QUESTION 301
Though management has stated otherwise, an IS auditor has reasons to believe that the organization is using software that is not licensed. In this situation, the IS auditor should:
A. Include the statement of management in the audit report.
B. Identify whether such software is, indeed, being used by the organization.
C. Reconfirm with management the usage of the software.
D. Discuss the issue with senior management since reporting this could have a negative impact on the organization.
Correct Answer: B
Explanation: The IS auditor must gather sufficient evidence before reporting the use of unlicensed software. Simply relying on management's claims is not enough; independent verification is required to maintain objectivity.

QUESTION 302
While reviewing sensitive electronic work papers, the IS auditor noticed that they were not encrypted. This could compromise the:
A. Audit trail of the versioning of the work papers.
B. Approval of the audit phases.
C. Access rights to the work papers.
D. Confidentiality of the work papers.
Correct Answer: D
Explanation: Encryption is essential to ensure the confidentiality of sensitive electronic work papers. Without encryption, they are vulnerable to unauthorized access.

QUESTION 303
The MOST important reason for an IS auditor to obtain sufficient and appropriate audit evidence is to:
A. Comply with regulatory requirements.
B. Provide a basis for drawing reasonable conclusions.
C. Ensure complete audit coverage.
D. Perform the audit according to the defined scope.
Correct Answer: B
Explanation: The purpose of gathering evidence is to support the audit conclusions. This helps in identifying and validating control weaknesses.

QUESTION 304
After initial investigation, an IS auditor has reasons to believe that fraud may be present. The IS auditor should:
A. Expand activities to determine whether an investigation is warranted.
B. Report the matter to the audit committee.
C. Report the possibility of fraud to top management and ask how they would like to proceed.
D. Consult with external legal counsel to determine the course of action to be taken.
Correct Answer: A
Explanation: The IS auditor must evaluate fraud indicators further before recommending a formal investigation, ensuring that the fraud suspicion is substantial.

QUESTION 305
Which of the following should an IS auditor use to detect duplicate invoice records within an invoice master file?
A. Attribute sampling
B. Generalized audit software (GAS)
C. Test data
D. Integrated test facility (ITF)

Correct Answer: B
Explanation: GAS allows for a comprehensive review of all records and can easily identify duplicate invoices, which sampling methods or other tests might miss.

QUESTION 306
Which of the following would be the MOST effective audit technique for identifying segregation of duties violations in a new ERP implementation?
A. Reviewing a report of security rights in the system
B. Reviewing the complexities of authorization objects
C. Building a program to identify conflicts in authorization
D. Examining recent access rights violation cases
Correct Answer: C
Explanation: Developing a program that can systematically identify authorization conflicts is the most efficient and effective way to identify segregation of duties violations in an ERP system.

QUESTION 307
Which of the following would an IS auditor use to determine if unauthorized modifications were made to production programs?
A. System log analysis
B. Compliance testing
C. Forensic analysis
D. Analytical review
Correct Answer: B
Explanation: Compliance testing helps verify whether the change management process was followed consistently and only authorized changes were made to production programs.

QUESTION 308
During a change control audit of a production system, an IS auditor finds that the change management process is not formally documented and that some migration procedures failed. What should the IS auditor do next?
A. Recommend redesigning the change management process.
B. Gain more assurance on the findings through root cause analysis.
C. Recommend that program migration be stopped until the change process is documented.
D. Document the finding and present it to management.
Correct Answer: B
Explanation: Before making recommendations, the auditor must ensure that the incidents were indeed due to deficiencies in the change management process and not another cause.

QUESTION 309
During the collection of forensic evidence, which of the following actions would MOST likely result in the destruction or corruption of evidence on a compromised system?
A. Dumping the memory content to a file
B. Generating disk images of the compromised system
C. Rebooting the system
D. Removing the system from the network
Correct Answer: C
Explanation: Rebooting a compromised system can change the system state and potentially destroy evidence, especially in volatile memory.

QUESTION 310
An IS auditor who was involved in designing an organization's business continuity plan (BCP) has been assigned to audit the plan. The IS auditor should:

A. Decline the assignment.
B. Inform management of the possible conflict of interest after completing the audit assignment.
C. Inform the business continuity planning (BCP) team of the possible conflict of interest prior to beginning the assignment.
D. Communicate the possibility of conflict of interest to management prior to starting the assignment.
Correct Answer: D
Explanation: It is important to disclose any potential conflicts of interest, like involvement in the design of the BCP, to management before proceeding with the audit.

QUESTION 311
An IS auditor conducting a review of software usage and licensing discovers that numerous PCs contain unauthorized software. Which of the following actions should the IS auditor take?
A. Personally delete all copies of the unauthorized software.
B. Inform the auditee of the unauthorized software, and follow up to confirm deletion.
C. Report the use of the unauthorized software and the need to prevent recurrence to auditee management.
D. Take no action, as it is a commonly accepted practice and operations management is responsible for monitoring such use.
Correct Answer: C
Explanation: The use of unauthorized or illegal software should be prohibited by an organization. Software piracy results in inherent exposure and can result in severe fines. An IS auditor must convince the user and user management of the risk and the need to eliminate the risk.

QUESTION 312
Corrective action has been taken by an auditee immediately after the identification of a reportable finding. The auditor should:
A. Include the finding in the final report, because the IS auditor is responsible for an accurate report of all findings.
B. Not include the finding in the final report, because the audit report should include only unresolved findings.
C. Not include the finding in the final report, because corrective action can be verified by the IS auditor during the audit.
D. Include the finding in the closing meeting for discussion purposes only.
Correct Answer: A
Explanation: Including the finding in the final report is a generally accepted audit practice. If an action is taken after the audit started and before it ended, the audit report should identify the finding and describe the corrective action taken.

QUESTION 313
During an implementation review of a multiuser distributed application, an IS auditor finds minor weaknesses in three areas - the initial setting of parameters is improperly installed, weak passwords are being used, and some vital reports are not being checked properly. While preparing the audit report, the IS auditor should:
A. Record the observations separately with the impact of each of them marked against each respective finding.
B. Advise the manager of probable risks without recording the observations, as the control weaknesses are minor ones.
C. Record the observations and the risk arising from the collective weaknesses.
D. Apprise the departmental heads concerned with each observation and properly document it in the report.
Correct Answer: C
Explanation: Individually the weaknesses are minor; however, together they have the potential to substantially weaken the overall control structure.

QUESTION 314
During an exit interview, in cases where there is disagreement regarding the impact of a finding, an IS auditor should:
A. Ask the auditee to sign a release form accepting full legal responsibility.
B. Elaborate on the significance of the finding and the risks of not correcting it.
C. Report the disagreement to the audit committee for resolution.
D. Accept the auditee's position since they are the process owners.
Correct Answer: B
Explanation: If the auditee disagrees with the impact of a finding, it is important for an IS auditor to elaborate and clarify the risks and exposures, as the auditee may not fully appreciate the magnitude of the exposure.

QUESTION 315
When preparing an audit report, the IS auditor should ensure that the results are supported by:
A. Statements from IS management.
B. Workpapers of other auditors.
C. An organizational control self-assessment.
D. Sufficient and appropriate audit evidence.
Correct Answer: D
Explanation: ISACA's standard on 'reporting' requires the IS auditor to have sufficient and appropriate audit evidence to support the reported results.

QUESTION 316
The final decision to include a material finding in an audit report should be made by the:
A. Audit committee.
B. Auditee's manager.
C. IS auditor.
D. CEO of the organization.
Correct Answer: C
Explanation: The IS auditor should make the final decision about what to include or exclude from the audit report to maintain independence.

QUESTION 317
A PRIMARY benefit derived from an organization employing control self-assessment (CSA) techniques is that it:
A. Can identify high-risk areas that might need a detailed review later.
B. Is a cost-effective way to conduct a comprehensive audit.
C. Engages staff in the risk management process.
D. Reduces the need for external audits.
Correct Answer: C
Explanation: Engaging staff in the risk management process is a significant advantage of using CSA techniques. It enhances accountability and promotes a control-conscious culture.

QUESTION 318
Which of the following would an IS auditor recommend for ensuring compliance with privacy regulations?
A. Conducting periodic employee training on data protection.
B. Using encryption technology for all sensitive data.
C. Implementing a data classification policy.
D. Establishing an incident response plan.
Correct Answer: A
Explanation: Regular training helps ensure that employees are aware of privacy regulations and the organization’s policies, making them more effective at compliance.

QUESTION 319
An IS auditor is preparing an audit report on an application under development. Which of the following aspects should be emphasized as the MOST important?
A. That the project is on schedule.
B. That proper change management processes are followed.
C. That the application meets the user requirements.
D. That the application is developed using a formal methodology.
Correct Answer: B
Explanation: Emphasizing proper change management is crucial in development projects, as it mitigates risks associated with unauthorized changes.

QUESTION 320
An IS auditor has identified that an organization's firewall is configured to allow outbound traffic on all ports. What is the MOST significant risk associated with this configuration?
A. Exposure to external threats.
B. Data leakage.
C. Misconfiguration of security policies.
D. Increased administrative overhead.
Correct Answer: B
Explanation: Allowing unrestricted outbound traffic significantly increases the risk of data leakage, as sensitive information could be exfiltrated easily without appropriate controls.

QUESTION 321
An IT steering committee should review information systems PRIMARILY to assess:
- A. whether IT processes support business requirements.
- B. if proposed system functionality is adequate.
- C. the stability of existing software.
- D. the complexity of installed technology.

Correct Answer: A
Section: IT GOVERNANCE
Explanation: The primary role of an IT steering committee is to ensure that the IS department aligns with the organization's mission and objectives. This involves assessing whether IT processes support business requirements. The other options are too narrow in scope.

QUESTION 322
The MOST likely effect of the lack of senior management commitment to IT strategic planning is:
- A. a lack of investment in technology.
- B. a lack of a methodology for systems development.
- C. technology not aligning with the organization's objectives.
- D. an absence of control over technology contracts.

Correct Answer: C
Section: IT GOVERNANCE
Explanation: The absence of a senior management commitment can lead to misalignment between IT and organizational strategy, increasing the risk of IT projects not meeting business objectives.

QUESTION 323
Which of the following is a function of an IS steering committee?
- A. Monitoring vendor-controlled change control and testing
- B. Ensuring a separation of duties within the information's processing environment
- C. Approving and monitoring major projects, the status of IS plans and budgets
- D. Liaising between the IS department and the end users

Correct Answer: C
Section: IT GOVERNANCE
Explanation: The IS steering committee primarily serves as a review board for major IS projects, approving and monitoring their progress without becoming involved in routine operations.

QUESTION 324
An IS steering committee should:
- A. include a mix of members from different departments and staff levels.
- B. ensure that IS security policies and procedures have been executed properly.
- C. have formal terms of reference and maintain minutes of its meetings.
- D. be briefed about new trends and products at each meeting by a vendor.

Correct Answer: C
Section: IT GOVERNANCE
Explanation: Maintaining detailed minutes is crucial for documenting decisions and activities. This accountability is important for informing the board of directors about the committee's actions.

QUESTION 325
Involvement of senior management is MOST important in the development of:
- A. strategic plans.
- B. IS policies.
- C. IS procedures.
- D. standards and guidelines.

Correct Answer: A
Section: IT GOVERNANCE
Explanation: Senior management involvement is critical to ensure that strategic plans align with organizational goals and objectives.

QUESTION 326
Effective IT governance will ensure that the IT plan is consistent with the organization's:
- A. business plan.
- B. audit plan.
- C. security plan.
- D. investment plan.

Correct Answer: A
Section: IT GOVERNANCE
Explanation: IT governance requires that IT and business strategies are aligned to support the organization’s goals.

QUESTION 327
Establishing the level of acceptable risk is the responsibility of:
- A. quality assurance management.
- B. senior business management.
- C. the chief information officer.
- D. the chief security officer.

Correct Answer: B
Section: IT GOVERNANCE
Explanation: Senior management is responsible for establishing acceptable risk levels due to their accountability for organizational operations.

QUESTION 328
IT governance is PRIMARILY the responsibility of the:
- A. chief executive officer.
- B. board of directors.

- C. IT steering committee.
- D. audit committee.

Correct Answer: B
Section: IT GOVERNANCE
Explanation: IT governance is the responsibility of the board of directors, who provide strategic direction and oversight.

QUESTION 329
As an outcome of information security governance, strategic alignment provides:
- A. security requirements driven by enterprise requirements.
- B. baseline security following best practices.
- C. institutionalized and commoditized solutions.
- D. an understanding of risk exposure.

Correct Answer: A
Section: IT GOVERNANCE
Explanation: Strategic alignment ensures that security requirements are aligned with the overall enterprise goals and objectives.

QUESTION 330
Which of the following IT governance best practices improves strategic alignment?
- A. Supplier and partner risks are managed.
- B. A knowledge base on customers, products, markets, and processes is in place.
- C. A structure is provided that facilitates the creation and sharing of business information.
- D. Top management mediate between the imperatives of business and technology.

Correct Answer: D
Section: IT GOVERNANCE
Explanation: Top management mediation is essential for ensuring that IT strategies align with business needs and objectives.

QUESTION 331
Effective IT governance requires organizational structures and processes to ensure that:
- A. the organization's strategies and objectives extend the IT strategy.
- B. the business strategy is derived from an IT strategy.
- C. IT governance is separate and distinct from the overall governance.
- D. the IT strategy extends the organization's strategies and objectives.

Correct Answer: D
Section: IT GOVERNANCE
Explanation: IT governance must align IT strategies with organizational goals, ensuring IT supports and extends those objectives.

QUESTION 332
Which of the following is the MOST important element for the successful implementation of IT governance?
- A. Implementing an IT scorecard
- B. Identifying organizational strategies
- C. Performing a risk assessment
- D. Creating a formal security policy

Correct Answer: B
Section: IT GOVERNANCE
Explanation: Identifying organizational strategies is crucial for aligning IT governance with business objectives.

QUESTION 333

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.

Correct Answer: C
Section: IT GOVERNANCE
Explanation: The alignment of IT projects with the business plan is critical for funding and prioritizing IT initiatives.

QUESTION 334
When implementing an IT governance framework in an organization, the MOST important objective is:

- A. IT alignment with the business.
- B. accountability.
- C. value realization with IT.
- D. enhancing the return on IT investments.

Correct Answer: A
Section: IT GOVERNANCE
Explanation: The primary goal of IT governance is to ensure that IT aligns with the organization's strategic objectives.

QUESTION 335
The ultimate purpose of IT governance is to:

- A. encourage optimal use of IT.
- B. reduce IT costs.
- C. decentralize IT resources across the organization.
- D. centralize control of IT.

Correct Answer: A
Section: IT GOVERNANCE
Explanation: IT governance aims to optimize the use of IT resources to support business objectives, not necessarily to reduce costs or centralize/decentralize resources.

QUESTION 336
What is the lowest level of the IT governance maturity model where an IT balanced scorecard exists?

- A. Repeatable but Intuitive
- B. Defined
- C. Managed and Measurable
- D. Optimized

Correct Answer: B
Section: IT GOVERNANCE
Explanation: The IT balanced scorecard is established at the Defined level (level 3) of the IT governance maturity model.

QUESTION 337
Responsibility for the governance of IT should rest with the:

- A. IT strategy committee.
- B. chief information officer (CIO).
- C. audit committee.
- D. board of directors.

Correct Answer: D
Section: IT GOVERNANCE
Explanation: The ultimate accountability for IT governance resides with the board of directors, who set strategic direction and oversight.

QUESTION 338
An IS auditor identifies that reports on product profitability produced by an organization's finance and marketing departments give different results. Further investigation reveals that the product definition being used by the two departments is different. What should the IS auditor recommend?
- A. User acceptance testing (UAT) occur for all reports before release into production
- B. Organizational data governance practices be put in place
- C. Standard software tools be used for report development
- D. Management sign-off on requirements for new reports

Correct Answer: B
Section: IT GOVERNANCE
Explanation: Implementing data governance practices will standardize definitions and improve consistency in reporting across departments.

QUESTION 339
From a control perspective, the key element in job descriptions is that they:
- A. provide instructions on how to do the job and define authority.
- B. are current, documented, and readily available to the employee.
- C. communicate management's specific job performance expectations.
- D. establish responsibility and accountability for the employee's actions.

Correct Answer: D
Section: IT GOVERNANCE
Explanation: Job descriptions are essential for establishing accountability and responsibility, which are crucial from a control perspective.

QUESTION 340
Which of the following would BEST provide assurance of the integrity of new staff?
- A. Background screening
- B. References
- C. Bonding
- D. Qualifications listed on a resume

Correct Answer: A
Section: IT GOVERNANCE
Explanation: Background screening is the most reliable method for verifying the integrity of prospective employees.

QUESTION 341
When an employee is terminated from service, the MOST important action is to:
A. Hand over all of the employee's files to another designated employee.
B. Complete a backup of the employee's work.
C. Notify other employees of the termination.
D. Disable the employee's logical access.
Correct Answer: D
Section: IT GOVERNANCE
Explanation: Disabling the terminated employee's logical access is critical to prevent potential misuse of access rights.

QUESTION 342
Many organizations require an employee to take a mandatory vacation (holiday) of a week or more to:
A. Ensure the employee maintains a good quality of life, which will lead to greater productivity.
B. Reduce the opportunity for an employee to commit an improper or illegal act.
C. Provide proper cross-training for another employee.
D. Eliminate the potential disruption caused when an employee takes vacation one day at a time.

Correct Answer: B
Section: IT GOVERNANCE
Explanation: Mandatory vacations help reduce the opportunity for improper or illegal acts by allowing another employee to review the work.

QUESTION 343
A local area network (LAN) administrator normally would be restricted from:
A. Having end-user responsibilities.
B. Reporting to the end-user manager.
C. Having programming responsibilities.
D. Being responsible for LAN security administration.
Correct Answer: C
Section: IT GOVERNANCE
Explanation: A LAN administrator should not have programming responsibilities to prevent conflicts of interest.

QUESTION 344
A long-term IS employee with a strong technical background and broad managerial experience has applied for a vacant position in the IS audit department. Determining whether to hire this individual for this position should be based on the individual's experience and:
A. Length of service, since this will help ensure technical competence.
B. Age, as training in audit techniques may be impractical.
C. IS knowledge, since this will bring enhanced credibility to the audit function.
D. Ability, as an IS auditor, to be independent of existing IS relationships.
Correct Answer: D
Section: IT GOVERNANCE
Explanation: The candidate's ability to maintain independence is crucial for effective auditing.

QUESTION 345
An IS auditor should be concerned when a telecommunication analyst:
A. Monitors systems performance and tracks problems resulting from program changes.
B. Reviews network load requirements in terms of current and future transaction volumes.
C. Assesses the impact of the network load on terminal response times and network data transfer rates.
D. Recommends network balancing procedures and improvements.
Correct Answer: A
Section: IT GOVERNANCE
Explanation: Monitoring system performance puts the analyst in a self-monitoring role, which can compromise objectivity.

QUESTION 346
When segregation of duties concerns exist between IT support staff and end users, what would be a suitable compensating control?
A. Restricting physical access to computing equipment
B. Reviewing transaction and application logs
C. Performing background checks prior to hiring IT staff
D. Locking user sessions after a specified period of inactivity
Correct Answer: B
Section: IT GOVERNANCE
Explanation: Reviewing logs directly addresses the threat posed by inadequate segregation of duties.

QUESTION 347
An IS auditor reviewing an organization that uses cross-training practices should assess the risk of:

A. Dependency on a single person.
B. Inadequate succession planning.
C. One person knowing all parts of a system.
D. A disruption of operations.
Correct Answer: C
Section: IT GOVERNANCE
Explanation: Assessing the risk of any single employee knowing all parts of a system is critical to identifying potential exposures.

QUESTION 348
Which of the following controls would an IS auditor look for in an environment where duties cannot be appropriately segregated?
A. Overlapping controls
B. Boundary controls
C. Access controls
D. Compensating controls
Correct Answer: D
Section: IT GOVERNANCE
Explanation: Compensating controls are essential to mitigate risks when segregation of duties is not feasible.

QUESTION 349
Which of the following reduces the potential impact of social engineering attacks?
A. Compliance with regulatory requirements
B. Promoting ethical understanding
C. Security awareness programs
D. Effective performance incentives
Correct Answer: C
Section: IT GOVERNANCE
Explanation: Security awareness programs educate users, making them less susceptible to social engineering.

QUESTION 350
Which of the following activities performed by a database administrator (DBA) should be performed by a different person?
A. Deleting database activity logs
B. Implementing database optimization tools
C. Monitoring database usage
D. Defining backup and recovery procedures
Correct Answer: A
Section: IT GOVERNANCE
Explanation: Deleting activity logs should be done by someone other than the DBA to ensure proper segregation of duties.

QUESTION 351
To gain an understanding of the effectiveness of an organization's planning and management of investments in IT assets, an IS auditor should review the:
A. Enterprise data model.
B. IT balanced scorecard (BSC).
C. IT organizational structure.
D. Historical financial statements.
Correct Answer: B
Section: IT GOVERNANCE

Explanation: The IT balanced scorecard links IT objectives to business objectives, providing insight into IT investment management.

QUESTION 352
Which of the following is the BEST performance criterion for evaluating the adequacy of an organization's security awareness training?
A. Senior management is aware of critical information assets and demonstrates adequate concern for their protection.
B. Job descriptions contain clear statements of accountability for information security.
C. In accordance with the degree of risk and business impact, there is adequate funding for security efforts.
D. No actual incidents have occurred that have caused a loss or public embarrassment.
Correct Answer: B
Section: IT GOVERNANCE
Explanation: Including security responsibilities in job descriptions ensures staff awareness of their roles regarding information security.

QUESTION 353
Which of the following is a risk of cross-training?
A. Increases the dependence on one employee
B. Does not assist in succession planning
C. One employee may know all parts of a system
D. Does not help in achieving a continuity of operations
Correct Answer: C
Section: IT GOVERNANCE
Explanation: Cross-training may lead to a situation where one individual knows all aspects of a system, increasing risk exposure.

QUESTION 354
Which of the following is normally a responsibility of the chief security officer (CSO)?
A. Periodically reviewing and evaluating the security policy
B. Executing user application and software testing and evaluation
C. Granting and revoking user access to IT resources
D. Approving access to data and applications
Correct Answer: A
Section: IT GOVERNANCE
Explanation: The CSO is responsible for ensuring that security policies are adequate to protect company assets.

QUESTION 355
To support an organization's goals, an IS department should have:
A. A low-cost philosophy.
B. Long- and short-range plans.
C. Leading-edge technology.
D. Plans to acquire new hardware and software.
Correct Answer: B
Section: IT GOVERNANCE
Explanation: Long- and short-range plans should align with organizational goals to effectively support them.

QUESTION 356
In reviewing the IS short-range (tactical) plan, an IS auditor should determine whether:

A. There is an integration of IS and business staffs within projects.
B. There is a clear definition of the IS mission and vision.
C. A strategic information technology planning methodology is in place.
D. The plan correlates business objectives to IS goals and objectives.
Correct Answer: A
Section: IT GOVERNANCE
Explanation: Integration of IS and business staff within projects is critical for successful tactical planning.

QUESTION 357
Which of the following would an IS auditor consider the MOST relevant to short-term planning for an IS department?
A. Allocating resources
B. Keeping current with technology advances
C. Conducting control self-assessment
D. Evaluating hardware needs
Correct Answer: A
Section: IT GOVERNANCE
Explanation: Allocating resources is crucial in short-term planning to align IT investments with management strategies.

QUESTION 358
Which of the following goals would you expect to find in an organization's strategic plan?
A. Test a new accounting package.
B. Perform an evaluation of information technology needs.
C. Implement a new project planning system within the next 12 months.
D. Become the supplier of choice for the product offered.
Correct Answer: D
Section: IT GOVERNANCE
Explanation: Strategic planning focuses on long-term objectives; thus, becoming a preferred supplier represents a significant business goal.

QUESTION 359
Which of the following would an IS auditor consider to be the MOST important when evaluating an organization's IS strategy? That it:
A. Has been approved by line management.
B. Does not vary from the IS department's preliminary budget.
C. Complies with procurement procedures.
D. Supports the business objectives of the organization.
Correct Answer: D
Section: IT GOVERNANCE
Explanation: The IS strategy must align with the organization's business objectives to be deemed effective.

QUESTION 360
An IS auditor reviewing an organization's IT strategic plan should FIRST review:
A. The existing IT environment.
B. The IT governance structure.
C. The overall corporate strategy.
D. The current IT budget.
Correct Answer: C
Section: IT GOVERNANCE

Explanation: Understanding the overall corporate strategy provides context for evaluating the effectiveness of the IT strategic plan.

QUESTION 361
When reviewing IS strategies, an IS auditor can BEST assess whether IS strategy supports the organizations' business objectives by determining if IS:

- A. has all the personnel and equipment it needs.
- **B. plans are consistent with management strategy.**
- C. uses its equipment and personnel efficiently and effectively.
- D. has sufficient excess capacity to respond to changing directions.

Correct Answer: B
Section: IT GOVERNANCE
Explanation: Determining if the IS plan is consistent with management strategy relates IS/IT planning to business plans. Choices A, C, and D are effective methods for determining the alignment of IS plans with business objectives and the organization's strategies.

QUESTION 362
In an organization, the responsibilities for IT security are clearly assigned and enforced, and an IT security risk and impact analysis is consistently performed. This represents which level of ranking in the information security governance maturity model?

- A. Optimized
- **B. Managed**
- C. Defined
- D. Repeatable

Correct Answer: B
Section: IT GOVERNANCE
Explanation: Boards of directors and executive management can use the information security governance maturity model to establish rankings for security in their organizations. The ranks are nonexistent, initial, repeatable, defined, managed, and optimized. When the responsibilities for IT security in an organization are clearly assigned and enforced and an IT security risk and impact analysis is consistently performed, it is said to be 'managed and measurable.'

QUESTION 363
To aid management in achieving IT and business alignment, an IS auditor should recommend the use of:

- A. control self-assessments.
- B. a business impact analysis.
- **C. an IT balanced scorecard.**
- D. business process reengineering.

Correct Answer: C
Section: IT GOVERNANCE
Explanation: An IT balanced scorecard (BSC) provides the bridge between IT objectives and business objectives by supplementing the traditional financial evaluation with measures to evaluate customer satisfaction, internal processes, and the ability to innovate. Control self-assessment (CSA), business impact analysis (BIA), and business process reengineering (BPR) are insufficient to align IT with organizational objectives.

QUESTION 364
When reviewing the IT strategic planning process, an IS auditor should ensure that the plan:

- A. incorporates state of the art technology.
- B. addresses the required operational controls.
- **C. articulates the IT mission and vision.**
- D. specifies project management practices.

Correct Answer: C
Section: IT GOVERNANCE
Explanation: The IT strategic plan must include a clear articulation of the IT mission and vision. The plan need not address the technology, operational controls, or project management practices.

QUESTION 365
When developing a formal enterprise security program, the MOST critical success factor (CSF) would be the:

- A. establishment of a review board.
- B. creation of a security unit.
- **C. effective support of an executive sponsor.**
- D. selection of a security process owner.

Correct Answer: C
Section: IT GOVERNANCE
Explanation: The executive sponsor would be in charge of supporting the organization's strategic security program, and would aid in directing the organization's overall security management activities. Therefore, support by the executive level of management is the most critical success factor (CSF). None of the other choices are effective without visible sponsorship of top management.

QUESTION 366
When reviewing an organization's strategic IT plan, an IS auditor should expect to find:

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

Correct Answer: A
Section: IT GOVERNANCE
Explanation: An assessment of how well an organization's application portfolio supports the organization's business objectives is a key component of the overall IT strategic planning process. This drives the demand side of IT planning and should convert into a set of strategic IT intentions.

QUESTION 367
The advantage of a bottom-up approach to the development of organizational policies is that the policies:

- A. are developed for the organization as a whole.
- **B. are more likely to be derived as a result of a risk assessment.**
- C. will not conflict with overall corporate policy.
- D. ensure consistency across the organization.

Correct Answer: B
Section: IT GOVERNANCE
Explanation: A bottom-up approach begins by defining operational-level requirements and policies, which are derived and implemented as the result of risk assessments. Choices A, C, and D are advantages of a top-down approach for developing organizational policies.

QUESTION 368
Which of the following is the GREATEST risk of an inadequate policy definition for ownership of data and systems?

- A. User management coordination does not exist.
- **B. Specific user accountability cannot be established.**
- C. Unauthorized users may have access to originate, modify or delete data.
- D. Audit recommendations may not be implemented.

Correct Answer: C
Section: IT GOVERNANCE

Explanation: Without a policy defining who has the responsibility for granting access to specific systems, there is an increased risk that unauthorized users may have access to originate, modify, or delete data.

QUESTION 369
The PRIMARY objective of an audit of IT security policies is to ensure that:

- A. they are distributed and available to all staff.
- **B. security and control policies support business and IT objectives.**
- C. there is a published organizational chart with functional descriptions.
- D. duties are appropriately segregated.

Correct Answer: B
Section: IT GOVERNANCE
Explanation: Business orientation should be the main theme in implementing security. Hence, an IS audit of IT security policies should primarily focus on whether the IT and related security and control policies support business and IT objectives.

QUESTION 370
The rate of change in technology increases the importance of:

- A. outsourcing the IS function.
- **B. implementing and enforcing good processes.**
- C. hiring personnel willing to make a career within the organization.
- D. meeting user requirements.

Correct Answer: B
Section: IT GOVERNANCE
Explanation: Change requires that good change management processes be implemented and enforced.

QUESTION 371
An IS auditor finds that not all employees are aware of the enterprise's information security policy. The IS auditor should conclude that:

- **A. this lack of knowledge may lead to unintentional disclosure of sensitive information.**
- B. information security is not critical to all functions.
- C. IS audit should provide security training to the employees.
- D. the audit finding will cause management to provide continuous training to staff.

Correct Answer: A
Section: IT GOVERNANCE
Explanation: All employees should be aware of the enterprise's information security policy to prevent unintentional disclosure of sensitive information.

QUESTION 372
The development of an IS security policy is ultimately the responsibility of the:

- A. IS department.
- B. security committee.
- C. security administrator.
- **D. board of directors.**

Correct Answer: D
Section: IT GOVERNANCE
Explanation: Normally, the designing of an information systems security policy is the responsibility of top management or the board of directors.

QUESTION 373
Which of the following programs would a sound information security policy MOST likely include to handle suspected intrusions?

- **A. Response**
- B. Correction
- C. Detection
- D. Monitoring

Correct Answer: A
Section: IT GOVERNANCE
Explanation: A sound IS security policy will most likely outline a response program to handle suspected intrusions.

QUESTION 374
Which of the following should be included in an organization's IS security policy?

- A. A list of key IT resources to be secured
- **B. The basis for access authorization**
- C. Identity of sensitive security features
- D. Relevant software security features

Correct Answer: B
Section: IT GOVERNANCE
Explanation: The security policy provides the broad framework of security, as laid down and approved by senior management.

QUESTION 375
Which of the following is the initial step in creating a firewall policy?

- A. A cost-benefit analysis of methods for securing the applications
- **B. Identification of network applications to be externally accessed**
- C. Identification of vulnerabilities associated with network applications to be externally accessed
- D. Creation of an applications traffic matrix showing protection methods

Correct Answer: B
Section: IT GOVERNANCE
Explanation: Identification of the applications required across the network should be identified first.

QUESTION 376
The management of an organization has decided to establish a security awareness program. Which of the following would MOST likely be a part of the program?

- A. Utilization of an intrusion detection system to report incidents
- B. Mandating the use of passwords to access all software
- C. Installing an efficient user log system to track the actions of each user
- **D. Training provided on a regular basis to all current and new employees**

Correct Answer: D
Section: IT GOVERNANCE
Explanation: Training is the only choice that is directed at security awareness.

QUESTION 377
Which of the following is MOST critical for the successful implementation and maintenance of a security policy?

- **A. Assimilation of the framework and intent of a written security policy by all appropriate parties**
- B. Management support and approval for the implementation and maintenance of a security policy
- C. Enforcement of security rules by providing punitive actions for any violation of security rules
- D. Stringent implementation, monitoring, and maintenance of technical controls

Correct Answer: A
Section: IT GOVERNANCE

Explanation: All employees should understand the purpose and implications of the security policy for it to be effective.

QUESTION 378
When reviewing the information security governance framework, an IS auditor should ensure that:
- A. compliance with policies and standards is effectively monitored.
- **B. information security management is aligned with business objectives.**
- C. the organization has adequate resources to support security management.
- D. controls are in place to protect sensitive information.

Correct Answer: B
Section: IT GOVERNANCE
Explanation: The governance framework must be aligned with business objectives; if it is not, information security will not effectively support the business.

QUESTION 379
The PRIMARY objective of security awareness training is to:
- A. comply with regulatory requirements.
- B. define security roles and responsibilities.
- **C. minimize human error.**
- D. ensure that security technology is used properly.

Correct Answer: C
Section: IT GOVERNANCE
Explanation: The purpose of security awareness training is to ensure employees understand their responsibilities regarding security and to reduce the risk of security breaches caused by human error.

QUESTION 380
Which of the following is the BEST approach to protect data integrity in a database management system (DBMS)?
- A. Implementing periodic backups.
- **B. Using data encryption and access controls.**
- C. Using transaction logging and recovery methods.
- D. Using redundant systems.

Correct Answer: B
Section: IT GOVERNANCE
Explanation: Data encryption and access controls provide the most comprehensive protection for data integrity, as they restrict access to authorized users and protect data from unauthorized changes.

QUESTION 381
A top-down approach to the development of operational policies will help ensure:
- **A. that they are consistent across the organization.**
- B. that they are implemented as a part of risk assessment.
- C. compliance with all policies.
- D. that they are reviewed periodically.

Correct Answer: A
Section: IT GOVERNANCE
Explanation: Deriving lower-level policies from corporate policies ensures consistency across the organization. A top-down approach does not ensure compliance or guarantee regular reviews.

QUESTION 382
Which of the following would MOST likely indicate that a customer data warehouse should remain in-house rather than be outsourced to an offshore operation?

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

Correct Answer: C
Section: IT GOVERNANCE
Explanation: Privacy laws prohibiting the cross-border flow of personally identifiable information would necessitate keeping the data warehouse in-house.

QUESTION 383
A retail outlet has introduced radio frequency identification (RFID) tags to create unique serial numbers for all products. Which of the following is the PRIMARY concern associated with this initiative?

- **A. Issues of privacy**
- B. Wavelength can be absorbed by the human body.
- C. RFID tags may not be removable.
- D. RFID eliminates line-of-sight reading.

Correct Answer: A
Section: IT GOVERNANCE
Explanation: Privacy violations are a significant concern as RFID tags can track purchases, potentially linking them to individuals.

QUESTION 384
When developing a security architecture, which of the following steps should be executed FIRST?

- A. Developing security procedures.
- **B. Defining a security policy.**
- C. Specifying an access control methodology.
- D. Defining roles and responsibilities.

Correct Answer: B
Section: IT GOVERNANCE
Explanation: Defining a security policy is the first step in building a security architecture, providing a foundation for other steps.

QUESTION 385
An IS auditor finds that, in accordance with IS policy, IDs of terminated users are deactivated within 90 days of termination. The IS auditor should:

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

Correct Answer: C
Section: IT GOVERNANCE
Explanation: Best practice dictates that user IDs should be deactivated immediately upon termination, regardless of the policy timeframe.

QUESTION 386
An IS auditor is reviewing a project to implement a payment system between a parent bank and a subsidiary. The IS auditor should FIRST verify that the:

- A. technical platforms between the two companies are interoperable.
- **B. parent bank is authorized to serve as a service provider.**
- C. security features are in place to segregate subsidiary trades.
- D. subsidiary can join as a co-owner of this payment system.

Correct Answer: B
Section: IT GOVERNANCE
Explanation: Contractual agreements are crucial for shared services, especially in regulated sectors like banking.

QUESTION 387
IT control objectives are useful to IS auditors, as they provide the basis for understanding the:

- **A. desired result or purpose of implementing specific control procedures.**
- B. best IT security control practices relevant to a specific entity.
- C. techniques for securing information.
- D. security policy.

Correct Answer: A
Section: IT GOVERNANCE
Explanation: IT control objectives articulate the desired outcomes for implementing control procedures in IT activities.

QUESTION 388
The initial step in establishing an information security program is the:

- A. development and implementation of an information security standards manual.
- B. performance of a comprehensive security control review by the IS auditor.
- **C. adoption of a corporate information security policy statement.**
- D. purchase of security access control software.

Correct Answer: C
Section: IT GOVERNANCE
Explanation: A policy statement reflects executive management's intent and support for security, serving as the foundation for the security program.

QUESTION 389
Which of the following provides the best evidence of the adequacy of a security awareness program?

- A. The number of stakeholders including employees trained at various levels.
- B. Coverage of training at all locations across the enterprise.
- C. The implementation of security devices from different vendors.
- **D. Periodic reviews and comparison with best practices.**

Correct Answer: D
Section: IT GOVERNANCE
Explanation: Regular reviews and comparisons with best practices are the best indicators of the adequacy of security awareness content.

QUESTION 390
The PRIMARY objective of implementing corporate governance by an organization's management is to:

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

Correct Answer: A
Section: IT GOVERNANCE
Explanation: Corporate governance aims to provide strategic direction, ensuring that risks are managed and resources utilized effectively.

QUESTION 391
Which of the following should an IS auditor recommend to BEST enforce alignment of an IT project portfolio with strategic organizational priorities?

- A. Define a balanced scorecard (BSC) for measuring performance.

- B. Consider user satisfaction in the key performance indicators (KPIs).
- **C. Select projects according to business benefits and risks.**
- D. Modify the yearly process of defining the project portfolio.

Correct Answer: C
Section: IT GOVERNANCE
Explanation: Selecting projects based on expected business benefits and related risks is the most effective way to align with strategic priorities.

QUESTION 392
An example of a direct benefit to be derived from a proposed IT-related business investment is:

- A. enhanced reputation.
- B. enhanced staff morale.
- C. the use of new technology.
- **D. increased market penetration.**

Correct Answer: D
Section: IT GOVERNANCE
Explanation: Direct benefits from IT investments are quantifiable financial benefits, such as increased market penetration.

QUESTION 393
To assist an organization in planning for IT investments, an IS auditor should recommend the use of:

- A. project management tools.
- B. an object-oriented architecture.
- C. tactical planning.
- **D. enterprise architecture (EA).**

Correct Answer: D
Section: IT GOVERNANCE
Explanation: Enterprise architecture helps document IT assets and processes, facilitating understanding and planning for IT investments.

QUESTION 394
A benefit of open system architecture is that it:

- **A. facilitates interoperability.**
- B. facilitates the integration of proprietary components.
- C. will be a basis for volume discounts from equipment vendors.
- D. allows for the achievement of more economies of scale for equipment.

Correct Answer: A
Section: IT GOVERNANCE
Explanation: Open systems allow for components from different vendors to work together due to defined public standards.

QUESTION 395
In the context of effective information security governance, the primary objective of value delivery is to:

- **A. optimize security investments in support of business objectives.**
- B. implement a standard set of security practices.
- C. institute a standards-based solution.
- D. implement a continuous improvement culture.

Correct Answer: A
Section: IT GOVERNANCE
Explanation: Value delivery aims to ensure security investments are optimized to align with business objectives.

QUESTION 396

Which of the following BEST supports the prioritization of new IT projects?

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

Correct Answer: C
Section: IT GOVERNANCE
Explanation: Investment portfolio analysis clarifies investment strategy and justifies project prioritization.

QUESTION 397
After the merger of two organizations, multiple self-developed legacy applications from both companies are to be replaced by a new common platform. Which of the following would be the GREATEST risk?

- A. Project management and progress reporting is combined in a project management office driven by external consultants.
- **B. The replacement effort consists of several independent projects without integrating the resource allocation in a portfolio management approach.**
- C. The resources of each organization are inefficiently allocated while familiarizing with the other company's legacy systems.
- D. The new platform will force the business areas of both organizations to change their work processes, which will result in extensive training needs.

Correct Answer: B
Section: IT GOVERNANCE
Explanation: Lack of centralized resource allocation in independent projects increases the risk of misestimating resource availability.

QUESTION 398
Which of the following is the MOST important function to be performed by IS management when a service has been outsourced?

- A. Ensuring that invoices are paid to the provider.
- B. Participating in systems design with the provider.
- C. Renegotiating the provider's fees.
- **D. Monitoring the outsourcing provider's performance.**

Correct Answer: D
Section: IT GOVERNANCE
Explanation: Monitoring the provider's performance is crucial to ensure services meet contractual obligations.

QUESTION 399
Is it appropriate for an IS auditor from a company that is considering outsourcing its IS processing to request and review a copy of each vendor's business continuity plan?

- **A. Yes, to assess the potential risks associated with outsourcing.**
- B. No, it is inappropriate as it could compromise the vendor's confidentiality.
- C. No, it is unnecessary since IS processing is not a critical function.
- D. Yes, but only after a formal non-disclosure agreement is signed.

Correct Answer: A
Section: IT GOVERNANCE
Explanation: Understanding vendors' business continuity plans is essential to evaluate risks and ensure preparedness.

QUESTION 400
An organization wants to ensure that a new information system is cost-effective. The BEST approach is to:

- A. adopt a vendor solution to minimize integration costs.
- **B. conduct a cost-benefit analysis (CBA) prior to investment.**
- C. purchase the most up-to-date technology.
- D. develop the system in-house to reduce licensing costs.

Correct Answer: B
Section: IT GOVERNANCE
Explanation: A cost-benefit analysis helps evaluate whether expected benefits justify the costs involved.