## DOMAIN 3—INFORMATION SYSTEMS ACQUISITION, DEVELOPMENT AND IMPLEMENTATION (12%)

A3-1 Who should review and approve system deliverables as they are defined and accomplished, to ensure the successful completion and implementation of a new business system application?

A. User management
B. Project steering committee
C. Senior management
D. Quality assurance staff

**A is the correct answer.**

**Justification:**

A. **User management assumes ownership of the project and resulting system, allocates qualified representatives to the team and actively participates in system requirements definition, acceptance testing and user training. User management should review and approve system deliverables as they are defined and accomplished, or implemented.**
B. A project steering committee provides overall direction, ensures appropriate representation of the major stakeholders in the project's outcome, reviews project progress regularly and holds emergency meetings when required. A project steering committee is ultimately responsible for all deliverables, project costs and schedules.
C. Senior management demonstrates commitment to the project and approves the necessary resources to complete the project. This commitment from senior management helps ensure involvement by those who are needed to complete the project.
D. Quality assurance staff review results and deliverables within each phase, and at the end of each phase confirm compliance with standards and requirements. The timing of reviews depends on the system development life cycle, the impact of potential deviation methodology used, the structure and magnitude of the system and the impact of potential deviation.

A3-2 Which of the following **BEST** helps to prioritize project activities and determine the time line for a project?

A. A Gantt chart
B. Earned value analysis
C. Program evaluation review technique
D. Function point analysis

**C is the correct answer.**

**Justification:**

A. A Gantt chart is a simple project management tool and would help with the prioritization requirement, but it is not as effective as program evaluation review technique (PERT).
B. Earned value analysis is a technique to track project cost versus project deliverables but does not assist in prioritizing tasks.
C. **The PERT method works on the principle of obtaining project time lines based on project events for three likely scenarios—worst, best and normal. The timeline is calculated by a predefined formula and identifies the critical path, which identifies the key activities that must be prioritized.**
D. Function point analysis measures the complexity of input and output and does not help to prioritize project activities.

A3-3 An IS auditor reviewing a series of completed projects finds that the implemented functionality often exceeded requirements and most of the projects ran significantly over budget. Which of these areas of the organization's project management process is the **MOST** likely cause of this issue?

A. Project scope management
B. Project time management
C. Project risk management
D. Project procurement management

**A is the correct answer.**

**Justification:**

A. **Because the implemented functionality is greater than what was required, the most likely cause of the budget issue is failure to effectively manage project scope. Project scope management is defined as the processes required to ensure that the project includes all of the required work, and only the required work, to complete the project.**
B. Project time management is defined as the processes required to ensure timely completion of the project. The issue noted in the question does not mention whether projects were completed on time, so this is not the most likely cause.
C. Project risk management is defined as the processes concerned with identifying, analyzing and responding to project risk. Although the budget overruns mentioned above represent one form of project risk, they appear to be caused by implementing too much functionality, which relates more directly to project scope.
D. Project procurement management is defined as the processes required to acquire goods and services from outside the performing organization. Although purchasing goods and services that are too expensive can cause budget overruns, in this case the key to the question is that implemented functionality is greater than what was required, which is more likely related to project scope.

A3-4 An IS auditor is reviewing the software development process for an organization. Which of the following functions are appropriate for the end users to perform?

A. Program output testing
B. System configuration
C. Program logic specification
D. Performance tuning

**A is the correct answer.**

**Justification:**

A. **A user can test program output by checking the program input and comparing it with the system output. This task, although usually done by the programmer, can also be done effectively by the user.**
B. System configuration is usually too technical to be accomplished by a user and this situation could create security issues. This could introduce a segregation of duties issue.
C. Program logic specification is a very technical task that is normally performed by a programmer. This could introduce a segregation of duties issue.
D. Performance tuning also requires high levels of technical skill and will not be effectively accomplished by a user. This could introduce a segregation of duties issue.

A3-5 An IS auditor is reviewing system development for a health care organization with two application environments—production and test. During an interview, the auditor notes that production data are used in the test environment to test program changes. What is the **MOST** significant potential risk from this situation?

A. The test environment may not have adequate controls to ensure data accuracy.
B. The test environment may produce inaccurate results due to use of production data.
C. Hardware in the test environment may not be identical to the production environment.
D. The test environment may not have adequate access controls implemented to ensure data confidentiality.

**D is the correct answer.**

**Justification:**

A. The accuracy of data used in the test environment is not of significant concern as long as these data are representative of the production environment.
B. Using production data in the test environment does not cause test results to be inaccurate. If anything, using production data improves the accuracy of testing processes, because the data most closely mirror the production environment. In spite of that fact, the risk of data disclosure or unauthorized access in the test environment is still significant and, as a result, production data should not be used in the test environment. This is especially important in a health care organization where patient data confidentiality is critical and privacy laws in many countries impose strict penalties on misuse of these data.
C. Hardware in the test environment should mirror the production environment to ensure that testing is reliable. However, this does not relate to the risk from using live data in a test environment. This is not the correct answer because it does not relate to the risk presented in the scenario.
**D. In many cases, the test environment is not configured with the same access controls that are enabled in the production environment. For example, programmers may have privileged access to the test environment (for testing), but not to the production environment. If the test environment does not have adequate access control, the production data are subject to risk of unauthorized access and/or data disclosure. This is the most significant risk of the choices listed.**

A3-6 The IS auditor is reviewing a recently completed conversion to a new enterprise resource planning system. In the final stage of the conversion process, the organization ran the old and new systems in parallel for 30 days before allowing the new system to run on its own. What is the **MOST** significant advantage to the organization by using this strategy?

A. Significant cost savings over other testing approaches
B. Assurance that new, faster hardware is compatible with the new system
C. Assurance that the new system meets functional requirements
D. Increased resiliency during the parallel processing time

**C is the correct answer.**

**Justification:**

A. Parallel operation provides a high level of assurance that the new system functions properly compared to the old system. Parallel operation is generally expensive and does not provide a cost savings over most other testing approaches. In many cases, parallel operation is the most expensive form of system testing due to the need for dual data entry, dual sets of hardware, dual maintenance and dual backups—it is twice the amount of work as running a production system and, therefore, costs more time and money.

B. Hardware compatibility should be determined and tested much earlier in the conversion project and is not an advantage of parallel operation. Compatibility is generally determined based on the application's published specifications and on system testing in a lab environment. Parallel operation is designed to test the application's effectiveness and integrity of application data, not hardware compatibility. In general, hardware compatibility relates more to the operating system level than to a particular application. Although new hardware in a system conversion must be tested under a real production load, this can be done without parallel systems.

C. **Parallel operation is designed to provide assurance that a new system meets its functional requirements. This is the safest form of system conversion testing because, if the new system fails, the old system is still available for production use. In addition, this form of testing allows the application developers and administrators to simultaneously run operational tasks (e.g., batch jobs and backups) on both systems, to ensure that the new system is reliable before unplugging the old system.**

D. Increased resiliency during parallel processing is a legitimate outcome from this scenario, but the advantage it provides is temporary and minor, so this is not the correct answer.

A3-7 What kind of software application testing is considered the final stage of testing and typically includes users outside of the development team?

A. Alpha testing
B. White box testing
C. Regression testing
D. Beta testing

**D is the correct answer.**

**Justification:**

A. Alpha testing is the testing stage just before beta testing. Alpha testing is typically performed by programmers and business analysts, instead of users. Alpha testing is used to identify bugs or glitches that can be fixed before beta testing begins with external users.

B. White box testing is performed much earlier in the software development life cycle than alpha or beta testing. White box testing is used to assess the effectiveness of software program logic, where test data are used to determine procedural accuracy of the programs being tested. In other words, does the program operate the way it is supposed to at a functional level? White box testing does not typically involve external users.

C. Regression testing is the process of re-running a portion of a test scenario to ensure that changes or corrections have not introduced more errors. In other words, the same tests are run after multiple successive program changes to ensure that the "fix" for one problem did not "break" another part of the program. Regression testing is not the last stage of testing and does not typically involve external users.

**D. Beta testing is the final stage of testing and typically includes users outside of the development area. Beta testing is a form of user acceptance testing and generally involves a limited number of users who are external to the development effort.**

A3-8 During which phase of software application testing should an organization perform the testing of architectural design?

A. Acceptance testing
B. System testing
C. Integration testing
D. Unit testing

**C is the correct answer.**

**Justification:**

A. Acceptance testing determines whether the solution meets the requirements of the business and is performed after system staff has completed the initial system test. This testing includes both quality assurance testing and user acceptance testing, although not combined.

B. System testing relates a series of tests by the test team or system maintenance staff to ensure that the modified program interacts correctly with other components. System testing references the functional requirements of the system.

**C. Integration testing evaluates the connection of two or more components that pass information from one area to another. The objective is to use unit-tested modules, thus building an integrated structure according to the design.**

D. Unit testing references the detailed design of the system and uses a set of cases that focus on the control structure of the procedural design to ensure that the internal operation of the program performs according to specification.

A3-9 Which of the following is an advantage of an integrated test facility?

A. It uses actual master files or dummies, and the IS auditor does not have to review the source of the transaction.
B. Periodic testing does not require separate test processes.
C. It validates application systems and ensures the correct operation of the system.
D. The need to prepare test data is eliminated.

**B is the correct answer.**

**Justification:**

A. The integrated test facility (ITF) tests a test transaction as if it were a real transaction and validates that transaction processing is being done correctly. It is not related to reviewing the source of a transaction.
**B. An ITF creates a fictitious entity in the database to process test transactions simultaneously with live input. Its advantage is that periodic testing does not require separate test processes. Careful planning is necessary, and test data must be isolated from production data.**
C. An ITF does validate the correct operation of a transaction in an application, but it does not ensure that a system is being operated correctly.
D. The ITF is based on the integration of test data into the normal process flow, so test data is still required.

A3-10 An organization is replacing a payroll program that it developed in-house, with the relevant subsystem of a commercial enterprise resource planning (ERP) system. Which of the following would represent the **HIGHEST** potential risk?

A. Undocumented approval of some project changes
B. Faulty migration of historical data from the old system to the new system
C. Incomplete testing of the standard functionality of the ERP subsystem
D. Duplication of existing payroll permissions on the new ERP subsystem

**B is the correct answer.**

**Justification:**

A. Undocumented changes (leading to scope creep) are a risk, but the greatest risk is the loss of data integrity when migrating data from the old system to the new system.
**B. The most significant risk after a payroll system conversion is loss of data integrity and not being able to pay employees in a timely and accurate manner or have records of past payments. As a result, maintaining data integrity and accuracy during migration is paramount.**
C. A lack of testing is always a risk; however, in this case, the new payroll system is a subsystem of an existing commercially available (and therefore probably well-tested) system.
D. Setting up the new system, including access permissions and payroll data, always presents some level of risk; however, the greatest risk is related to the migration of data from the old system to the new system.

A3-11 An enterprise is developing a strategy to upgrade to a newer version of its database software. Which of the following tasks can an IS auditor perform without compromising the objectivity of the IS audit function?

A. Advise on the adoption of application controls to the new database software.
B. Provide future estimates of the licensing expenses to the project team.
C. Recommend to the project manager how to improve the efficiency of the migration.
D. Review the acceptance test case documentation before the tests are carried out.

**D is the correct answer.**

**Justification:**
A. Independence can be compromised if the IS auditor advises on the adoption of specific application controls.
B. Independence can be compromised if the IS auditor were to audit the estimate of future expenses used to support a business case for management approval of the project.
C. Advising the project manager on how to increase the efficiency of the migration may compromise the IS auditor's independence.
**D. The review of the test cases will facilitate the objective of a successful migration and ensure that proper testing is conducted. An IS auditor can advise as to the completeness of the test cases.**

A3-12 During a postimplementation review, which of the following activities should be performed?

A. User acceptance testing
B. Return on investment analysis
C. Activation of audit trails
D. Updates of the state of enterprise architecture diagrams

**B is the correct answer.**

**Justification:**
A. User acceptance testing should be performed prior to the implementation (perhaps during the development phase), not after the implementation.
**B. Following implementation, a cost-benefit analysis or return on investment should be reperformed to verify that the original business case benefits are delivered.**
C. The audit trail should be activated during the implementation of the application.
D. While updating the enterprise architecture diagrams is a good practice, it would not normally be part of a postimplementation review.

A3-13 Which of the following is the **BEST** approach to ensure that sufficient test coverage will be achieved for a project with a strict end date and a fixed time to perform testing?

A. Requirements should be tested in terms of importance and frequency of use.
B. Test coverage should be restricted to functional requirements.
C. Automated tests should be performed through the use of scripting.
D. The number of required test runs should be reduced by retesting only defect fixes.

**A is the correct answer.**

**Justification:**

**A. The idea is to maximize the usefulness of testing by concentrating on the most important aspects of the system and on the areas where defects represent the greatest risk to user acceptance. A further extension of this approach is to also consider the technical complexity of requirements, because complexity tends to increase the likelihood of defects.**
B. The problem with testing only functional requirements is that nonfunctional requirement areas, such as usability and security, which are important to the overall quality of the system, are ignored.
C. Increasing the efficiency of testing by automating test execution is a good idea. However, by itself, this approach does not ensure the appropriate targeting of test coverage and so is not as effective an alternative.
D. Retesting only defect fixes has a considerable risk that it will not detect instances in which defect fixes may have caused the system to regress (i.e., introduced errors in parts of the system that were previously working correctly). For this reason, it is a good practice to undertake formal regression testing after defect fixes have been implemented.

A3-14 By evaluating application development projects against the capability maturity model, an IS auditor should be able to verify that:

A. Reliable products are guaranteed.
B. Programmers' efficiency is improved.
C. Security requirements are designed.
D. Predictable software processes are followed.

**D is the correct answer.**

**Justification:**

A. Although the likelihood of success should increase as the software processes mature toward the optimizing level, mature processes do not guarantee a reliable product.
B. The capability maturity model (CMM) does not evaluate technical processes such as programming efficiency.
C. The CMM does not evaluate security requirements or other application controls.
**D. By evaluating the organization's development projects against the CMM, an IS auditor determines whether the development organization follows a stable, predictable software development process.**

A3-15 An IS auditor is performing a post-implementation review of an organization's system and identifies output errors within an accounting application. The IS auditor determined this was caused by input errors. Which of the following controls should the IS auditor recommend to management?

A. Recalculations
B. Limit checks
C. Run-to-run totals
D. Reconciliations

**B is the correct answer.**

**Justification:**

A. A sample of transactions may be recalculated manually to ensure that processing is accomplishing the anticipated task. Recalculations are performed after the output phase.
**B. Processing controls should be implemented as close as possible to the point of data entry. Limit checks are one type of input validation check that provides a preventive control to ensure that invalid data cannot be entered because values must fall within a predetermined limit.**
C. Run-to-run totals provide the ability to verify data values through the stages of application processing. Run-to-run total verification ensures that data read into the computer were accepted and then applied to the updating process. Run-to-run totals are performed after the output phase.
D. Reconciliation of file totals should be performed on a routine basis. Reconciliations may be performed through the use of a manually maintained account, a file control record or an independent control file. Reconciliations are performed after the output phase.

A3-16 Due to a reorganization, a business application system will be extended to other departments. Which of the following should be of the **GREATEST** concern for an IS auditor?

A. Process owners have not been identified.
B. The billing cost allocation method has not been determined.
C. Multiple application owners exist.
D. A training program does not exist.

**A is the correct answer.**

**Justification:**

**A. When one application is expanded to multiple departments, it is important to ensure the mapping between the process owner and system functions. The absence of a defined process owner, may cause issues with monitoring or authorization controls.**
B. The allocation method of application usage cost is of less importance.
C. The fact that multiple application owners exist is not a concern for an IS auditor as long as process owners have been identified.
D. The fact that a training program does not exist is only be a minor concern for the IS auditor.

A3-17 When auditing the proposed acquisition of a new computer system, an IS auditor should **FIRST** ensure that:

A. A clear business case has been approved by management.
B. Corporate security standards will be met.
C. Users will be involved in the implementation plan.
D. The new system will meet all required user functionality.

**A is the correct answer.**

**Justification:**

**A. The first concern of an IS auditor is to ensure that the proposal meets the needs of the business. This should be established by a clear business case.**
B. Compliance with security standards is essential, but it is too early in the procurement process for this to be an IS auditor's first concern.
C. Having users involved in the implementation process is essential, but it is too early in the procurement process for this to be an IS auditor's first concern.
D. Meeting the needs of the users is essential, and this should be included in the business case presented to management for approval.

A3-18 Which of the following types of risk is **MOST** likely encountered in a software as a service environment?

A. Noncompliance with software license agreements
B. Performance issues due to Internet delivery method
C. Higher cost due to software licensing requirements
D. Higher cost due to the need to update to compatible hardware

**B is the correct answer.**

**Justification:**

A. Software as a service (SaaS) is provisioned on a usage basis and the number of users is monitored by the SaaS provider; therefore, there should be no risk of noncompliance with software license agreements.
**B. The risk that can be most likely encountered in a SaaS environment is speed and availability issues, because SaaS relies on the Internet for connectivity.**
C. The costs for a SaaS solution should be fixed as a part of the services contract and considered in the business case presented to management for approval of the solution.
D. The open design and Internet connectivity allow most SaaS to run on virtually any type of hardware.

A3-19 The most common reason for the failure of information systems to meet the needs of users is that:

A. user needs are constantly changing.
B. the growth of system requirements was forecast inaccurately.
C. the hardware system limits the number of concurrent users.
D. user participation in defining the system's requirements was inadequate.

**D is the correct answer.**

**Justification:**

A. Although changing user needs has an effect on the success or failure of many projects, the core problem is usually a lack of getting the initial requirements correct at the beginning of the project.
B. Projects may fail as the needs of the users increase; however, this can be mitigated through better change control procedures.
C. Rarely do hardware limitations affect the usability of the project as long as the requirements were correctly documented at the beginning of the project.
**D. Lack of adequate user involvement, especially in the system's requirements phase, will usually result in a system that does not fully or adequately address the needs of the user. Only users can define what their needs are and, therefore, what the system should accomplish.**

**A3-20** Many IT projects experience problems because the development time and/or resource requirements are underestimated. Which of the following techniques provides the **GREATEST** assistance in developing an estimate of project duration?

A. Function point analysis
B. Program evaluation review technique chart
C. Rapid application development
D. Object-oriented system development

**B is the correct answer.**

**Justification:**

A. Function point analysis is a technique for determining the size of a development task based on the number of function points. Function points are factors such as inputs, outputs, inquiries and logical internal files. While this will help determine the size of individual activities, it will not assist in determining project duration because there are many overlapping tasks.
**B. A program evaluation review technique (chart will help determine project duration once all the activities and the work involved with those activities are known.**
C. Rapid application development is a methodology that enables organizations to develop strategically important systems faster while reducing development costs and maintaining quality.
D. Object-oriented system development is the process of solution specification and modeling but will not assist in calculating project duration.

**A3-21** An IS auditor is reviewing IT projects for a large company and wants to determine whether the IT projects undertaken in a given year are those which have been assigned the highest priority by the business and which will generate the greatest business value. Which of the following is **MOST** relevant?

A. A capability maturity model
B. Portfolio management
C. Configuration management
D. Project management body of knowledge

**B is the correct answer.**

**Justification:**

A. A capability maturity model (CMM) would not help determine the optimal portfolio of capital projects because it is a means of assessing the relative maturity of the IT processes within an organization: running from Level 0 (Incomplete—Processes are not implemented or fail to achieve their purpose) to Level 5 (Optimizing—Metrics are defined and measured, and continuous improvement techniques are in place).
**B. Portfolio management is designed to assist in the definition, prioritization, approval and running of a set of projects within a given organization. These tools offer data capture, workflow and scenario planning functionality, which can help identify the optimum set of projects (from the full set of ideas) to take forward within a given budget.**
C. A configuration management database (which stores the configuration details for an organization's IT systems) is an important tool for IT service delivery and, in particular, change management. It may provide information that would influence the prioritization of projects but is not designed for that purpose.
D. The project management body of knowledge is a methodology for the management and delivery of projects. It offers no specific guidance or assistance in optimizing a project portfolio.

A3-22 The reason for establishing a stop or freezing point on the design of a new system is to:

A. prevent further changes to a project in process.
B. indicate the point at which the design is to be completed.
C. require that changes after that point be evaluated for cost-effectiveness.
D. provide the project management team with more control over the project design.

**C is the correct answer.**

**Justification:**
A. The stop point is intended to provide greater control over changes but not to prevent them.
B. The stop point is used for project control but not to create an artificial fixed point that requires the design of the project to cease.
**C. Projects often tend to expand, especially during the requirements definition phase. This expansion often grows to a point where the originally anticipated cost-benefits are diminished because the cost of the project has increased. When this occurs, it is recommended that the project be stopped or frozen to allow a review of all of the cost-benefits and the payback period.**
D. A stop point is used to control requirements, not systems design.

A3-23 Change control for business application systems being developed using prototyping could be complicated by the:

A. iterative nature of prototyping.
B. rapid pace of modifications in requirements and design.
C. emphasis on reports and screens.
D. lack of integrated tools.

**B is the correct answer.**

**Justification:**
A. A characteristic of prototyping is its iterative nature, but it does not have an adverse effect on change control.
**B. Changes in requirements and design happen so quickly that they are seldom documented or approved.**
C. A characteristic of prototyping is its emphasis on reports and screens, but it does not have an adverse effect on change control.
D. Lack of integrated tools is a characteristic of prototyping, but it does not have an adverse effect on change control.

A3-24 An IS auditor performing a review of a major software development project finds that it is on schedule and under budget even though the software developers have worked considerable amounts of unplanned overtime. The IS auditor should:

A. conclude that the project is progressing as planned because dates are being met.
B. question the project manager further to identify whether overtime costs are being tracked accurately.
C. conclude that the programmers are intentionally working slowly to earn extra overtime pay.
D. investigate further to determine whether the project plan may not be accurate.

**D is the correct answer.**

**Justification:**

A. Although the project is on time and budget, there may be problems with the project plan because considerable amounts of unplanned overtime have been required.
B. There is a possibility that the project manager has hidden some costs to make the project look better; however, the real problem may be with whether the project plan is realistic, not just the accounting.
C. It is possible that the programmers are trying to take advantage of the time system, but if the overtime has been required to keep the project on track it is more likely that the time lines and expectations of the project are unrealistic.
**D. Although the dates on which key projects are completed are important, there may be issues with the project plan if an extraordinary amount of unplanned overtime is required to meet those dates. In most cases, the project plan is based on a certain number of hours, and requiring programmers to work considerable overtime is not a good practice. Although overtime costs may be an indicator that something is wrong with the plan, in many organizations, the programming staff may be salaried, so overtime costs may not be directly recorded.**

A3-25 A project development team is considering using production data for its test deck. The team removed sensitive data elements before loading it into the test environment. Which of the following additional concerns should an IS auditor have with this practice?

A. Not all functionality will be tested.
B. Production data are introduced into the test environment.
C. Specialized training is required.
D. The project may run over budget.

**A is the correct answer.**

**Justification:**

**A. A primary risk of using production data in a test deck is that not all transactions or functionality may be tested if there are no data that meet the requirement.**
B. The presence of production data in a test environment is not a concern if the sensitive elements have been scrubbed.
C. Creation of a test deck from production data does not require specialized knowledge, so this is not a concern.
D. The risk of a project running over budget is always a concern, but it is not related to the practice of using production data in a test environment.

A3-26 Which of the following considerations is the **MOST** important while evaluating a business case for the acquisition of a new accounting application?

A. Total cost of ownership of the application
B. The resources required for implementation
C. Return on investment to the company
D. The cost and complexity of security requirements

**C is the correct answer.**

**Justification:**

A. Total cost of ownership of the application is important to understand the resource and budget requirements in the short and long term; however, decisions should be based on benefits realization from this investment. Therefore, return on investment (ROI) is the most important consideration.
B. The resources required for implementation of the application are an important consideration; however, decisions should be based on benefits realization from this investment. Therefore, ROI should be carefully considered.
C. **The proposed ROI benefits, along with targets or metrics that can be measured, are the most important aspects of a business case. While reviewing the business case, it should be verified that the proposed ROI is achievable, does not make unreasonable assumptions and can be measured for success. (Benefits realization should look beyond project cycles to longer-term cycles that consider the total benefits and total costs throughout the life of the new system.)**
D. The cost and complexity of security requirements are important considerations, but they need to be weighed against the proposed benefits of the application. Therefore, ROI is more important.

A3-27 The development of an application has been outsourced to an offshore vendor. Which of the following should be of **GREATEST** concern to an IS auditor?

A. The right to audit clause was not included in the contract.
B. The business case was not established.
C. There was no source code escrow agreement.
D. The contract does not cover change management procedures.

**B is the correct answer.**

**Justification:**

A. The lack of the right to audit clause presents a risk to the organization; however, the risk is not as consequential as the lack of a business case.
B. **Because the business case was not established, it is likely that the business rationale, risk and risk mitigation strategies for outsourcing the application development were not fully evaluated and the appropriate information was not provided to senior management for formal approval. This situation presents the biggest risk to the organization.**
C. If the source code is held by the provider and not provided to the organization, the lack of source code escrow presents a risk to the organization; however, the risk is not as consequential as the lack of a business case.
D. The lack of change management procedures presents a risk to the organization, especially with the possibility of extraordinary charges for any required changes; however, the risk is not as consequential as the lack of a business case.

A3-28 Before implementing controls in a newly developed system, management should **PRIMARILY** ensure that the controls:

A. satisfy a requirement in addressing a risk.
B. do not reduce productivity.
C. are based on a minimized cost analysis.
D. are detective or corrective.

**A is the correct answer.**

**Justification:**

A. **The purpose of a control is to mitigate a risk; therefore, the primary consideration when selecting a control is that it effectively mitigates an identified risk. When designing controls, it is necessary to consider all of the aspects in choices A through D. In an ideal situation, controls that address all of these aspects would be the best controls. Realistically, it may not be possible to design them all and the cost may be prohibitive; therefore, it is necessary to consider the controls related primarily to the treatment of existing risk in the organization.**
B. Controls will often affect productivity and performance; however, this must be balanced against the benefit obtained from the implementation of the control.
C. The most important reason for a control is to mitigate a risk—and the selection of a control is usually based on a cost-benefit analysis, not on selecting just the least expensive control.
D. A good control environment will include preventive, detective and corrective controls.

A3-29 Information for detecting unauthorized input from a user workstation would be **BEST** provided by the:

A. console log printout.
B. transaction journal.
C. automated suspense file listing.
D. user error report.

**B is the correct answer.**

**Justification:**

A. A console log printout is not the best because it does not record activity from a specific terminal.
B. **The transaction journal records all transaction activity, which then can be compared to the authorized source documents to identify any unauthorized input.**
C. An automated suspense file listing lists only transaction activity where an edit error occurred.
D. The user error report lists only input that resulted in an edit error and does not record improper user input.

A3-30 Which of the following has the **MOST** significant impact on the success of an application systems implementation?

A. The prototyping application development methodology
B. Compliance with applicable external requirements
C. The overall organizational environment
D. The software reengineering technique

**C is the correct answer.**

**Justification:**

A. The prototyping application development technique reduces the time to deploy systems primarily by using faster development tools that allow a user to see a high-level view of the workings of the proposed system within a short period of time. The use of any one development methodology will have a limited impact on the success of the project.
B. Compliance with applicable external requirements has an impact on the implementation success, but the impact is not as significant as the impact of the overall organizational environments.
C. **The overall organizational environment has the most significant impact on the success of applications systems implemented. This includes the alignment between IT and the business, the maturity of the development processes and the use of change control and other project management tools.**
D. The software reengineering technique is a process of updating an existing system by extracting and reusing design and program components. This is used to support major changes in the way an organization operates. Its impact on the success of the application systems that are implemented is small compared with the impact of the overall organizational environment.

A3-31 The editing/validation of data entered at a remote site is performed **MOST** effectively at the:

A. central processing site after running the application system.
B. central processing site during the running of the application system.
C. remote processing site after transmission of the data to the central processing site.
D. remote processing site prior to transmission of the data to the central processing site.

**D is the correct answer.**

**Justification:**

A. Validating data prior to transmission is the most efficient method and saves the effort of transmitting or processing invalid data. However, due to the risk of errors being introduced during transmission it is also good practice to re-validate the data at the central processing site.
B. Validating data prior to transmission is the most efficient method and saves the effort of transmitting or processing invalid data. However, due to the risk of errors being introduced during transmission it is also good practice to re-validate the data at the central processing site.
C. To validate the data after it has been transmitted is not a valid control.
D. **It is important that the data entered from a remote site is edited and validated prior to transmission to the central processing site.**

A3-32 The **MAJOR** consideration for an IS auditor reviewing an organization's IT project portfolio is the:

A. IT budget.
B. existing IT environment.
C. business plan.
D. investment plan.

**C is the correct answer.**

**Justification:**
A. The IT budget is important to ensure that the resources are being used in the best manner, but this is secondary to the importance of reviewing the business plan.
B. The existing IT environment is important and used to determine gap analysis but is secondary to the importance of reviewing the business plan.
**C. One of the most important reasons for which projects get funded is how well a project meets an organization's strategic objectives. Portfolio management takes a holistic view of a company's overall IT strategy. IT strategy should be aligned with the business strategy and, hence, reviewing the business plan should be the major consideration.**
D. The investment plan is important to set out project priorities, but secondary to the importance of reviewing the business plan.

A3-33 Regression testing is undertaken **PRIMARILY** to ensure that:

A. system functionality meets customer requirements.
B. a new system can operate in the target environment.
C. applicable development standards have been maintained.
D. applied changes have not introduced new errors.

**D is the correct answer.**

**Justification:**
A. Validation testing is used to test the functionality of the system against detailed requirements to ensure that software construction is traceable to customer requirements.
B. Sociability testing is used to see whether the system can operate in the target environment without adverse impacts on the existing systems.
C. Software quality assurance and code reviews are used to determine whether development standards are maintained.
**D. Regression testing is used to test for the introduction of new errors in the system after changes have been applied.**

A3-34 A proposed transaction processing application will have many data capture sources and outputs in paper and electronic form. To ensure that transactions are not lost during processing, an IS auditor should recommend the inclusion of:

A. validation controls.
B. internal credibility checks.
C. clerical control procedures.
D. automated systems balancing.

**D is the correct answer.**

**Justification:**

A. Input and output validation controls are certainly valid controls but will not detect and report lost transactions.
B. Internal credibility checks are valid controls to detect errors in processing but will not detect and report lost transactions.
C. A clerical procedure could be used to summarize and compare inputs and outputs; however, an automated process is less susceptible to error.
**D. Automated systems balancing would be the best way to ensure that no transactions are lost as any imbalance between total inputs and total outputs would be reported for investigation and correction.**

A3-35 Which of the following should be an IS auditor's **PRIMARY** concern after discovering that the scope of an IS project has changed, and an impact study has not been performed?

A. The time and cost implications caused by the change
B. The risk that regression tests will fail
C. Users not agreeing with the change
D. The project team not having the skills to make the necessary change

**A is the correct answer.**

**Justification:**

**A. Any scope change might have an impact on duration and cost of the project; that is the reason why an impact study is conducted, and the client is informed of the potential impact on the schedule and cost.**
B. A change in scope does not necessarily impact the risk that regression tests will fail.
C. An impact study will not determine whether users will agree with a change in scope.
D. Conducting an impact study could identify a lack of resources such as the project team lacking the skills necessary to make the change; however, this is only part of the impact on the overall time lines and cost to the project due to the change.

A3-36 An IS auditor is reviewing the software development capabilities of an organization that has adopted the agile methodology. The IS auditor would be the **MOST** concerned if:

A. certain project iterations produce proof-of-concept deliverables and unfinished code.
B. application features and development processes are not extensively documented.
C. software development teams continually re-plan each step of their major projects.
D. project managers do not manage project resources, leaving that to project team members.

**A is the correct answer.**

**Justification:**

A. **The agile software development methodology is an iterative process where each iteration or "sprint" produces functional code. If a development team was producing code for demonstration purposes, this would be an issue because the following iterations of the project build on the code developed in the prior sprint.**
B. One focus of agile methodology is to rely more on team knowledge and produce functional code quickly. These characteristics would result in less extensive documentation or documentation embedded in the code itself.
C. After each iteration or "sprint," agile development teams re-plan the project so that unfinished tasks are performed, and resources can be reallocated as needed. The continual re-planning is a key component of agile development methodology.
D. The management of agile software development is different from conventional development approaches in that leaders act as facilitators and allow team members to determine how to manage their own resources to get each sprint completed. Because the team members are performing the work, they are in a good position to understand how much time/effort is required to complete a sprint.

A3-37 Which of the following data validation edits is effective in detecting transposition and transcription errors?

A. Range check
B. Check digit
C. Validity check
D. Duplicate check

**B is the correct answer.**

**Justification:**

A. A range check is checking data that matches a predetermined range of allowable values.
B. **A check digit is a numeric value that is calculated mathematically and is appended to data to ensure that the original data have not been altered (e.g., an incorrect, but valid, value substituted for the original). This control is effective in detecting transposition and transcription errors.**
C. A validity check is programmed checking of the data validity in accordance with predetermined criteria.
D. In a duplicate check, new or fresh transactions are matched to those previously entered to ensure that they are not already in the system.

A3-38 Two months after a major application implementation, management, who assume that the project went well, requests that an IS auditor perform a review of the completed project. The IS auditor's **PRIMARY** focus should be to:

A. determine whether user feedback on the system has been documented.
B. assess whether the planned cost benefits are being measured, analyzed and reported.
C. review controls built into the system to assure that they are operating as designed.
D. review subsequent program change requests.

**C is the correct answer.**

**Justification:**

A. The IS auditor should check whether user feedback has been provided, but this is not the most important area for audit.
B. It is important to assess the effectiveness of the project; however, assuring that the production environment is adequately controlled after the implementation is of primary concern.
C. **Because management is assuming that the implementation went well, the primary focus of the IS auditor is to test the controls built into the application to assure that they are functioning as designed.**
D. Reviewing change requests may be a good idea, but this is more important if the application is perceived to have a problem.

A3-39 Which of the following types of risk could result from inadequate software project baselining?

A. Sign-off delays
B. Software integrity violations
C. Scope creep
D. Inadequate controls

**C is the correct answer.**

**Justification:**

A. Sign-off delays may occur due to inadequate software baselining; however, these are most likely caused by scope creep.
B. Software integrity violations can be caused by hardware or software failures, malicious intrusions or user errors. Software baselining does not help prevent software integrity violations.
C. **A software baseline is the cutoff point in the design and development of a system. Beyond this point, additional requirements or modifications to the scope must go through formal, strict procedures for approval based on a business cost-benefit analysis. Failure to adequately manage a system through baselining can result in uncontrolled changes in a project's scope and may incur time and budget overruns.**
D. Inadequate controls are most likely present in situations in which information security is not duly considered from the beginning of system development; they are not a risk that can be adequately addressed by software baselining.

A3-40 An organization implemented a distributed accounting system, and the IS auditor is conducting a postimplementation review to provide assurance of the data integrity controls. Which of the following choices should the auditor perform **FIRST**?

A. Review user access.
B. Evaluate the change request process.
C. Evaluate the reconciliation controls.
D. Review the data flow diagram.

**D is the correct answer.**

**Justification:**
A. The review of user access would be important; however, in terms of data integrity it would be better to review the data flow diagram.
B. The lack of an adequate change control process could impact the integrity of the data; however, the system should be documented first to determine whether the transactions flow to other systems.
C. Evaluating the reconciliation controls would help to ensure data integrity; however, it is more important to understand the data flows of the application to ensure that the reconciliation controls are located in the correct place.
**D. The IS auditor should review the application data flow diagram to understand the flow of data within the application and to other systems. This will enable the IS auditor to evaluate the design and effectiveness of the data integrity controls.**

A3-41 During the audit of an acquired software package, an IS auditor finds that the software purchase was based on information obtained through the Internet, rather than from responses to a request for proposal. The IS auditor should **FIRST**:

A. test the software for compatibility with existing hardware.
B. perform a gap analysis.
C. review the licensing policy.
D. ensure that the procedure had been approved.

**D is the correct answer.**

**Justification:**
A. Because the software package has already been acquired, it is most likely that it is in use and therefore compatible with existing hardware. Further, the first responsibility of the IS auditor is to ensure that the purchasing procedures have been approved.
B. Because there was no request for proposal, there may be no documentation of the expectations of the product and nothing to measure a gap against. The first task for the IS auditor is to ensure that the purchasing procedures were approved.
C. The licensing policy should be reviewed to ensure proper licensing but only after the purchasing procedures are checked.
**D. In the case of a deviation from the predefined procedures, an IS auditor should first ensure that the procedure followed for acquiring the software is consistent with the business objectives and has been approved by the appropriate authorities.**

A3-42 A failure discovered in which of the following testing stages would have the **GREATEST** impact on the implementation of new application software?

A. System testing
B. Acceptance testing
C. Integration testing
D. Unit testing

**B is the correct answer.**

**Justification:**

A. System testing is undertaken by the development team to determine if the combined units of software work together and that the software meets user requirements per specifications. A failure here would be expensive but easier to fix than a failure found later in the testing process.
**B. Acceptance testing is the final stage before the software is installed and is available for use. The greatest impact would occur if the software fails at the acceptance testing level because this could result in delays and cost overruns.**
C. Integration testing examines the units/modules as one integrated system and unit testing examines the individual units or components of the software. A failure here would be expensive and require re-work of the modules but would not be as expensive as a problem found just prior to implementation.
D. System, integration and unit testing are all performed by the developers at various stages of development; the impact of failure is comparatively less for each than failure at the acceptance testing stage.

A3-43 Which of the following is the **MOST** likely benefit of implementing a standardized infrastructure?

A. Improved cost-effectiveness of IT service delivery and operational support
B. Increased security of the IT service delivery center
C. Reduced level of investment in the IT infrastructure
D. Reduced need for testing future application changes

**A is the correct answer.**

**Justification:**

**A. A standardized IT infrastructure provides a consistent set of platforms and operating systems across the organization. This standardization reduces the time and effort required to manage a set of disparate platforms and operating systems. In addition, the implementation of enhanced operational support tools (e.g., password management tools, patch management tools and auto provisioning of user access) is simplified. These tools can help the organization reduce the cost of IT service delivery and operational support.**
B. A standardized infrastructure results in a more homogeneous environment, which is more prone to attacks.
C. While standardization can reduce support costs, the transition to a standardized kit can be expensive; therefore, the overall level of IT infrastructure investment is not likely to be reduced.
D. A standardized infrastructure may simplify testing of changes, but it does not reduce the need for such testing.

A3-44 Which of the following is the **MOST** important element in the design of a data warehouse?

A. Quality of the metadata
B. Speed of the transactions
C. Volatility of the data
D. Vulnerability of the system

**A is the correct answer.**

**Justification:**

A. **Quality of the metadata is the most important element in the design of a data warehouse. A data warehouse is a copy of transaction data specifically structured for query and analysis. Metadata describes the data in the warehouse and aims to provide a table of contents to the stored information. Companies that have built warehouses believe that metadata are the most important component of the warehouse.**
B. A data warehouse is used for analysis and research, not for production operations, so the speed of transactions is not relevant.
C. Data in a data warehouse is frequently received from many sources and vast amounts of information may be received on an hourly or daily basis. Except to ensure adequate storage capability, this is not a primary concern of the designer.
D. Data warehouses may contain sensitive information, or can be used to research sensitive information, so the security of the data warehouse is important. However, this is not the primary concern of the designer.

A3-45 Ideally, stress testing should be carried out in a:

A. test environment using test data.
B. production environment using live workloads.
C. test environment using live workloads.
D. production environment using test data.

**C is the correct answer.**

**Justification:**

A. A test environment should always be used to avoid damaging the production environment, but only testing with test data may not test all aspects of the system adequately.
B. Testing should never take place in a production environment.
C. **Stress testing is carried out to ensure that a system can cope with production workloads. Testing with production level workloads is important to ensure that the system will operate effectively when moved into production.**
D. It is not advisable to do stress testing in a production environment. Additionally, if only test data are used, there is no certainty that the system was stress tested adequately.

A3-46 Assignment of process ownership is essential in system development projects because it:

A. enables the tracking of the development completion percentage.
B. optimizes the design cost of user acceptance test cases.
C. minimizes the gaps between requirements and functionalities.
D. ensures that system design is based on business needs.

**D is the correct answer.**

**Justification:**

A. Process ownership assignment does not have a feature to track the completion percentage of deliverables.
B. Whether the design cost of test cases will be optimized is not determined from the assignment of process ownership. It may help to some extent; however, there are many other factors involved in the design of test cases.
C. For gap minimization, a specific requirements analysis framework should be in place and then applied; however, a gap may be found between the design and the as-built system that could lead to system functionality not meeting requirements. This will be identified during user acceptance testing. Process ownership alone does not have the capability to minimize requirement gaps.
**D. The involvement of process owners will ensure that the system will be designed according to the needs of the business processes that depend on system functionality. A sign-off on the design by the process owners is crucial before development begins.**

A3-47 The **BEST** time for an IS auditor to assess the control specifications of a new application software package which is being considered for acquisition is during:

A. the internal lab testing phase.
B. testing and prior to user acceptance.
C. the requirements gathering process.
D. the implementation phase.

**C is the correct answer.**

**Justification:**

A. During testing, the IS auditor will ensure that the security requirements are met. This is not the time to assess the control specifications.
B. The control specifications will drive the security requirements that are built into the contract and should be assessed before the product is acquired and tested.
**C. The best time for the involvement of an IS auditor is at the beginning of the requirements definition of the development or acquisition of applications software. This provides maximum opportunity for review of the vendors and their products. Early engagement of an IS auditor also minimizes the potential of a business commitment to a given solution that might be inadequate and more difficult to overcome as the process continues.**
D. During the implementation phase, the IS auditor may check whether the controls have been enabled; however, this is not the time to assess the control requirements.

A3-48 The phases and deliverables of a system development life cycle project should be determined:

A. during the initial planning stages of the project.
B. after early planning has been completed but before work has begun.
C. throughout the work stages, based on risk and exposures.
D. only after all risk and exposures have been identified and the IS auditor has recommended appropriate controls.

**A is the correct answer.**

**Justification:**

A. **It is extremely important that the project be planned properly, and that the specific phases and deliverables are identified during the early stages of the project. This enables project tracking and resource management.**
B. Determining the deliverables and time lines of a project are a part of the early project planning work.
C. The requirements may change over the life of a project, but the initial deliverables should be documented from the beginning of the project.
D. Risk management is a never-ending process, so project planning cannot wait until all risk has been identified.

A3-49 Management observed that the initial phase of a multiphase implementation was behind schedule and over budget. Prior to commencing with the next phase, an IS auditor's **PRIMARY** suggestion for a postimplementation focus should be to:

A. assess whether the planned cost benefits are being measured, analyzed and reported.
B. review control balances and verify that the system is processing data accurately.
C. review the impact of program changes made during the first phase on the remainder of the project.
D. determine whether the system's objectives were achieved.

**C is the correct answer.**

**Justification:**

A. While all choices are valid, the postimplementation focus and primary objective should be understanding the impact of the problems in the first phase on the remainder of the project.
B. The review should assess whether the control is working correctly but should focus on the problems that led to project overruns in budget and time.
C. **Because management is aware that the project had problems, reviewing the subsequent impact will provide insight into the types and potential causes of the project issues. This will help to identify whether IT has adequately planned for those issues in subsequent projects.**
D. Ensuring that the system works is a primary objective for the IS auditor, but in this case because the project planning was a failure, the IS auditor should focus on the reasons for, and impact of, the failure.

A3-50 When implementing an application software package, which of the following presents the **GREATEST** risk?

A. Uncontrolled multiple software versions
B. Source programs that are not synchronized with object code
C. Incorrectly set parameters
D. Programming errors

**C is the correct answer.**

**Justification:**

A. Having multiple versions is a problem, but as long as the correct version is implemented, the most serious risk during implementation is to have the parameters for the program set incorrectly.
B. Lack of synchronization between source and object code will be a serious risk for later maintenance of compiled programs, but this will not affect other types of programs and is not the most serious risk at the time of implementation.
**C. Parameters that are not set correctly would be the greatest concern when implementing an application software package. Incorrectly set parameters are an immediate problem that could lead to system breach, failure or noncompliance.**
D. Programming errors should be found during testing, not at the time of implementation.

A3-51 Which of the following is an advantage of prototyping?

A. The finished system normally has strong internal controls.
B. Prototype systems can provide significant time and cost savings.
C. Change control is often less complicated with prototype systems.
D. Prototyping ensures that functions or extras are not added to the intended system.

**B is the correct answer.**

**Justification:**

A. Prototyping often has poor internal controls because the focus is primarily on functionality, not on security.
**B. Prototype systems can provide significant time and cost savings through better user interaction and the ability to rapidly adapt to changing requirements; however, they also have several disadvantages, including loss of overall security focus, project oversight and implementation of a prototype that is not yet ready for production.**
C. Change control becomes much more complicated with prototyping.
D. Prototyping often leads to functions or extras being added to the system that were not originally intended.

A3-52 The **PRIMARY** objective of performing a postincident review is that it presents an opportunity to:

A. improve internal control procedures.
B. harden the network to industry good practices.
C. highlight the importance of incident response management to management.
D. improve employee awareness of the incident response process.

**A is the correct answer.**

**Justification:**

A. **A postincident review examines both the cause and response to an incident. The lessons learned from the review can be used to improve internal controls. Understanding the purpose and structure of postincident reviews and follow-up procedures enables the information security manager to continuously improve the security program. Improving the incident response plan based on the incident review is an internal (corrective) control.**
B. A postincident review may result in improvements to controls, but its primary purpose is not to harden a network.
C. The purpose of postincident review is to ensure that the opportunity is presented to learn lessons from the incident. It is not intended as a forum to educate management.
D. An incident may be used to emphasize the importance of incident response, but that is not the intention of the postincident review.

A3-53 An advantage of using sanitized live transactions in test data is that:

A. all transaction types will be included.
B. every error condition is likely to be tested.
C. no special routines are required to assess the results.
D. test transactions are representative of live processing.

**D is the correct answer.**

**Justification:**

A. Sanitized production data may not contain all transaction types. The test data may need to be modified to ensure that all data types are represented.
B. Not all error types are sure to be tested because most production data will only contain certain types of errors.
C. The results can be tested using normal routines, but that is not a significant advantage of using sanitized live data.
D. **Test data will be representative of live processing; however, it is important that all sensitive information in the live transaction file is sanitized to prevent improper data disclosure.**

A3-54 An IS auditor's **PRIMARY** concern when application developers wish to use a copy of yesterday's production transaction file for volume tests is that:

A. users may prefer to use contrived data for testing.
B. unauthorized access to sensitive data may result.
C. error handling and credibility checks may not be fully proven.
D. the full functionality of the new process may not necessarily be tested.

**B is the correct answer.**

**Justification:**
A. Production data are easier for users to use for comparison purposes.
**B. Unless the data are sanitized, there is a risk of disclosing sensitive data.**
C. There is a risk that former production data may not test all error routines; however, this is not as serious as the risk of release of sensitive data.
D. Using a copy of production data may not test all functionality, but this is not as serious as the risk of disclosure of sensitive data.

A3-55 Which of the following is the **PRIMARY** purpose for conducting parallel testing?

A. To determine whether the system is cost-effective
B. To enable comprehensive unit and system testing
C. To highlight errors in the program interfaces with files
D. To ensure the new system meets user requirements

**D is the correct answer.**

**Justification:**
A. Parallel testing may show that the old system is, in fact, more cost-effective than the new system, but this is not the primary reason for parallel testing.
B. Unit and system testing are completed before parallel testing.
C. Program interfaces with files are tested for errors during system testing.
**D. The purpose of parallel testing is to ensure that the implementation of a new system will meet user requirements by comparing the results of the old system with the new system to ensure correct processing.**

A3-56 The knowledge base of an expert system that uses questionnaires to lead the user through a series of choices before a conclusion is reached is known as:

A. rules.
B. decision trees.
C. semantic nets.
D. dataflow diagrams.

**B is the correct answer.**

**Justification:**
A. Rules refer to the expression of declarative knowledge through the use of if-then relationships.
**B. Decision trees use questionnaires to lead a user through a series of choices until a conclusion is reached.**
C. Semantic nets consist of a graph in which nodes represent physical or conceptual objects and the arcs describe the relationship between the nodes.
D. A dataflow diagram is used to map the progress of data through a system and examine logic, error handling and data management.

A3-57 An advantage in using a bottom-up versus a top-down approach to software testing is that:

A. interface errors are detected earlier.
B. confidence in the system is achieved earlier.
C. errors in critical modules are detected earlier.
D. major functions and processing are tested earlier.

**C is the correct answer.**

**Justification:**
A. Interface errors will not be found until later in the testing process—as a result of integration or system testing.
B. Confidence in the system cannot be obtained until the testing is completed.
C. **The bottom-up approach to software testing begins with the testing of atomic units, such as programs and modules, and works upward until a complete system testing has taken place. The advantages of using a bottom-up approach to software testing are the fact that errors in critical modules are found earlier.**
D. Bottom-up testing tests individual components and major functions and processing will not be adequately tested until systems and integration testing is completed.

A3-58 During which of the following phases in system development would user acceptance test plans normally be prepared?

A. Feasibility study
B. Requirements definition
C. Implementation planning
D. Post-implementation review

**B is the correct answer.**

**Justification:**
A. The feasibility study is too early for such detailed user involvement.
B. **During requirements definition, the project team will be working with the users to define their precise objectives and functional needs. At this time, the users should be working with the team to consider and document how the system functionality can be tested to ensure that it meets their stated needs. An IS auditor should know at what point user testing should be planned to ensure that it is most effective and efficient.**
C. The implementation planning phase is when the tests are conducted. It is too late in the process to develop the test plan.
D. User acceptance testing should be completed prior to implementation.

A3-59 The use of object-oriented design and development techniques would **MOST** likely:

A. facilitate the ability to reuse modules.
B. improve system performance.
C. enhance control effectiveness.
D. speed up the system development life cycle.

**A is the correct answer.**

**Justification:**
**A. One of the major benefits of object-oriented design and development is the ability to reuse modules.**
B. Object-oriented design is not intended as a method of improving system performance.
C. Control effectiveness is not an objective of object-oriented design and control effectiveness may, in fact, be reduced through this approach.
D. The use of object-oriented design may speed up the system development life cycle (SDLC) for future projects through the reuse of modules, but it will not speed up development of the initial project.

A3-60 Which of the following should be included in a feasibility study for a project to implement an electronic data interchange process?

A. The encryption algorithm format
B. The detailed internal control procedures
C. The necessary communication protocols
D. The proposed trusted third-party agreement

**C is the correct answer.**

**Justification:**
A. Encryption algorithms are too detailed for this phase. They would only be outlined, and any cost or performance implications shown.
B. Internal control procedures are too detailed for this phase. They would only be outlined, and any cost or performance implications shown.
**C. The communications protocols must be included because there may be significant cost implications if new hardware and software are involved, and risk implications if the technology is new to the organization.**
D. Third-party agreements are too detailed for this phase. They would only be outlined, and any cost or performance implications shown.

A3-61 When a new system is to be implemented within a short time frame, it is **MOST** important to:

A. finish writing user manuals.
B. perform user acceptance testing.
C. add last-minute enhancements to functionalities.
D. ensure that the code has been documented and reviewed.

**B is the correct answer.**

**Justification:**
A. The completion of the user manuals is less important than the need to test the system adequately.
**B. It would be most important to complete the user acceptance testing to ensure that the system to be implemented is working correctly.**
C. If time is tight, the last thing one would want to do is add another enhancement because it would be necessary to freeze the code and complete the testing, then make any other changes as future enhancements.
D. It would be appropriate to have the code documented and reviewed, but unless the acceptance testing is completed, there is no guarantee that the system will work correctly and meet user requirements.

A3-62 Once an organization has finished the business process reengineering (BPR) of all its critical operations, an IS auditor would **MOST** likely focus on a review of:

A. pre-BPR process flowcharts.
B. post-BPR process flowcharts.
C. BPR project plans.
D. continuous improvement and monitoring plans.

**B is the correct answer.**

**Justification:**
A. An IS auditor must review the process as it is today, not as it was in the past.
**B. An IS auditor's task is to identify and ensure that key controls have been incorporated into the reengineered process.**
C. Business process reengineering (BPR) project plans are a step within a BPR project.
D. Continuous improvement and monitoring plans are steps within a BPR project.

A3-63 An IS auditor finds that a system under development has 12 linked modules and each item of data can carry up to 10 definable attribute fields. The system handles several million transactions a year. Which of these techniques could an IS auditor use to estimate the size of the development effort?

A. Program evaluation review technique
B. Function point analysis
C. Counting source lines of code
D. White box testing

**B is the correct answer.**

**Justification:**
A. Program evaluation review technique is a project management technique used in the planning and control of system projects.
**B. Function point analysis is a technique used to determine the size of a development task based on the number of function points. Function points are factors such as inputs, outputs, inquiries and logical internal sites.**
C. The number of source lines of code gives a direct measure of program size, but it does not allow for the complexity that may be caused by having multiple, linked modules and a variety of inputs and outputs.
D. White box testing involves a detailed review of the behavior of program code. It is a quality assurance technique suited to simpler applications during the design and building stage of development.

A3-64 A company has contracted with an external consulting firm to implement a commercial financial system to replace its existing system developed in-house. In reviewing the proposed development approach, which of the following would be of **GREATEST** concern?

A. Acceptance testing is to be managed by users.
B. A quality plan is not part of the contracted deliverables.
C. Not all business functions will be available on initial implementation.
D. Prototyping is being used to confirm that the system meets business requirements.

**B is the correct answer.**

**Justification:**
A. Acceptance is normally managed by the user area because users must be satisfied that the new system will meet their requirements.
**B. A quality plan is an essential element of all projects. It is critical that the contracted supplier be required to produce such a plan. The quality plan for the proposed development contract should be comprehensive and encompass all phases of the development and include which business functions will be included and when.**
C. If the system is large, a phased-in approach to implementing the application is a reasonable approach.
D. Prototyping is a valid method of ensuring that the system will meet business requirements.

A3-65 When preparing a business case to support the need of an electronic data warehouse solution, which of the following choices is the **MOST** important to assist management in the decision-making process?

A. Discuss a single solution.
B. Consider security controls.
C. Demonstrate feasibility.
D. Consult the audit department.

**C is the correct answer.**

**Justification:**
A. A business case should discuss all possible solutions to a given problem, which would enable management to select the best option. This may include the option not to undertake the project.
B. It may be important to include security considerations in the business case if security is important to the solution and will address the problem; however, the feasibility study is more important and is necessary regardless of the type of problem.
**C. The business case should demonstrate feasibility for any potential project. By including a feasibility study in the business case along with a cost-benefit analysis, management can make an informed decision.**
D. While the person preparing the business case may consult with the organization's audit department, this would be situational and is not necessary to include in the business case.

A3-66 Functionality is a characteristic associated with evaluating the quality of software products throughout their life cycle, and is **BEST** described as the set of attributes that bear on the:

A. existence of a set of functions and their specified properties.
B. ability of the software to be transferred from one environment to another.
C. capability of software to maintain its level of performance under stated conditions.
D. relationship between the performance of the software and the amount of resources used.

**A is the correct answer.**

**Justification:**
A. **Functionality is the set of attributes that bears on the existence of a set of functions and their specified properties. The functionality of a system represents the tasks, operations and purpose of the system in achieving its objective (i.e., supporting a business requirement).**
B. The ability of the software to be transferred from one environment to another refers to portability.
C. The capability of software to maintain its level of performance under stated conditions refers to reliability.
D. The relationship between the performance of the software and the amount of resources used refers to efficiency.

A3-67 During the development of an application, quality assurance testing and user acceptance testing were combined. The **MAJOR** concern for an IS auditor reviewing the project is that there will be:

A. increased maintenance.
B. improper documentation of testing.
C. improper acceptance of a program.
D. delays in problem resolution.

**C is the correct answer.**

**Justification:**
A. The method of testing used will not affect the maintenance of the system.
B. Quality assurance and user acceptance testing are often led by business representatives according to a defined test plan. The combination of these two tests will not affect documentation.
C. **The major risk of combining quality assurance testing and user acceptance testing is that the users may apply pressure to accept a program that meets their needs even though it does not meet quality assurance standards.**
D. The method of testing should not affect the time lines for problem resolution.

A3-68 The **GREATEST** advantage of rapid application development over the traditional system development life cycle is that it:

A. facilitates user involvement.
B. allows early testing of technical features.
C. facilitates conversion to the new system.
D. shortens the development time frame.

**D is the correct answer.**

**Justification:**
A. Rapid application development (RAD) emphasizes greater user involvement to ensure that the system meets user requirements; however, its primary objective is to speed up development.
B. RAD does allow early testing, but this is also true for the traditional system development life cycle models.
C. RAD does not facilitate conversion to a new system.
D. **The greatest advantage and core objective of RAD is a shorter time frame for the development of a system.**

A3-69 An IS auditor reviewing a proposed application software acquisition should ensure that the:

A. operating system (OS) being used is compatible with the existing hardware platform.
B. planned OS updates have been scheduled to minimize negative impacts on company needs.
C. OS has the latest versions and updates.
D. product is compatible with the current or planned OS.

**D is the correct answer.**

**Justification:**

A. If the operating system (OS) is currently being used, it is compatible with the existing hardware platform; if it were incompatible, it would not operate properly.
B. The planned OS updates should be scheduled to minimize negative impacts on the organization, but this is not an issue when considering the acquisition of new software.
C. The installed OS should be equipped with the most recent versions and updates (with sufficient history and stability). Because this is installed, it is not a consideration at the time of considering acquisition of a new application.
**D. In reviewing the proposed application, the auditor should ensure that the products to be purchased are compatible with the current or planned OS.**

A3-70 Which of the following is of **GREATEST** concern to an IS auditor when performing an audit of a client relationship management system migration project?

A. The technical migration is planned for a Friday preceding a long weekend, and the time window is too short for completing all tasks.
B. Employees pilot-testing the system are concerned that the data representation in the new system is completely different from the old system.
C. A single implementation is planned, immediately decommissioning the legacy system.
D. Five weeks prior to the target date, there are still numerous defects in the printing functionality of the new system's software.

**C is the correct answer.**

**Justification:**

A. A weekend can be used as a time buffer so that the new system will have a better chance of being up and running after the weekend.
B. A different data representation does not mean different data presentation at the front end. Even when this is the case, this issue can be solved by adequate training and user support.
**C. Major system migrations should include a phase of parallel operation or a phased cut-over to reduce implementation risk. Decommissioning or disposing of the old hardware would complicate any fallback strategy, should the new system not operate correctly.**
D. The printing functionality is commonly one of the last functions to be tested in a new system because it is usually the last step performed in any business event. Thus, meaningful testing and the respective error fixing are only possible after all other parts of the software have been successfully tested.

A3-71 Which of the following types of testing would determine whether a new or modified system can operate in its target environment without adversely impacting other existing systems?

A. Parallel testing
B. Pilot testing
C. Interface/integration testing
D. Sociability testing

**D is the correct answer.**

**Justification:**

A. Parallel testing is the process of feeding data into two systems—the modified system and an alternate system—and comparing the results. In this approach, the old and new systems operate concurrently for a period of time and perform the same processing functions. This allows a new system to be tested without affecting existing systems.
B. Pilot testing takes place first at one location and is then extended to other locations. The purpose is to see if the new system operates satisfactorily in one place before implementing it at other locations. In most cases the cutover to the new system will disable existing systems.
C. Interface/integration testing is a hardware or software test that evaluates the connection of two or more components that pass information from one area to another. The objective is to take unit-tested modules and build an integrated structure. This will not test in a true production environment.
**D. The purpose of sociability testing is to confirm that a new or modified system can operate in its target environment without adversely impacting existing systems. This should cover the platform that will perform primary application processing and interfaces with other systems, as well as changes to the desktop in a client-server or web development.**

A3-72 At the end of the testing phase of software development, an IS auditor observes that an intermittent software error has not been corrected. No action has been taken to resolve the error. The IS auditor should:

A. report the error as a finding and leave further exploration to the auditee's discretion.
B. attempt to resolve the error.
C. recommend that problem resolution be escalated.
D. ignore the error because it is not possible to get objective evidence for the software error.

**C is the correct answer.**

**Justification:**

A. Recording it as a minor error and leaving it to the auditee's discretion would be inappropriate. Action should be taken before the application goes into production.
B. The IS auditor is not authorized to resolve the error.
**C. When an IS auditor observes such conditions, it is best to fully apprise the auditee and suggest that further problem resolutions be attempted including escalation if necessary.**
D. Neglecting the error would indicate that the IS auditor has not taken steps to further probe the issue to its logical end.

A3-73 Which of the following is the **GREATEST** risk to the effectiveness of application system controls?

A. Removal of manual processing steps
B. Inadequate procedure manuals
C. Collusion between employees
D. Unresolved regulatory compliance issues

**C is the correct answer.**

**Justification:**

A. Automation should remove manual processing steps wherever possible. The only risk would be the removal of manual security controls without replacement with automated controls.
B. The lack of documentation is a problem on many systems but not a serious risk in most cases.
C. **Collusion is an active attack where users collaborate to bypass controls such as separation of duties. Such breaches may be difficult to identify because even well-thought-out application controls may be circumvented.**
D. Unregulated compliance issues are a risk but do not measure the effectiveness of the controls.

A3-74 An organization is implementing a new system to replace a legacy system. Which of the following conversion practices creates the **GREATEST** risk?

A. Pilot
B. Parallel
C. Direct cutover
D. Phased

**C is the correct answer.**

**Justification:**

A. All other alternatives are done gradually and, thus, provide greater recoverability and are less risky. A pilot implementation is the implementation of the system at a single location or region and then a rollout of the system to the rest of the organization after the application and implementation plan have been proven to work correctly at the pilot location.
B. A parallel test requires running both the old and new system in parallel for a time period. This would highlight any problems or inconsistencies between the old and new systems.
C. **Direct cutover implies switching to the new system immediately, usually without the ability to revert to the old system in the event of problems. This is the riskiest approach and may cause a significant impact on the organization.**
D. A phased approach is used to implement the system in phases or sections—this minimizes the overall risk by only affecting one area at a time.

A3-75 During the requirements definition stage of a proposed enterprise resource planning system, the project sponsor requests that the procurement and accounts payable modules be linked. Which of the following test methods would be the **BEST** to perform?

A. Unit testing
B. Integration testing
C. Sociability testing
D. Quality assurance testing

**B is the correct answer.**

**Justification:**

A. Unit testing is a technique that is used to test program logic within a particular program or module and does not specifically address the linkage between software modules. Integration testing is the best answer.
**B. Integration testing is a hardware or software test that evaluates the connection of two or more components that pass information from one area to another. The objective is to take unit-tested modules and build an integrated structure dictated by design.**
C. Sociability testing confirms that the new or modified system can operate in its target environment without adversely impacting existing systems and does not specifically address the linkage between software modules. Integration testing is the best answer.
D. Quality assurance testing is primarily used to ensure that the logic of the application is correct and does not specifically address the linkage between software modules. Integration testing is the best answer.

A3-76 During a post-implementation review of an enterprise resource management system, an IS auditor would **MOST** likely:

A. review access control configuration.
B. evaluate interface testing.
C. review detailed design documentation.
D. evaluate system testing.

**A is the correct answer.**

**Justification:**

**A. Reviewing access control configuration would be the first task performed to determine whether security has been appropriately mapped in the system.**
B. Because a post-implementation review is done after user acceptance testing and actual implementation, one would not engage in interface testing or detailed design documentation. Evaluating interface testing would be part of the implementation process.
C. The issue of reviewing detailed design documentation is not generally relevant to an enterprise resource management system because these are usually vendor packages with user manuals. Further, because the system has been implemented, the IS auditor would only check the detailed design if there appeared to be a gap between design and functionality.
D. System testing should be performed before final user signoff. The IS auditor should not need to review the system tests post-implementation.

A3-77 An organization recently deployed a customer relationship management application that was developed in-house. Which of the following is the **BEST** option to ensure that the application operates as designed?

A. User acceptance testing
B. Project risk assessment
C. Post-implementation review
D. Management approval of the system

**C is the correct answer.**

**Justification:**

A. User acceptance testing (UAT) verifies that the system functionality has been deemed acceptable by the end users of the system; however, a review of UAT will not validate whether the system is performing as designed because UAT would be performed on a subset of system functionality. The UAT review is a part of the post-implementation review.
B. While a risk assessment would highlight the risk of the system, it would not include an analysis to verify that the system is operating as designed.
**C. The purpose of a post-implementation review is to evaluate how successfully the project results match original goals, objectives and deliverables. The post-implementation review also evaluates how effective the project management practices were in keeping the project on track.**
D. Management approval of the system could be based on reduced functionality and does not verify that the system is operating as designed. Management approval is a part of post-implementation review.

A3-78 In an online transaction processing system, data integrity is maintained by ensuring that a transaction is either completed in its entirety or not at all. This principle of data integrity is known as:

A. isolation.
B. consistency.
C. atomicity.
D. durability.

**C is the correct answer.**

**Justification:**

A. Isolation ensures that each transaction is isolated from other transactions; hence, each transaction can only access data if it is not being simultaneously accessed or modified by another process.
B. Consistency ensures that all integrity conditions in the database are maintained with each transaction.
**C. The principle of atomicity requires that a transaction be completed in its entirety or not at all. If an error or interruption occurs, all changes made up to that point are backed out.**
D. Durability ensures that, when a transaction has been reported back to a user as complete, the resultant changes to the database will survive subsequent hardware or software failures.

A3-79 A company undertakes a business process reengineering project in support of a new and direct marketing approach to its customers. Which of the following would be an IS auditor's main concern about the new process?

A. Whether key controls are in place to protect assets and information resources
B. Whether the system addresses corporate customer requirements
C. Whether the system can meet the performance goals
D. Whether the new system will support separation of duties

**A is the correct answer.**

**Justification:**

A. **The audit team must advocate the inclusion of the key controls and verify that the controls are in place before implementing the new process.**
B. The system must meet the requirements of all customers not just corporate customers. This is not the IS auditor's main concern.
C. The system must meet performance requirements, but this is of secondary concern to the need to ensure that key controls are in place.
D. Separation of duties is a key control—but only one of the controls that should be in place to protect the assets of the organization.

A3-80 A company has implemented a new client-server enterprise resource planning (ERP) system. Local branches transmit customer orders to a central manufacturing facility. Which of the following would **BEST** ensure that the orders are processed accurately, and the corresponding products are produced?

A. Verifying production of customer orders
B. Logging all customer orders in the ERP system
C. Using hash totals in the order transmitting process
D. Approving (production supervisor) orders prior to production

**A is the correct answer.**

**Justification:**

A. **Verification of the products produced will ensure that the produced products match the orders in the order system.**
B. Logging can be used to detect inaccuracies but does not, in itself, guarantee accurate processing.
C. Hash totals will ensure accurate order transmission, but not accurate processing centrally.
D. Production supervisory approval is a time consuming, manual process that does not guarantee proper control.

A3-81 When two or more systems are integrated, the IS auditor must review input/output controls in the:

A. Systems receiving the output of other systems.
B. Systems sending output to other systems.
C. Systems sending and receiving data.
D. Interfaces between the two systems.

**C is the correct answer.**

**Justification:**

A. A responsible control is to protect downstream systems from contamination from an upstream system. This requires a system that sends data to review its output and the receiving system to review its input.
B. Systems sending data to other systems should ensure that the data they send are correct, but that would not protect the receiving system from transmission errors.
**C. Both of the systems must be reviewed for input/output controls because the output for one system is the input for the other.**
D. The interfaces must be set up correctly and provide error controls, but good practice is to review the data before sending and after receipt.

A3-82 An IS auditor recommends that an initial validation control be programmed into a credit card transaction capture application. The initial validation process would **MOST** likely:

A. check to ensure that the type of transaction is valid for the card type.
B. verify the format of the number entered, then locate it on the database.
C. ensure that the transaction entered is within the cardholder's credit limit.
D. confirm that the card is not shown as lost or stolen on the master file.

**B is the correct answer.**

**Justification:**

A. The initial validation would not be used to check the transaction type—just the validity of the card number.
**B. The initial validation should confirm whether the card is valid. This validity is established through the card number and personal identification number entered by the user.**
C. The initial validation is to prove the card number entered is valid—only then can the transaction amount be checked for approval from the bank.
D. The verification that the card has not been reported as lost or stolen is only done after the card number has been validated as correctly entered.

A3-83 A small company cannot segregate duties between its development processes and its change control function. What is the **BEST** way to ensure that the tested code that is moved into production is the same?

A. Release management software
B. Manual code comparison
C. Regression testing in preproduction
D. Management approval of changes

**A is the correct answer.**

**Justification:**

A. **Automated release management software can prevent unauthorized changes by moving code into production without any manual intervention.**
B. Manual code comparison can detect whether the wrong code has been moved into production; however, code comparison does not prevent the code from being migrated and is not as good a control as using release management software. In addition, manual code comparison is not always efficient and requires highly skilled personnel.
C. Regression testing ensures that changes do not break the current system functionality or unwittingly overwrite previous changes. Regression testing does not prevent untested code from moving into production.
D. Although management should approve every change to production, approvals do not prevent untested code from being migrated into the production environment.

A3-84 Which of the following will **BEST** ensure the successful offshore development of business applications?

A. Stringent contract management practices
B. Detailed and correctly applied specifications
C. Awareness of cultural and political differences
D. Post-implementation review

**B is the correct answer.**

**Justification:**

A. Contract management practices, although important, will not ensure successful development if the specifications are incorrect.
B. **When dealing with offshore operations, it is essential that detailed specifications be created. Language differences and a lack of interaction between developers and physically remote end users could create gaps in communication in which assumptions and modifications may not be adequately communicated. Inaccurate specifications cannot easily be corrected.**
C. Cultural and political differences, although important, should not affect the delivery of a good product.
D. Post-implementation review, although important, is too late in the process to ensure successful project delivery and is not as pivotal to the success of the project.

A3-85 When planning to add personnel to tasks imposing time constraints on the duration of a project, which of the following should be revalidated **FIRST**?

A. The project budget
B. The critical path for the project
C. The length of the remaining tasks
D. The personnel assigned to other tasks

**B is the correct answer.**

**Justification:**

A. Given that there may be slack time available on some of the other tasks not on the critical path, the resource allocation should be based on the project segments that affect delivery dates.
**B. Adding resources may change the route of the critical path, the critical path must be reevaluated to ensure that additional resources will, in fact, shorten the project duration.**
C. Given that there may be slack time available on some of the other tasks not on the critical path, a factor such as the length of other tasks may or may not be affected.
D. Depending on the skill level of the resources required or available, the addition of resources may not, in fact, shorten the time line. Therefore, the first step is to examine what resources are required to address the times on the critical path.

A3-86 When reviewing a project where quality is a major concern, an IS auditor should use the project management triangle to explain that:

A. Increases in quality can be achieved, if resource allocation is decreased.
B. Increases in quality are only achieved if resource allocation is increased.
C. Decreases in delivery time can be achieved, if resource allocation is decreased.
D. Decreases in delivery time can only be achieved if quality is decreased.

**A is the correct answer.**

**Justification:**

**A. The three primary dimensions of a project are determined by the deliverables, the allocated resources and the delivery time. The area of the project management triangle, comprised of these three dimensions, is fixed. Depending on the degree of freedom, changes in one dimension might be compensated by changing either one or both remaining dimensions. Thus, if resource allocation is decreased, an increase in quality can be achieved if a delay in the delivery time of the project will be accepted. The area of the triangle always remains constant.**
B. Increases in quality can be achieved if resource allocation is increased or through increases in delivery time, not only through increases in resource allocation.
C. A decrease in both delivery time and resource allocation would mean that quality would have to decrease.
D. A decrease in delivery time may also be addressed through an increase in resource allocation, even if the quality remains constant.

A3-87 Which of the following is a characteristic of timebox management?

A. Not suitable for prototyping or rapid application development
B. Eliminates the need for a quality process
C. Prevents cost overruns and delivery delays
D. Separates system and user acceptance testing

**C is the correct answer.**

**Justification:**

A. Timebox management is very suitable for prototyping and rapid application development.
B. Timebox management does not eliminate the need for a quality process.
C. **Timebox management, by its nature, sets specific time and cost boundaries. It is effective in controlling costs and delivery time lines by ensuring that each segment of the project is divided into small controllable time frames.**
D. Timebox management integrates system and user acceptance testing.

A3-88 The waterfall life cycle model of software development is **MOST** appropriately used when:

A. requirements are well understood and are expected to remain stable, as is the business environment in which the system will operate.
B. requirements are well understood and the project is subject to time pressures.
C. the project intends to apply an object-oriented design and programming approach.
D. the project will involve the use of new technology.

**A is the correct answer.**

**Justification:**

A. **Historically, the waterfall model has been best suited to stable conditions and well-defined requirements.**
B. When the degree of uncertainty of the system to be delivered and the conditions in which it will be used rises, the waterfall model has not been successful. In these circumstances, the various forms of iterative development life cycle gives the advantage of breaking down the scope of the overall system to be delivered, making the requirements gathering and design activities more manageable. The ability to deliver working software earlier also acts to alleviate uncertainty and may allow an earlier realization of benefits.
C. The choice of a design and programming approach is not, itself, a determining factor of the type of software development life cycle that is appropriate.
D. The use of new technology in a project introduces a significant element of risk. An iterative form of development, particularly one of the agile or exploratory methods that focuses on early development of actual working software, is likely to be the better option to manage this uncertainty.

A3-89 Which of the following is **MOST** critical when creating data for testing the logic in a new or modified application system?

A. A sufficient quantity of data for each test case
B. Data representing conditions that are expected in actual processing
C. Completing the test on schedule
D. A random sample of actual data

**B is the correct answer.**

**Justification:**

A. The quantity of data for each test case is not as important as having test cases that will address all types of operating conditions.
**B. Selecting the right kind of data is key in testing a computer system. The data should not only include valid and invalid data but should be representative of actual processing; quality is more important than quantity.**
C. It is more important to have adequate test data than to complete the testing on schedule.
D. It is unlikely that a random sample of actual data would cover all test conditions and provide a reasonable representation of actual data.

A3-90 Which of the following should an IS auditor review to gain an understanding of the effectiveness of controls over the management of multiple projects?

A. Project database
B. Policy documents
C. Project portfolio database
D. Program organization

**C is the correct answer.**

**Justification:**

A. A project database may contain the information about control effectiveness for one specific project and updates to various parameters pertaining to the current status of that single project.
B. Policy documents on project management set direction for the design, development, implementation and monitoring of the project.
**C. A project portfolio database is the basis for project portfolio management. It includes project data such as owner, schedules, objectives, project type, status and cost. Project portfolio management requires specific project portfolio reports.**
D. Program organization is the team required (steering committee, quality assurance, systems personnel, analyst, programmer, hardware support, etc.) to meet the delivery objectives of the projects.

A3-91 Documentation of a business case used in an IT development project should be retained until:

A. the end of the system's life cycle.
B. the project is approved.
C. user acceptance of the system.
D. the system is in production.

**A is the correct answer.**

**Justification:**

A. **A business case can and should be used throughout the life cycle of the product. It serves as an anchor for new (management) personnel, helps to maintain focus and provides valuable information on estimates versus actuals. Questions such as "Why do we do that?", "What was the original intent?" and "How did we perform against the plan?" can be answered, and lessons for developing future business cases can be learned.**
B. The business case should be retained even after project approval to provide ability to review and validate the business case once the project is implemented.
C. The business case will be retained throughout the system development life cycle for later reference and validation.
D. Once the system is in production, the business case can be validated to ensure that the promised costs and benefits were correct.

A3-92 During the review of a web-based software development project, an IS auditor realizes that coding standards are not enforced, and code reviews are rarely carried out. This will **MOST** likely increase the likelihood of a successful:

A. Buffer overflow.
B. Brute force attack.
C. Distributed denial-of-service attack.
D. War dialing attack.

**A is the correct answer.**

**Justification:**

A. **Poorly written code, especially in web-based applications, is often exploited by hackers using buffer overflow techniques.**
B. A brute force attack is used to crack passwords, but this is not related to coding standards.
C. A distributed denial-of-service attack floods its target with numerous packets, to prevent it from responding to legitimate requests. This is not related to coding standards.
D. War dialing uses modem-scanning tools to hack private branch exchanges or other telecommunications services.

A3-93 Which testing approach is **MOST** appropriate to ensure that internal application interface errors are identified as soon as possible?

A. Bottom-up testing
B. Sociability testing
C. Top-down testing
D. System testing

**C is the correct answer.**

**Justification:**
A. A bottom-up approach to testing begins with atomic units, such as programs and modules, and works upward until a complete system test has taken place.
B. Sociability testing takes place at a later stage in the development process.
C. **The top-down approach to testing ensures that interface errors are detected early and that testing of major functions is conducted early.**
D. System tests take place at a later stage in the development process.

A3-94 When reviewing input controls, an IS auditor observes that, in accordance with corporate policy, procedures allow supervisory override of data validation edits. The IS auditor should:

A. not be concerned because there may be other compensating controls to mitigate the risk.
B. ensure that overrides are automatically logged and subject to review.
C. verify whether all such overrides are referred to senior management for approval.
D. recommend that overrides not be permitted.

**B is the correct answer.**

**Justification:**
A. An IS auditor should not assume that compensating controls exist.
B. **If input procedures allow overrides of data validation and editing, automatic logging should occur. A management individual who did not initiate the override should review this log.**
C. The log may be reviewed by another manager but does not require senior management approval.
D. As long as the overrides are policy-compliant, there is no need for senior management approval or a blanket prohibition.

A3-95 To minimize the cost of a software project, quality management techniques should be applied:

A. as close to their writing (i.e., point of origination) as possible.
B. primarily at project start to ensure that the project is established in accordance with organizational governance standards.
C. continuously throughout the project with an emphasis on finding and fixing defects primarily through testing to maximize the defect detection rate.
D. mainly at project close-down to capture lessons learned that can be applied to future projects.

**C is the correct answer.**

**Justification:**

A. Quality assurance (QA) should start as early as possible but continue through the entire development process.
B. Only performing QA during the start of the project will not detect problems that appear later in the development cycle.
C. **Although it is important to properly establish a software development project, quality management should be effectively practiced throughout the project. The major source of unexpected costs on most software projects is rework. The general rule is that the earlier in the development life cycle that a defect occurs, and the longer it takes to find and fix that defect, the more effort will be needed to correct it. A well-written quality management plan is a good start, but it must also be actively applied. Simply relying on testing to identify defects is a relatively costly and less effective way of achieving software quality. For example, an error in requirements discovered in the testing phase can result in scrapping significant amounts of work.**
D. Capturing lessons learned will be too late for the current project. Additionally, applying quality management techniques throughout a project is likely to yield its own insights into the causes of quality problems and assist in staff development.

A3-96 When identifying an earlier project completion time, which is to be obtained by paying a premium for early completion, the activities that should be selected are those:

A. whose sum of activity time is the shortest.
B. that have zero slack time.
C. that give the longest possible completion time.
D. whose sum of slack time is the shortest.

**B is the correct answer.**

**Justification:**

A. Attention should focus on the tasks within the critical path that have no slack time.
B. **A critical path's activity time is longer than that for any other path through the network. This path is important because if everything goes as scheduled, its length gives the shortest possible completion time for the overall project. Activities on the critical path become candidates for crashing (i.e., for reduction in their time by payment of a premium for early completion). Activities on the critical path have zero slack time and conversely, activities with zero slack time are on a critical path. By successively relaxing activities on a critical path, a curve showing total project costs versus time can be obtained.**
C. The critical path is the longest time length of the activities but is not based on the longest time of any individual activity.
D. A task on the critical path has no slack time.

A3-97 An IS auditor is assigned to audit a software development project, which is more than 80 percent complete, but has already overrun time by 10 percent and costs by 25 percent. Which of the following actions should the IS auditor take?

A. Report that the organization does not have effective project management
B. Recommend the project manager be changed
C. Review the IT governance structure
D. Review the business case and project management

**D is the correct answer.**

**Justification:**

A. The organization may have effective project management practices and still be behind schedule or over budget.
B. There is no indication that the project manager should be changed without looking into the reasons for the overrun.
C. The organization may have sound IT governance and still be behind schedule or over budget.
**D. Before making any recommendations, an IS auditor needs to understand the project and the factors that have contributed to bringing the project over budget and over schedule.**

A3-98 Which of the following should an IS auditor review to understand project progress in terms of time, budget and deliverables for early detection of possible overruns and for projecting estimates at completion?

A. Function point analysis
B. Earned value analysis
C. Cost budget
D. Program evaluation and review technique

**B is the correct answer.**

**Justification:**

A. Function point analysis is an indirect measure of software size and complexity and, therefore, does not address the elements of time and budget.
**B. Earned value analysis (EVA) is an industry standard method for measuring a project's progress at any given point in time, forecasting its completion date and final cost, and analyzing variances in the schedule and budget as the project proceeds. It compares the planned amount of work with what has actually been completed to determine if the cost, schedule and work accomplished are progressing in accordance with the plan. EVA works most effectively if a well-formed work breakdown structure exists.**
C. Cost budgets do not address time.
D. Program evaluation and review technique aids time and deliverables management but lacks projections for estimates at completion and overall financial management.

A3-99 Which of the following system and data conversion strategies provides the **GREATEST** redundancy?

A. Direct cutover
B. Pilot study
C. Phased approach
D. Parallel run

**D is the correct answer.**

**Justification:**
A. Direct cutover is actually quite risky because it does not provide for a "shake down period" nor does it provide an easy fallback option.
B. A pilot study approach is performed incrementally, making rollback procedures difficult to execute.
C. A phased approach is performed incrementally, making rollback procedures difficult to execute.
**D. Parallel runs are the safest—though the most expensive—approach because both the old and new systems are run, thus incurring what might appear to be double costs.**

A3-100 Which of the following should be developed during the requirements definition phase of a software development project to address aspects of software testing?

A. Test data covering critical applications
B. Detailed test plans
C. Quality assurance test specifications
D. User acceptance test specifications

**D is the correct answer.**

**Justification:**
A. Test data will usually be created during the system testing phase.
B. Detailed test plans are created during system testing.
C. Quality assurance test specifications are set out later in the development process.
**D. A key objective in any software development project is to ensure that the developed software will meet the business objectives and the requirements of the user. The users should be involved in the requirements definition phase of a development project and user acceptance test specification should be developed during this phase.**

A3-101 At the completion of a system development project, a post-project review should include which of the following?

A. Assessing risk that may lead to downtime after the production release
B. Identifying lessons learned that may be applicable to future projects
C. Verifying that the controls in the delivered system are working
D. Ensuring that test data are deleted

**B is the correct answer.**

**Justification:**
A. An assessment of potential downtime should be made with the operations group and other specialists before implementing a system.
**B. A project team has something to learn from each and every project. As risk assessment is a key issue for project management, it is important for the organization to accumulate lessons learned and integrate them into future projects.**
C. Verifying that controls are working should be covered during the acceptance test phase and possibly, again in the post-implementation review. The post-project review will focus on project-related issues.
D. Test data should be retained for future regression testing.

A3-102 An IS auditor has been asked to participate in project initiation meetings for a critical project. The IS auditor's **MAIN** concern should be that the:

A. complexity and risk associated with the project have been analyzed.
B. resources needed throughout the project have been determined.
C. technical deliverables have been identified.
D. a contract for external parties involved in the project has been completed.

**A is the correct answer.**

**Justification:**
A. **Understanding complexity and risk, and actively managing these throughout a project are critical to a successful outcome.**
B. The resources needed will be dependent on the complexity of the project.
C. It is too early to identify the technical deliverables.
D. Not all projects will require contracts with external parties.

A3-103 From a risk management point of view, the **BEST** approach when implementing a large and complex IT infrastructure is:

A. a major deployment after proof of concept.
B. prototyping and a one-phase deployment.
C. a deployment plan based on sequenced phases.
D. to simulate the new infrastructure before deployment.

**C is the correct answer.**

**Justification:**
A. A major deployment would pose a higher risk of implementation failure.
B. Prototyping may reduce development failure, but a large environment will usually require a phased approach.
C. **When developing a large and complex IT infrastructure, a good practice is to use a phased approach to fit the entire system together. This will provide greater assurance of quality results.**
D. It is not usually feasible to simulate a large and complex IT infrastructure prior to deployment.

A3-104 When reviewing an active project, an IS auditor observed that the business case was no longer valid because of a reduction in anticipated benefits and increased costs. The IS auditor should recommend that the:

A. project be discontinued.
B. business case be updated and possible corrective actions be identified.
C. project be returned to the project sponsor for re-approval.
D. project be completed and the business case be updated later.

**B is the correct answer.**

**Justification:**
A. An IS auditor should not recommend discontinuing or completing the project before reviewing an updated business case.
B. **The IS auditor should recommend that the business case be kept current throughout the project because it is a key input to decisions made throughout the life of any project.**
C. The project cannot be returned to the sponsor until the business case has been updated.
D. An IS auditor should not recommend completing the project before reviewing an updated business case and ensuring approval from the project sponsor.

A3-105 Which of the following is an advantage of the top-down approach to software testing?

A. Interface errors are identified early
B. Testing can be started before all programs are complete
C. It is more effective than other testing approaches
D. Errors in critical modules are detected sooner

**A is the correct answer.**

**Justification:**

A. **The advantage of the top-down approach is that tests of major functions are conducted early, thus enabling the detection of interface errors sooner.**
B. That testing can be started before all programs are complete is an advantage of the bottom-up approach to system testing.
C. The most effective testing approach is dependent on the environment being tested.
D. Detecting errors in critical modules sooner is an advantage of the bottom-up approach to system testing.

A3-106 During the system testing phase of an application development project the IS auditor should review the:

A. conceptual design specifications.
B. vendor contract.
C. error reports.
D. program change requests.

**C is the correct answer.**

**Justification:**

A. A conceptual design specification is a document prepared during the requirements definition phase. The system testing will be based on a test plan.
B. A vendor contract is prepared during a software acquisition process and may be reviewed to ensure that all the deliverables in the contract have been delivered, but the most important area of review is the error reports.
C. **Testing is crucial in determining that user requirements have been validated. The IS auditor should be involved in this phase and review error reports for their precision in recognizing erroneous data and review the procedures for resolving errors.**
D. Program change requests would be reviewed normally as a part of the post-implementation phase.

A3-107 Which of the following would be the **MOST** cost-effective recommendation for reducing the number of defects encountered during software development projects?

A. Increase the time allocated for system testing
B. Implement formal software inspections
C. Increase the development staff
D. Require the sign-off of all project deliverables

**B is the correct answer.**

**Justification:**

A. Allowing more time for testing may discover more defects; however, little is revealed as to why the quality problems are occurring, and the cost of the extra testing and the cost of rectifying the defects found will be greater than if they had been discovered earlier in the development process.
**B. Inspections of code and design are a proven software quality technique. An advantage of this approach is that defects are identified before they propagate through the development life cycle. This reduces the cost of correction because less rework is involved.**
C. The ability of the development staff can have a bearing on the quality of what is produced; however, replacing staff can be expensive and disruptive, and the presence of a competent staff cannot guarantee quality in the absence of effective quality management processes.
D. Sign-off of deliverables may help detect defects if signatories are diligent about reviewing deliverable content; however, this is difficult to enforce and may occur too late in the process to be cost-effective. Deliverable reviews normally do not go down to the same level of detail as software inspections.

A3-108 An IS auditor invited to a project development meeting notes that no project risk has been documented. When the IS auditor raises this issue, the project manager responds that it is too early to identify risk and that, if risk starts impacting the project, a risk manager will be hired. The appropriate response of the IS auditor would be to:

A. stress the importance of spending time at this point in the project to consider and document risk and to develop contingency plans.
B. accept the project manager's position because the project manager is accountable for the outcome of the project.
C. offer to work with the risk manager when one is appointed.
D. inform the project manager that the IS auditor will conduct a review of the risk at the completion of the requirements definition phase of the project.

**A is the correct answer.**

**Justification:**

**A. The majority of project risk can be identified before a project begins, allowing mitigation/ avoidance plans to be put in place to deal with this risk. A project should have a clear link back to corporate strategy, enterprise risk management, and tactical plans to support this strategy. The process of setting corporate strategy, setting objectives and developing tactical plans should include the consideration of risk.**
B. The project manager cannot accept responsibility for risk acceptance. The risk must be addressed continuously—starting as early in the process as possible.
C. Appointing a risk manager is a good practice but waiting until the project has been impacted by risk is misguided. Risk management needs to be forward looking; allowing risk to evolve into issues that adversely impact the project represents a failure of risk management. With or without a risk manager, persons within and outside of the project team need to be consulted and encouraged to comment when they believe new risk has emerged or risk priorities have changed. The IS auditor has an obligation to the project sponsor and the organization to advise on appropriate project management practices. Waiting for the possible appointment of a risk manager represents an unnecessary and dangerous delay to implement risk management.
D. IS auditors cannot provide risk review without impairing their independence.

A3-109 The **MAIN** purpose of a transaction audit trail is to:

A. reduce the use of storage media.
B. determine accountability and responsibility for processed transactions.
C. help an IS auditor trace transactions.
D. provide useful information for capacity planning.

**B is the correct answer.**

**Justification:**
A. Enabling audit trails increases the use of disk space.
**B. Enabling audit trails aids in establishing the accountability and responsibility for processed transactions by tracing them through the information system.**
C. A transaction log file would be used to trace transactions, but the primary purpose of an audit trail is to support accountability, not to support the work of the IS auditor.
D. The objective of capacity planning is the efficient and effective use of IT resources and requires information such as central processing unit utilization, bandwidth and the number of users.

A3-110 An organization is implementing an enterprise resource planning application. Of the following, who is **PRIMARILY** responsible for overseeing the project to ensure that it is progressing in accordance with the project plan and that it will deliver the expected results?

A. Project sponsor
B. System development project team
C. Project steering committee
D. User project team

**C is the correct answer.**

**Justification:**
A. A project sponsor is typically the senior manager in charge of the primary business unit that the application will support. The sponsor provides funding for the project and works closely with the project manager to define the critical success factors or metrics for the project. The project sponsor is not responsible for reviewing the progress of the project.
B. A system development project team completes the assigned tasks, works according to the instructions of the project manager and communicates with the user project team. The SDPT is not responsible for overseeing the progress of the project.
**C. A project steering committee that provides an overall direction for the enterprise resource planning (ERP) implementation project is responsible for reviewing the project's progress to ensure that it will deliver the expected results.**
D. A user project team (UPT) completes the assigned tasks, communicates effectively with the system development team and works according to the advice of the project manager. A UPT is not responsible for reviewing the progress of the project.

A3-111 A legacy payroll application is migrated to a new application. Which of the following stakeholders should be **PRIMARILY** responsible for reviewing and signing-off on the accuracy and completeness of the data before going live?

A. IS auditor
B. Database administrator
C. Project manager
D. Data owner

**D is the correct answer.**

**Justification:**

A. An IS auditor should ensure that there is a review and sign-off by the data owner during the data conversion stage of the project.
B. A database administrator's primary responsibility is to maintain the integrity of the database and make the database available to users. A database administrator is not responsible for reviewing migrated data.
C. A project manager provides day-to-day management and leadership of the project but is not responsible for the accuracy and integrity of the data.
**D. During the data conversion stage of a project, the data owner is primarily responsible for reviewing and signing-off that the data are migrated completely and accurately and are valid. An IS auditor is not responsible for reviewing and signing-off on the accuracy of the converted data.**

A3-112 An organization is migrating from a legacy system to an enterprise resource planning system. While reviewing the data migration activity, the **MOST** important concern for the IS auditor is to determine that there is a:

A. correlation of semantic characteristics of the data migrated between the two systems.
B. correlation of arithmetic characteristics of the data migrated between the two systems.
C. correlation of functional characteristics of the processes between the two systems.
D. relative efficiency of the processes between the two systems.

**A is the correct answer.**

**Justification:**

**A. Due to the fact that the two systems could have a different data representation, including the database schema, the IS auditor's main concern should be to verify that the interpretation of the data (structure) is the same in the new as it was in the old system.**
B. Arithmetic characteristics represent aspects of data structure and internal definition in the database and, therefore, are less important than the semantic characteristics.
C. A review of the correlation of the functional characteristics between the two systems is not relevant to a data migration review.
D. A review of the relative efficiencies of the processes between the two systems is not relevant to a data migration review.

A3-113 Normally, it would be essential to involve which of the following stakeholders in the initiation stage of a project?

A. System owners
B. System users
C. System designers
D. System builders

**A is the correct answer.**

**Justification:**

A. **System owners are the information systems (project) sponsors or chief advocates. They normally are responsible for initiating and funding projects to develop, operate and maintain information systems.**
B. System users are the individuals who use or are affected by the information system. Their requirements are crucial in the requirements definition, design and testing stages of a project.
C. System designers translate business requirements and constraints into technical solutions.
D. System builders construct the system based on the specifications from the systems designers. In most cases, the designers and builders are one and the same.

A3-114 A project manager for a project that is scheduled to take 18 months to complete announces that the project is in a healthy financial position because, after six months, only one-sixth of the budget has been spent. The IS auditor should **FIRST** determine:

A. the amount of progress achieved compared to the project schedule.
B. if the project budget can be reduced.
C. if the project could be brought in ahead of schedule.
D. if the budget savings can be applied to increase the project scope.

**A is the correct answer.**

**Justification:**

A. **Cost performance of a project cannot be properly assessed in isolation of schedule performance. Cost cannot be assessed simply in terms of elapsed time on a project.**
B. To properly assess the project budget position, it is necessary to know how much progress has actually been made and, given this, what level of expenditure would be expected. It is possible that project expenditure appears to be low because actual progress has been slow. Until the analysis of project against schedule has been completed, it is impossible to know whether there is any reason to reduce budget. If the project has slipped behind schedule, then not only may there be no spare budget, but it is possible that extra expenditure may be needed to retrieve the slippage. The low expenditure could actually be representative of a situation where the project is likely to miss deadlines rather than potentially come in ahead of time.
C. If the project is found to be ahead of budget after adjusting for actual progress, this is not necessarily a good outcome because it points to flaws in the original budgeting process; and, as said previously, until further analysis is undertaken, it cannot be determined whether any spare funds actually exist.
D. If the project is behind schedule, adding scope may be the wrong thing to do.

A3-115 The **MAJOR** advantage of a component-based development approach is the:

A. ability to manage an unrestricted variety of data types.
B. provision for modeling complex relationships.
C. capacity to meet the demands of a changing environment.
D. support of multiple development environments.

**D is the correct answer.**

**Justification:**
A. The data types must be defined within each component, and it is not sure that any component will be able to handle multiple data types.
B. Component-based development is no better than many other development methods at modeling complex relationships.
C. Component-based development is one of the methodologies that can be effective at meeting changing requirements, but this is not its primary benefit or purpose.
**D. Component-based development that relies on reusable modules can increase the speed of development. Software developers can then focus on business logic.**

A3-116 The specific advantage of white box testing is that it:

A. verifies a program can operate successfully with other parts of the system.
B. ensures a program's functional operating effectiveness without regard to the internal program structure.
C. determines procedural accuracy or conditions of a program's specific logic paths.
D. examines a program's functionality by executing it in a tightly controlled or virtual environment with restricted access to the host system.

**C is the correct answer.**

**Justification:**
A. Verifying the program can operate successfully with other parts of the system is sociability testing.
B. Testing the program's functionality without knowledge of internal structures is black box testing.
**C. White box testing assesses the effectiveness of software program logic. Specifically, test data are used in determining procedural accuracy or conditions of a program's logic paths.**
D. Controlled testing of programs in a semi-debugged environment, either heavily controlled step-by-step or via monitoring in virtual machines, is sand box testing.

A3-117 Following good practices, formal plans for implementation of new information systems are developed during the:

A. development phase.
B. design phase.
C. testing phase.
D. deployment phase.

**B is the correct answer.**

**Justification:**
A. The implementation plans are updated during the development of the system, but the plans were already addressed during the design phase.
**B. The method of implementation may affect the design of the system. Therefore, planning for implementation should begin well in advance of the actual implementation date. A formal implementation plan should be constructed in the design phase and revised as the development progresses.**
C. The testing phase focuses on testing the system and is not concerned with implementation planning.
D. The deployment phase implements the system according to the plans set out earlier in the design phase.

**A3-118** An IS auditor is reviewing a project that is using an agile software development approach. Which of the following should the IS auditor expect to find?

A. Use of a capability maturity model
B. Regular monitoring of task-level progress against schedule
C. Extensive use of software development tools to maximize team productivity
D. Postiteration reviews that identify lessons learned for future use in the project

**D is the correct answer.**

**Justification:**

A. The capability maturity model places heavy emphasis on predefined formal processes and formal project management and software development deliverables, while agile software development projects, by contrast, rely on refinement of process as dictated by the particular needs of the project and team dynamics.
B. Task-level tracking is not used because daily meetings identify challenges and impediments to the project.
C. Agile projects make use of suitable development tools; however, tools are not seen as the primary means of achieving productivity. Team harmony, effective communications and collective ability to solve challenges are of greater importance.
**D. A key tenet of the agile approach to software project management is ongoing team learning to refine project management and software development processes as the project progresses. One of the best ways to achieve this is that the team considers and documents what worked well and what could have worked better at the end of each iteration and identifies improvements to be implemented in subsequent iterations. Additionally, less importance is placed on formal paper-based deliverables, with the preference being effective informal communication within the team and with key outside contributors. Agile projects produce releasable software in short iterations, typically ranging from four to eight weeks. This, in itself, instills considerable performance discipline within the team. This, combined with short daily meetings to agree on what the team is doing and the identification of any impediments, renders task-level tracking against a schedule redundant.**

**A3-119** An organization sells books and music online at its secure web site. Transactions are transferred to the accounting and delivery systems every hour to be processed. Which of the following controls **BEST** ensures that sales processed on the secure web site are transferred to both the delivery and accounting systems?

A. Transaction totals are recorded on a daily basis in the sales systems. Daily sales system totals are aggregated and totaled.
B. Transactions are automatically numerically sequenced. Sequences are checked and gaps in continuity are accounted for.
C. Processing systems check for duplicated transaction numbers. If a transaction number is duplicated (already present), it is rejected.
D. System time is synchronized hourly using a centralized time server. All transactions have a date/time stamp.

**B is the correct answer.**

**Justification:**

A. Totaling transactions on the sales system does not address the transfer of data from the online systems to the accounting system, but rather considers only the sales system.
**B. Automatic numerical sequencing is the only option that accounts for completeness of transactions because any missing transactions would be identified by a gap.**
C. Checking for duplicates is a valid control; however, it does not address whether the sales transactions processed are complete (ensuring that all transactions are recorded).
D. A date/time stamp does not help account for transactions that are missing or incomplete by the accounting and delivery department.

A3-120 Which of the following techniques would **BEST** help an IS auditor gain reasonable assurance that a project can meet its target date?

A. Estimation of the actual end date based on the completion percentages and estimated time to complete, taken from status reports
B. Confirmation of the target date based on interviews with experienced managers and staff involved in the completion of the project deliverables
C. Extrapolation of the overall end date based on completed work packages and current resources
D. Calculation of the expected end date based on current resources and remaining available project budget

**C is the correct answer.**

**Justification:**

A. The IS auditor cannot count on the accuracy of data in status reports for reasonable assurance.
B. Interviews are a valuable source of information but will not necessarily identify any project challenges because the people being interviewed are involved in project.
C. **Direct observation of results is better than estimations and qualitative information gained from interviews or status reports. Project managers and involved staff tend to underestimate the time needed for completion and the necessary time buffers for dependencies between tasks, while overestimating the completion percentage for tasks underway (i.e., 80:20 rule).**
D. The calculation based on remaining budget does not consider the speed at which the project has been progressing.

A3-121 An IS auditor finds that user acceptance testing of a new system is being repeatedly interrupted by defect fixes from the developers. Which of the following would be the **BEST** recommendation for an IS auditor to make?

A. Consider the feasibility of a separate user acceptance environment
B. Schedule user testing to occur at a given time each day
C. Implement a source code version control tool
D. Only retest high-priority defects

**A is the correct answer.**

**Justification:**

A. **A separate environment or environments is normally necessary for testing to be efficient and effective and to ensure the integrity of production code. It is important that the development and test code bases be separate. When defects are identified they can be fixed in the development environment, without interrupting testing, before being migrated in a controlled manner to the test environment. A separate test environment can also be used as the final staging area from which code is migrated to production. This enforces a separation between development and production code. The logistics of setting up and refreshing customized test data is easier if a separate environment is maintained.**
B. If developers and testers are sharing the same environment, they have to work effectively at separate times of the day. It is unlikely that this would provide optimum productivity.
C. Use of a source code control tool is a good practice, but it does not properly mitigate the lack of an appropriate test environment.
D. Even low priority fixes run the risk of introducing unintended results when combined with the rest of the system code. To prevent this, regular regression testing covering all code changes should occur. A separate test environment makes the logistics of regression testing easier to manage.

A3-122 An IS auditor has found time constraints and expanded needs to be the root causes for recent violations of corporate data definition standards in a new business intelligence project. Which of the following is the **MOST** appropriate suggestion for an auditor to make?

A. Achieve standards alignment through an increase of resources devoted to the project
B. Align the data definition standards after completion of the project
C. Delay the project until compliance with standards can be achieved
D. Enforce standard compliance by adopting punitive measures against violators

**A is the correct answer.**

**Justification:**

A. **Provided that data architecture, technical and operational requirements are sufficiently documented, the alignment to standards could be treated as a specific work package assigned to new project resources.**
B. The usage of nonstandard data definitions would lower the efficiency of the new development and increase the risk of errors in critical business decisions. To change data definition standards after project conclusion is risky and is not a viable solution.
C. Delaying the project would be an inappropriate suggestion because of business requirements or the likely damage to entire project profitability.
D. Punishing the violators would be outside the authority of the auditor and inappropriate until the reason for the violations have been determined.

A3-123 What is the **PRIMARY** reason that an IS auditor would verify that the process of post-implementation review of an application was completed after a release?

A. To make sure that users are appropriately trained
B. To verify that the project was within budget
C. To check that the project meets expectations
D. To determine whether proper controls were implemented

**C is the correct answer.**

**Justification:**

A. Post-implementation review does not target verifying user training needs.
B. Project costs are monitored during development and are not the primary reason for a post-implementation review.
C. **The objective of a post-implementation review is to reveal whether the implementation of a system has achieved planned objectives (i.e., meets business objectives and risk acceptance criteria).**
D. While an IS auditor would be interested in ensuring that proper controls were implemented, the most important consideration would be that the project meets expectations.

A3-124 An IS auditor is reviewing an enterprise's system development testing policy. Which of the following statements concerning use of production data for testing would the IS auditor consider to be **MOST** appropriate?

A. Senior IS and business management must approve use before production data can be used for testing
B. Production data can be used if they are copied to a secure test environment
C. Production data can never be used. All test data must be developed and based on documented test cases
D. Production data can be used provided that confidentiality agreements are in place

**A is the correct answer.**

**Justification:**

A. **There is risk associated with the use of production data for testing. These include compromising customer or employee confidentiality (which may also involve breaching legislation) and corrupting production of the data. Additionally, there are certain cases in which effective testing requires specifically designed data. There are other cases in which using production data would provide insights that are difficult or impossible to get from manufactured test data. One example is testing of interfaces to legacy systems. Management information systems are a further example where access to "real" data is likely to enhance testing. Some flexibility on the use of production data is likely to be the best option. In addition to obtaining senior management approval, conditions that mitigate the risk associated with using production data can be agreed on, such as masking names and other identifying fields to protect privacy.**
B. Copying production data to a secure environment is a good practice, but this should only be done with the approval of management. Management must accept the risk of using production data for testing.
C. Creating a complete set of test data would be an ideal situation but is not always possible due to the volume of test data that would be required.
D. Production data could only be used with management's permission. Then it can be appropriate to require the use of confidentiality agreements.

A3-125 An enterprise is developing a new procurement system, and things are behind schedule. As a result, it is proposed that the time originally planned for the test phase be shortened. The project manager asks the IS auditor for recommendations to mitigate the risk associated with reduced testing. Which of the following is a suitable risk mitigation strategy?

A. Test and release a pilot with reduced functionality
B. Fix and retest the highest-severity functional defects
C. Eliminate planned testing by the development team, and proceed straight to acceptance testing
D. Implement a test tool to automate defect tracking

**A is the correct answer.**

**Justification:**

A. **Testing and releasing a pilot with reduced functionality reduces risk in a number of ways. Reduced functionality should result in fewer overall test cases to run and defects to fix and retest, and in less regression testing. A pilot release made available to a select group of users will reduce the risk associated with a full implementation. All of the benefits of releasing the system to the full user population will not be realized, but some benefits should start to flow. Additionally, some useful comments from real users should be obtained to guide what extra functionality and other improvements need to be included in a full release.**

B. When testing starts, a significant number of defects is likely to exist. Focusing only on the highest-severity functional defects runs the risk that other important aspects such as usability problems and nonfunctional requirements of performance and security will be ignored. The system may go live, but users may struggle to use the system as intended to realize business benefits.

C. Eliminating testing by development is usually a bad idea. Before system acceptance testing begins, some prior testing should occur to establish that the system is ready to proceed to acceptance evaluation. If prior testing by the development team does not occur, there is a considerable risk that the software will have a significant number of low-level defects, such as transactions that cause the system to hang and unintelligible error messages. This can prove frustrating for users or testers tasked with acceptance testing and, ultimately, could cause the overall test time to increase rather than decrease.

D. The use of a defect tracking tool could help in improving test efficiency, but it does not address the fundamental risk caused by reducing the testing effort on a system in which quality is uncertain. Given the build problems experienced, there is reason to suspect that quality problems could exist.

A3-126 An IS auditor is involved in the reengineering process that aims to optimize IT infrastructure. Which of the following will **BEST** identify the issues to be resolved?

A. Self-assessment
B. Reverse engineering
C. Prototyping
D. Gap analysis

**D is the correct answer.**

**Justification:**

A. Self-assessment may be one of the viable options with which to start; however, the results only indicate current conditions, not desired state, and tend to become subjective.

B. Reverse engineering is a technique applied to analyze how a device or program works and is not appropriate here.

C. Prototyping is applied to ensure that user requirements are met prior to being engaged in a full-blown development process.

D. **Gap analysis would be the best method to identify issues that need to be addressed in the reengineering process. Gap analysis indicates which parts of current processes conform to good practices (desired state) and which do not.**

A3-127 An IS audit group has been involved in the integration of an automated audit tool kit with an existing enterprise resource planning system. Due to ERP performance issues, the audit tool kit is not permitted to go live. What should the IS auditor's **BEST** recommendation be?

A. Review the implementation of selected integrated controls
B. Request additional IS audit resources
C. Request vendor technical support to resolve performance issues
D. Review the results of stress tests during user acceptance testing

**D is the correct answer.**

**Justification:**

A. Reviewing the implementation of selected integrated controls validates the technical design and the control objective, but integrated controls over transactional tables consume large resources. They should be reviewed carefully to determine whether they are mandatory or can be implemented and integrated for only specific transactions over the enterprise resource planning application.
B. The inability to implement the automated tool may necessitate additional audit resources because many audits will require more manual effort; however, the first step should be to try to resolve the performance issues.
C. Requesting vendor technical support to resolve performance issues is a good option, but not the first recommendation.
**D. The appropriate recommendation is to review the results of stress tests during user acceptance testing that demonstrated the performance issues.**

A3-128 What is the **BEST** method to facilitate successful user testing and acceptance of a new enterprise resource planning payroll system that is replacing an existing legacy system?

A. Multiple testing
B. Parallel testing
C. Integration testing
D. Prototype testing

**B is the correct answer.**

**Justification:**

A. Multiple testing will not compare results from the old and new systems.
**B. Parallel testing is the best method for testing data results and system behavior because it allows the users to compare results from both systems before decommissioning the legacy system. Parallel testing also results in better user adoption of the new system.**
C. Integration testing refers to how the system interacts with other systems, and it is not performed by end users.
D. Prototype testing is used during design and development to ensure that user input is received; however, this method is not used for acquired systems or during user acceptance testing.

A3-129 A rapid application development methodology has been selected to implement a new enterprise resource planning system. All of the project activities have been assigned to the contracted consulting company because internal employees are not available. What is the IS auditor's **FIRST** step to compensate for the lack of resources?

A. Review the project plan and approach
B. Ask the vendor to provide additional external staff
C. Recommend that the company hire more people
D. Stop the project until all human resources are available

**A is the correct answer.**

**Justification:**

A. **Rapid methodologies require available resources with good expertise and a fast decision-making process because the plan duration is usually short. Reviewing the project plan and approach is the best recommendation to make the appropriate changes to compensate for the missing end users.**
B. Adding external people to the project will not resolve the problem because they will not be able to decide on behalf of the internal employees who are usually end users from the business side.
C. Hiring new people will take time and does not guarantee the readiness of new hires to make appropriate decisions in this project.
D. Stopping the project could be a good option but reviewing the project and considering all of the aspects should be done first.

A3-130 An IS auditor who is auditing the software acquisition process will ensure that the:

A. contract is reviewed and approved by the legal counsel before it is signed.
B. requirements cannot be met with the systems already in place.
C. requirements are found to be critical for the business.
D. user participation is adequate in the process.

**A is the correct answer.**

**Justification:**

A. **The process to review and approve the contract is one of the most important steps in the software acquisition process. An IS auditor should verify that legal counsel reviewed and approved the contract before management signs the contract.**
B. Existing systems may meet the requirements, but management may choose to acquire software for other reasons.
C. Not all of the requirements in the contract need to support critical business needs; some requirements may be there for ease-of-use or other purposes.
D. User participation is not necessarily required in the software acquisition process. Instead, users would most likely participate in requirements definition and user acceptance testing.

A3-131 Which of the following controls helps prevent duplication of vouchers during data entry?

A. A range check
B. Transposition and substitution
C. A sequence check
D. A cyclic redundancy check

**C is the correct answer.**

**Justification:**

A. A range check works over a range of numbers. Even if the same voucher number reappears, it will satisfy the range and, therefore, not be useful.
B. Transposition and substitution are used in encoding but will not help in establishing unique voucher numbers.
**C. A sequence check involves increasing the order of numbering and would validate whether the vouchers are in sequence and, thus, prevent duplicate vouchers.**
D. A cyclic redundancy check is used for completeness of data received over the network but is not useful in application code level validations.

A3-132 Which of the following test techniques would the IS auditor use to identify specific program logic that has not been tested?

A. A snapshot
B. Tracing and tagging
C. Logging
D. Mapping

**D is the correct answer.**

**Justification:**

A. A snapshot records the flow of designated transactions through logic paths within programs.
B. Tracing and tagging shows the trail of instructions executed during an application.
C. Logging is the activity of recording specific tasks for future review.
**D. Mapping identifies specific program logic that has not been tested and analyzes programs during execution to indicate whether program statements have been executed.**

A3-133 The **PRIMARY** objective of conducting a post-implementation review for a business process automation project is to:

A. ensure that the project meets the intended business requirements.
B. evaluate the adequacy of controls.
C. confirm compliance with technological standards.
D. confirm compliance with regulatory requirements.

**A is the correct answer.**

**Justification:**

**A. Ensuring that the project meets the intended business requirements is the primary objective of a post-implementation review.**
B. Evaluating the adequacy of controls may be part of the review but is not the primary objective.
C. Confirming compliance with technological standards is normally not part of the post-implementation review because this should be addressed during the design and development phase.
D. Confirming compliance with regulatory requirements is normally not part of the post-implementation review because this should be addressed during the design and development phase.

A3-134 While evaluating the "out of scope" section specified in a project plan, an IS auditor should ascertain whether the section:

A. effectively describes unofficial project objectives.
B. effectively describes project boundaries.
C. clearly states the project's "nice to have" objectives.
D. provides the necessary flexibility to the project team.

**B is the correct answer.**

**Justification:**
A. Out-of-scope items are not part of the project. There should be no unofficial project objectives. Reasonable objectives should be considered by the project leadership and either accepted (in scope) or rejected (out of scope).
**B. The purpose of the out of scope section is to make clear to readers what items are not considered project objectives so that all project stakeholders understand the project boundaries and what is in scope versus out of scope. This applies to all types of projects, including individual audits.**
C. Out-of-scope items are not part of the project, while nice to have items may be included in the project objectives. However, they may be the last priority on the list of all project objectives.
D. Out-of-scope items are not part of the project; the project team's flexibility regarding project objectives should be managed through a robust change request process. This is particularly important to avoid scope creep.

A3-135 An IS auditor assesses the project management process for an internal software development project. In respect to the software functionality, the IS auditor should look for sign-off by:

A. the project manager.
B. systems development management.
C. business unit management.
D. the quality assurance team.

**C is the correct answer.**

**Justification:**
A. The project manager provides day-to-day management and leadership of the project and ensures that project activities remain in line with the overall direction. The project manager cannot sign off on project requirements; that would be a violation of separation of duties.
B. Systems development management provides technical support for hardware and software environments.
**C. Business unit management assumes ownership of the project and the resulting system. It is responsible for acceptance testing and confirming that the required functions are available in the software.**
D. The quality assurance team ensures the quality of the project by measuring adherence to the organization's system development life cycle. They will conduct testing but not sign off on the project requirements.

A3-136 Which of the following is **MOST** relevant to an IS auditor evaluating how the project manager has monitored the progress of the project?

A. Critical path diagrams
B. Program evaluation review technique diagrams
C. Function point analysis
D. Gantt charts

**D is the correct answer.**

**Justification:**

A. Critical path diagrams are used to determine the critical path for the project that represents the shortest possible time required for completing the project.
B. Program evaluation review technique diagrams are a critical path method technique in which three estimates (as opposed to one) of time lines required to complete activities are used to determine the critical path.
C. Function point analysis is a technique used to determine the size of a development task, based on the number of function points.
**D. Gantt charts help to identify activities that have been completed early or late through comparison to a baseline. Progress of the entire project can be read from the Gantt chart to determine whether the project is behind, ahead of or on schedule.**

A3-137 While reviewing an ongoing project, the IS auditor notes that the development team has spent eight hours of activity on the first day against a budget of 24 hours (over three days). The projected time to complete the remainder of the activity is 20 hours. The IS auditor should report that the project:

A. is behind schedule.
B. is ahead of schedule.
C. is on schedule.
D. cannot be evaluated until the activity is completed.

**A is the correct answer.**

**Justification:**

**A. Earned value analysis (EVA) is based on the premise that if a project task is assigned 24 hours for completion, it can be reasonably completed during that time frame. According to EVA, the project is behind schedule because the value of the eight hours spent on the task should be only four hours, considering that 20 hours of effort remain to be completed.**
B. The project is not ahead of schedule because the work remaining exceeds the time allotted.
C. The project is not on schedule because only 16 hours remain to do 20 hours work.
D. The amount of work left has been evaluated at 20 hours and the time left on the project is 16 hours, so the auditor can evaluate the current status of the project.

A3-138 Which of the following **BEST** helps an IS auditor evaluate the quality of programming activities related to future maintenance capabilities?

A. The programming language
B. The development environment
C. A version control system
D. Program coding standards

**D is the correct answer.**

**Justification:**

A. The programming language may be a concern if it is not a commonly used language; however, program coding standards are more important.
B. The development environment may be relevant to evaluate the efficiency of the program development process but not future maintenance of the program.
C. A version control system helps manage software code revisions; however, it does not ensure that coding standards are consistently applied.
**D. Program coding standards are required for efficient program maintenance and modifications. To enhance the quality of programming activities and future maintenance capabilities, program coding standards should be applied. Program coding standards are essential to writing, reading and understanding code, simply and clearly, without having to refer back to design specifications.**

A3-139 During a system development life cycle audit of a human resources and payroll application, the IS auditor notes that the data used for user acceptance testing have been masked. The purpose of masking the data is to ensure the:

A. confidentiality of the data.
B. accuracy of the data.
C. completeness of the data.
D. reliability of the data.

**A is the correct answer.**

**Justification:**

**A. Masking is used to ensure the confidentiality of data, especially in a user acceptance testing exercise in which the testers have access to data that they would not have access to in normal production environments.**
B. Masking does not ensure accuracy of the data. If the underlying data are inaccurate, the masked data also would be inaccurate.
C. Masking does not ensure completeness of the data. If the underlying data are incomplete, the masked data also would be incomplete.
D. Masking does not ensure reliability of the data. If the underlying data are unreliable, the masked data also would be unreliable.

A3-140 Which of the following helps an IS auditor evaluate the quality of new software that is developed and implemented?

A. The reporting of the mean time between failures over time
B. The overall mean time to repair failures
C. The first report of the mean time between failures
D. The overall response time to correct failures

**C is the correct answer.**

**Justification:**

A. The mean time between failures that are repetitive includes the inefficiency in fixing the first reported failures and is a reflection on the response team or help desk team in fixing the reported issues.
B. The mean time to repair is a reflection on the response team or help desk team in addressing reported issues.
**C. The mean time between failures that are first reported represents flaws in the software that are reported by users in the production environment. This information helps the IS auditor in evaluating the quality of the software that is developed and implemented.**
D. The response time reflects the agility of the response team or the help desk team in addressing reported issues.

A3-141 Which of the following carries the **LOWEST** risk when managing failures while transitioning from legacy applications to new applications?

A. Phased changeover
B. Abrupt changeover
C. Rollback procedure
D. Parallel changeover

**D is the correct answer.**

**Justification:**

A. Phased changeover involves the changeover from the old system to the new system in a phased manner. Therefore, at no time will the old system and the new system both be fully operational as one integrated system.
B. In abrupt changeover, the new system is changed from the old system on a cutoff date and time, and the old system is discontinued after changeover to the new system takes place. Therefore, the old system is not available as a backup if there are problems when the new system is implemented.
C. Rollback procedures involve restoring all systems to their previous working state; however, parallel changeover is the better strategy.
**D. Parallel changeover involves first running the old system, then running both the old and new systems in parallel, and finally fully changing to the new system after gaining confidence in the functionality of the new system.**

A3-142 Which of the following **BEST** helps an IS auditor assess and measure the value of a newly implemented system?

A. Review of business requirements
B. System certification
C. Post-implementation review
D. System accreditation

**C is the correct answer.**

**Justification:**

A. While reviewing the business requirements is important, only a post-implementation review provides evidence that the project met the business requirements.
B. System certification involves performing a comprehensive assessment against a standard of management, operational and technical controls in an information system to examine the level of compliance in meeting certain requirements such as standards, policies, processes, procedures, work instructions and guidelines.
C. **One key objective of a post-implementation review is to evaluate the projected cost-benefits or the return on investment measurements.**
D. System accreditation is an official management decision to authorize operation of an information system and to explicitly accept the risk to the organization's operations, assets or individuals based on the implementation of an agreed-on set of requirements and security controls.

A3-143 A large industrial organization is replacing an obsolete legacy system and evaluating whether to buy a custom solution or develop a system in-house. Which of the following will **MOST** likely influence the decision?

A. Technical skills and knowledge within the organization related to sourcing and software development
B. Privacy requirements as applied to the data processed by the application
C. Whether the legacy system being replaced was developed in-house
D. The users not devoting reasonable time to define the functionalities of the solution

**A is the correct answer.**

**Justification:**

A. **Critical core competencies will most likely be carefully considered before outsourcing the planning phase of the application.**
B. Privacy regulations would apply to both solutions.
C. While individuals with knowledge of the legacy system are helpful, they may not have the technical skills to build a new system. Therefore, this is not the primary factor influencing the make versus buy decision.
D. Unclear business requirements (functionalities) will similarly affect either development process but are not the primary factor influencing the make versus buy decision.

A3-144 A company's development team does not follow generally accepted system development life cycle practices. Which of the following is **MOST** likely to cause problems for software development projects?

A. Functional verification of the prototypes is assigned to end users
B. The project is implemented while minor issues are open from user acceptance testing
C. Project responsibilities are not formally defined at the beginning of a project
D. Program documentation is inadequate

**C is the correct answer.**

**Justification:**
A. Prototypes are verified by users.
B. User acceptance testing is seldom completely successful. If errors are not critical, they may be corrected after implementation without seriously affecting usage.
**C. Errors or lack of attention in the initial phases of a project may cause costly errors and inefficiencies in later phases. Proper planning is required at the beginning of a project.**
D. Lack of adequate program documentation, while a concern, is not as big a risk as the lack of assigned responsibilities during the initial stages of the project.

A3-145 An IS auditor has been asked to review the implementation of a customer relationship management system for a large organization. The IS auditor discovered the project incurred significant over-budget expenses and scope creep caused the project to miss key dates. Which of the following should the IS auditor recommend for future projects?

A. Project management training
B. A software baseline
C. A balanced scorecard
D. Automated requirements software

**B is the correct answer.**

**Justification:**
A. While project management training is a good practice, it does not necessarily prevent scope creep without the use of a software baseline and a robust requirements change process.
**B. Use of a software baseline provides a cutoff point for the design of the system and allows the project to proceed as scheduled without being delayed by scope creep.**
C. A balanced scorecard is a coherent set of performance measures organized into four categories that includes traditional financial measures, but adds customer, internal business process, and learning and growth perspectives. It does not prevent scope creep.
D. Use of automated requirements software does not decrease the risk of scope creep.

A3-146 Which of the following is the **BEST** indicator that a newly developed system will be used after it is in production?

A. Regression testing
B. User acceptance testing
C. Sociability testing
D. Parallel testing

**B is the correct answer.**

**Justification:**

A. Regression test results do not assist with the user experience and are primarily concerned with new functionality or processes and whether those changes altered or broke previous functionality.
**B. User acceptance testing is undertaken to provide confidence that a system or system component operates as intended, to provide a basis for evaluating the implementation of the requirements or to demonstrate the effectiveness or efficiency of the system or component. If the results of the testing are poor, then the system is unlikely to be adopted by the users.**
C. Sociability test results indicate how the application works with other components within the environment and is not indicative of the user experience.
D. Parallel testing is performed when the comparison of two applications is needed but will not provide feedback on user satisfaction.

A3-147 The project steering committee is ultimately responsible for:

A. day-to-day management and leadership of the project.
B. allocating the funding for the project.
C. project deliverables, costs and timetables.
D. ensuring that system controls are in place.

**C is the correct answer.**

**Justification:**

A. Day-to-day management and leadership of the project is the function of the project manager.
B. Providing the funding for the project is the function of the project sponsor.
**C. The project steering committee provides overall direction; ensures appropriate representation of the major stakeholders in the project's outcome; and takes ultimate responsibility for the deliverables, costs and timetables.**
D. Ensuring that system controls are in place is the function of the project security officer.

A3-148 Which of the following **BEST** helps ensure that deviations from the project plan are identified?

A. A project management framework
B. A project management approach
C. A project resource plan
D. Project performance criteria

**D is the correct answer.**

**Justification:**

A. Establishment of a project management framework identifies the scope and boundaries of managing projects and the consistent method to be applied when initiating a project but does not define the criteria used to measure project success.
B. A project management approach defines guidelines for project management processes and deliverables but does not define the criteria used to measure project success.
C. A project resource plan defines the responsibilities, relationships, authorities and performance criteria of project team members but does not wholly define the criteria used to measure project success.
**D. To identify deviations from the project plan, project performance criteria must be established as a baseline. Successful completion of the project plan is indicative of project success.**

A3-149 An IS auditor is reviewing a project for the implementation of a mission-critical system and notes that, instead of parallel implementation, the team opted for an immediate cutover to the new system. Which of the following is the **GREATEST** concern?

A. The implementation phase of the project has no back out plan
B. User acceptance testing was not properly documented
C. Software functionality tests were completed, but stress testing was not performed
D. The go-live date is over a holiday weekend when key IT staff are on vacation

**A is the correct answer.**

**Justification:**

**A. One of the benefits of deploying a new system in parallel with an existing system is that the original system can always be used as a back out plan. In an immediate cutover scenario, not having a back out plan can create significant issues because it can take considerable time and cost to restore operations to the prior state if there is no viable plan to do so.**
B. The documentation of user acceptance testing is a much less important concern than not having a viable back out plan.
C. The lack of stress testing is a much less important concern than not having a viable back out plan.
D. If there are support issues, having the go-live date happen over a holiday weekend may create some delays, but project managers should account for this to ensure that the required staff are available as needed. The greater risk is if there is no back out plan.

A3-150 Which of the following software testing methods provides the **BEST** feedback on how software will perform in the live environment?

A. Alpha testing
B. Regression testing
C. Beta testing
D. White box testing

**C is the correct answer.**

**Justification:**

A. Alpha testing is often performed only by users within the organization developing the software. Alpha testing generally involves a software version that does not contain all the features of the final product and may be a simulated test.
B. Regression testing is used to determine whether system changes have introduced new errors to existing functionality.
**C. Beta testing follows alpha testing and involves real-world exposure with external user involvement. Beta testing is the last stage of testing and involves sending the beta version of the product to independent beta test sites or offering it free to interested users.**
D. White box testing is used to assess the effectiveness of program logic.

A3-151 Which of the following is the **BEST** method of controlling scope creep in a system development project?

A. Defining penalties for changes in requirements
B. Establishing a software baseline
C. Adopting a matrix project management structure
D. Identifying the critical path of the project

**B is the correct answer.**

**Justification:**

A. While defining penalties for changes in requirements may help to prevent scope creep, software baselining is a better way to accomplish this goal.
**B. Software baselining, the cutoff point in the design phase, occurs after a rigorous review of user requirements. Any changes thereafter will undergo strict formal change control and approval procedures. Scope creep refers to uncontrolled change within a project resulting from improperly managed requirements.**
C. In a matrix project organization, management authority is shared between the project manager and the department heads. Adopting a matrix project management structure will not address the problem of scope creep.
D. Although the critical path is important, it will change over time and will not control scope creep.

A3-152 The **PRIMARY** purpose of a post-implementation review is to ascertain that:

A. The lessons learned have been documented.
B. Future enhancements can be identified.
C. The project has been delivered on time and budget.
D. Project objectives have been met.

**D is the correct answer.**

**Justification:**

A. It is important to ensure that lessons learned during the project are not forgotten; however, it is more important to ascertain whether the project solved the problem it was designed to address.
B. Identifying future enhancements is not the primary objective of a post-implementation review.
C. Although it is important to review whether the project was completed on time and budget, it is more important to determine whether the project met the business needs.
**D. A project manager performs a post-implementation review to obtain feedback regarding the project deliverables and business needs and to determine whether the project has successfully met them.**

A3-153 Results of a post-implementation review indicate that only 75 percent of the users can log in to the application concurrently. Which of the following could have **BEST** discovered the identified weakness of the application?

A. Load testing
B. Stress testing
C. Recovery testing
D. Volume testing

**A is the correct answer.**

**Justification:**

**A. Load testing evaluates the performance of the software under normal and peak conditions. Because this application is not supporting normal numbers of concurrent users, the load testing must not have been adequate.**
B. Stress testing determines the capacity of the software to cope with an abnormal number of users or simultaneous operations. Because the number of concurrent users in this question is within normal limits, the answer is load testing, not stress testing.
C. Recovery testing evaluates the ability of a system to recover after a failure.
D. Volume testing evaluates the impact of incremental volume of records (not users) on a system.

A3-154 An IS auditor reviewing the IT project management process is reviewing a feasibility study for a critical project to build a new data center. The IS auditor is **MOST** concerned about the fact that:

A. it has not been determined how the project fits into the overall project portfolio.
B. the organizational impact of the project has not been assessed.
C. not all IT stakeholders have been given an opportunity to provide input.
D. the environmental impact of the data center has not been considered.

**B is the correct answer.**

**Justification:**

A. While projects must be assigned a priority and managed as a portfolio, this most likely occurs after the feasibility study determines that the project is viable.
**B. The feasibility study determines the strategic benefits of the project. Therefore, the result of the feasibility study determines the organizational impact—a comparison report of costs, benefits, risk, etc. The project portfolio is a part of measuring the organizational strategy.**
C. A feasibility study is ordinarily conducted by those with the knowledge to make the decision because the involvement of the entire IT organization is not needed.
D. The environmental impact should be part of the feasibility study however the organizational impact is more important.

Page intentionally left blank