PassQueen
a.k.a dumpsqueen.com

ACCA CIA Challenge Exam

IIA IIA-ACCA

Version Demo

Total Demo Questions: 70

Total Premium Questions: 708

Buy Premium PDF

https://passqueen.com

support@passqueen.com

Topic Break Down

Topic	No. of Questions
Topic 1, Essentials of Internal Auditing	143
Topic 2, Practice of Internal Auditing	211
Topic 3, Business Knowledge for Internal Auditing	354
Total	708

QUESTION NO: 1

According to MA guidance on IT. which of the following controls the routing of data packets to link computers?

A. Operating system.

B. Control environment.

C. Network.

D. Application program code.

ANSWER: C

Explanation:

Network. is correct because the network infrastructure provides the communications paths that connect computers, servers, and other devices. Its networking components and protocols—such as routers, switches, routing tables, and Internet Protocol—determine how packets are forwarded from a source device toward the appropriate destination. A router makes forwarding decisions using destination addressing and available route information, enabling data to travel across one or more interconnected networks. This packet-routing function is a fundamental network-service responsibility and is essential to the availability, integrity, and timely transmission of organizational information.

For an internal auditor assessing IT controls, this means that network controls should address the secure and reliable configuration, administration, monitoring, and change management of routing devices and network paths. Such controls help ensure that communications are directed only through authorized paths and that connectivity supports business processes. The IIA's technology audit guidance discusses the importance of evaluating IT infrastructure and related controls, while the Internet Engineering Task Force's Internet Protocol specification describes the addressing and forwarding model used for packet delivery. See the IIA's Global Technology Audit Guides and RFC 791: Internet Protocol.

QUESTION NO: 2

An organization has established key performance indicators for customer-service response times. Department managers receive a monthly dashboard showing actual performance against the target and are required to explain significant unfavorable variances.

Which of the following best describes this control activity?

A. Management review of performance information.

B. Segregation of duties.

C. Physical safeguarding of assets.

D. Independent reconciliation of records.

ANSWER: A

Explanation:

Management review of performance information. is correct because managers compare reported results with established expectations, investigate significant deviations, and are expected to take or propose corrective action. This type of review is a common control activity that helps management monitor whether operations are achieving intended objectives.

The effectiveness of the control depends on more than producing the dashboard. Management should receive reliable information promptly, defined variance thresholds should trigger review, explanations should be supported, and corrective actions should be monitored when needed. The control is not a reconciliation because it does not compare two independent records to establish agreement, and it is not segregation of duties because it does not separate incompatible responsibilities. COSO's Internal Control—Integrated Framework identifies review and analysis of performance measures as a common form of control activity.

QUESTION NO: 3

In creating a risk-based plan, which of the following best describes a top-down approach to understanding business processes?

A. Identifying the processes at the activity level.

B. Analyzing the organization's strategic plan where the business processes are defined.

C. Analyzing the organization's objectives and identifying the processes needed to achieve the objectives.

D. Identifying the risks affecting the organization, the objectives, and then the processes concerned.

ANSWER: C

Explanation:

Analyzing the organization's objectives and identifying the processes needed to achieve the objectives is the best description of a top-down approach. Top-down analysis starts with the organization’s purpose, strategic objectives, and major objectives for the period. Internal audit then identifies the business processes, activities, resources, and supporting arrangements that are material to delivering those objectives. This establishes a clear line of sight from what the organization is trying to accomplish to the processes whose failure, weakness, or disruption could prevent that accomplishment.

This perspective supports a risk-based internal audit plan because risks are meaningful in relation to objectives. Once objectives and the processes that enable them are understood, internal audit can assess relevant risks, consider the significance of those risks, and prioritize potential engagements accordingly. The approach also helps ensure that planning addresses enterprise-level and strategic concerns rather than beginning with isolated detailed activities. The IIA’s Global Internal Audit Standards require the chief audit executive to develop a risk-based strategy and plan aligned with the organization’s objectives and risk-management processes. See The IIA’s Global Internal Audit Standards and Standard 9.4: Internal Audit Plan.

QUESTION NO: 4

A credit card company detects potential errors in credit card numbers by checking whether all entered numbers contain the correct amount of digits. This is an example of which of the following IT controls?

A. Logic test.

B. Check digits.

C. Data integrity tests.

D. Balancing control activities.

ANSWER: A

Explanation:

Logic test. is correct because it is an input-validation control that evaluates whether entered data satisfies a predefined rule. In this case, the rule is that a credit card number must have the expected number of digits. The application applies that rule at data entry and flags or rejects a value that does not conform, helping prevent incomplete or malformed data from being accepted into processing.

Logic tests support the reliability of application processing by checking relationships, formats, permitted values, or other conditions that should be true before data is accepted. A length requirement is a straightforward logical condition: the entered value either meets the required digit count or it does not. This type of preventive validation is particularly useful for transaction data because it identifies an apparent input error before downstream authorization, posting, reporting, or customer-account processes rely on the value.

The control aligns with secure-development and data-quality practices that require systems to validate input against defined syntactic rules, such as expected length and structure. See the NIST definition of input validation and OWASP’s Input Validation Cheat Sheet.

QUESTION NO: 5

According to IIA guidance, which of the following should be included in the internal audit charter?

A. The minimum resources and competencies needed for the internal audit activity.

B. Identification of the organizational units where engagements are to be performed.

C. Organizational relationships and reporting lines.

D. Assigned responsibilities for designing and implementing controls.

ANSWER: C

Explanation:

Organizational relationships and reporting lines should be included in the internal audit charter because the charter formally establishes the internal audit activity's mandate, authority, and position within the organization. A clear statement of reporting relationships—particularly the chief audit executive's functional reporting relationship to the board and administrative reporting relationship to management—supports the internal audit activity's organizational independence. It also makes clear who approves the charter, risk-based audit plan, budget, and appointment or removal of the chief audit executive, as applicable to the organization's governance structure.

The IIA's Global Internal Audit Standards require the board and chief audit executive to establish, approve, and periodically review an internal audit charter. The charter is expected to document the internal audit activity's position in the organization and its reporting relationships, helping ensure that internal audit has direct access to the board, sufficient authority, and freedom from undue interference when performing its responsibilities. This documentation is foundational to effective governance and enables internal audit to provide independent assurance and advice. See the IIA's Global Internal Audit Standards and its Standards resource page.

QUESTION NO: 6

Which of the following conditions could lead an organization to enter into a new business through internal development rather than through acquisition?

A. It is expected that there will be slow retaliation from incumbents.

B. The acquiring organization has information that the selling organization is weak.

C. The number of bidders to acquire the organization for sale is low.

D. The condition of the economy is poor.

ANSWER: A

Explanation:

It is expected that there will be slow retaliation from incumbents. is correct because internal development, or "build," normally takes time: the organization must develop capabilities, recruit people, create offerings, establish operations, and build customer relationships. A market in which established competitors are expected to respond slowly gives the entrant a valuable window in which to complete this process and gain a foothold. That reduced urgency makes organic entry more feasible and can allow the organization to tailor the new business's resources, systems, culture, and market position to its strategy rather than integrating an acquired entity.

Strategic-entry decisions commonly weigh the speed required to enter, the availability of suitable acquisition targets, transaction and integration risks, and the expected competitive response. When incumbent retaliation is likely to be delayed, the speed advantage that an acquisition can provide is less critical. The organization can therefore capture the benefits of internal development, including gradual investment, direct control over capability creation, and closer alignment with its intended operating model. Competitive rivalry and the reactions of existing firms are central elements of industry analysis, as described in Harvard Business School's overview of the Five Forces. For further discussion of growth through internal development and acquisitions, see OpenStax, Corporate Strategies.

QUESTION NO: 7

Which of the following statements are true regarding the use of heat maps as risk assessment tools?

1. They focus primarily on known risks, limiting the ability to identify new risks.

2. They rely heavily on objective assessments and related risk tolerances.

3. They are too complex to provide an easily understandable view of key risks.

4. They are helpful but limited in value in a rapidly changing environment.

A. 1 and 2 only

B. 1 and 4 only

C. 2 and 3 only

D. 3 and 4 only

ANSWER: B

Explanation:

1 and 4 only is correct. A heat map is a visual risk-reporting and prioritization tool that plots risks according to assessed likelihood and impact, often using color to highlight relative exposure. In practice, it is generally populated from an established risk register or from risks already identified through management's risk-assessment process. Consequently, its usefulness depends on the completeness and currency of those inputs; by itself, it does not function as a forward-looking risk-identification method and may give limited visibility to emerging or previously unidentified risks.

Heat maps are also a point-in-time representation of risk judgments. Their value can therefore diminish quickly when the business environment, strategy, technology, regulation, or threat landscape changes rapidly. Effective risk management requires management and internal audit to refresh risk information, reassess likelihood and impact, and supplement the heat map with ongoing environmental scanning and dialogue about emerging risks. This aligns with the IIA's expectation that internal audit's risk-based planning be dynamic and responsive to changes in risks, opportunities, programs, systems, and controls. See the IIA Global Internal Audit Standards and ISO's overview of ISO 31000 risk management.

QUESTION NO: 8

Which of the following is an example of a risk management avoidance response?

A. Exiting a marketplace.

B. Recalling a product.

C. Obtaining product insurance.

D. Outsourcing production.

ANSWER: A

Explanation:

Exiting a marketplace is a risk-avoidance response because management eliminates the activity, exposure, and associated uncertainty that create the risk. Risk avoidance is an intentional decision not to start, continue, or participate in an activity when the residual exposure is beyond the organization's risk appetite or cannot be managed economically. In this case, leaving the marketplace removes the organization's ongoing exposure to market-specific risks, such as adverse regulation, political instability, sustained losses, or unacceptable strategic uncertainty. The action is therefore directed at the risk source itself, rather than attempting to reduce the likelihood or impact of an event after continuing the activity.

Risk responses should be selected in alignment with the organization's objectives, risk appetite, and governance arrangements. Internal audit may assess whether management has identified and evaluated significant risks and whether the selected response supports organizational objectives, while management remains responsible for making risk decisions.

The IIA's Global Internal Audit Standards describe internal auditing's role in evaluating and contributing to risk management processes. COSO's enterprise risk management framework also recognizes avoiding an activity as a means of addressing risk when exposure is not acceptable. See the IIA Global Internal Audit Standards and COSO Enterprise Risk Management guidance.

QUESTION NO: 9

New environmental regulations require the board to certify that the organization's reported pollutant emissions data is accurate. The chief audit executive (CAE) is planning an audit to provide assurance over the organization's compliance with the environmental regulations. Which of the following groups or individuals is most important for the CAE to consult to determine the scope of the audit?

A. The audit committee of the board.

B. The environmental, health, and safety manager.

C. The organization's external environmental lawyers.

D. The organization's insurance department.

ANSWER: B

Explanation:

The environmental, health, and safety manager is the most important person for the CAE to consult when defining this engagement's scope. This manager ordinarily owns, coordinates, or has detailed operational knowledge of the environmental compliance framework: applicable regulatory requirements, emission sources, monitoring methods, calculation rules, data capture systems, control activities, reporting deadlines, and identified compliance issues. That knowledge enables internal audit to translate the board's certification requirement into a risk-based scope that addresses both the completeness and accuracy of reported emissions data and the controls supporting management's compliance assertion.

Consultation does not transfer responsibility for audit planning or conclusions to management. Rather, it gives the audit team the process understanding needed to identify relevant auditable activities, select significant locations or emission categories, determine appropriate period coverage, and establish suitable testing procedures. The CAE can then independently assess whether the design and operation of governance, risk management, and control processes provide reliable assurance for the required certification.

This approach aligns with the IIA Global Internal Audit Standards' requirements for engagement planning based on objectives, risks, and relevant processes. Environmental compliance programs also commonly depend on documented monitoring, recordkeeping, and reporting controls, as reflected in The IIA Global Internal Audit Standards and the U.S. EPA's compliance resources.

QUESTION NO: 10

Which of the following network types should an organization choose if it wants to allow access only to its own personnel?

A. An extranet

B. A local area network.

C. An intranet

D. The internet

ANSWER: C

Explanation:

An intranet is the appropriate network type because it is a private network designed for use within an organization by its authorized personnel. It commonly uses the same underlying web technologies and Internet Protocol standards as the public

internet, but access is restricted through organizational controls such as user accounts, passwords, multifactor authentication, network segmentation, and access-control rules. This lets employees securely access internal communications, policies, applications, knowledge repositories, and business resources while limiting availability to the organization's workforce.

The defining feature is the intended audience: an intranet serves internal users. Access may be provided on-site or remotely through secure mechanisms such as a virtual private network or identity-aware access controls; it does not need to be confined to one physical location. The IIA's Global Internal Audit Standards emphasize protecting information through appropriate access controls and restricting access according to authorized business need. See the IIA Global Internal Audit Standards. For further technical context on securing access to organizational resources, see NIST SP 800-53 security and privacy controls.

QUESTION NO: 11

Which of the following is the primary purpose of an internal audit activity's ongoing monitoring as part of its quality assurance and improvement program?

A. Provide continual assessment of conformance through routine supervision and review activities.

B. Replace the need for an external quality assessment.

C. Determine whether management has implemented all audit recommendations.

D. Establish the organization's enterprise risk appetite.

ANSWER: A

Explanation:

Ongoing monitoring provides continual assessment of whether internal audit work is performed in conformance with applicable standards and internal methodology. It is embedded in the routine supervision, review, and management of internal audit work. Examples include engagement supervision, workpaper reviews, performance metrics, stakeholder feedback, and review of whether reports and follow-up activities meet established quality requirements.

Ongoing monitoring differs from periodic self-assessments and external quality assessments, which provide more structured evaluations at defined intervals. Together, these activities support continuous improvement and help the CAE maintain an effective quality assurance and improvement program. See the IIA Global Internal Audit Standards and the IIA's Quality Assurance and Improvement Program guidance.

QUESTION NO: 12

Which of the following risks is best addressed by encryption?

A. Information integrity risk.

B. Privacy risk

C. Access risk

D. Software risk

ANSWER: B

Explanation:

Privacy risk is best addressed by encryption because encryption transforms readable information (plaintext) into an unreadable form (ciphertext) that can be restored only by an authorized party holding the appropriate cryptographic key. This protects the confidentiality of sensitive information when it is stored on devices, databases, backups, or cloud services, and when it is transmitted across networks. Consequently, if data are intercepted, lost, or accessed outside an approved process, encryption reduces the likelihood that the exposed data can be understood or misused.

For an internal auditor, the relevant control objective is protecting information from unauthorized disclosure. Audit work should therefore assess whether encryption is applied according to data classification and risk, whether approved cryptographic methods are used, and whether keys are securely generated, stored, rotated, and access-controlled. Encryption is especially important for personal data, financial records, credentials, and other confidential business information. NIST defines confidentiality as preserving authorized restrictions on information access and disclosure, including protecting personal privacy and proprietary information. NIST also identifies cryptography as a mechanism that protects information against unauthorized disclosure. See the NIST definition of confidentiality and NIST cryptography glossary entry.

QUESTION NO: 13

According to IIA guidance, which of the following individuals should receive the final audit report on a compliance engagement for the organization's cash disbursements process?

A. The accounts payable supervisor, accounts payable manager, and controller.

B. The accounts payable manager, purchasing manager, and receiving manager.

C. The accounts payable supervisor, controller, and treasurer.

D. The accounts payable manager, chief financial officer, and audit committee.

ANSWER: A

Explanation:

The accounts payable supervisor, accounts payable manager, and controller should receive the final audit report because they are the appropriate levels of management to act on results from a cash-disbursements compliance engagement. The accounts payable supervisor is positioned to address day-to-day processing practices and implement operational corrections. The accounts payable manager has responsibility for the overall accounts payable function, including policies, staffing, supervision, and remediation of control or compliance issues. The controller has broader financial-control responsibility and sufficient authority to evaluate the significance of the results, oversee corrective action where needed, and ensure matters affecting financial processes receive appropriate attention.

IIA guidance requires the chief audit executive to communicate final engagement results to parties that can ensure the results are given due consideration. Distribution should therefore reach accountable management with both direct process responsibility and adequate authority to initiate, monitor, and sustain corrective actions. For a cash-disbursements process, this distribution group provides an appropriate operational and financial-management path for considering findings and implementing agreed actions. See the IIA's Global Internal Audit Standards, particularly the requirements on communicating engagement results, and the IIA's Standards resources.

QUESTION NO: 14

The following transactions and events occurred during the year:

	January 1	December 31
Finished goods	$90,000	$260,000
Raw materials	$105,000	$130,000
Work in process	$220,000	$175,000

- $300,000 of raw materials were purchased, of which $20,000 were returned because ofdefects

- $600,000 of direct labor costs were incurred.

- S750.000 of manufacturing overhead costs were incurred.

What is the organization's cost of goods sold for the year?

A. $1,480,000

B. $1,500,000

C. $1,610,000

D. $1,650,000

ANSWER: B

Explanation:

$1,500,000 is the organization's cost of goods sold. First, net raw-material purchases are $280,000: the $20,000 returned for defects reduces the $300,000 purchased. Direct labor of $600,000 and manufacturing overhead of $750,000 are then added to materials as manufacturing costs. The inventory amounts in the schedule must also be incorporated: raw-material inventory determines the materials used in production, work-in-process inventory reconciles total manufacturing costs to cost of goods manufactured, and finished-goods inventory reconciles cost of goods manufactured to the cost assigned to goods sold. Applying the beginning and ending inventory balances shown produces a net $130,000 increase in inventory costs that remain unsold or unfinished at year-end. Therefore, the $1,630,000 total current-period manufacturing-cost amount is reduced by $130,000, resulting in cost of goods sold of $1,500,000. This follows the standard inventory-cost flow: materials used plus conversion costs, adjusted for work in process, determines completed production; completed production adjusted for finished-goods inventory determines the expense recognized as cost of goods sold. The IFRS inventory standard describes inventories as costs recognized as expense when the related inventories are sold: IAS 2 Inventories. See also the cost-flow discussion in OpenStax managerial accounting materials.

QUESTION NO: 15

Which of the following scenarios best illustrates the principle of due professional care?

A. An internal auditor evaluates the significant risks arising from a consulting engagement.

B. An internal auditor declares that he would have a conflict of interest in providing planned audit support.

C. An internal auditor has been given sufficient authority to access documents needed to make an appraisal of an issue.

D. An internal auditor uses technology-based audit techniques to ensure that all significant risks are identified.

ANSWER: A

Explanation:

An internal auditor evaluates the significant risks arising from a consulting engagement. This illustrates due professional care because professional care requires internal auditors to apply sound judgment, attentiveness, and an appropriately risk-focused approach when performing their work. Consulting engagements may expose the organization to risks arising from the nature, scope, objectives, stakeholders, and potential effects of the advice provided. Evaluating significant risks helps the auditor determine the level of work, expertise, procedures, and safeguards needed to perform the engagement responsibly.

The IIA's Global Internal Audit Standards describe due professional care as applying the knowledge, skills, and judgment expected of a prudent and competent internal auditor. This includes considering the engagement's complexity, materiality or significance of risks, and the likelihood of errors, fraud, noncompliance, and other adverse outcomes. A deliberate evaluation of significant risks in a consulting engagement directly reflects these expectations and supports advice that is appropriately scoped and reliable. See the IIA's Global Internal Audit Standards and its Standards resources.

QUESTION NO: 16

Which is the least effective form of risk management?

A. Systems-based preventive control.

B. People-based preventive control.

C. Systems-based detective control.

D. People-based detective control.

ANSWER: D

Explanation:

People-based detective control is the least effective form of risk management because it combines two comparatively weaker control characteristics: it relies on human performance and it operates after an event or error has occurred. Human controls can be affected by judgment, attention, training, workload, fatigue, inconsistency, and the possibility of deliberate override. Detective activity can identify a control failure, irregularity, or undesirable outcome, but it generally does not stop the underlying event before its impact begins. The organization may therefore incur losses, operational disruption, compliance exposure, or reputational damage before the matter is detected and addressed.

A sound risk-and-control design gives priority to controls that prevent unwanted events where practical, and uses detective controls to provide monitoring, confirmation, and timely escalation when prevention cannot fully eliminate risk. Where an automated control is appropriately designed, configured, secured, and monitored, its consistent execution generally reduces dependency on individual action. The control framework described by the Committee of Sponsoring Organizations of the Treadway Commission emphasizes controls that help manage risks to acceptable levels, while the Global Internal Audit Standards support evaluating whether governance, risk management, and controls are suitably designed and operating effectively. Thus, a people-dependent control that only discovers problems afterward provides the weakest risk response among the stated choices.

QUESTION NO: 17

When developing the scope of an audit engagement, which of the following would the internal auditor typically not need to consider?

A. The need and availability of automated support.

B. The potential impact of key risks.

C. The expected outcomes and deliverables.

D. The operational and geographic boundaries.

ANSWER: A

Explanation:

The need and availability of automated support is correct because it primarily concerns how the engagement will be performed, including the audit tools and resources that may be used, rather than defining the engagement's scope. Automated support can improve the efficiency, coverage, or analysis performed during an audit, but it does not ordinarily determine the subject matter, organizational units, locations, period, processes, systems, records, or activities included in the engagement.

Under the IIA's Global Internal Audit Standards, engagement planning establishes objectives, scope, timing, and resources. The scope must be sufficient to achieve the engagement objectives and should clearly identify boundaries of the work. Risk considerations and the expected engagement results help ensure that the scope focuses on matters that are meaningful to the organization and capable of meeting the engagement objectives. Operational and geographic boundaries likewise define what is included and excluded. Decisions about automated audit techniques are instead normally addressed as part of selecting appropriate methodologies and allocating resources after, or alongside, planning the work needed to satisfy the defined scope. See the IIA's Global Internal Audit Standards and its Standards resources.

QUESTION NO: 18

During an assurance engagement, an internal auditor discovered that a sales manager approved numerous sales contracts for values exceeding his authorization limit. The auditor reported the finding to the audit supervisor, noting that the sales

manager had additional new contracts under negotiation. According to IIA guidance, which of the following would be the most appropriate next step?

A. The audit supervisor should include the new contracts in the finding for the final audit report.

B. The audit supervisor should communicate the finding to the supervisor of the sales manager through an interim report.

C. The audit supervisor should remind the sales manager of his authority limit for the contracts under negotiation.

D. The auditor should not reference the new contracts, because they are not yet signed and therefore cannot be included in the final report.

ANSWER: B

Explanation:

The audit supervisor should communicate the finding to the supervisor of the sales manager through an interim report. The unauthorized approvals indicate a control failure that may still be operating: additional contracts are being negotiated, so further commitments could be approved beyond delegated authority before the engagement is completed. Timely interim communication gives the responsible level of management an opportunity to intervene promptly, such as by clarifying approval authorities, reviewing pending contracts, and establishing an appropriate approval process. This protects the organization from ongoing exposure while preserving the internal audit activity's role of communicating significant engagement results to the appropriate parties.

IIA guidance recognizes that engagement communications need not wait for the final report when the nature or significance of a matter warrants prompt attention. Communications should be objective, clear, constructive, complete, and timely, and they should be directed to parties able to take corrective action. Escalating the matter to the sales manager's supervisor is therefore appropriate because that person has the managerial authority to address the active control issue and oversee remediation. The final engagement communication can subsequently document the condition, risk, corrective action, and management's response. See the IIA's Global Internal Audit Standards and its guidance on implementation guides.

QUESTION NO: 19

Which of the following is least likely to help ensure that risk is considered in a work program?

A. Risks are discussed with audit client.

B. All available information from the risk-based plan is used.

C. Client efforts to affect risk management are considered.

D. Prior risk assessments are considered.

ANSWER: C

Explanation:

"Client efforts to affect risk management are considered." is least likely to help ensure that risk is appropriately considered in an engagement work program. A work program should translate the engagement risk assessment into specific procedures that address the risks relevant to the engagement's objectives. The most useful inputs are therefore information that identifies, evaluates, or documents those risks—for example, discussions with the auditee about relevant risks, risk information already developed during risk-based planning, and prior risk assessments that remain relevant.

Merely considering an audit client's efforts to affect risk management does not necessarily provide a reliable assessment of the risks that the work program must address. Such efforts may be informal, incomplete, or focused on influencing how risk is perceived rather than identifying and analyzing the underlying risks, their causes, and the controls intended to manage them. Internal audit should use objective, documented, and sufficiently current risk information to determine the procedures needed to achieve engagement objectives.

The IIA's Global Internal Audit Standards require internal auditors to assess risks relevant to the engagement and identify the priority risks to be evaluated, then develop a work program that achieves the engagement objectives. See Standard 13.2: Engagement Risk Assessment and Domain IV of the Global Internal Audit Standards.

QUESTION NO: 20

An internal auditor is evaluating techniques management uses to mitigate risks within a particular product division. Which of the following is an example of risk reduction?

A. Management sells the product division to a competitor.

B. Management outsources the product division to a third party.

C. Management allows the product division to remain unchanged.

D. Management modifies the product division to minimize errors.

ANSWER: D

Explanation:

Management modifies the product division to minimize errors. This is risk reduction because management is changing the process, product design, controls, or operating practices to decrease the likelihood that errors will occur and, potentially, to lessen their resulting impact. Examples could include redesigning workflow steps, automating error-prone activities, adding validation checks, improving quality assurance, or strengthening supervisory review. These actions leave the organization operating the division and retaining the underlying business risk, but they deliberately bring the residual risk down to a level management considers acceptable.

This approach aligns with the IIA's risk-based view of governance, risk management, and control: management identifies and assesses risks, then designs and implements controls or other responses to manage those risks within the organization's risk appetite. In an audit engagement, the internal auditor would assess whether the modifications are suitably designed, implemented, and effective in reducing errors and achieving the intended risk level. The IIA's Global Internal Audit Standards describe the internal audit function's role in evaluating the effectiveness of risk management and control processes. See the IIA Global Internal Audit Standards and the IIA's International Professional Practices Framework.

QUESTION NO: 21

Which of the following does not provide operational assurance that a computer system is operating properly?

A. Performing a system audit.

B. Making system changes.

C. Testing policy compliance.

D. Conducting system monitoring.

ANSWER: B

Explanation:

Making system changes does not itself provide operational assurance that a computer system is operating properly. A system change is an action that modifies software, infrastructure, configuration, interfaces, or operating procedures. Even when it is properly authorized and controlled, implementing a change does not create independent evidence that the system is operating reliably, securely, or in accordance with requirements after the change. In fact, a change can introduce new risks and should be subject to validation, testing, monitoring, and review once implemented.

Operational assurance depends on obtaining objective, timely evidence about the effectiveness of system operations and controls. Assurance work should be sufficiently independent of the activity being assessed and should use evaluation procedures that support a conclusion about whether controls are designed and functioning as intended. The IIA's Global Internal Audit Standards emphasize evaluating governance, risk management, and control processes using appropriate, reliable information. Similarly, continuous monitoring is a recognized approach for maintaining awareness of a system's security and operational condition. See the IIA Global Internal Audit Standards and NIST's Information Security Continuous Monitoring guidance.

QUESTION NO: 22

Which of the following statements accurately describes an internal auditor's responsibility with regard to due professional care?

A. An internal auditor should express an opinion only when consensus with top management has been achieved.

B. An internal auditor's opinion should be based on experience and free of all bias.

C. An internal auditor's opinion should be based on factual evidence.

D. An internal auditor's opinion should be limited to the effectiveness of internal controls.

ANSWER: C

Explanation:

An internal auditor's opinion should be based on factual evidence. Due professional care requires internal auditors to perform their work with the care, skill, and diligence reasonably expected of a prudent and competent internal auditor. A sound conclusion or engagement opinion therefore must arise from an appropriate evaluation of relevant information, rather than from unsupported assumptions or personal preference. Evidence provides the objective foundation for assessing the condition being reviewed, determining whether criteria have been met, and forming conclusions that are credible and adequately supported.

The Global Internal Audit Standards require internal auditors to base conclusions and engagement results on appropriate analyses and evaluations. They must also obtain information that is relevant, reliable, and sufficient to support engagement results and recommendations. Applying due professional care includes considering the nature and significance of the work, the likelihood of material errors or nonconformance, and the relative cost of assurance in relation to potential benefits. In this context, factual evidence is essential because it enables an auditor to exercise professional judgment responsibly and communicate an opinion that stakeholders can rely upon. See the IIA Global Internal Audit Standards and the IIA Standards resources.

QUESTION NO: 23 - (SIMULATION)

According to IIA guidance, which of the following scenarios demonstrates an internal auditor exercising due professional care?

When auditing investments, the auditor identified instruments with which he was unfamiliar. He decided not to select that type of investment in his sample, as he did not have the knowledge needed to A. perform a proper assessment.

B. An auditor was reviewing inventory counts conducted by the warehouse staff. One truck containing an immaterial amount of inventory was off-site and wasn't verified by the auditor.

C. An auditor visited a plant that produces a significant portion of the organization's inventory. The day he arrived, the plant manager was out sick, so the auditor issued the report without interviewing the manager.

D. An auditor in charge needed to have testing completed by the end of the month, but was behind schedule. He identified a junior auditor to conduct the work for him on a complex area of the organization.

ANSWER: See the explanation for the answer

Explanation:

Correct answer: B. The auditor exercised due professional care by not verifying a truck containing an *immaterial* amount of inventory that was off-site.

Due professional care requires auditors to consider the relative materiality, risk, and cost-benefit of audit procedures. It does not require auditing every item when the item is not material and its omission would not reasonably affect the audit conclusion.

A is inappropriate because the auditor should obtain needed competence or assistance rather than exclude an investment type solely because it is unfamiliar.

C is inappropriate because issuing a report without obtaining relevant management input may result in incomplete or unsupported conclusions.
D is inappropriate because assigning a complex area to a junior auditor merely to meet a deadline may not provide the competence and supervision required.

QUESTION NO: 24

A snow removal company is conducting a scenario planning exercise where participating employees consider the potential impacts of a significant reduction in annua snowfall for the coming winter. Which of the following best describes this type of risk?

A. Residual.

B. Net.

C. Inherent.

D. Accepted.

ANSWER: C

Explanation:

Inherent. is correct because the scenario describes the exposure that naturally arises from the snow removal company's business model: its revenue and operational demand depend substantially on snowfall. A significant reduction in annual snowfall could reduce customer demand, contracts, utilization of equipment, and cash flow. Scenario planning identifies and evaluates this underlying uncertainty and its potential effect on objectives before considering specific controls, mitigation actions, insurance, diversification, or management responses.

Inherent risk is therefore the appropriate classification because it represents the level of risk present in the absence of actions designed to alter its likelihood or impact. For a weather-dependent business, variability in snowfall is an external source of uncertainty that is embedded in the nature of the organization's operations. Considering a low-snowfall scenario helps management understand the magnitude of that exposure and make informed decisions about preparedness, strategy, and risk treatment.

This use of scenario analysis aligns with enterprise risk management practices, which consider how uncertainty may affect strategy and performance. See the COSO Enterprise Risk Management executive summary and The IIA's Global Internal Audit Standards for risk-based concepts and terminology.

QUESTION NO: 25

Which of the following is a product-oriented definition of a business rather than a market-oriented definition of a business?

A. We are a people-and-goods mover.

B. We supply energy.

C. We make movies.

D. We provide climate control in the home.

ANSWER: C

Explanation:

"We make movies." is a product-oriented business definition because it defines the organization by the specific thing it produces: movies. A product orientation centers management attention on the current offering, its production, and product-related capabilities. This framing can be useful operationally, but it is narrower than defining the business in terms of the customer need or market problem being served. In marketing strategy, market-oriented definitions are generally broader and customer-focused: they describe the value, outcome, or need fulfilled for customers rather than the particular product currently used to do so. A business defined as making movies may overlook alternative ways audiences could satisfy

entertainment, storytelling, education, or leisure needs, including formats and technologies beyond traditional films. By identifying the business through its present product, the statement illustrates the classic product-versus-market distinction associated with marketing myopia. The concept emphasizes that organizations should understand customer needs and changing markets rather than become limited by a narrow view of their own products. See Harvard Business Review's discussion of Marketing Myopia and the American Marketing Association's definition of marketing.

QUESTION NO: 26

Which of the following methods, if used in conjunction with electronic data interchange (EDI), will improve the organization's cash management program, reduce transaction data input time and errors, and allow the organization to negotiate discounts with EDI vendors based on prompt payment?

A. Electronic funds transfer.

B. Knowledge-based systems.

C. Biometrics.

D. Standardized graphical user interface.

ANSWER: A

Explanation:

Electronic funds transfer is correct because it complements electronic data interchange by enabling the actual movement of payment funds electronically after EDI communicates the associated business documents, such as invoices, purchase orders, and remittance information. Together, these technologies automate the procure-to-pay cycle: EDI reduces manual rekeying of transaction data, which improves speed and accuracy, while electronic funds transfer enables prompt, controlled settlement of obligations. Faster processing and settlement give the organization better visibility over cash outflows and payment timing, strengthening cash-management decisions. It also allows payments to be made within agreed early-payment terms, supporting negotiation and realization of prompt-payment discounts with trading partners or EDI vendors. The combined use of structured electronic transaction data and electronic payment instructions also improves reconciliation because payment and remittance details can be matched systematically. The U.S. Federal Reserve explains that electronic payments transfer value without paper instruments and support efficient payment processing, while the National Institute of Standards and Technology describes EDI as the computer-to-computer exchange of standardized business transaction information. See the Federal Reserve payment systems resources and NIST definition of electronic data interchange.

QUESTION NO: 27

Which of the following options correctly defines a transmission control protocol/Internet protocol (TCP/IP)?

A. System software that acts as an interface between a user and a computer.

B. A standardized set of guidelines that facilitates communication between computers on different networks.

C. System software that translates hypertext markup language to allow users to view a remote webpage.

D. A network of servers used to control a variety of mission-critical operations.

ANSWER: B

Explanation:

TCP/IP is correctly defined as a standardized suite of communication protocols that enables computers and other devices to exchange data across interconnected networks, including the internet. The Internet Protocol component provides addressing and routing so that data packets can be directed toward the intended destination network and host. The Transmission Control Protocol component provides reliable, connection-oriented delivery for applications that need assurance that data arrives accurately and in the correct sequence. Together, these protocols establish common rules that allow systems using different hardware, operating systems, and local networks to communicate interoperably. Although the wording refers to a "set of guidelines," the more precise technical term is a protocol suite: defined rules, message formats, addressing

conventions, and procedures for transmitting data. TCP/IP is foundational to modern network communications because its layered design separates application services from transport, internet-routing, and network-access functions. The Internet Engineering Task Force's foundational TCP specification describes TCP as providing reliable interprocess communication between hosts, while its Internet Protocol specification describes the addressing and routing functions that support packet delivery. See RFC 9293: Transmission Control Protocol and RFC 791: Internet Protocol.

QUESTION NO: 28

A government agency maintains a system of internal control, according to the COSO model, and has made a change to its employee performance reviews and rewards program. This change relates to which of the following components of COSO's internal control framework?

A. Control environment.

B. Control activities.

C. Information and communication.

D. Monitoring activities.

ANSWER: A

Explanation:

Control environment. is correct because COSO identifies the control environment as the foundation for an effective system of internal control. It establishes the standards, structures, and expectations that shape how people perform their responsibilities. A key control-environment principle is that the organization demonstrates a commitment to attracting, developing, and retaining competent individuals in alignment with its objectives. Employee performance evaluations and reward programs directly support this principle: they establish accountability for performance, reinforce desired ethical and control-conscious behaviors, and align employees' incentives with the agency's objectives and internal-control responsibilities.

In a government agency, performance and rewards arrangements are particularly important because management uses them to communicate expectations and ensure that personnel are motivated and held accountable for carrying out assigned duties appropriately. Changes to these human-resource practices therefore affect the tone, accountability, competence, and performance expectations established throughout the organization—core features of the control environment. COSO's Internal Control—Integrated Framework describes the control environment and its principles in its internal control guidance. The U.S. Government Accountability Office likewise identifies human capital and competence-related practices as part of the control environment in the Standards for Internal Control in the Federal Government.

QUESTION NO: 29

An internal auditor is reviewing user access to a purchasing application. The auditor finds that several employees retain access to approve purchase orders after transferring to departments with no purchasing responsibilities.

Which of the following control deficiencies most directly contributed to this condition?

A. Inadequate periodic review of user access.

B. Inadequate physical security over purchasing records.

C. Failure to reconcile supplier statements to accounts payable records.

D. Failure to perform background checks before hiring employees.

ANSWER: A

Explanation:

Inadequate periodic review of user access most directly contributed to the condition. Transfers and role changes can leave users with access that was appropriate under a prior job assignment but is no longer necessary. Periodic access reviews by

responsible managers help identify and remove obsolete, excessive, or incompatible entitlements across the user population.

New-user provisioning controls and termination procedures are important, but they would not necessarily identify access that becomes inappropriate when an employee remains with the organization and changes roles. Effective access governance includes timely updates following personnel changes and periodic recertification of access. See NIST SP 800-53, AC-2 Account Management and the IIA Global Internal Audit Standards.

QUESTION NO: 30

In order to provide useful information for an organization's risk management decisions, which of the following factors is least important to assess?

A. The underlying causes of the risk.

B. The impact of the risk on the organization's objectives.

C. The risk levels of current and future events.

D. The potential for eliminating risk factors.

ANSWER: D

Explanation:

The potential for eliminating risk factors is the least important factor to assess because useful risk-management information must support practical, informed decisions about how risks affect the achievement of objectives. In many circumstances, a risk cannot be eliminated completely: risk is inherent in pursuing opportunities, operating processes, using technology, dealing with third parties, and making strategic choices. Accordingly, decision-makers need information that enables them to understand and manage risk within the organization’s risk appetite rather than assuming that every source of risk can be removed.

Elimination may be an available response in limited cases, such as stopping an activity entirely, but it is not the central basis for evaluating risks or selecting a proportionate response. A meaningful assessment should instead equip management and the board to determine an appropriate treatment approach and whether residual risk is acceptable. The IIA’s Global Internal Audit Standards describe risk management as processes for identifying, assessing, managing, and monitoring risks to the achievement of objectives. ISO 31000 likewise frames risk treatment as selecting and implementing options to modify risk, recognizing that treatment is tailored to the context and need not mean elimination. See the IIA Global Internal Audit Standards and ISO 31000:2018 Risk Management.

QUESTION NO: 31

Which of the following are typical responsibilities for operational management within a risk management program?

1. Implementing corrective actions to address process deficiencies.

2. Identifying shifts in the organization's risk management environment.

3. Providing guidance and training on risk management processes.

4. Assessing the impact of mitigation strategies and activities.

A. 1 and 2 only

B. 1 and 4 only

C. 2 and 3 only

D. 3 and 4 only

ANSWER: B

Explanation:

“1 and 4 only” is correct because operational management owns and manages risk in the processes and activities for which it is accountable. This includes taking timely corrective action when a process deficiency, control gap, or other issue is identified. Corrective actions turn risk-response decisions into operational changes, such as revising procedures, strengthening controls, assigning ownership, or correcting underlying process conditions.

Operational management also needs to assess whether mitigation strategies and related activities are achieving their intended effect. Risk treatment is not complete merely because an action has been implemented; management should monitor results, evaluate the residual risk, and determine whether further adjustment is needed. This ongoing assessment supports informed operational decisions and helps ensure that risk responses remain appropriate as conditions evolve.

The IIA’s Global Internal Audit Standards describe management’s role in establishing and operating processes to manage risks and controls, while internal audit provides independent assurance and advice rather than assuming management responsibility. The IIA’s Three Lines Model likewise places responsibility for managing risk and implementing controls with management. See the IIA Global Internal Audit Standards and IIA Three Lines Model.

QUESTION NO: 32

Due to price risk from the foreign currency purchase of aviation fuel, an airliner has purchased forward contracts to hedge against fluctuations in the exchange rate. When recalculating the exchange losses from individual purchases of jet fuel, which of the following details does the internal auditor need to validate?

1. The hedge documentation designating the hedge.

2. The spot exchange rate on the transaction date.

3. The terms of the forward contract.

4. The amount of fuel purchased.

A. 1 and 2

B. 1 and 4

C. 2 and 3

D. 3 and 4

ANSWER: C

Explanation:

2 and 3 is correct because the recalculation of the foreign-exchange effect associated with a hedged fuel purchase requires the auditor to establish both the relevant market exchange rate and the contractual rate locked in through the forward. The spot exchange rate on the transaction date provides the observable rate used to translate the foreign-currency transaction at initial recognition. This is the essential benchmark for calculating the exchange difference attributable to the underlying purchase. IAS 21 requires a foreign-currency transaction to be recorded using the spot exchange rate at the transaction date; see IAS Plus: IAS 21, The Effects of Changes in Foreign Exchange Rates.

The forward contract terms establish the hedge’s economic inputs, including the contracted forward rate, notional currency amount, maturity date, settlement provisions, and any relevant premium or discount. Validating these terms allows the auditor to independently recompute the amount arising from the forward and assess how it offsets the exchange-rate exposure of the fuel transaction. Forward contracts are derivatives whose value changes in response to underlying variables such as foreign-exchange rates; the contractual terms are therefore fundamental audit evidence for the calculation. The hedge-accounting framework and derivative requirements are addressed in IFRS 9 Financial Instruments.

QUESTION NO: 33

What kind of strategy would be most effective for an organization to adopt in order to implement a unique advertising campaign for selling identical product lines across all of its markets?

A. Export strategy

B. Transnational strategy.

C. Multi-domestic strategy

D. Globalization strategy.

ANSWER: D

Explanation:

Globalization strategy is correct because the organization intends to sell identical product lines in every market and support them with one distinctive advertising campaign across those markets. This reflects a globally integrated, standardized approach: the organization seeks consistency in product positioning, brand identity, and marketing communications rather than tailoring its core offering and campaign separately for each country or region. Standardization can strengthen worldwide brand recognition, create a consistent customer experience, and allow the organization to gain economies of scale by developing campaign assets and product messaging once for broad use. It also supports centralized coordination of the brand and helps ensure that customers encounter the same essential value proposition regardless of where they purchase the product. Globalization is the process through which markets and business activities become increasingly interconnected, enabling organizations to coordinate offerings across national boundaries; see the International Monetary Fund's overview of globalization. The standardized product-and-campaign approach described is therefore most aligned with a globalization strategy, provided the organization has determined that its target markets share sufficiently similar customer needs and response to the campaign's core message. For further context on global business activity and integration, see the World Trade Organization's World Trade Report.

QUESTION NO: 34

Which of the following behaviors could represent a significant ethical risk if exhibited by an organization's board?

1. Intervening during an audit involving ethical wrongdoing.

2. Discussing periodic reports of ethical breaches.

3. Authorizing an investigation of an unsafe product.

4. Negotiating a settlement of an employee claim for personal damages.

A. 1 and 2

B. 1 and 4

C. 2 and 3

D. 3 and 4

ANSWER: B

Explanation:

1 and 4 is correct because both actions can place the board in a position that compromises ethical oversight, accountability, or the perceived integrity of governance. Intervening in an audit concerning ethical wrongdoing may impair the objectivity and independence needed for the matter to be examined and reported without inappropriate influence. The board's oversight role includes supporting an environment in which significant concerns can be escalated, investigated, and addressed fairly.

Negotiating a settlement of an employee's personal-damages claim can also create a significant ethical risk, particularly when the board becomes involved in operational handling of a matter that it may later need to oversee. Direct participation can create actual or perceived conflicts of interest, encourage decisions driven by reputational or financial concerns, and blur the boundary between management's responsibilities and the board's independent oversight role. Sound governance requires appropriate safeguards, transparent handling of conflicts, and clear accountability for sensitive claims.

The IIA's Global Internal Audit Standards emphasize board responsibility for enabling internal audit independence and effective governance arrangements. See the IIA Global Internal Audit Standards and the IIA's Standards and guidance resources.

QUESTION NO: 35

The security department uncovered what appears to be a complex fraud in the accounting department. The CEO has requested the internal audit activity to investigate the fraud. If the internal audit staff lacks the expertise to conduct the investigation, how should the chief audit executive proceed?

A. Disclose the deficiency, and request that the investigation be reassigned to the first line of defense.

B. Proceed with the investigation, as internal auditors are not required to have fraud expertise.

C. Outsource the sensitive investigation to a third-party consultant with fraud expertise.

D. Select a member of the accounting department who is not involved in the fraud to join the investigation team in a consulting capacity.

ANSWER: C

Explanation:

Outsource the sensitive investigation to a third-party consultant with fraud expertise. The chief audit executive is responsible for ensuring that the internal audit activity collectively has, or obtains, the competencies needed to perform its planned services. A complex accounting fraud investigation can require specialized forensic accounting, evidence-preservation, interviewing, data-analysis, and legal-regulatory expertise that the existing internal audit staff may not possess. In this situation, obtaining qualified external assistance enables the investigation to be performed competently, objectively, and with appropriate professional care.

The chief audit executive should establish the external provider's qualifications, scope of work, confidentiality obligations, reporting arrangements, and safeguards for independence and objectivity. Internal audit retains responsibility for appropriately overseeing the engagement and communicating results through established governance channels. Using a specialist also helps protect the integrity of sensitive evidence and supports a defensible investigation process while allowing the internal audit activity to meet its responsibility to provide assurance and advisory services within its available competencies. The IIA's Global Internal Audit Standards require the chief audit executive to ensure access to the knowledge, skills, and other competencies necessary to fulfill the internal audit mandate. See the IIA Global Internal Audit Standards and the IIA's Internal Auditing and Fraud practice guidance.

QUESTION NO: 36

An internal auditor has been asked to conduct an investigation involving allegations of independent contractor fraud. Which of the following controls would be least effective in detecting any potential fraudulent activity?

A. Exception report identifying payment anomalies.

B. Documented policy and procedures.

C. Periodic account reconciliation of contractor charges.

D. Monthly management review of all contractor activity.

ANSWER: B

Explanation:

Documented policy and procedures is the least effective control for detecting potential independent-contractor fraud because its primary purpose is to establish expected conduct, responsibilities, approval requirements, and operating rules. Although well-designed policies and procedures provide an important control foundation and may support prevention, they do not themselves actively identify whether improper payments, fictitious contractors, duplicate billings, inflated charges, or conflicts

of interest have occurred. Detection requires controls that examine actual transactions and activity for evidence of anomalies or noncompliance.

In a fraud investigation, the auditor needs evidence-oriented procedures that compare records, identify unusual patterns, and assess whether payments and contractor activity are valid, authorized, and supported. A documented policy can define the criteria against which conduct is assessed, but it will not reveal potential fraud unless it is accompanied by monitoring, review, reconciliation, data analysis, or other mechanisms that test compliance and highlight exceptions. The IIA describes internal audit's role in evaluating fraud risk and considering whether controls are designed and operating effectively. See the IIA's Global Internal Audit Standards and its Fraud Risk Management resources.

QUESTION NO: 37

Which of the following is not a barrier to effective communication?

A. Filtering.

B. Communication overload.

C. Similar frames of reference.

D. Lack of source credibility.

ANSWER: C

Explanation:

Similar frames of reference is the correct answer because shared experience, knowledge, language, culture, and expectations help a sender and receiver assign similar meaning to a message. Effective communication depends not merely on transmitting information but on achieving mutual understanding. When communicators have similar frames of reference, they are more likely to interpret terminology, context, priorities, and implied meanings consistently. This reduces ambiguity and facilitates accurate feedback, making the communication process more effective.

For internal auditors, establishing a common frame of reference is especially important when discussing audit observations, risks, control deficiencies, and recommendations with stakeholders. Auditors can promote this alignment by using language suited to the audience, defining technical terms, connecting issues to the organization's objectives, and confirming understanding through discussion and feedback. These practices support clear reporting and constructive engagement with management and the board, consistent with the communication expectations in the Global Internal Audit Standards. See the IIA's Global Internal Audit Standards and the OpenStax discussion of communication and shared meaning.

QUESTION NO: 38

According to the International Professional Practices Framework, which of the following are allowable activities for an internal auditor?

1. Advocating the establishment of a risk management function.

2. Identifying and evaluating significant risk exposures during audit engagements.

3. Developing a risk response for the organization if there is no chief risk officer.

4. Benchmarking risk management activities with other organizations.

5. Documenting risk mitigation strategies and techniques.

A. 4 and 5 only.

B. 1, 2, and 3 only.

C. 1, 2, 4, and 5 only.

D. 2, 3, 4, and 5 only.

ANSWER: C

Explanation:

“1, 2, 4, and 5 only” is correct because internal audit may support, assess, and promote effective risk management without taking ownership of management’s risk decisions. Advocating for the establishment of a risk management function is an appropriate advisory activity: internal audit can communicate the value of structured risk management to the board and senior management. Identifying and evaluating significant risk exposures is fundamental to risk-based internal auditing and to providing assurance on the effectiveness of governance, risk management, and control processes.

Internal audit may also benchmark the organization’s risk management practices against relevant peers, frameworks, or leading practices. This can provide useful insight to management and the board while preserving internal audit’s independent role. Similarly, documenting risk mitigation strategies and techniques may be performed as part of audit work, consulting work, or reporting observations, provided that management retains responsibility for selecting, implementing, and accepting risk responses. The critical boundary is that internal audit provides assurance, insight, and advice rather than assuming management responsibility for risk ownership and response decisions. This aligns with the IIA’s requirements for evaluating risk management and safeguarding objectivity. See the IIA Global Internal Audit Standards and the IIA’s standards resources.

QUESTION NO: 39

Which of the following statements is true regarding the capital budgeting procedure known as discounted payback period?

A. It calculates the overall value of a project

B. It ignores the time value of money

C. It calculates the time a project takes to break even.

D. It begins at time zero for the project.

ANSWER: C

Explanation:

The statement *“It calculates the time a project takes to break even.”* is correct because the discounted payback period measures how long it takes for an investment’s cumulative *discounted* net cash inflows to recover its initial cash outlay. In other words, the calculation identifies the point at which the present value of cash received from the project equals the amount initially invested. This is the project’s discounted cash-flow break-even point.

To calculate it, expected future cash flows are first discounted to present value using the required rate of return or cost of capital. Those discounted amounts are then accumulated period by period until they equal the initial investment. If recovery occurs during a period, interpolation may be used to estimate the fraction of that period required. Incorporating discounting is the defining feature of this method: it recognizes that cash received sooner has a higher value than the same nominal amount received later. The approach is therefore useful when management wants to assess how quickly an investment recovers its cost while accounting for the time value of money. ACCA’s investment-appraisal guidance discusses discounted cash-flow methods and the importance of discounting future cash flows: ACCA: Investment appraisal. Further background on the time value of money is available from Investopedia: Time Value of Money.

QUESTION NO: 40

An organization is beginning to implement an enterprise risk management program. One of the first steps is to develop a common risk language. Which of the following statements about a common risk language is true?

A. Management will be able to reduce inherent risk because they will have a better understanding of risk.

B. Internal auditors will be able to reduce their sample sizes because controls will be more consistent.

C. Stakeholders will have more assurance that the risks are assessed consistently.

D. Decision makers will understand that the likelihood of missing or ineffective controls will be reduced.

ANSWER: C

Explanation:

Stakeholders will have more assurance that the risks are assessed consistently. A common risk language establishes shared, organization-wide definitions for fundamental risk concepts, such as risk, risk appetite, risk tolerance, likelihood, impact, inherent risk, residual risk, and control effectiveness. When management, risk owners, assurance providers, and governing bodies use these terms consistently, they can interpret risk information in the same way and apply comparable assessment criteria across business units and activities.

This consistency supports meaningful aggregation and reporting of risks to senior management and the board. It also improves the quality of discussions and decisions because reported risk ratings reflect a common basis rather than differing local terminology or scales. In an enterprise risk management program, a shared vocabulary is therefore a foundation for coherent risk identification, assessment, communication, monitoring, and oversight. The IIA's Global Internal Audit Standards emphasize the need for effective communication and a common understanding of risk and control matters, while COSO's enterprise risk management framework describes risk management as integrated with governance, strategy, and performance across the entity. See the IIA Global Internal Audit Standards and COSO Enterprise Risk Management guidance.

QUESTION NO: 41

Which of the following is a type of network in which an organization permits specific users (such as existing customers) to have access to its internal network through the Internet by building a virtual private network?

A. Intranet.

B. Extranet.

C. Digital subscriber line.

D. Broadband.

ANSWER: B

Explanation:

Extranet. is correct because an extranet extends selected, controlled parts of an organization's internal network to authorized external parties, such as customers, suppliers, business partners, or vendors. It is not a network open to all internet users. Instead, the organization establishes access controls so that each external user can reach only the applications, data, and services required for the business relationship.

A virtual private network is a common method of implementing this arrangement over the public internet. VPN technology creates an encrypted connection and authenticates the user or connecting organization, helping protect data in transit while allowing approved external users to access designated internal resources. From an internal-audit perspective, this arrangement should be governed by appropriate identity management, least-privilege authorization, encryption, monitoring, and periodic review of third-party access.

This use of controlled connectivity for parties outside the organization is the defining purpose of an extranet. Cisco describes VPNs as encrypted connections over a less secure network, such as the internet, and Oracle describes an extranet as a private network that uses internet technology to share information with authorized external entities. See Cisco's VPN overview and Oracle's extranet overview.

QUESTION NO: 42

An organization's balance sheet indicates that the total asset amount and the total capital stock amount remained unchanged from one year to the next, and no dividends were declared or paid. However, the organization reported a loss of $200,000. Which of the following describes the most likely year-over-year change to the organization's total liabilities and total stockholder equity?

A. The total liabilities and total stockholder equity both increased.

B. The total liabilities and total stockholder equity both decreased.

C. The total liabilities decreased, and the total stockholder equity increased.

D. The total liabilities increased, and the total stockholder equity decreased.

ANSWER: D

Explanation:

The total liabilities increased, and the total stockholder equity decreased. Under the fundamental accounting equation, total assets equal total liabilities plus total stockholders' equity. A reported loss decreases retained earnings, which is a component of stockholders' equity. Because no dividends were declared or paid, there is no additional reduction to retained earnings from distributions to owners. Further, because capital stock remained unchanged, the loss is the stated cause of the decrease in total stockholders' equity—specifically, by $200,000.

Total assets remained unchanged over the same period. Therefore, to preserve the accounting equation after stockholders' equity declines by $200,000, total liabilities must increase by an equal $200,000. This conclusion follows regardless of which specific liability accounts changed; the aggregate balance-sheet relationship requires the offsetting increase. The Financial Accounting Standards Board's conceptual framework describes assets, liabilities, and equity as the fundamental elements reported in financial statements, while standard accounting education materials present their relationship through the accounting equation. See the FASB Conceptual Framework and OpenStax's explanation of the accounting equation.

QUESTION NO: 43

An internal auditor is conducting a review of the procurement function and uncovers a potential conflict of interest between the chief operating officer and a significant supplier of IT software development services. Which of the following actions is most appropriate for the internal auditor to take?

A. Inform the audit supervisor.

B. Investigate the potential conflict of interest.

C. Inform the external auditors of the potential conflict of interest.

D. Disregard the potential conflict, because it is outside the scope of the audit assignment.

ANSWER: A

Explanation:

Inform the audit supervisor. A potential conflict of interest involving a chief operating officer and a significant procurement supplier is a potentially material governance, ethics, and fraud-risk matter. The internal auditor should promptly communicate the observation through established internal audit reporting and escalation channels, beginning with the audit supervisor or engagement leader. This ensures that the chief audit executive can assess the significance of the issue, preserve appropriate confidentiality, determine whether the engagement scope or procedures should be expanded, and decide whether communication to senior management, the board, legal counsel, or another appropriate authority is necessary.

This response also respects the internal auditor's role. Auditors must exercise due professional care, document relevant facts, and report significant risks or control issues; however, they do not independently determine culpability or take management action. Escalating the matter to the supervisor enables a consistent, authorized response under the internal audit activity's methodology and protects the integrity of any subsequent investigation. The IIA's Global Internal Audit Standards emphasize communicating engagement results and significant risk information to the appropriate parties, while maintaining objectivity and confidentiality. See the IIA Global Internal Audit Standards and the IIA's standards resource page.

QUESTION NO: 44

According to IIA guidance, which of the following are macro-level audit activities performed for an assurance engagement of the purchasing department?

1. Obtain and review all purchasing-related audit reports issued within the past year.

2. Meet with the quality assurance group to discuss its previous reports of any purchasingrelated findings.

3. Review a memo written by the purchasing manager that outlines ongoing problems withthe purchasing software.

4. Request a copy of the report from a purchasing audit conducted last year by an externalservice provider.

A. 1 and 2.

B. 1 and 3.

C. 2 and 4.

D. 3 and 4.

ANSWER: A

Explanation:

1 and 2. is correct because macro-level audit activities are used early in engagement planning to build a broad understanding of the area under review, its overall risk environment, and the assurance work already performed. Reviewing purchasing-related audit reports issued during the previous year helps internal auditors identify themes, recurring control concerns, significant prior observations, and areas where corrective actions may still affect the purchasing function. Meeting with the quality assurance group similarly provides a higher-level perspective from an independent monitoring function and helps the audit team understand patterns in previously reported purchasing findings.

This information supports a risk-based engagement approach: it informs the preliminary understanding of the purchasing department, assists in identifying relevant risks and controls, and helps auditors focus subsequent work on matters that are significant to the engagement objectives. The IIA's Global Internal Audit Standards require internal auditors to perform an engagement risk assessment and consider relevant information about the activity under review when planning assurance work. See The IIA Global Internal Audit Standards, particularly the engagement-planning requirements, and The IIA Guidance resources.

QUESTION NO: 45

Which of the following is the most appropriate test to assess the privacy risks associated with an organization's workstations?

A. Penetration test.

B. Social engineering test.

C. Vulnerability test.

D. Physical control test.

ANSWER: D

Explanation:

Physical control test. is the most appropriate test because privacy exposures at workstations often arise from the physical environment and users' day-to-day handling of information. An auditor can directly observe whether workstations containing personal or confidential information are left unattended and unlocked, whether screens are visible to visitors or unauthorized employees, whether privacy screens are used where appropriate, and whether printed records, removable media, or notes containing sensitive information are securely stored or disposed of. The test may also assess access to work areas, visitor controls, clean-desk practices, and automatic screen-lock settings as implemented controls. These observations provide evidence about the likelihood that personal information can be viewed, taken, or used by an unauthorized person without needing to compromise the organization's network. This aligns with privacy risk management principles: controls should be evaluated in relation to realistic processing and disclosure risks affecting individuals' information. NIST's privacy guidance describes privacy risk as the potential for problematic data actions and emphasizes selecting safeguards suited to the context in which information is handled. NIST also identifies physical and environmental protections as a control family

relevant to safeguarding systems and the information accessible through them. See the NIST Privacy Framework and NIST SP 800-53 Rev. 5.

QUESTION NO: 46

Which of the following statements regarding organizational governance is not correct?

A. An effective internal audit function is one of the four cornerstones of good governance.

B. Those performing governance activities are accountable to the customer.

C. Accountability is one of the key elements of organizational governance.

D. Governance principles and the need for an internal audit function are applicable to governmental and not-for-profit activities.

ANSWER: D

Explanation:

“Governance principles and the need for an internal audit function are applicable to governmental and not-for-profit activities.” is the statement that is not correct because it improperly limits the relevance of governance and internal auditing to those sectors. Sound governance is relevant to organizations of every type, including private-sector companies, public-sector bodies, not-for-profit entities, and other organizations. Although governance structures, legal obligations, stakeholder expectations, and accountability arrangements differ by sector, the underlying need to direct, oversee, manage risk, and provide assurance remains broadly applicable.

The IIA’s professional framework presents internal auditing as a function that helps organizations accomplish their objectives by evaluating and improving the effectiveness of governance, risk management, and control processes. This role is not restricted to government or charitable entities. The Global Internal Audit Standards likewise are designed for internal audit functions in organizations with varying purposes, sizes, complexities, and structures. An effective internal audit function can therefore provide objective assurance and advice wherever an organization has governance responsibilities and objectives to achieve. See the IIA’s Global Internal Audit Standards and its explanation of what internal auditing is.

QUESTION NO: 47

Refer to the exhibit.

	Company A	Company B
Cash	$100	$200
Accounts receivable	unknown	$100
Accounts payable	$100	$50
Long-term debt	$200	$50
Sales	$600	$5,800
Cost of goods sold	$300	$5,000
Administrative expenses	$100	$500
Depreciation expense	$100	$100
Interest expense	$20	$10

Presented below are partial year-end financial statement data (000 omitted from dollar amounts) for companies A and B:

If company A has a quick ratio of 2:1, then it has an accounts receivable balance of:

A. $100

B. $200

C. $300

D. $500

ANSWER: A

Explanation:

The correct answer is **$100**. The quick ratio measures an entity's ability to settle current obligations using its most liquid current assets. It is calculated as quick assets divided by current liabilities. Quick assets generally include cash, short-term marketable securities, and accounts receivable; inventory is excluded because it may not be converted to cash promptly enough to support immediate liquidity.

For Company A, a 2:1 quick ratio means that total quick assets must equal twice the current-liability balance shown in the exhibit. The cash and other qualifying quick-asset amounts presented for Company A are first included in that required quick-assets total. The remaining amount needed to reach twice current liabilities is the accounts receivable balance. That residual is $100 (with dollar amounts stated in thousands as specified in the exhibit).

This approach applies the ratio directly rather than using the current ratio, which would include inventory and could produce an incorrect receivables amount. The quick ratio is commonly expressed as: (cash + short-term investments + accounts receivable) ÷ current liabilities. See AccountingCoach's explanation of the quick ratio and OpenStax's financial-statement-analysis discussion.

QUESTION NO: 48

Organization X owns a 38 percent equity stake in Organization Y. Which of the following statements is true regarding the financial treatment for this relationship?

A. Y should be listed as an investment asset on X's balance sheet

B. X must consolidate the financial statements for both organizations

C. Y should be reported as a footnote to X's financial statements

D. Y should not be reported by X as X does not have a controlling interest

ANSWER: A

Explanation:

Y should be listed as an investment asset on X's balance sheet. A 38 percent ownership interest ordinarily gives Organization X significant influence over Organization Y, assuming there is no evidence that such influence is absent. Under IAS 28, significant influence is presumed when an investor holds, directly or indirectly, 20 percent or more of an investee's voting power. An investee subject to significant influence is an associate, and the investor accounts for its interest using the equity method.

Under the equity method, X initially recognizes its interest in Y as an investment and subsequently adjusts the carrying amount for X's share of Y's profit or loss and other changes in Y's net assets. Accordingly, the interest is presented as an investment asset in X's statement of financial position, rather than being omitted. The 38 percent interest is therefore material to X's financial reporting and is reflected through the investment balance and related equity-method income or loss. This treatment follows the principles in IAS 28, Investments in Associates and Joint Ventures; see also the IAS 28 summary published by IAS Plus.

QUESTION NO: 49

For a multinational organization, which of the following is a disadvantage of an ethnocentric staffing policy?

1. It significantly raises compensation and staffing costs.

2. It produces resentment among the organization's employees in host countries.

3. It limits career mobility for parent-country nationals.

4. It can lead to cultural myopia.

A. 1 and 4 only

B. 2 and 3 only

C. 1, 2, and 3 only

D. 1, 2, and 4 only

ANSWER: D

Explanation:

1, 2, and 4 only is correct. Under an ethnocentric staffing policy, key positions in foreign subsidiaries are predominantly filled by parent-country nationals. Sending employees abroad commonly increases staffing costs because the organization may need to provide expatriate premiums, relocation assistance, housing, tax equalization, travel, and family-support benefits. These costs can be materially higher than employing suitably qualified host-country nationals.

This approach can also create resentment among host-country employees when they perceive that senior roles and advancement opportunities are reserved for employees from headquarters. Such perceptions can weaken motivation, retention, and local management development. In addition, reliance on parent-country managers may foster cultural myopia: decisions, practices, and assumptions developed at headquarters can be applied without sufficient adaptation to the host-country market, workforce, and business culture.

These consequences reflect the need for multinational organizations to align staffing choices with local capability, cultural awareness, succession planning, and the cost of international assignments. The Society for Human Resource Management's global workforce resources discuss considerations in managing international assignments, while the CIPD guidance on international assignment management addresses the practical costs and people-management demands of expatriate staffing.

QUESTION NO: 50

Which of the following is an example of a nonfinancial internal failure quality cost?

A. Decreasing gross profit margins over time.

B. Foregone contribution margin on lost sales.

C. Defective units shipped to customers.

D. Excessive time to convert raw materials into finished goods.

ANSWER: D

Explanation:

Excessive time to convert raw materials into finished goods is a nonfinancial internal failure quality cost because it reflects an operational loss that arises within the production process, before the output reaches a customer. Internal failures occur when processes do not produce conforming output efficiently and require additional processing, correction, waiting, inspection, or other non-value-adding activity. Although the effect may ultimately be translated into a monetary amount, the measure stated here is nonfinancial: elapsed conversion time.

Quality-cost analysis is not limited to accounting entries. It also uses operational measures that help management and internal audit identify process-performance problems early. An extended conversion time can signal defects, rework, bottlenecks, machine downtime, poor material quality, or ineffective production controls. Monitoring this time helps reveal whether internal process failures are consuming capacity and delaying delivery. The Institute of Internal Auditors' Global Internal Audit Standards emphasize evaluating governance, risk management, and control processes using relevant, reliable performance information. See the IIA Global Internal Audit Standards. The American Society for Quality's cost of quality overview also describes internal failure as quality problems identified before delivery to the customer.

QUESTION NO: 51

Which of the following authentication controls combines what a user knows with the unique characteristics of the user respectively?

A. Voice recognition and token.

B. Password and fingerprint.

C. Fingerprint and voice recognition

D. Password and token

ANSWER: B

Explanation:

Password and fingerprint is correct because it combines two distinct authentication-factor categories in the order specified. A password is "something you know": it is secret information that the legitimate user should be able to recall and present. A fingerprint is "something you are": a biometric characteristic based on a unique physical attribute of the individual. Using both factors provides multifactor authentication, which gives stronger assurance of a user's identity than relying on a password alone. The essential principle is that authentication factors should be independent: compromise of a password does not give an attacker the user's fingerprint, and possession of a biometric characteristic does not reveal the password. This layered approach is widely used to reduce the risk of unauthorized access, particularly for systems or transactions requiring higher confidence in identity verification. NIST's Digital Identity Guidelines categorize memorized secrets, including passwords, as knowledge-based authenticators and biometrics, such as fingerprints, as inherence factors. The Cybersecurity and Infrastructure Security Agency likewise describes multifactor authentication as using two or more different authentication factors to validate identity. See NIST SP 800-63B: Authentication and Authenticator Management and CISA: Implementing Multifactor Authentication.

QUESTION NO: 52

While auditing an organization's credit approval process, an internal auditor learns that the organization has made a large loan to another auditor's relative. Which course of action should the auditor take?

A. Proceed with the audit engagement, but do not include the relative's information.

B. Have the chief audit executive and management determine whether the auditor should continue with the audit engagement.

C. Disclose in the engagement final communication that the relative is a customer.

D. Immediately withdraw from the audit engagement.

ANSWER: B

Explanation:

Have the chief audit executive and management determine whether the auditor should continue with the audit engagement. is correct because a substantial loan involving an internal auditor's relative creates at least an apparent threat to that auditor's objectivity. Objectivity requires internal auditors to perform work without allowing personal interests or relationships

to bias, or appear to bias, their professional judgment. Once the potential impairment is identified, it must be promptly disclosed rather than handled informally by omitting the information or simply reporting it at the end of the engagement.

The chief audit executive is responsible for ensuring that actual or potential impairments are appropriately evaluated and that safeguards are implemented. Depending on the circumstances, appropriate action may include changing the auditor's assignment, adding independent review, limiting the auditor's work on the affected area, or determining that the auditor may continue because effective safeguards remove the threat. Management's involvement is appropriate because it is a relevant recipient of disclosure and may need to support a practical reassignment or other safeguard. This approach preserves both actual objectivity and stakeholders' confidence in the engagement's results. The IIA's Global Internal Audit Standards require internal auditors to identify, disclose, and manage impairments to objectivity. See the IIA Global Internal Audit Standards and the IIA Standards resources.

QUESTION NO: 53

Which of the following activities is most likely to require a fraud specialist to supplement the knowledge and skills of the internal audit activity?

A. Planning an engagement of the area in which fraud is suspected.

B. Employing audit tests to detect fraud.

C. Interrogating a suspected fraudster.

D. Completing a process review to improve controls to prevent fraud.

ANSWER: C

Explanation:

Interrogating a suspected fraudster is most likely to require a fraud specialist because it is an investigative activity that demands expertise beyond the level ordinarily expected of internal auditors. Effective questioning of a subject requires careful interview planning, knowledge of investigative interviewing techniques, an understanding of evidentiary requirements, and sensitivity to employment-law, privacy, and due-process considerations. The interviewer must obtain reliable information without making improper accusations, coercing statements, compromising evidence, or prejudicing a potential disciplinary or legal proceeding. A qualified fraud investigator can also help coordinate the interview with legal counsel, human resources, security, or law enforcement as appropriate, while preserving confidentiality and the integrity of the investigation.

The IIA's competency expectations require internal auditors to possess or obtain the knowledge and skills needed to perform their responsibilities. Internal audit is expected to understand fraud risks and assess how they are managed, but it need not maintain the specialist-level expertise required for every fraud investigation. Accordingly, obtaining competent specialist assistance for a suspected-fraud interrogation is consistent with the IIA's Global Internal Audit Standards and with sound investigation practice. See the IIA Global Internal Audit Standards and the IIA's Fraud Risk Management guidance.

QUESTION NO: 54

Which of the following are appropriate reasons for internal auditors to document processes as part of an audit engagement?

1. To determine areas of primary concern.

2. To establish a standard format for process mapping.

3. To define areas of responsibility within the organization.

4. To assess the performance of employees.

A. 1 and 2 only

B. 1 and 3 only

C. 2 and 3 only

D. 2 and 4 only

ANSWER: B

Explanation:

“1 and 3 only” is correct because documenting a process gives internal auditors a structured understanding of how work flows, where key decisions and handoffs occur, and which controls operate at each point. This understanding supports engagement risk assessment by helping auditors identify activities, risks, control gaps, and process points that warrant primary audit attention. Process documentation may take forms such as narratives, flowcharts, walkthrough records, or responsibility matrices, depending on what most clearly communicates the process being audited.

Documentation also clarifies areas of responsibility. Recording the process makes visible which functions or roles initiate, approve, perform, review, and monitor activities. This enables auditors to assess whether accountability and segregation of duties are appropriately designed and whether control responsibilities are clearly allocated. The resulting documentation provides evidence for audit conclusions and helps the engagement team communicate its understanding with process owners.

The IIA’s Global Internal Audit Standards require internal auditors to obtain and assess information relevant to engagement objectives, risks, and controls, including understanding relevant activities and processes during engagement risk assessment. See the IIA Global Internal Audit Standards and the IIA’s Standards resources.

QUESTION NO: 55

An organization facing rapid growth decides to employ a third party service provider to manage its customer relationship management function. Which of the following is true regarding the supporting application software used by that provider compared to an in-house developed system?

1. Updating documentation is always a priority.

2. System availability is usually more reliable.

3. Data security risks are lower.

4. Overall system costs are lower.

A. 1 and 2 only

B. 1 and 3 only

C. 2 and 4 only

D. 3 and 4 only

ANSWER: C

Explanation:

2 and 4 only is correct. A specialist third-party provider will commonly operate a standardized, mature application environment and support it with dedicated technical staff, established monitoring, resilient infrastructure, backup arrangements, and service-level commitments. These features generally make system availability more reliable than an application developed and maintained internally by an organization that is growing rapidly and may have limited IT capacity or experience supporting the customer relationship management platform. The provider can also spread the fixed costs of application development, licensing, security tooling, infrastructure, upgrades, and specialist personnel over many customers. This economy of scale commonly reduces the client organization’s overall system cost compared with building, operating, and continually enhancing an equivalent in-house system. Internal audit should nevertheless evaluate whether the organization has established appropriate governance over the outsourced arrangement, including measurable service levels, access controls, resilience requirements, incident reporting, and a right to obtain assurance over the provider’s controls. The IIA’s guidance on third-party relationships emphasizes that accountability remains with the organization even where operational activities are performed externally. See the IIA’s Global Internal Audit Standards and practice guides.

QUESTION NO: 56

Which of the following statements pertaining to a market skimming pricing strategy is not true?

A. The strategy is favored when unit costs fall with the increase in units produced.

B. The strategy is favored when buyers are relatively insensitive to price increases.

C. The strategy is favored when there is insufficient market capacity and competitors cannot increase market capacity.

D. The strategy is favored when high price is perceived as high quality.

ANSWER: A

Explanation:

"The strategy is favored when unit costs fall with the increase in units produced." is not true for market skimming. Market-skimming pricing sets a relatively high initial price, typically for a new, differentiated, or innovative offering, in order to earn higher margins from customer segments that place a high value on early access or distinctive benefits. The approach emphasizes capturing revenue from these segments before progressively lowering the price as the product moves through its life cycle or as broader market adoption occurs.

Falling unit costs as production volume rises describes economies of scale. A business seeking to obtain those volume-related cost reductions generally has an incentive to build sales volume rapidly, which is aligned with a market-penetration approach rather than skimming. Penetration pricing uses a comparatively low initial price to encourage broad and rapid adoption, helping the organization spread fixed costs across more units and potentially achieve lower per-unit costs. Thus, the stated production-cost condition does not support selecting a skimming strategy. See OpenStax's discussion of pricing strategies and the economies-of-scale concept.

QUESTION NO: 57

When assessing the adequacy of a risk mitigation strategy, an internal auditor should consider which of the following?

1. Management's tolerance for specific risks.

2. The cost versus benefit of implementing a control.

3. Whether a control can mitigate multiple risks.

4. The ability to test the effectiveness of the control.

A. 1, 2, and 3

B. 1, 2, and 4

C. 1, 3, and 4

D. 2, 3, and 4

ANSWER: A

Explanation:

The correct response is **1, 2, and 3**. A risk mitigation strategy is adequate when it reduces risk to a level that management is willing to accept, considering the organization's established risk appetite and tolerance for the particular risk. Internal auditors should therefore evaluate whether the planned or existing response leaves an appropriate level of residual risk.

Assessing adequacy also requires consideration of proportionality. Controls consume financial, operational, and human resources, so the expected benefit of reducing risk should reasonably justify their cost. This does not require a precisely quantified calculation in every case, but it does require sound management judgment that the response is economically and operationally practical.

Finally, a control that addresses several related risks may provide an efficient and integrated mitigation approach. The auditor should consider that broader coverage when evaluating the overall control design and whether the collection of responses adequately addresses the organization's risk exposures. The IIA's standards emphasize evaluating the

effectiveness of risk management processes, including whether risks are identified and managed within acceptable parameters. See the IIA Global Internal Audit Standards and COSO's Enterprise Risk Management guidance.

QUESTION NO: 58

Which of the following best ensures the independence of the internal audit activity?

1. The CEO and audit committee review and endorse any changes to the approved auditplan on an annual basis.

2. The audit committee reviews the performance of the chief audit executive (CAE) periodically.

3. The internal audit charter requires the CAE to report functionally to the audit committee.

A. 3 only

B. 1 and 2 only

C. 2 and 3 only

D. 1, 2, and 3

ANSWER: C

Explanation:

"2 and 3 only" is correct because internal audit independence is principally protected through an appropriate functional reporting relationship between the chief audit executive and the board or audit committee. Requiring functional reporting in the internal audit charter formally establishes the audit committee's authority and oversight role. This arrangement enables the audit committee to support the CAE's unrestricted access, organizational standing, and freedom to determine audit priorities and communicate results without undue management influence.

Periodic audit-committee review of the CAE's performance is also a key element of functional oversight. It gives the audit committee a direct role in evaluating whether the CAE is effectively leading the internal audit activity and helps preserve the CAE's accountability to the governing body rather than solely to executive management. The IIA's Global Internal Audit Standards describe board responsibilities that support independent positioning, including oversight of the CAE's performance and confirmation of appropriate reporting relationships. These safeguards provide a practical governance structure that allows internal audit to remain objective while performing assurance and advisory work. See the IIA's Global Internal Audit Standards and its Standards resource page.

QUESTION NO: 59

According to IIA guidance, which of the following describes the primary reason to implement environmental and social safeguards within an organization?

A. To enable Triple Bottom Line reporting capability.

B. To facilitate the conduct of risk assessment.

C. To achieve and maintain sustainable development.

D. To fulfill regulatory and compliance requirements.

ANSWER: C

Explanation:

To achieve and maintain sustainable development is correct because environmental and social safeguards are designed to ensure that organizational decisions, projects, and operations identify, avoid, minimize, and manage adverse effects on people and the environment. Their central purpose is to support outcomes that can endure over time by balancing economic objectives with environmental stewardship and social responsibility. This focus aligns with the widely accepted concept of sustainable development: meeting current needs without compromising the ability of future generations to meet their own

needs. The United Nations describes sustainable development as integrating economic growth, social inclusion, and environmental protection, which are mutually reinforcing dimensions of long-term development.

From an internal audit perspective, safeguards form part of the organization's governance, risk management, and control framework. Internal audit can provide assurance that relevant sustainability-related risks, commitments, controls, and reporting processes are understood and appropriately managed. The IIA's Global Internal Audit Standards emphasize that internal auditing supports organizational success by enhancing governance, risk management, and control processes. Accordingly, implementing safeguards is principally about sustaining responsible organizational performance and protecting stakeholders over the long term. See the United Nations Sustainable Development Goals and the IIA Global Internal Audit Standards.

QUESTION NO: 60

Which of the following is an example of a smart device security control intended to prevent unauthorized users from gaining access to a device's data or applications?

A. Anti-malware software.

B. Authentication.

C. Spyware.

D. Rooting.

ANSWER: B

Explanation:

Authentication is the appropriate smart-device security control because it verifies the identity of a person or process before allowing access to the device, its applications, or the data stored on it. On smart devices, authentication can be implemented through something the user knows, such as a PIN or password; something the user has, such as a hardware-backed credential; or something the user is, such as a fingerprint or facial biometric. Requiring successful authentication at device unlock and, where appropriate, again for sensitive applications or actions, establishes an access barrier that prevents an unauthorized person who possesses or encounters the device from simply opening its content. Strong device authentication should be supported by secure configuration features such as automatic locking after inactivity, limits or delays on repeated failed attempts, and encryption that protects stored data when the device is locked. These measures make authentication a fundamental logical access control for mobile and smart-device environments. NIST's guidance on digital identity explains authentication as establishing confidence that a claimant controls one or more authenticators associated with an identity: NIST SP 800-63B. Further mobile-device security guidance is available from NIST SP 800-124 Rev. 2.

QUESTION NO: 61

According to IIA guidance, which of the following strategies would add the least value to the achievement of the internal audit activity's (IAA's) objectives?

A. Align organizational activities to internal audit activities and measure according to the approved IAA performance measures.

B. Establish a periodic review of monitoring and reporting processes to help ensure relevant IAA reporting.

C. Use the results of IAA engagement and advisory reporting to guide current and future internal audit activities.

D. Establish a format and frequency for IAA reporting that is appropriate and aligns with the organization's governance structure.

ANSWER: A

Explanation:

“Align organizational activities to internal audit activities and measure according to the approved IAA performance measures.” would add the least value because it reverses the appropriate relationship between the organization and internal audit. The internal audit activity exists to support the organization’s purpose, strategy, objectives, governance, risk management, and control processes. It should therefore align its strategy, plans, priorities, and performance measures with organizational needs—not attempt to align the organization’s operating activities to internal audit’s activities.

IIA guidance requires the chief audit executive to develop an internal audit strategy that supports the organization’s strategic objectives and success. Internal audit performance measures should then help the governing body and senior management evaluate whether the activity is delivering on that organizationally aligned strategy. While audit insights may appropriately influence management decisions and improvements, internal audit must retain its independent assurance role and cannot become the driver to which organizational operations are aligned. This inverted alignment would risk misunderstanding internal audit’s mandate and reduce its value as an independent, objective function. See the IIA’s Global Internal Audit Standards, particularly the requirements for internal audit strategy and performance management, and the IIA’s standards resources.

QUESTION NO: 62

According to COSO, which of the following is not considered one of the components of an organization's internal environment?

A. Authority and responsibility to resolve issues.

B. Framework to plan, execute and monitor activities.

C. Integrated responses to multiple risks.

D. Knowledge and skills needed to perform activities.

ANSWER: C

Explanation:

Integrated responses to multiple risks. is correct because it describes risk response activity rather than the internal environment. In COSO’s Enterprise Risk Management framework, the internal environment establishes the foundation for how risk is viewed and addressed throughout the organization. It encompasses matters such as management’s risk philosophy, risk appetite, board oversight, integrity and ethical values, commitment to competence, organizational structure, and the assignment of authority and responsibility. These elements shape the culture, capabilities, accountability, and governance context in which people perform their work and manage risk.

Risk responses occur later in the ERM process, after risks have been identified and assessed. Management selects and implements responses—such as avoiding, accepting, reducing, or sharing risk—to bring residual risk within the organization’s risk appetite. Coordinating or integrating responses across several risks may be a sensible management practice, particularly where risks are interrelated, but it is not itself an internal-environment component. The distinction is important for auditors: internal-environment evaluation focuses on the organization’s underlying governance and behavioral conditions, whereas risk-response evaluation focuses on whether management has chosen and implemented suitable treatments for specific risks. COSO’s ERM resources are available at COSO Enterprise Risk Management guidance and its ERM—Integrated Framework page.

QUESTION NO: 63

Which of the following is a major advantage of decentralized organizations, compared to centralized organizations?

A. Decentralized organizations are more focused on organizational goals.

B. Decentralized organizations streamline organizational structure.

C. Decentralized organizations tend to be less expensive to operate.

D. Decentralized organizations tend to be more responsive to market changes.

ANSWER: D

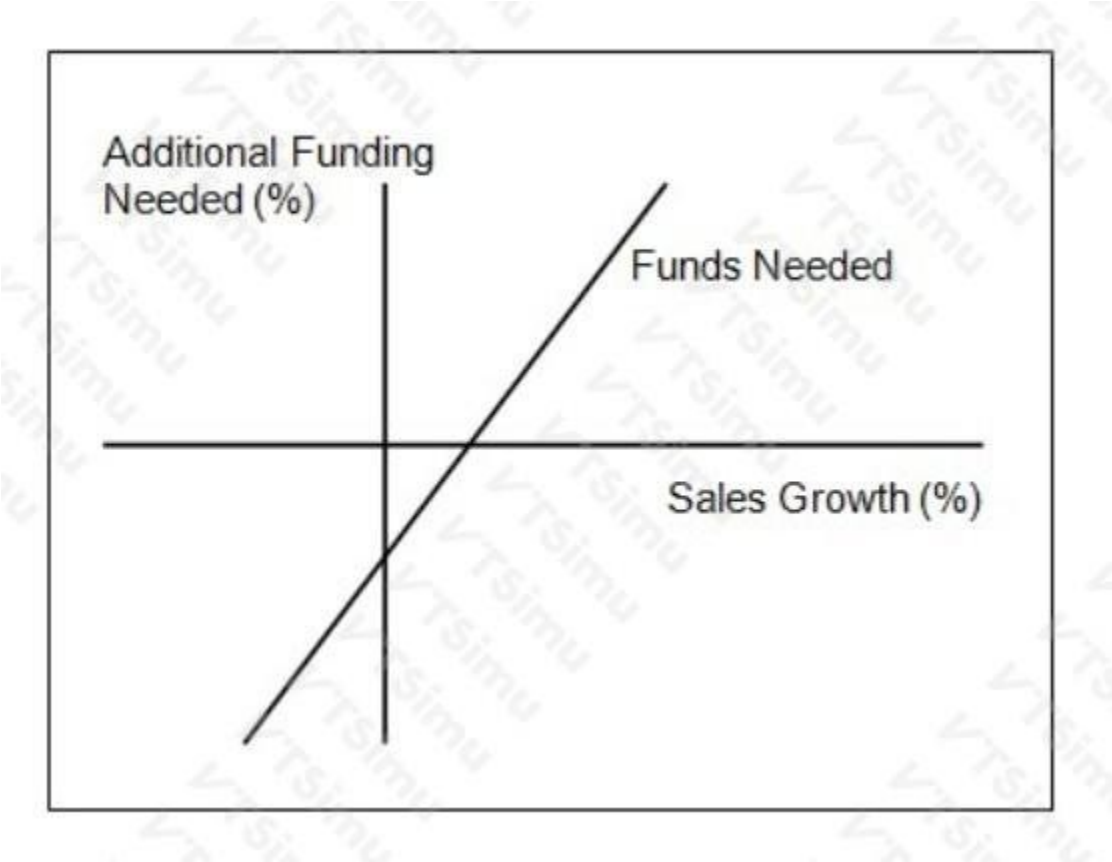
Explanation:

Decentralized organizations tend to be more responsive to market changes. Decentralization places significant decision-making authority closer to operating units, customers, and local markets rather than reserving it primarily for senior management. Managers with direct knowledge of local conditions can therefore identify changes in customer preferences, competitor activity, supply conditions, or regulatory requirements and act without waiting for decisions to move through several centralized management levels. This shorter decision path can improve the speed and relevance of operational responses, particularly where business environments vary across products, regions, or customer segments.

From an internal audit perspective, decentralization does not eliminate accountability: governance arrangements should clearly establish delegated authorities, risk limits, reporting requirements, and monitoring mechanisms. The IIA's Global Internal Audit Standards emphasize that governance structures, risk management, and controls must support the organization's objectives, regardless of how authority is distributed. Properly designed delegation allows local responsiveness while retaining appropriate oversight. General management guidance similarly identifies faster decision-making and greater responsiveness to local needs as central benefits of decentralized organizational structures. See the IIA Global Internal Audit Standards and OpenStax's discussion of organizational design.

QUESTION NO: 64

Refer to the exhibit.



If the profit margin of an organization decreases, and all else remains equal, which of the following describes how the "Funds Needed" line in the graph below will shift?

A. The "Funds Needed" line will remain pointed upward, but will become less steep.

B. The "Funds Needed" line will remain pointed upward, but will become more steep.

C. The "Funds Needed" line will point downward with a minimal slope.

D. The "Funds Needed" line will point downward with an extreme slope.

ANSWER: B

Explanation:

The "Funds Needed" line will remain pointed upward, but will become more steep. In a typical additional-funds-needed (AFN) or external-financing-needed model, sales growth increases the investment required in operating assets, such as receivables, inventory, and fixed assets. A portion of that investment can be financed internally through retained earnings. Profit margin is a direct driver of net income and, assuming the retention policy does not change, of the earnings retained in the business.

When profit margin decreases, each dollar of sales produces less profit and therefore less internally generated funding. Consequently, for any given increase in sales, the organization must obtain more external financing than it previously required. The relationship between sales and funds needed remains positive because growth still requires additional asset investment under the stated all-else-equal assumption. However, the reduction in internal financing causes the required external funds to rise faster for each incremental level of sales. Graphically, this is represented by an upward-sloping Funds Needed line with a greater slope. This application is consistent with the financial-planning relationship that includes projected profit margin and retained earnings as sources that reduce external financing needs; see OpenStax, Financial Planning and Forecasting and CFA Institute, Corporate Issuers.

QUESTION NO: 65

According to IIA guidance, which of the following best describes internal auditors' responsibility regarding fraud?

A. Internal auditors should take a leading role in investigating all fraud-related cases.

B. Internal auditors must have sufficient knowledge to evaluate the risk of fraud.

C. Internal auditors should report all fraud cases to law enforcement agents, in accordance with the Code of Ethics.

D. Internal auditors are responsible for ensuring that fraud does not occur.

ANSWER: B

Explanation:

“Internal auditors must have sufficient knowledge to evaluate the risk of fraud.” is correct because the IIA requires internal auditors to possess enough knowledge to assess fraud risk and how the organization manages that risk. This responsibility is integral to planning and performing assurance engagements: auditors should recognize fraud indicators, consider incentives and opportunities that could enable fraud, evaluate relevant controls, and determine whether identified risks require further audit work or communication to appropriate parties.

The required knowledge is risk-focused. It enables internal audit to make an informed professional assessment of whether fraud risks have been properly identified and addressed within governance, risk management, and control processes. The requirement does not make internal auditors the owners of fraud prevention or investigation. Rather, management is responsible for establishing controls and maintaining processes to prevent and detect fraud, while internal audit provides independent assurance and advice within its mandate.

This principle appeared expressly in former IIA Standard 1210.A2 and remains consistent with the competency and fraud-risk expectations in the current Global Internal Audit Standards. See the IIA’s Global Internal Audit Standards and its mandatory guidance resources.

QUESTION NO: 66

During which phase of disaster recovery planning should an organization identify the business units, assets, and systems that are critical to continuing an acceptable level of operations?

A. Scope and initiation phase.

B. Business impact analysis.

C. Plan development.

D. Testing.

ANSWER: B

Explanation:

Business impact analysis is correct because it is the structured process used to determine which business activities, supporting assets, applications, infrastructure, personnel, suppliers, and facilities are essential to sustaining operations at an acceptable level following a disruption. During this analysis, the organization identifies critical business units and processes, evaluates the operational and financial consequences of an outage, and establishes recovery priorities. It also determines time-based recovery requirements, such as the maximum tolerable period of disruption and recovery time objectives, along with dependencies between processes and systems.

These results provide the factual basis for disaster recovery and business continuity strategies. Once critical systems and assets have been identified and prioritized, the organization can select appropriate recovery capabilities, allocate resources, and document recovery procedures that support the most time-sensitive operations. The IIA's Global Technology Audit Guide on business continuity management describes business impact analysis as a key activity for identifying critical processes, their dependencies, and the impacts of disruption. NIST similarly identifies the BIA as the mechanism for characterizing criticality and recovery requirements for information systems. See IIA GTAG: Business Continuity Management and NIST SP 800-34 Rev. 1.

QUESTION NO: 67

The chief audit executive is evaluating whether the internal audit activity's quality assurance and improvement program is operating effectively. Which of the following is an example of an external assessment?

A. An audit manager reviews working papers before engagement reports are issued.

B. The CAE performs an annual self-assessment of the internal audit methodology.

C. An independent qualified assessor evaluates conformance with the Global Internal Audit Standards at least once every five years.

D. Internal auditors obtain client feedback after each completed engagement.

ANSWER: C

Explanation:

An independent qualified assessor evaluates conformance with the Global Internal Audit Standards at least once every five years. is correct because an external assessment is performed by a qualified, independent assessor or assessment team from outside the organization. Its purpose is to evaluate the internal audit function's conformance with the Global Internal Audit Standards and to identify opportunities to improve quality and effectiveness.

Ongoing supervision of engagement work and periodic self-assessments are important components of internal quality assessment, but they do not replace an external assessment. The chief audit executive should communicate the results of external assessments, including the assessor's qualifications and independence, to senior management and the board. See the IIA's Global Internal Audit Standards and its Quality Assurance and Improvement Program guidance.

QUESTION NO: 68

According to IIA guidance, which of the following statements are true regarding the internal audit plan?

1. The audit plan is based on an assessment of risks to the organization.

2. The audit plan is designed to determine the effectiveness of the organization ' s risk management process.

3. The audit plan is developed by senior management of the organization.

4. The audit plan is aligned with the organization ' s goals.

A. 1 and 2 only

B. 3 and 4 only

C. 1, 2, and 4

D. 1, 3, and 4

ANSWER: C

Explanation:

1, 2, and 4 is correct. IIA guidance requires the chief audit executive to develop a risk-based internal audit plan. This means audit priorities are determined from a documented assessment of the organization's strategies, objectives, and relevant risks, with consideration of the board's and senior management's expectations. Accordingly, the plan should direct internal audit resources toward the matters that could most significantly affect the organization's ability to achieve its objectives.

The plan also supports internal audit's responsibility to assess and contribute to the improvement of governance, risk management, and control processes. Audits included in the plan may therefore be designed to evaluate whether risk management processes are effective, including whether significant risks are identified, assessed, and managed appropriately. Alignment with organizational goals is inherent in a risk-based approach: risks are evaluated in relation to strategies and objectives, so the resulting plan helps provide assurance and advice that support achievement of those goals.

The current requirements for risk-based planning are set out in the IIA's Global Internal Audit Standards, particularly the planning requirements under Domain III. See the IIA Global Internal Audit Standards and the IIA's Standards resource page.

QUESTION NO: 69

According to The IIA's Code of Ethics, which of the following statements is true?

A. When an internal auditor releases required information to a regulator, resulting in a significant loss through fines and penalties for the organization, he fails to add value.

B. When an internal auditor limits the scope of the audit engagement after learning that management is hiding relevant information, he demonstrates integrity.

C. When an internal auditor disagrees with the treatment received by workers in the organization's foreign subsidiary and alters the audit program to highlight the issue, he fails to demonstrate objectivity.

D. When an internal auditor continues with an audit engagement, despite the audit client's claims that the work performed is unnecessary and redundant he fails to demonstrate competency.

ANSWER: C

Explanation:

When an internal auditor disagrees with the treatment received by workers in the organization's foreign subsidiary and alters the audit program to highlight the issue, he fails to demonstrate objectivity. Objectivity requires internal auditors to perform their work with an impartial, unbiased mental attitude and to avoid allowing personal interests, opinions, or preferences to override a risk-based and evidence-based audit approach. A personal disagreement with management's labor practices may be sincere and may identify an area that merits consideration, but changing the audit program specifically to emphasize that issue because of the auditor's own views creates a risk that the engagement will be directed by bias rather than by the approved objectives, relevant risks, and available evidence. The auditor should instead raise the potential issue through appropriate planning, risk assessment, and communication processes, ensuring that any changes in scope are professionally justified and authorized. The IIA's ethical requirements treat objectivity as essential to credible assurance and advice because stakeholders must be able to rely on auditors' judgments as fair and independent. The current Global Internal Audit Standards similarly require auditors to maintain objectivity and manage circumstances that could impair it. See also The IIA's Code of Ethics.

QUESTION NO: 70

According to the International Professional Practices Framework, which of the following statements is true regarding a corporate social responsibility (CSR) program?

1. Every employee generally has a responsibility for ensuring the success of CSRobjectives.

2. The board has overall responsibility for the effectiveness of internal control processesassociated with CSR.

3. Public reporting on the CSR governance process is expected.

4. Organizations generally have flexibility regarding what is included in a CSR program.

A. 1, 2, and 3 only

B. 1, 2, and 4 only

C. 1, 3, and 4 only

D. 2, 3, and 4 only

ANSWER: B

Explanation:

1, 2, and 4 only is correct. A CSR program is an organization-wide undertaking: employees at all levels contribute to achieving CSR objectives through their decisions, conduct, and execution of assigned responsibilities. This reflects the governance principle that management and personnel implement internal control and organizational objectives in day-to-day operations.

The board retains overall accountability for governance and oversight, including overseeing whether internal control processes supporting significant organizational activities, such as CSR, are effective. Internal audit may evaluate and provide assurance on CSR governance, risk management, and controls, but it does not assume management's operational responsibilities or the board's governance accountability.

CSR is also inherently adaptable. Organizations may design their programs around the social, environmental, ethical, stakeholder, regulatory, and business issues that are relevant to their own purpose and circumstances. Accordingly, the content and scope of a CSR program can differ substantially between organizations while remaining consistent with sound governance. The IIA's guidance recognizes internal audit's role in assessing governance and control arrangements, while the COSO framework describes the respective governance and management responsibilities for effective internal control. See the IIA International Professional Practices Framework and COSO's Internal Control guidance.