QUESTION 401
When performing a review of the structure of an electronic funds transfer (EFT) system, an IS auditor observes that the technological infrastructure is based on a centralized processing scheme that has been outsourced to a provider in another country. Based on this information, which of the following conclusions should be the main concern of the IS auditor?

- A. There could be a question regarding the legal jurisdiction.
- B. Having a provider abroad will cause excessive costs in future audits.
- C. The auditing process will be difficult because of the distance.
- D. There could be different auditing norms.

Correct Answer: A
Section: IT GOVERNANCE
Explanation: In the funds transfer process, when the processing scheme is centralized in a different country, there could be legal issues of jurisdiction that might affect the right to perform a review in the other country. The other choices, though possible, are not as relevant as the issue of legal jurisdiction.

QUESTION 402
An IS auditor should expect which of the following items to be included in the request for proposal (RFP) when IS is procuring services from an independent service provider (ISP)?

- A. References from other customers
- B. Service level agreement (SLA) template
- C. Maintenance agreement
- D. Conversion plan

Correct Answer: A
Section: IT GOVERNANCE
Explanation: An IS auditor should look for an independent verification that the ISP can perform the tasks being contracted for. References from other customers would provide an independent, external review and verification of procedures and processes the ISP follows—issues which would be of concern to an IS auditor.

QUESTION 403
To minimize costs and improve service levels an outsourcer should seek which of the following contract clauses?

- A. O/S and hardware refresh frequencies
- B. Gain-sharing performance bonuses
- C. Penalties for noncompliance
- D. Charges tied to variable cost metrics

Correct Answer: B
Section: IT GOVERNANCE
Explanation: Gain-sharing performance bonuses provide a financial incentive for the outsourcer to exceed the stated contract terms and can lead to cost savings for the client.

QUESTION 404
When an organization is outsourcing their information security function, which of the following should be kept in the organization?

- A. Accountability for the corporate security policy
- B. Defining the corporate security policy
- C. Implementing the corporate security policy
- D. Defining security procedures and guidelines

Correct Answer: A
Section: IT GOVERNANCE
Explanation: Accountability cannot be transferred to external parties. Choices B, C, and D can be performed by outside entities as long as accountability remains within the organization.

QUESTION 405
An IS auditor has been assigned to review IT structures and activities recently outsourced to various providers. Which of the following should the IS auditor determine FIRST?
- A. That an audit clause is present in all contracts
- B. That the SLA of each contract is substantiated by appropriate KPIs
- C. That the contractual warranties of the providers support the business needs of the organization
- D. That at contract termination, support is guaranteed by each outsourcer for new outsourcers

Correct Answer: C
Section: IT GOVERNANCE
Explanation: The complexity of IT structures matched by the complexity and interplay of responsibilities and warranties may affect or void the effectiveness of those warranties and the reasonable certainty that the business needs will be met.

QUESTION 406
With respect to the outsourcing of IT services, which of the following conditions should be of GREATEST concern to an IS auditor?
- A. Outsourced activities are core and provide a differentiated advantage to the organization.
- B. Periodic renegotiation is specified in the outsourcing contract.
- C. The outsourcing contract fails to cover every action required by the arrangement.
- D. Similar activities are outsourced to more than one vendor.

Correct Answer: A
Section: IT GOVERNANCE
Explanation: An organization's core activities generally should not be outsourced because they are what the organization does best; an IS auditor observing that should be concerned.

QUESTION 407
While conducting an audit of a service provider, an IS auditor observes that the service provider has outsourced a part of the work to another provider. Since the work involves confidential information, the IS auditor's PRIMARY concern should be that the:
- A. requirement for protecting confidentiality of information could be compromised.
- B. contract may be terminated because prior permission from the outsourcer was not obtained.
- C. other service provider to whom work has been outsourced is not subject to audit.
- D. outsourcer will approach the other service provider directly for further work.

Correct Answer: A
Section: IT GOVERNANCE
Explanation: The potential risk that the confidentiality of the information will be compromised is the primary concern in this scenario.

QUESTION 408
Which of the following is the BEST information source for management to use as an aid in the identification of assets that are subject to laws and regulations?
- A. Security incident summaries
- B. Vendor best practices
- C. CERT coordination center
- D. Significant contracts

Correct Answer: D
Section: IT GOVERNANCE
Explanation: Contractual requirements are one of the sources that should be consulted to identify the requirements for the management of information assets.

QUESTION 409

An organization has outsourced its help desk activities. An IS auditor's GREATEST concern when reviewing the contract and associated service level agreement (SLA) between the organization and vendor should be the provisions for:

- A. documentation of staff background checks.
- B. independent audit reports or full audit access.
- C. reporting the year-to-year incremental cost reductions.
- D. reporting staff turnover, development or training.

Correct Answer: B
Section: IT GOVERNANCE
Explanation: Ensuring that independent audit reports are available is crucial to verify that the outsourced functions meet the necessary standards.

QUESTION 410
Which of the following is the MOST important IS audit consideration when an organization outsources a customer credit review system to a third-party service provider? The provider:

- A. meets or exceeds industry security standards.
- B. agrees to be subject to external security reviews.
- C. has a good market reputation for service and experience.
- D. complies with security policies of the organization.

Correct Answer: B
Section: IT GOVERNANCE
Explanation: It is critical that an independent security review of an outsourcing vendor be obtained because customer credit information will be kept there.

QUESTION 411
The risks associated with electronic evidence gathering would MOST likely be reduced by an email:

- A. destruction policy.
- B. security policy.
- C. archive policy.
- D. audit policy.

Correct Answer: C
Section: IT GOVERNANCE
Explanation: A well-archived email policy allows for specific email records to be retrieved without disclosing other confidential records.

QUESTION 412
The output of the risk management process is an input for making:

- A. business plans.
- B. audit charters.
- C. security policy decisions.
- D. software design decisions.

Correct Answer: C
Section: IT GOVERNANCE
Explanation: The risk management process focuses on making security-related decisions, such as the level of acceptable risk.

QUESTION 413
An IS auditor was hired to review e-business security. The IS auditor's first task was to examine each existing e-business application looking for vulnerabilities. What would be the next task?

- A. Report the risks to the CIO and CEO immediately
- B. Examine e-business applications in development
- C. Identify threats and likelihood of occurrence
- D. Check the budget available for risk management

Correct Answer: C
Section: IT GOVERNANCE
Explanation: After identifying vulnerabilities, the next step is to assess the threats and their likelihood of occurrence.

QUESTION 414
Which of the following is a mechanism for mitigating risks?
- A. Security and control practices
- B. Property and liability insurance
- C. Audit and certification
- D. Contracts and service level agreements (SLAs)

Correct Answer: A
Section: IT GOVERNANCE
Explanation: Risks are mitigated by implementing appropriate security and control practices.

QUESTION 415
When developing a risk management program, what is the FIRST activity to be performed?
- A. Threat assessment
- B. Classification of data
- C. Inventory of assets
- D. Criticality analysis

Correct Answer: C
Section: IT GOVERNANCE
Explanation: Identification of the assets to be protected is the first step in the development of a risk management program.

QUESTION 416
A team conducting a risk analysis is having difficulty projecting the financial losses that could result from a risk. To evaluate the potential losses, the team should:
- A. compute the amortization of the related assets.
- B. calculate a return on investment (ROI).
- C. apply a qualitative approach.
- D. spend the time needed to define exactly the loss amount.

Correct Answer: C
Section: IT GOVERNANCE
Explanation: When it is difficult to calculate financial losses, a qualitative approach is often the best method to assess potential impact.

QUESTION 417
Which of the following does a lack of adequate security controls represent?
- A. Threat
- B. Asset
- C. Impact
- D. Vulnerability

Correct Answer: D
Section: IT GOVERNANCE
Explanation: The lack of adequate security controls is considered a vulnerability, exposing information to risks.

QUESTION 418
Assessing IT risks is BEST achieved by:
- A. evaluating threats associated with business processes.
- B. applying regulatory requirements to controls.

- C. calculating the return on investment (ROI) on security controls.
- D. defining and assessing security controls.

Correct Answer: A
Section: IT GOVERNANCE
Explanation: Business process assessment helps evaluate threats to information and IT risks, aligning with operational requirements.

QUESTION 419
During an audit, the IS auditor finds that a large number of employees have been accessing files that they have no business reason to view. The BEST recommendation is to implement:

- A. access controls based on business functions.
- B. a monitoring tool to track employee file access.
- C. mandatory training sessions on security policy.
- D. an audit of employee access to critical files.

Correct Answer: A
Section: IT GOVERNANCE
Explanation: Implementing access controls based on business functions will help ensure employees can only access files relevant to their roles.

QUESTION 420
In the context of business continuity, the primary purpose of an incident management process is to ensure:

- A. all incidents are managed to minimize their impact on business operations.
- B. training for incident management staff is conducted.
- C. the incident response team is notified quickly.
- D. audits of incident management practices are performed regularly.

Correct Answer: A
Section: IT GOVERNANCE
Explanation: The main objective of incident management is to minimize the impact of incidents on business operations

QUESTION 421
An IS auditor reviewing the risk assessment process of an organization should FIRST:

- **A.** identify the reasonable threats to the information assets.
- **B.** analyze the technical and organizational vulnerabilities.
- **C.** identify and rank the information assets.
- **D.** evaluate the effect of a potential security breach.

Correct Answer: C
Section: IT GOVERNANCE
Explanation: Identification and ranking of information assets set the scope for assessing risk, guiding the analysis of threats and vulnerabilities.

QUESTION 422
An IS auditor is reviewing an IT security risk management program. Measures of security risk should:

- **A.** address all of the network risks.
- **B.** be tracked over time against the IT strategic plan.
- **C.** take into account the entire IT environment.
- **D.** result in the identification of vulnerability tolerances.

Correct Answer: C
Section: IT GOVERNANCE
Explanation: Security risk measures must consider the entire IT environment to prioritize critical areas for risk reduction.

QUESTION 423
Which of the following should be considered FIRST when implementing a risk management program?
- **A.** An understanding of the organization's threat, vulnerability and risk profile.
- **B.** An understanding of the risk exposures and the potential consequences of compromise.
- **C.** A determination of risk management priorities based on potential consequences.
- **D.** A risk mitigation strategy sufficient to keep risk consequences at an acceptable level.

Correct Answer: A
Section: IT GOVERNANCE
Explanation: Understanding the organization's threat, vulnerability, and risk profile is crucial as a foundational step in risk management.

QUESTION 424
As a driver of IT governance, transparency of IT's cost, value and risks is primarily achieved through:
- **A.** performance measurement.
- **B.** strategic alignment.
- **C.** value delivery.
- **D.** resource management.

Correct Answer: A
Section: IT GOVERNANCE
Explanation: Performance measurement provides stakeholders with information on IT performance compared to objectives, ensuring transparency.

QUESTION 425
Which of the following should be the MOST important consideration when deciding areas of priority for IT governance implementation?
- **A.** Process maturity.
- **B.** Performance indicators.
- **C.** Business risk.
- **D.** Assurance reports.

Correct Answer: C
Section: IT GOVERNANCE
Explanation: Prioritizing areas representing known risks to the enterprise's operations is essential for effective governance implementation.

QUESTION 426
The PRIMARY benefit of implementing a security program as part of a security governance framework is the:
- **A.** alignment of the IT activities with IS audit recommendations.
- **B.** enforcement of the management of security risks.
- **C.** implementation of the chief information security officer's (CISO) recommendations.
- **D.** reduction of the cost for IT security.

Correct Answer: B
Section: IT GOVERNANCE
Explanation: The main benefit is the effective management of security risks and monitoring residual risks post-implementation.

QUESTION 427
An IS auditor who is reviewing incident reports discovers that, in one instance, an important document left on an employee's desk was removed and put in the garbage by the outsourced cleaning staff. Which of the following should the IS auditor recommend to management?
- **A.** Stricter controls should be implemented by both the organization and the cleaning agency.
- **B.** No action is required since such incidents have not occurred in the past.

- **C.** A clear desk policy should be implemented and strictly enforced in the organization.
- **D.** A sound backup policy for all important office documents should be implemented.

Correct Answer: A
Section: IT GOVERNANCE
Explanation: Implementing strict controls with the cleaning agency is necessary to prevent unauthorized access to sensitive documents.

QUESTION 428
During an audit, an IS auditor notices that the IT department of a medium-sized organization has no separate risk management function, and the organization's operational risk documentation only contains a few broadly described IT risks. What is the MOST appropriate recommendation in this situation?

- **A.** Create an IT risk management department and establish an IT risk framework with the aid of external risk management experts.
- **B.** Use common industry standard aids to divide the existing risk documentation into several individual risks which will be easier to handle.
- **C.** No recommendation is necessary since the current approach is appropriate for a medium-sized organization.
- **D.** Establish regular IT risk management meetings to identify and assess risks, and create a mitigation plan as input to the organization's risk management.

Correct Answer: D
Section: IT GOVERNANCE
Explanation: Regular meetings for risk identification and assessment are vital for managing risks effectively in a medium-sized organization.

QUESTION 429
The IT balanced scorecard is a business governance tool intended to monitor IT performance evaluation indicators other than:

- **A.** financial results.
- **B.** customer satisfaction.
- **C.** internal process efficiency.
- **D.** innovation capacity.

Correct Answer: A
Section: IT GOVERNANCE
Explanation: The IT balanced scorecard focuses on key performance indicators beyond just financial results.

QUESTION 430
Before implementing an IT balanced scorecard, an organization must:

- **A.** deliver effective and efficient services.
- **B.** define key performance indicators.
- **C.** provide business value to IT projects.
- **D.** control IT expenses.

Correct Answer: B
Section: IT GOVERNANCE
Explanation: Defining key performance indicators is essential for the successful implementation of an IT balanced scorecard.

QUESTION 431
Which of the following is the PRIMARY objective of an IT performance measurement process?

- **A.** Minimize errors.
- **B.** Gather performance data.
- **C.** Establish performance baselines.
- **D.** Optimize performance.

Correct Answer: D
Section: SYSTEMS AND INFRASTRUCTURE LIFECYCLE MANAGEMENT
Explanation: The primary objective is to optimize performance across IT services and products.

QUESTION 432
When auditing the proposed acquisition of a new computer system, an IS auditor should FIRST establish 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.

Correct Answer: A
Section: SYSTEMS AND INFRASTRUCTURE LIFECYCLE MANAGEMENT
Explanation: A clear business case is essential to ensure the acquisition aligns with business needs.

QUESTION 433
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.

Correct Answer: A
Section: SYSTEMS AND INFRASTRUCTURE LIFECYCLE MANAGEMENT
Explanation: The business case should be retained throughout the life cycle for reference and evaluation.

QUESTION 434
Which of the following risks could result from inadequate software baselining?

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

Correct Answer: A
Section: SYSTEMS AND INFRASTRUCTURE LIFECYCLE MANAGEMENT
Explanation: Inadequate baselining can lead to scope creep due to uncontrolled changes during development.

QUESTION 435
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 user 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.

Correct Answer: D
Section: SYSTEMS AND INFRASTRUCTURE LIFECYCLE MANAGEMENT
Explanation: Lack of adequate user involvement often results in systems that do not meet user needs.

QUESTION 436
Many IT projects experience problems because the development time and/or resource requirements are underestimated. Which of the following techniques would provide the GREATEST assistance in developing an estimate of project duration?

- **A.** Function point analysis.
- **B.** PERT chart.

- **C.** Rapid application development.
- **D.** Object-oriented system development.

Correct Answer: B
Section: SYSTEMS AND INFRASTRUCTURE LIFECYCLE MANAGEMENT
Explanation: A PERT chart helps in determining project duration by analyzing the tasks and their interdependencies.

QUESTION 437
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.

Correct Answer: C
Section: SYSTEMS AND INFRASTRUCTURE LIFECYCLE MANAGEMENT
Explanation: A freezing point allows for a review of changes to ensure they are cost-effective and justified.

QUESTION 438
Change control for business application systems being developed using prototyping could be complicated by the:

- **A.** iterative nature of prototyping.
- **B.** need for constant user feedback.
- **C.** complexity of the proposed systems.
- **D.** lack of documentation.

Correct Answer: A
Section: SYSTEMS AND INFRASTRUCTURE LIFECYCLE MANAGEMENT
Explanation: The iterative nature of prototyping makes it difficult to control changes since prototypes are continuously modified based on feedback.

QUESTION 439
An IS auditor is reviewing the project management practices of a large organization. The organization is implementing a major information system and, at the project's outset, has not established a formal project management process. Which of the following would be the MOST effective recommendation for the organization?

- **A.** Establish a project steering committee.
- **B.** Implement project management software tools.
- **C.** Develop a project charter and project management plan.
- **D.** Hire an external project manager.

Correct Answer: C
Section: SYSTEMS AND INFRASTRUCTURE LIFECYCLE MANAGEMENT
Explanation: Establishing a project charter and plan is fundamental to ensure proper project management practices are followed.

QUESTION 440
Which of the following is MOST important to consider when determining whether to convert to an automated system?

- **A.** Cost of system maintenance.
- **B.** Internal controls needed to secure the data.
- **C.** User training requirements.
- **D.** Efficiency of the new system.

Correct Answer: D
Section: SYSTEMS AND INFRASTRUCTURE LIFECYCLE MANAGEMENT

Explanation: The efficiency of the new system is crucial to determine whether automation provides a net benefit over current processes.

QUESTION 440

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

Correct Answer: B

Explanation:

Adding personnel may alter the sequence of activities on the critical path, potentially reducing the overall project duration. The critical path determines the longest stretch of dependent activities, so adding resources must be evaluated against its impact on this path before adjusting the budget, remaining task lengths, or personnel assignments. Other tasks might not be directly impacted since they may have slack time available.

QUESTION 441

Which of the following is a characteristic of timebox management?

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

Correct Answer: C

Explanation:

Timebox management sets strict boundaries for time and cost, making it suitable for rapid application development (RAD) and preventing cost overruns and delivery delays. It encourages focused work within limited timeframes but does not eliminate the need for a quality process. System and user acceptance testing are integrated, rather than separated.

QUESTION 442

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

Correct Answer: C

Explanation:

A project portfolio database contains data such as project owner, schedules, objectives, type, status, and costs, which are necessary for managing multiple projects. This helps in evaluating the effectiveness of controls. A project database pertains to single projects, while policy documents provide guidance, and program organization defines team roles but does not give a holistic view of project management controls.

QUESTION 443

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-up 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 during testing to maximize the defect detection rate.
- **D.** Mainly at project close-down to capture lessons learned that can be applied to future projects.

Correct Answer: A
Explanation:
Quality management techniques are most cost-effective when applied early, close to the point of origination. The earlier defects are identified and resolved, the lower the cost of correcting them. Waiting until later phases, such as during testing, increases rework costs. Lessons learned should be captured but applying techniques throughout the project yields better outcomes.

QUESTION 444
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.

Correct Answer: B
Explanation:
Activities with zero slack time are on the critical path, which determines the overall project duration. Reducing time on these activities, often through paying a premium (crashing), can shorten the total project time. Activities with slack time do not impact the overall project duration and thus are not suitable for speeding up completion.

QUESTION 445
At the completion of a system development project, a postproject review should include which of the following?

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

Correct Answer: B
Explanation:
A postproject review aims to gather lessons learned for future projects. While assessing risks and verifying controls are important, they are more relevant to the acceptance testing and production phases. Deleting test data is a separate operational procedure, not a key focus of postproject reviews.

QUESTION 446
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 risks associated with the project have been analyzed.
- **B.** Resources needed throughout the project have been determined.
- **C.** Project deliverables have been identified.
- **D.** A contract for external parties involved in the project has been completed.

Correct Answer: A
Explanation:
At the project initiation stage, the IS auditor’s main focus should be on ensuring that the complexity and risks have been properly analyzed, as these factors are critical to a project’s success. Other aspects like resources, deliverables, and contracts are important but are determined based on the complexity and risk assessment.

QUESTION 447
An IS auditor invited to a development project meeting notes that no project risks have been documented. When the IS auditor raises this issue, the project manager responds that it is too early to identify risks and that, if risks do start 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 risks, and to develop contingency plans.
- **B.** Accept the project manager's position as 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 risks at the completion of the requirements definition phase of the project.

Correct Answer: A
Explanation:
The IS auditor should emphasize the importance of early risk identification and documentation, as this is a critical aspect of effective project management. Waiting until risks materialize can lead to project failure, while early risk management allows for mitigation strategies.

QUESTION 448
While evaluating software development practices in an organization, an IS auditor notes that the quality assurance (QA) function reports to project management. The MOST important concern for an IS auditor is the:

- **A.** effectiveness of the QA function because it should interact between project management and user management.
- B. efficiency of the QA function because it should interact with the project implementation team.
- C. effectiveness of the project manager because the project manager should interact with the QA function.
- D. efficiency of the project manager because the QA function will need to communicate with the project implementation team.

Correct Answer: A
Explanation: To be effective, the quality assurance (QA) function should be independent of project management. The QA function should interact between project management and user management but should not be directly involved with the project implementation team, as that could compromise its independence and effectiveness.

QUESTION 449
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, even 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, even if resource allocation is decreased.
- D. decreases in delivery time can only be achieved if quality is decreased.

Correct Answer: A
Explanation: The project management triangle consists of three dimensions: scope, time, and cost. If resource allocation is decreased, quality can still be improved if there is flexibility in extending the project's delivery time. Therefore, adjusting one dimension can impact the others to maintain the balance.

QUESTION 450
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 conduct of the project and the business case.

Correct Answer: D

Explanation: The IS auditor should first review the project and its business case to understand the reasons for the time and cost overruns before making recommendations. It's essential to assess the situation fully before concluding whether governance or management issues are present.

QUESTION 451
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 (EACs)?

- A. Function point analysis
- **B.** Earned value analysis
- C. Cost budget
- D. Program Evaluation and Review Technique (PERT)

Correct Answer: B
Explanation: Earned value analysis (EVA) is a widely used method to measure project progress and forecast completion time and costs. EVA compares the planned work with actual work completed to determine if the project is progressing according to plan.

QUESTION 452
When reviewing an active project, an IS auditor observed that, because of a reduction in anticipated benefits and increased costs, the business case was no longer valid. 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 reapproval.
- D. project be completed and the business case be updated later.

Correct Answer: B
Explanation: The IS auditor should recommend updating the business case as it is a key input for decision-making during the project's lifecycle. It's important to keep the business case current and reassess the project's value before deciding on any course of action.

QUESTION 453
An organization is implementing an enterprise resource planning (ERP) application to meet its business objectives. 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 (SPDT)
- **C.** Project steering committee
- D. User project team (UPT)

Correct Answer: C
Explanation: The project steering committee is responsible for overseeing the project's progress to ensure it meets business objectives. The project sponsor funds the project but does not oversee daily progress, while the development and user teams focus on specific tasks rather than overall project direction.

QUESTION 454
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

Correct Answer: D

Explanation: The data owner is responsible for ensuring that data migration is complete, accurate, and valid before going live. The IS auditor may verify that this process is followed, but the primary responsibility for data sign-off rests with the data owner.

QUESTION 455
A project manager of a project that is scheduled to take 18 months to complete announces that the project is in a healthy financial position because, after 6 months, only one-sixth of the budget has been spent. The IS auditor should FIRST determine:

- **A.** what amount of progress against the schedule has been achieved.
- 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.

Correct Answer: A
Explanation:
The IS auditor should assess the actual progress made relative to the project schedule to understand the relationship between the time elapsed and the budget spent. Spending less than anticipated could be a sign of slow progress, and without knowing the amount of work done, the project's status cannot be properly assessed.

QUESTION 456
A manager of a project was not able to implement all audit recommendations by the target date. The IS auditor should:

- A. recommend that the project be halted until the issues are resolved.
- B. recommend that compensating controls be implemented.
- **C.** evaluate risks associated with the unresolved issues.
- D. recommend that the project manager reallocate test resources to resolve the issues.

Correct Answer: C
Explanation:
The IS auditor should first assess the risks posed by the unresolved audit recommendations. Once the risks are evaluated, management can make informed decisions, such as implementing compensating controls or accepting the risk, if appropriate.

QUESTION 457
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.

Correct Answer: C
Explanation:
Extrapolating the overall end date based on completed work packages and current resources gives the IS auditor a realistic estimation of the project's final completion date. This method relies on actual progress, making it more reliable than subjective estimations or calculations based on the budget alone.

QUESTION 458
Which of the following situations would increase the likelihood of fraud?

- **A.** Application programmers are implementing changes to production programs.

- B. Application programmers are implementing changes to test programs.
- C. Operations support staff are implementing changes to batch schedules.
- D. Database administrators are implementing changes to data structures.

Correct Answer: A
Explanation:
Allowing application programmers to implement changes directly to production programs could lead to fraudulent activity. This situation bypasses segregation of duties and introduces the risk of unauthorized modifications to critical applications.

QUESTION 459
The purpose of a checksum on an amount field in an electronic data interchange (EDI) communication of financial transactions is to ensure:

- **A.** integrity.
- B. authenticity.
- C. authorization.
- D. nonrepudiation.

Correct Answer: A
Explanation:
A checksum is used to verify the integrity of the data by ensuring that no unauthorized modifications have occurred. It helps detect accidental or intentional data alterations during transmission.

QUESTION 460
Before implementing controls, management should FIRST ensure that the controls:

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

Correct Answer: A
Explanation:
Controls should address specific risk issues effectively. While other factors like cost-benefit analysis and impact on productivity are important, the primary purpose of implementing a control is to mitigate a risk. Hence, management should first ensure that the control addresses the identified risk.

QUESTION 461
Information for detecting unauthorized input from a terminal would be BEST provided by the:

- **A.** Console log printout
- **B.** Transaction journal
- **C.** Automated suspense file listing
- **D.** User error report

Correct Answer: B
Explanation:
The transaction journal records all transaction activity, which can be compared to authorized source documents to identify any unauthorized input. The other options either do not capture all terminal activities or are specific to particular types of errors.

QUESTION 462
Which of the following types of data validation editing checks is used to determine if a field contains data and not zeros or blanks?

- **A.** Check digit
- **B.** Existence check
- **C.** Completeness check
- **D.** Reasonableness check

Correct Answer: C
Explanation:
A completeness check ensures that a field contains valid data (i.e., not zeros or blanks). A check digit validates data integrity, an existence check ensures data entry follows predetermined criteria, and a reasonableness check ensures input data fall within expected ranges.

QUESTION 463
The editing/validation of data entered at a remote site would be 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

Correct Answer: D
Explanation:
Data should be edited and validated at the remote site before transmission to the central site to prevent erroneous or incomplete data from entering the central system.

QUESTION 464
To reduce the possibility of losing data during processing, the FIRST point at which control totals should be implemented is:

- **A.** During data preparation
- **B.** In transit to the computer
- **C.** Between related computer runs
- **D.** During the return of the data to the user department

Correct Answer: A
Explanation:
Control totals should be implemented during data preparation, as it is the earliest opportunity to establish data integrity before processing begins.

QUESTION 465
Functional acknowledgements are used:

- **A.** As an audit trail for EDI transactions
- **B.** To functionally describe the IS department
- **C.** To document user roles and responsibilities
- **D.** As a functional description of application software

Correct Answer: A
Explanation:
Functional acknowledgements in EDI transactions confirm the receipt of electronic documents, which serves as an audit trail. The other choices are unrelated to functional acknowledgements.

QUESTION 466
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

Correct Answer: D
Explanation:
Automated systems balancing ensures that total inputs match total outputs, alerting the organization to any lost transactions. Other controls help validate data but do not specifically detect lost transactions.

QUESTION 467
What process uses test data as part of a comprehensive test of program controls in a continuous online manner?

- **A.** Test data/deck
- **B.** Base-case system evaluation
- **C.** Integrated test facility (ITF)
- **D.** Parallel simulation

Correct Answer: B
Explanation:
A base-case system evaluation involves using test data as part of a comprehensive test to verify correct system operations and validate them over time. The other methods focus on specific test types but lack the continuous monitoring element.

QUESTION 468
What control detects transmission errors by appending calculated bits onto the end of each segment of data?

- **A.** Reasonableness check
- **B.** Parity check
- **C.** Redundancy check
- **D.** Check digits

Correct Answer: C
Explanation:
A redundancy check appends calculated bits to detect transmission errors. Parity checks are hardware controls, reasonableness checks compare data to predefined limits, and check digits detect transposition or transcription errors.

QUESTION 469
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

Correct Answer: B
Explanation:
A check digit is calculated mathematically and appended to data to ensure its integrity. It is particularly effective in detecting transposition and transcription errors.

QUESTION 470
Which of the following is the GREATEST risk when implementing a data warehouse?

- **A.** Increased response time on the production systems
- **B.** Access controls that are not adequate to prevent data modification
- **C.** Data duplication
- **D.** Data that is not updated or current

Correct Answer: B
Explanation:
Access control deficiencies pose the greatest risk since data in a warehouse should not be modified. Data duplication is inherent in warehousing, and delayed updates are manageable risks, while response times typically don't affect the warehouse environment directly.

QUESTION 471
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.** Postimplementation reviews

Correct Answer: B

Explanation:

Detailed and correctly applied specifications are essential for offshore development projects to ensure that the business needs are communicated clearly despite any physical or cultural distance. While the other factors are important, well-defined specifications are most critical for success.

QUESTION 472

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

Correct Answer: C

Explanation:

Collusion between employees poses the greatest risk to system controls because it allows individuals to bypass even well-designed controls. Inadequate manuals or unresolved compliance issues are important but not as impactful as collusion in undermining controls.

QUESTION 473

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

Correct Answer: B

Explanation:

A transaction audit trail's main purpose is to ensure accountability and responsibility by tracking the entire transaction process. Although it helps an auditor trace transactions, its primary role is to establish responsibility for the actions taken.

QUESTION 474

An appropriate control for ensuring the authenticity of orders received in an EDI application is to:

- **A.** Acknowledge receipt of electronic orders with a confirmation message
- **B.** Perform reasonableness checks on quantities ordered before filling orders
- **C.** Verify the identity of senders and determine if orders correspond to contract terms
- **D.** Encrypt electronic orders

Correct Answer: C

Explanation:

Verifying the identity of the sender and ensuring the orders match contract terms is critical in an EDI system to confirm authenticity. While encryption and acknowledgment messages are important, they do not ensure authenticity by themselves.

QUESTION 475

A manufacturing firm wants to automate its invoice payment system. Objectives state that the system should require considerably less time for review and authorization, and the system should be capable of identifying errors that require follow-up. Which of the following would BEST meet these objectives?

- **A.** Establishing an inter-networked system of client servers with suppliers for increased efficiencies
- **B.** Outsourcing the function to a firm specializing in automated payments and accounts receivable/invoice processing

- **C.** Establishing an EDI system of electronic business documents and transactions with key suppliers, computer-to-computer, in a standard format
- **D.** Reengineering the existing processing and redesigning the existing system

Correct Answer: C

Explanation:

An EDI system provides real-time electronic document exchange between businesses, allowing automation of invoice payments and the ability to identify and resolve errors quickly, fulfilling the firm's objectives. Other options do not provide the same level of automation and efficiency.

QUESTION 476

An IS auditor is told by IS management that the organization has recently reached the highest level of the software capability maturity model (CMM). The software quality process MOST recently added by the organization is:

- **A.** Continuous improvement
- **B.** Quantitative quality goals
- **C.** A documented process
- **D.** A process tailored to specific projects

Correct Answer: A

Explanation:

The highest level of the CMM is Level 5 (Optimizing), which focuses on continuous improvement of processes. Quantitative quality goals are associated with Level 4 (Managed), and a documented process is a feature of Level 3 (Defined).

QUESTION 477

During the audit of an acquired software package, an IS auditor learned that the software purchase was based on information obtained through the Internet, rather than from responses to a request for proposal (RFP). 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

Correct Answer: D

Explanation:

The IS auditor should first confirm that the procedure followed for acquiring the software was approved by appropriate authorities. This ensures the process aligns with business objectives and established procedures.

QUESTION 478

Failure 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

Correct Answer: B

Explanation:

Failure during acceptance testing has the greatest impact since it is the final stage before the software is implemented. It would delay the deployment and result in costly fixes. Failures in system, integration, and unit testing occur earlier and are less impactful.

QUESTION 479

An organization has an integrated development environment (IDE) on which the program libraries reside

on the server, but modification/development and testing are done from PC workstations. Which of the following would be a strength of an IDE?

- **A.** Controls the proliferation of multiple versions of programs
- **B.** Expands the programming resources and aids available
- **C.** Increases program and processing integrity
- **D.** Prevents valid changes from being overwritten by other changes

Correct Answer: B
Explanation:
A strength of an IDE is that it provides programmers with enhanced resources and tools, which help in development and testing. The other options are weaknesses that can occur in an IDE environment.

QUESTION 480
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

Correct Answer: A
Explanation:
The quality of the metadata is the most crucial element in a data warehouse, as it defines the structure and meaning of the data. Accurate metadata ensures that users can efficiently query and analyze the data. Transaction speed and data volatility are less critical in this context.

QUESTION 481
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

Correct Answer: C
Explanation:
Stress testing should be conducted in a test environment using live workloads to simulate real-world conditions without affecting the production environment. Testing with live workloads ensures that the system can handle expected traffic and user behavior.

Question 482
Which of the following is an object-oriented technology characteristic that permits an enhanced degree of security over data?
A. Inheritance
B. Dynamic warehousing
C. Encapsulation
D. Polymorphism
Correct Answer: C
Explanation: Encapsulation is a property that restricts access to data by only allowing defined methods and properties to interact with it. This enhances security by preventing unauthorized access.

Question 483
Which of the following is a dynamic analysis tool for the purpose of testing software modules?
A. Black box test
B. Desk checking
C. Structured walkthrough
D. Design and code

Correct Answer: A
Explanation: A black box test is a dynamic analysis tool for testing software modules without internal knowledge, relying on input and output results.

Question 484
The phases and deliverables of a system development life cycle (SDLC) 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 risks and exposures.
D. Only after all risks and exposures have been identified and the IS auditor has recommended appropriate controls.
Correct Answer: A
Explanation: Proper project planning, including defining phases and deliverables, is crucial early in the project to ensure success and address risks from the start.

Question 485
Which of the following is a management technique that enables organizations to develop strategically important systems faster, while reducing development costs and maintaining quality?
A. Function point analysis
B. Critical path methodology
C. Rapid application development
D. Program evaluation review technique
Correct Answer: C
Explanation: Rapid application development (RAD) focuses on faster delivery of systems, reducing costs and ensuring quality.

Question 486
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
Correct Answer: C
Explanation: Incorrectly set parameters can significantly disrupt the functionality of the software, making it the greatest risk during implementation.

Question 487
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. It ensures that functions or extras are not added to the intended system.
Correct Answer: B
Explanation: Prototyping can save time and costs by allowing early user feedback and iterative adjustments, but it can also lead to weaker internal controls.

Question 488
A decision support system (DSS):
A. Is aimed at solving highly structured problems.
B. Combines the use of models with nontraditional data access and retrieval functions.
C. Emphasizes flexibility in the decision-making approach of users.
D. Supports only structured decision-making tasks.

Correct Answer: C
Explanation: DSS is designed to be flexible in supporting decision-making, especially for semi-structured or unstructured problems.

Question 489
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.
Correct Answer: D
Explanation: Using sanitized live transactions ensures that the test data closely resembles actual production data, making the tests more realistic.

Question 490
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.
Correct Answer: B
Explanation: Using a live production file poses a risk of exposing sensitive data unless the data is properly sanitized.

Question 491
Which of the following is the PRIMARY purpose for conducting parallel testing?
A. To determine if 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
Correct Answer: D
Explanation: Parallel testing is primarily conducted to verify that the new system meets user requirements by comparing its performance against the existing system.

Question 492
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
Correct Answer: B
Explanation: Decision trees guide users through a series of questions or choices to reach a conclusion, making them a key component of the knowledge base in expert systems.

Question 493
An advantage in using a bottom-up vs. 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.
Correct Answer: C

Explanation: Bottom-up testing identifies errors in critical modules earlier, as testing starts at the program or module level.

Question 494
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. Postimplementation review
Correct Answer: B
Explanation: During the requirements definition phase, user acceptance test plans are developed to ensure that the system meets user needs.

Question 495
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.
Correct Answer: A
Explanation: Object-oriented design encourages the reuse of modules, making it easier to repurpose components across different systems or applications.

Question 496
Which of the following should be included in a feasibility study for a project to implement an EDI process?
A. The encryption algorithm format
B. The detailed internal control procedures
C. The necessary communication protocols
D. The proposed trusted third-party agreement
Correct Answer: C
Explanation: Communication protocols must be included in the feasibility study to assess costs and technical risks associated with implementing the EDI process.

Question 497
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.
Correct Answer: B
Explanation: User acceptance testing is essential to verify that the system works as intended, especially when time is limited for implementation.

Question 498
An organization has contracted with a vendor for a turnkey solution for their electronic toll collection system (ETCS). The vendor has provided its proprietary application software as part of the solution. The contract should require that:
A. A backup server be available to run ETCS operations with up-to-date data.
B. A backup server be loaded with all the relevant software and data.
C. The systems staff of the organization be trained to handle any event.
D. Source code of the ETCS application be placed in escrow.

Correct Answer: D
Explanation: To ensure future maintenance or updates, the source code should be placed in escrow in case the vendor goes out of business.

Question 499
The MOST likely explanation for the use of applets in an Internet application is that:
A. It is sent over the network from the server.
B. The server does not run the program and the output is not sent over the network.
C. They improve the performance of the web server and network.
D. It is a JAVA program downloaded through the web browser and executed by the web server of the client machine.
Correct Answer: C
Explanation: Applets are small programs that run on the client side, reducing the load on the web server and improving overall network performance.

Question 500
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.
Correct Answer: B
Explanation: A quality plan is critical to ensure the project's success. Its absence is a major concern because it affects the overall quality and delivery of the system.