risk appetite.**

A2-132 As result of profitability pressure, senior management of an enterprise decided to keep investments in information security at an inadequate level, which of the following is the **BEST** recommendation of an IS auditor?

A. Use cloud providers for low-risk operations.
B. Revise compliance enforcement processes.
C. Request that senior management accept the risk.
D. Postpone low-priority security procedures.

C is the correct answer.

Justification:
A. The use of cloud providers may or may not provide cost savings or lower risk.
B. Compliance enforcement processes that identify high levels of residual risk are working as intended and should not be revised.
C. **Senior management determines resource allocations. Having established that the level of security is inadequate, it is imperative that senior management accept the risk resulting from their decisions.**
D. The IS auditor should not recommend postponing any procedures. This is a management decision, and management should first accept the risk.

A2-133 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

B is the correct answer.

Justification:
A. Business interruption insurance covers the loss of profit due to the disruption in the operations of an organization.
B. **Fidelity insurance covers the loss arising from dishonest or fraudulent acts by employees.**
C. 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.
D. Extra expense insurance is designed to cover the extra costs of continuing operations following a disaster/disruption within an organization.

A2-134 Errors in audit procedures **PRIMARILY** impact which of the following risks?

A. Detection risk
B. Inherent risk
C. Control risk
D. Business risk

A is the correct answer.

Justification:
A. **Detection risk is the probability that the audit procedures may fail to detect existence of a material error or fraud.**
B. Inherent risk refers to the risk involved in the nature of business or transaction and is not affected by human error.
C. Control risk is the risk that a material error exists that would not be prevented or detected on a timely basis by the system of internal controls.
D. Business risk is not a component of audit risk.

A2-135 Which of the following is **MOST** important to consider when reviewing the classification levels of information assets?

A. Potential loss
B. Financial cost
C. Potential threats
D. Cost of insurance

A is the correct answer.

Justification:

A. The best basis for asset classification is an understanding of the total losses a business may incur if the asset is compromised. Typically, estimating these losses requires a review of criticality and sensitivity beyond financial cost, such as operational and strategic.
B. The value of an asset can be greater than its monetary cost, such as impact to reputation and brand.
C. The classification of an asset does not change based on potential threats.
D. Insurance would be obtained based on asset classification.

A2-136 Which of the following is of **MOST** interest to an IS auditor reviewing an organization's risk strategy?

A. All risk is mitigated effectively.
B. Residual risk is zero after control implementation.
C. All likely risk is identified and ranked.
D. The organization uses an established risk framework.

C is the correct answer.

Justification:

A. Risk mitigation can only occur after all risk is identified and ranked.
B. It is highly unlikely residual risk would be zero.
C. Risk that is likely to impact the organization should be identified and documented as part of the risk strategy. Without knowing the risk, there is no risk strategy.
D. It is not as important to use an established risk framework as it is to identify and rank all likely risk so that it can be addressed.

A2-137 An enterprise is looking to obtain cloud hosting services from a cloud vendor with a high level of maturity. Which of the following is **MOST** important for the auditor to ensure continued alignment with the enterprise's security requirements?

A. The vendor provides the latest third-party audit report for verification.
B. The vendor provides the latest internal audit report for verification.
C. The vendor agrees to implement controls in alignment with the enterprise.
D. The vendor agrees to provide annual external audit reports in the contract.

D is the correct answer.

Justification:

A. Although the vendor is providing the most recent third-party audit report for review, there is no agreement contractually that would require the vendor to continue to provide annual reports for verification and review.
B. Although the vendor is providing the most recent internal audit report for review, there is no agreement contractually that would require the vendor to continue to provide annual reports for verification and review.
C. Without a clause in the contract, an agreement to implement controls does not provide assurance that controls will continue to be implemented in alignment with the enterprise.
D. The only way to ensure that any potential risk is mitigated today and in the future is to include a clause within the contract that the vendor will provide future external audit reports. Without the audit clause the vendor can choose to forego future audits.

A2-138 An IS auditor is evaluating the IT governance framework of an organization. Which of the following is the **GREATEST** concern?

A. Senior management has limited involvement.
B. Return on investment is not measured.
C. Chargeback of IT cost is not consistent.
D. Risk appetite is not quantified.

A is the correct answer.

Justification:

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 involvement of senior management when evaluating the soundness of IT governance.**
B. Ensuring revenue management 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.

A2-139 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 annual loss expectancy calculation
C. A comparison of the cost of the IPS and firewall and the cost of the business systems
D. A business impact analysis

A is the correct answer.

Justification:

A. **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 to choose the best technical, most profitable, least expensive or acceptable risk option.**
B. The annual loss expectancy 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.
C. 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.
D. Potential business impact is only one part of the cost-benefit analysis.

A2-140 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.

D is the correct answer.

Justification:

A. The capability of the organization to support the enterprise should extend beyond the time of execution of the immediate contract. The objective of financial evaluation should not be confined to the immediate contract but should be to provide assurance of sustainability over a longer time frame.
B. Whether the vendor is of similar financial standing as the purchaser is irrelevant to this review.
C. The vendor should not have financial obligations that could impose a liability to the purchaser; the financial obligations are usually from the purchaser to the vendor.
D. 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 and thereby more likely to be capable of providing long-term support for the purchased product.

A2-141 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

B is the correct answer.

Justification:

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.

A2-142 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.

D is the correct answer.

Justification:

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. 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.

A2-143 An enterprise hosts its data center onsite and has outsourced the management of its key financial applications to a service provider. Which of the following controls **BEST** ensures that the service provider'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.

B is the correct answer.

Justification:

A. Having users sign off on policies is a good practice; however, this only puts the onus of compliance on the individual user, not on the organization.
B. Having the service provider sign an indemnity clause will ensure compliance to the enterprise's security policies, because any violations discovered will lead to a financial liability for the service provider. This will also prompt the enterprise to monitor security violations closely.
C. Awareness training is an excellent control but will not ensure that the service provider's employees adhere to policy.
D. Modification of security policy does not ensure compliance by users unless the policies are appropriately communicated to users and enforced, and awareness training is provided.

A2-144 The corporate IT 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 IT policy to allow shared accounts.

C is the correct answer.

Justification:
A. Having the current configuration approved is a recommendation that is not in compliance with the enterprise's own policy and would violate good practice.
B. Having an audit trail for existing shared accounts would not provide accountability or resolve the problem of noncompliance with policy.
C. Individual user accounts allow for accountability of transactions and should be the most important recommendation, given the current scenario.
D. Shared user IDs do not allow for accountability of transactions and would not reflect good practice.

A2-145 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

C is the correct answer.

Justification:
A. Ensuring that employees are properly cross-trained in multiple functions improves the skills of employees and provides for succession planning but is not the primary purpose of mandatory vacations.
B. Improving employee morale helps in reducing employee burnout but is not the primary reason for mandatory vacations.
C. 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 often a regulatory requirement and, most importantly, a good way to uncover fraud.
D. Mandatory vacations may or may not be a cost-saving measure, depending on the enterprise.

A2-146 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.

D is the correct answer.

Justification:

A. It should be identified if the project portfolio exceeds the IT budget, but it is not as critical as ensuring that it is aligned with the business plan.
B. The project portfolio should be aligned with the investment strategy, but it is most important that it is aligned with the business plan.
C. Appropriate approval of the project portfolio should be granted. However, not every enterprise has an IT steering committee, and this is not as critical as ensuring that the projects are aligned with the business plan.
D. 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.

A2-147 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.

C is the correct answer.

Justification:

A. Although due diligence is a good practice, it does not ensure availability of the source code in the event of vendor failure.
B. Although a quarterly audit of vendor facilities is a good practice, it does not ensure availability of the source code in the event of failure of the start-up vendor.
C. A source code escrow agreement is primarily recommended to help protect the enterprise's investment in software, because the source code will be available through a trusted third party and can be retrieved if the start-up vendor goes out of business.
D. Although a penalty clause is a good practice, it does not provide protection or ensure availability of the source code in the event of vendor bankruptcy.

A2-148 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

D is the correct answer.

Justification:

A. Although chief legal officers can give guidance regarding legal issues on the policy, they cannot determine the risk appetite.
B. The security management team is concerned with managing the security posture but not with determining the posture.
C. The audit committee is not responsible for setting the risk tolerance or appetite of the enterprise.
D. The steering committee is best suited to determine the enterprise's risk appetite because the committee draws its representation from senior management.

A2-149 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 also performs data backups.

A is the correct answer.

Justification:

A. If developers have access to the production environment, there is a risk that untested code can be migrated into the production environment.
B. 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.
C. 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.
D. It may be part of the database administrator's duties to perform data backups.

A2-150 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

A is the correct answer.

Justification:

A. An IT steering committee typically has a variety of responsibilities, including approving IT project plans and budgets. Issues related to business objectives, risk and governance are responsibilities that are generally assigned to an IT strategy committee, because it provides insight and advice to the board.
B. Aligning IT to business objectives is a task usually assigned to an IT strategy committee. The steering committee would be more involved in approval and monitoring of individual projects and budgets.
C. Issues related to compliance are tasks usually assigned to an IT strategy committee. The steering committee would be more involved in approval and monitoring of individual projects and budgets.
D. IT governance is a task usually assigned to an IT strategy committee. The steering committee would be more involved in approval and monitoring of individual projects and budgets.

A2-151 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

B is the correct answer.

Justification:

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

A2-152 An IT steering committee should:

A. Include a mix of members from different departments and staff levels.
B. Ensure that information 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.

C is the correct answer.

Justification:

A. Only senior management or high-level staff members should be on this committee because of its strategic mission.
B. Ensuring that information security policies and procedures have been executed properly is not a responsibility of this committee, but the responsibility of IT management and the security administrator.
C. **It is important to keep detailed IT steering committee minutes to document the decisions and activities of the IT steering committee. The board of directors should be informed about those decisions on a timely basis.**
D. A vendor should be invited to meetings only when appropriate.

Page intentionally left blank