PassQueen
a.k.a dumpsqueen.com

CIA Exam Part Three: Business Knowledge for Internal Auditing

IIA IIA-CIA-Part3-3P

Version Demo

Total Demo Questions: 54

Total Premium Questions: 543

Buy Premium PDF

https://passqueen.com

support@passqueen.com

Topic Break Down

Topic	No. of Questions
Topic 1, Business Acumen	314
Topic 2, Information Security	77
Topic 3, Information Technology	148
Topic 4, Mix Questions	4
Total	543

QUESTION NO: 1

Which of the following assists in ensuring mat information exchanged over IT systems is encrypted?

A. Operating system

B. Utility software

C. Firewall

D. Application software

ANSWER: C

Explanation:

Firewall is correct because a firewall is a key network-security control that can enforce policies requiring communications to use approved, encrypted channels. For example, a firewall can restrict inbound and outbound traffic to encrypted protocols and approved ports, deny unencrypted remote-access traffic, and permit access only through an encrypted virtual private network (VPN) tunnel. Modern firewalls commonly integrate VPN capabilities or work with VPN gateways to apply IPsec or TLS protections at network boundaries. This helps ensure that information crossing between internal networks, external networks, remote users, cloud services, or business partners is protected against interception or unauthorized disclosure while in transit.

From an internal-audit perspective, firewall configurations and associated VPN policies are important evidence that management has implemented network-boundary controls to protect the confidentiality of information exchanged over IT systems. Auditors should verify that rules require encrypted remote administration and remote access, that only authorized encrypted services are allowed, and that configurations are monitored and periodically reviewed. NIST describes firewalls as controls that monitor and control communications at external and key internal boundaries, while its cryptographic-protection control addresses using cryptography to protect the confidentiality and integrity of transmitted information. See NIST SP 800-41 Rev. 1, Guidelines on Firewalls and Firewall Policy and NIST SP 800-53 SC-13, Cryptographic Protection.

QUESTION NO: 2

Which of the following is a typical example of structured data?

A. Production information maintained in relational tables.

B. Tweets and posts of users on social media.

C. Photos and videos stored in hard drive catalogs.

D. Sales reports documented in word processing software.

ANSWER: A

Explanation:

Production information maintained in relational tables is a typical example of structured data because its individual data elements are organized according to a predefined schema. A relational database stores information in tables composed of consistently defined rows and columns, with each column representing a specific attribute, such as production date, item identifier, quantity, location, or status. Data types, field lengths, allowed values, and relationships between tables can be defined in advance. This structure enables reliable querying, filtering, aggregation, validation, and reporting using database tools and SQL. For internal audit purposes, structured production data can be tested efficiently through data analytics because records can be joined, reconciled, and analyzed against business rules in a consistent format. The U.S. National Institute of Standards and Technology describes structured data as data that conform to a specified format, while relational databases are a common implementation that organizes data into tables and relationships. IBM likewise explains that relational databases store and provide access to data points related to one another, typically through tables. These characteristics make production information maintained in relational tables clearly structured data. See NIST data management guidance and IBM's overview of relational databases.

QUESTION NO: 3

Which of the following local area network physical layouts is subject to the greatest risk of failure if one device fails?

A. Star network.

B. Bus network.

C. Token ring network.

D. Mesh network.

ANSWER: C

Explanation:

Token ring network is correct because devices are arranged in a closed loop and network communication depends on maintaining that loop. In a traditional ring implementation, each connected device participates in forwarding the signal or token to the next device. Therefore, a failed workstation, network interface, or connection point can interrupt the path around the ring and prevent communications for the entire network segment. This creates a relatively high single-device failure risk compared with layouts that provide independent links or multiple alternate paths. The token-passing method also requires a continuous logical ring so that the token can circulate in an orderly manner; an interruption can stop normal access to the shared transmission medium. Some later ring products incorporated bypass mechanisms or fault-tolerant components to reduce this exposure, but the fundamental physical ring layout is classically characterized by vulnerability to a break at a device or link. Cisco's overview of network topologies describes the ring topology as devices connected in a circular path, while Britannica explains Token Ring's token-passing operation among connected stations. See Cisco: What Is Network Topology? and Encyclopaedia Britannica: Token Ring.

QUESTION NO: 4

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: B

Explanation:

"Those performing governance activities are accountable to the customer." is not correct because organizational governance concerns the arrangements through which an organization is directed, overseen, and held accountable to its stakeholders—not solely to customers. Depending on the organization's legal form and public purpose, the relevant stakeholders may include owners or shareholders, a board, regulators, employees, funders, beneficiaries, communities, and customers. The governing body has responsibility for organizational oversight, including setting direction, monitoring performance, supporting ethical conduct, and ensuring that risks are managed appropriately. It must therefore account for decisions and outcomes to the parties with legitimate interests in the organization and its mandate. Customers are important stakeholders in many organizations, but they are only one possible stakeholder group and are not the universal accountability recipient for governance activities. The IIA's Global Internal Audit Standards describe governance as the combination of processes and structures implemented by the board to inform, direct, manage, and monitor organizational activities, emphasizing the board's oversight role and broader accountability framework. This broader perspective is also consistent with internationally recognized governance principles addressing relationships with stakeholders. See the IIA Global Internal Audit Standards and the OECD G20/OECD Principles of Corporate Governance.

QUESTION NO: 5

Which of the following is true regarding the COSO enterprise risk management framework?

A. The framework categorizes an organization's objectives to distinct, non overlapping objectives.

B. Control environment is one of the framework's eight components.

C. The framework facilitates effective risk management, even if objectives have not been established.

D. The framework integrates with, but is not dependent upon, the corresponding internal control framework.

ANSWER: D

Explanation:

The COSO enterprise risk management framework integrates with internal control concepts while remaining a distinct, broader framework for managing risk in connection with strategy and performance. Enterprise risk management addresses how an organization identifies, assesses, and manages risks that may affect the achievement of its objectives, including the consideration of risk when setting strategy and business objectives. Internal control is an important part of sound governance and risk management, and COSO's ERM guidance recognizes the strong relationship between the two disciplines. However, an organization can use the ERM framework as its organizing model for managing risk across the entity rather than treating it as merely an extension that must rely on a separate internal control framework. This relationship supports coordinated governance, risk management, and control activities while preserving the ERM framework's broader focus on value creation, preservation, strategy, and performance. COSO describes ERM as integrating risk management with strategy-setting and performance, and its ERM materials explain its relationship to internal control. See COSO's Enterprise Risk Management guidance and its Internal Control guidance.

QUESTION NO: 6

According to IIA guidance, which of the following is a typical risk associated with the tender process and contracting stage of an organization's IT outsourcing life cycle?

A. The process is not sustained and is not optimized as planned.

B. There is a lack of alignment to organizational strategies.

C. The operational quality is less than projected.

D. There is increased potential for loss of assets.

ANSWER: D

Explanation:

There is increased potential for loss of assets. During tendering and contracting, the organization is selecting a provider and defining the legal, commercial, operational, and control terms under which that provider may handle organizational resources. Those resources can include information, intellectual property, software, equipment, funds, and access credentials. If due diligence is incomplete or the contract does not clearly establish ownership, permitted use, security responsibilities, access controls, insurance, liability, return or destruction requirements, and rights to monitor the provider, assets may be exposed to misuse, theft, disclosure, unavailability, or loss of control. This is a particularly important outsourcing risk because the service provider—and sometimes its subcontractors—may obtain physical or logical custody of assets that previously remained entirely within the organization. Internal audit should therefore assess whether the procurement and contract processes incorporate risk assessment, appropriate vendor evaluation, enforceable control requirements, and continuing oversight mechanisms. The IIA's guidance on third-party risk emphasizes governance and controls over external relationships, while the IIA Standards require internal auditors to evaluate risks relevant to the engagement's objectives. See the IIA Third-Party Risk Management practice guidance and the Global Internal Audit Standards.

QUESTION NO: 7

A manager has allowed a subordinate employee to have greater control and responsibility over the tasks that he performs. This is an example of which of the following?

A. Job enlargement.

B. Job enlargement.

C. Horizontal loading of the job.

D. Job rotation

E. Job enrichment.

ANSWER: E

Explanation:

Job enrichment. is correct because it increases the depth of an employee's job by giving the employee greater autonomy, responsibility, and control over how work is performed. Rather than merely changing the number or variety of tasks, job enrichment redesigns work so that the employee has more meaningful authority and accountability in carrying it out. In this situation, the manager has specifically allowed the subordinate greater control and responsibility over assigned tasks, which reflects the core characteristics of enriched work.

Job enrichment is closely associated with the job characteristics model, particularly autonomy. Autonomy gives an individual discretion in scheduling work and determining the procedures used, and it supports a stronger sense of personal responsibility for work outcomes. Providing this increased responsibility can improve intrinsic motivation, engagement, and satisfaction when the employee has the appropriate competence and support. The concept is also consistent with participative management practices, in which managers delegate meaningful decision-making authority rather than retaining all control. See OpenStax, Motivating Employees Through Job Design and CIPD, Job Quality and Good Work.

QUESTION NO: 8

Which of the following is always true regarding the use of encryption algorithms based on public key infrastructure (PKI)?

A. PKI uses an independent administrator to manage the public key.

B. The public key is authenticated against reliable third-party identification.

C. PKI's public accessibility allows it to be used readily for e-commerce.

D. The private key uniquely authenticates each party to a transaction.

ANSWER: B

Explanation:

The public key is authenticated against reliable third-party identification. PKI establishes trust by binding a subject's verified identity to that subject's public key in a digital certificate. A trusted certificate authority, often with support from a registration authority, performs or relies on identity-validation procedures before issuing the certificate. The certificate then contains the public key, subject-identifying information, issuer information, validity dates, and the issuer's digital signature. Relying parties can validate that signature and, where applicable, the certificate chain to determine whether they can trust the asserted connection between the public key and the identified entity. This trusted identity-to-key binding is the defining operational purpose of PKI: it allows a recipient to use a public key with confidence that it belongs to the named person, system, or organization. NIST describes PKI as providing the framework for managing public-key certificates and establishing trusted associations between identities and public keys. The certificate profile in RFC 5280 similarly defines certificates as structures issued and signed by certification authorities to support this trust relationship. See NIST SP 800-32 and RFC 5280.

QUESTION NO: 9

A software that translates hypertext markup language (HTML) documents and allows a user to view a remote web page is called:

A. A transmission control protocol/Internet protocol (TCP/IP).

B. An operating system.

C. A web browser.

D. A web server.

ANSWER: C

Explanation:

A web browser. is correct because a browser is client-side application software that retrieves web resources from remote servers, interprets HTML documents, and renders their content into a visual, interactive webpage for the user. When a user enters a URL or selects a hyperlink, the browser typically uses web protocols such as HTTP or HTTPS to request the resource. It then parses the returned HTML to establish the page's structure and processes related resources, including style sheets, scripts, images, and media, so that the page can be displayed and used. This role directly matches the description of software that translates HTML and enables a person to view a remote web page. Common examples include Chrome, Firefox, Safari, and Edge. From an audit and business-technology perspective, browsers are important endpoint applications because their settings, extensions, patching status, certificate handling, and support for secure protocols can affect organizational security and users' access to web-based systems. The World Wide Web Consortium describes HTML as the markup language used to structure web content, while Mozilla's web documentation explains the browser's role in retrieving and displaying web content. See the HTML Living Standard and Mozilla's overview of web browsing.

QUESTION NO: 10

The market price is the most appropriate transfer price to be charged by one department to another in the same organization for a service provided when:

A. There is an external market for that service.

B. The selling department operates at 50 percent of its capacity.

C. The purchasing department has more negotiating power than the selling department.

D. There is no external market for that service.

ANSWER: A

Explanation:

There is an external market for that service. A competitive external market supplies an objective, observable benchmark for the value of the service transferred internally. Using that market price supports decentralized decision-making because the selling department is credited at the amount it could generally obtain from an outside customer, while the purchasing department can compare the internal charge with the cost of obtaining the same service externally. Thus, the transfer price reflects the economic opportunity associated with using the department's resources internally rather than making an external sale. A market-based price also promotes meaningful performance evaluation of departmental managers: their reported results are less affected by an arbitrary internal allocation and more closely aligned with prices available in the marketplace. For this purpose, the market should be sufficiently active and competitive so that its price is a credible measure of the service's value. Transfer-pricing guidance commonly identifies an external market price as the preferred basis where such a market exists, because it can align divisional incentives with organizational value creation. See the OpenStax discussion of relevant costs and market alternatives and the ACCA overview of transfer pricing.

QUESTION NO: 11

The economic order quantity for inventory is higher for an organization that has:

A. Lower annual unit sales.

B. Higher fixed inventory ordering costs.

C. Higher annual carrying costs as a percentage of inventory value.

D. A higher purchase price per unit of inventory.

ANSWER: B

Explanation:

Higher fixed inventory ordering costs is correct because the economic order quantity (EOQ) model balances the cost of placing orders against the cost of holding inventory. The standard EOQ formula is EOQ = $\sqrt{}$(2DS/H), where D is annual demand in units, S is the fixed cost incurred for each order, and H is the annual holding cost per unit. Since the fixed ordering cost, S, is in the numerator, an increase in that cost increases the calculated EOQ, assuming demand and annual holding cost per unit remain constant.

Operationally, when every purchase order requires more administrative processing, receiving activity, supplier coordination, or transportation setup cost, the organization can reduce the number of orders placed during the year by ordering a larger quantity each time. The larger order quantity spreads each fixed ordering cost across more units. EOQ identifies the order size at which the combined annual ordering and holding costs are minimized under the model's assumptions. This relationship is a core inventory-management principle used in planning purchasing frequency and inventory replenishment. See the EOQ formula and its cost components in Corporate Finance Institute's EOQ overview and Accounting for Management's EOQ explanation.

QUESTION NO: 12

Which of the following types of data analytics would be used by a hospital to determine which patients are likely to require readmittance for additional treatment?

A. Predictive analytics

B. Prescriptive analytics

C. Descriptive analytics

D. Diagnostic analytics

ANSWER: A

Explanation:

Predictive analytics is the appropriate approach because the hospital is using available and historical patient information to estimate a future outcome: whether a patient is likely to be readmitted for further treatment. Predictive models identify patterns and relationships in data such as diagnoses, prior admissions, treatment history, test results, demographics, medication adherence, and discharge details. The resulting risk estimates can help clinicians and hospital management recognize patients who may benefit from enhanced discharge planning, follow-up appointments, care coordination, or other preventive interventions. In an internal audit context, analytics of this type may also support assurance or advisory work over the quality, governance, privacy, and reliability of models used in clinical or operational decision-making. The defining purpose is forecasting the probability of a future event rather than merely reporting past activity. IBM describes predictive analytics as using historical data, statistical algorithms, and machine-learning techniques to identify the likelihood of future outcomes. The U.S. Centers for Medicare & Medicaid Services also recognizes hospital readmissions as an important quality and performance measure, reinforcing the operational relevance of forecasting readmission risk. See IBM: Predictive analytics and CMS: Hospital Readmissions Reduction Program.

QUESTION NO: 13

Providing knowledge, motivating organizational members, controlling and coordinating individual efforts, and expressing feelings and emotions are all functions of:

A. Motivation.

B. Performance.

C. Organizational structure.

D. Communication.

ANSWER: D

Explanation:

Communication. is correct because communication performs several essential functions within an organization: it conveys information needed for informed decisions and task performance; it can motivate people by clarifying expectations, providing feedback, and reinforcing desired behavior; it supports control and coordination by communicating policies, procedures, responsibilities, and performance expectations; and it provides a channel through which people express social needs, feelings, and emotions. These functions enable organizational members to align their work with objectives, cooperate across roles and units, and respond effectively to change. For internal auditors, understanding communication is particularly important because audit results, recommendations, risk information, and assurance conclusions must be communicated clearly and appropriately to support sound governance and management action. The IIA Standards require internal audit communications to be accurate, objective, clear, concise, constructive, complete, and timely, reflecting communication's central role in effective organizational processes. See the IIA's Global Internal Audit Standards and OpenStax's discussion of organizational communication.

QUESTION NO: 14

Which of the following is an example of internal auditors applying data mining techniques for exploratory purposes?

A. Internal auditors perform reconciliation procedures to support an external audit of financial reporting.

B. Internal auditors perform a systems-focused analysis to review relevant controls.

C. Internal auditors perform a risk assessment to identify potential audit subjects as input for the annual internal audit plan.

D. Internal auditors test IT general controls with regard to operating effectiveness versus design.

ANSWER: C

Explanation:

Internal auditors perform a risk assessment to identify potential audit subjects as input for the annual internal audit plan. This is an exploratory use of data mining because it uses available organizational data to discover potential areas of risk, emerging trends, unusual relationships, concentrations of activity, or patterns that merit audit attention. At this stage, the auditors are not necessarily testing a predefined control objective or validating a known condition. Instead, they are examining the audit universe broadly to generate insights and identify subjects that may warrant further assessment or inclusion in the plan.

Exploratory analytics is especially useful in risk assessment because internal audit planning must be dynamic and risk-based. Data from finance, operations, compliance, incidents, customer activity, technology, and prior audit results can be analyzed to highlight where risk may be changing or where assurance coverage could be most valuable. Those results inform professional judgment in prioritizing potential engagements and allocating audit resources. The IIA's Global Internal Audit Standards require the chief audit executive to develop a risk-based internal audit plan, and the IIA describes data analytics as a means to obtain insights from data that support audit activities. See the IIA Global Internal Audit Standards and the IIA's Global Technology Audit Guide on Data Analytics.

QUESTION NO: 15

During a review of a web-based application used by customers to check the status of their bank accounts, it would be most important for the internal auditor to ensure that:

A. Access to read application logs is restricted to authorized users.

B. Account balance information is encrypted in the database.

C. The web server used to host the application is located in a physically secure area.

D. Sensitive data, such as account numbers, are submitted using encrypted communications.

ANSWER: D

Explanation:

Sensitive data, such as account numbers, are submitted using encrypted communications. This is the most important control because a customer-facing web application transmits information across networks outside the bank's direct physical control. Transport-layer encryption, normally HTTPS using current TLS configurations, protects the confidentiality and integrity of data while it travels between the customer's browser and the bank's web application. It reduces the risk that account numbers, authentication credentials, balances, session identifiers, or transaction-related data can be intercepted or modified by an unauthorized party on public Wi-Fi, an internet service provider path, or another untrusted network segment. For an internal auditor, the review should confirm that sensitive pages and application programming interfaces require HTTPS, that insecure protocol versions and weak cipher suites are disabled, that certificates are valid and properly managed, and that redirects and session cookies prevent accidental use of unencrypted connections. These measures address a fundamental exposure inherent in internet-facing banking services: protecting customer data in transit. NIST provides federal guidance on selecting and configuring TLS in SP 800-52 Revision 2, and OWASP describes practical TLS implementation practices in its Transport Layer Security Cheat Sheet.

QUESTION NO: 16

In an effort to increase business efficiencies and improve customer service offered to its major trading partners, management of a manufacturing and distribution company established a secure network, which provides a secure channel for electronic data interchange between the company and its partners.

Which of the following network types is illustrated by this scenario?

A. A value-added network.

B. A local area network.

C. A metropolitan area network.

D. A wide area network.

ANSWER: A

Explanation:

A value-added network is correct because it is a third-party, private communications service designed to support the secure exchange of electronic business documents between trading partners. In an electronic data interchange environment, a value-added network acts as an intermediary connection through which organizations can send, receive, route, store, and, in some cases, validate standardized transaction messages such as purchase orders, invoices, advance shipping notices, and payment-related documents. Its purpose is to make business-to-business document exchange dependable and efficient while avoiding the need for every partner to build and maintain separate direct connections with every other partner.

The scenario specifically emphasizes a secure channel established for electronic data interchange between a manufacturing and distribution company and its major trading partners. That business-to-business EDI use case is the defining application of a value-added network. Such networks historically supplied mailboxing, protocol conversion, message tracking, delivery confirmation, and security services, adding operational value beyond basic network connectivity. This helps management improve transaction speed, reliability, partner coordination, and customer service while supporting efficient supply-chain operations. IBM describes VANs as networks that facilitate EDI communications between trading partners in its overview of value-added networks. Additional background is available in Investopedia's definition of a value-added network.

QUESTION NO: 17

Which of the following is a key component of an organization's cybersecurity governance?

A. Administrators monitoring the use, assignment and configuration of privileges on the network.

B. The IT department establishing implementing, and actively managing security configurations.

C. Management identifying and classifying the types of critical data in the organization's system

D. Senior management of the organization setting the cybersecurity policy

ANSWER: D

Explanation:

Senior management of the organization setting the cybersecurity policy is a key component of cybersecurity governance because governance establishes the direction, authority, accountability, and oversight through which cybersecurity supports organizational objectives and manages risk. A cybersecurity policy approved and set by senior management communicates the organization's expectations for protecting information and technology assets. It provides the high-level foundation for such matters as risk tolerance, roles and responsibilities, compliance obligations, information protection, incident reporting, and the authority to issue supporting standards and procedures.

Senior management's involvement is essential because cybersecurity risk is an enterprise risk, rather than solely a technical concern. Its policy direction helps ensure that cybersecurity decisions are aligned with business strategy, that appropriate resources are assigned, and that management can be held accountable for implementation and ongoing risk reporting. The IIA's Global Internal Audit Standards emphasize the governing body's and senior management's roles in establishing risk-management expectations and supporting effective governance. Similarly, the NIST Cybersecurity Framework identifies governance as the function through which organizational cybersecurity risk-management strategy, expectations, and policy are established and monitored. See the IIA Global Internal Audit Standards and NIST Cybersecurity Framework.

QUESTION NO: 18

A company has a highly centralized organizational structure. Which of the following is most likely to be an advantage of this structure?

A. Greater consistency in decisions across business units.

B. Faster response to local customer needs by lower-level managers.

C. Greater autonomy for regional operating units.

D. Broader delegation of strategic decision-making authority.

ANSWER: A

Explanation:

Greater consistency in decisions across business units. is correct because centralized structures concentrate significant decision-making authority at higher levels of management. This can promote uniform policies, coordinated strategic direction, and consistent application of standards across business units, locations, or product lines.

Centralization may also create disadvantages, including slower response to local conditions and reduced autonomy for lower-level managers. Faster local decision-making and broad delegation of authority are more commonly associated with decentralized structures. Internal auditors should understand the organization's structure because reporting lines and delegated authority affect accountability, risk management, and control design. See OpenStax's discussion of organizational design considerations.

QUESTION NO: 19

The decision to implement enhanced failure detection and back-up systems to improve data integrity is an example of which risk response?

A. Risk acceptance.

B. Risk sharing.

C. Risk avoidance.

D. Risk reduction.

ANSWER: D

Explanation:

Risk reduction is correct because enhanced failure detection and backup systems are control measures intended to lower the likelihood that a system failure will result in compromised, unavailable, or inaccurate data, and to limit the impact if such a failure occurs. The organization is not discontinuing the activity that creates the exposure; it is continuing to operate its information systems while adding preventive, detective, and recovery capabilities. Failure detection can identify abnormal conditions promptly, allowing intervention before integrity is materially affected. Backups provide a means to restore reliable data after corruption, loss, or a disruptive event. Together, these measures reduce residual risk to a level within management's risk appetite or tolerance. This reflects the common risk-treatment approach of modifying risk through controls that reduce its likelihood, consequences, or both. The IIA's guidance describes risk management as selecting and implementing responses to manage risks within the organization's established tolerance, while the NIST contingency-planning guidance identifies backup and recovery capabilities as key controls for restoring systems and data following disruptions. See The IIA Global Internal Audit Standards and NIST SP 800-34 Rev. 1, Contingency Planning Guide.

QUESTION NO: 20

Which of the following is a characteristic of an emerging industry?

A. Established strategy of players.

B. Low number of new firms.

C. High unit costs.

D. Technical expertise.

ANSWER: C

Explanation:

High unit costs. is a characteristic of an emerging industry because organizations in a newly developing market generally operate at relatively low production volumes. They have not yet achieved the economies of scale, process efficiencies, stable supplier relationships, or fully optimized production methods that can reduce the cost of each unit produced. Early-stage firms may also face substantial up-front expenditures for research, product development, market education, distribution infrastructure, and capacity building. Those fixed and start-up costs are spread over a comparatively small number of sales, increasing per-unit costs.

From an industry-analysis perspective, emerging industries are often shaped by uncertainty about customer demand, technology, standards, and the eventual basis of competition. As demand grows and firms gain experience, learning effects and higher output can lower unit costs significantly. Internal auditors assessing businesses in such industries should recognize that high unit costs can be an expected feature of the industry's development stage, while also considering whether management's forecasts appropriately account for the timing and assumptions required to achieve scale. Porter's competitive-strategy framework discusses the distinctive structural conditions of emerging industries, and economies of scale explain why costs often decline as output expands. See Harvard Business School's Competitive Strategy reference and Economics Help: Economies of Scale.

QUESTION NO: 21

An organization uses the management-by-objectives method, whereby employee performance is based on defined goals Which of the following statements is true regarding this approach?

A. It is particularly helpful to management when the organization is facing rapid change

B. It is a more successful approach when adopted by mechanistic organizations

C. It is more successful when goal-setting is performed not only by management, but by all team members, including lower-level staff.

D. It is particularly successful in environments that are prone to having poor employer-employee relations

ANSWER: C

Explanation:

Management by objectives is more successful when goal setting involves managers and team members at all organizational levels. A defining feature of this approach is participative objective setting: employees and their supervisors jointly establish clear, measurable objectives that support broader organizational goals. This collaboration helps ensure that employees understand how their work contributes to results, regard the goals as achievable and relevant, and accept accountability for completing them. It also creates a practical basis for periodic performance discussions, feedback, and assessment against agreed results.

For internal auditors, the participative nature of the process is important when assessing whether a performance-management system is designed effectively. Auditors can look for alignment between individual and organizational objectives, evidence that objectives are communicated and agreed, documented measures and time frames, and regular monitoring of progress. These elements support both employee commitment and meaningful evaluation. Management-by-objectives principles emphasize that objectives should be established through a collaborative manager-employee process rather than imposed solely from the top. See OpenStax, Performance Management Systems and Encyclopaedia Britannica, management by objectives.

QUESTION NO: 22

Which of the following should software auditors do when reporting internal audit findings related to enterprise wide resource planning?

A. Draft separate audit reports for business and IT management

B. Connect IT audit findings to business issues

C. Include technical details to support IT issues

D. Include an opinion on financial reporting accuracy and completeness

ANSWER: B

Explanation:

Connect IT audit findings to business issues is correct because enterprise resource planning systems support core, cross-functional processes such as financial management, procurement, inventory, payroll, and operational reporting. Audit communication is most useful to senior management and the board when it translates a technical condition into its effect on organizational objectives, risks, controls, compliance obligations, data reliability, process performance, or decision-making. For example, a finding concerning excessive system access should be communicated in terms of the resulting risk to transaction authorization, segregation of duties, financial data integrity, or the reliability of management information. This framing enables management to understand the significance and priority of remediation, assign accountable owners, and make informed risk-based decisions. The IIA's Global Internal Audit Standards require communications to be clear, concise, constructive, complete, and timely, and require conclusions to address the significance of the engagement results in relation to objectives. Relating system-level observations to business impacts also supports a risk-based internal audit approach and promotes practical, value-adding recommendations. See the IIA's Global Internal Audit Standards and its Standards resources.

QUESTION NO: 23

Which of the following is true regarding an organization ' s relationship with external stakeholders?

A. Specific guidance must be followed when interacting with nongovernmental organizations.

B. Disclosure laws tend to be consistent from one jurisdiction to another.

C. There are several internationally recognized standards for dealing with financial donors.

D. Legal representation should be consulted before releasing internal audit information to other assurance providers.

ANSWER: D

Explanation:

Legal representation should be consulted before releasing internal audit information to other assurance providers. Internal audit reports, working papers, risk assessments, and audit-related communications can contain confidential business information, personally identifiable information, legally privileged material, regulatory-sensitive findings, or information subject to contractual restrictions. Before such material is provided outside the organization, legal counsel can determine whether disclosure is required, permitted, restricted, or subject to safeguards such as a nondisclosure agreement, redaction, or a formal information-sharing protocol. This review helps the organization meet applicable privacy, securities, regulatory, litigation-hold, and confidentiality obligations while preserving legal privilege where applicable.

The IIA's Global Internal Audit Standards require internal auditors to protect information acquired in the course of their work and to use it only for appropriate professional purposes. They also recognize coordination and communication with other assurance providers, which must be managed in a way that protects the organization's interests and complies with relevant requirements. Consulting legal representation before external release is therefore an appropriate governance and risk-management control, particularly when the recipient is an external assurance provider. See the IIA Global Internal Audit Standards and the IIA Standards resource page.

QUESTION NO: 24

An organization accumulated the following data for the prior fiscal year:

Value of Percentage of

Quarter

Output Produced

Cost X

1

$4,750,000

2.9

2

$4,700,000

3.0

3

$4,350,000

3.2

4

$4,000,000

3.5

Based on this data, which of the following describes the value of Cost X in relation to the value of Output Produced?

A. Cost X is a variable cost.

B. Cost X is a fixed cost.

C. Cost X is a semi-fixed cost.

D. Cost X and the value of Output Produced are unrelated.

ANSWER: B

Explanation:

Cost X is a fixed cost. Converting each reported percentage into a dollar amount shows that Cost X remains essentially constant despite changes in the value of output produced. For the first quarter, 2.9% of $4,750,000 is $137,750; for the second quarter, 3.0% of $4,700,000 is $141,000; for the third quarter, 3.2% of $4,350,000 is $139,200; and for the fourth quarter, 3.5% of $4,000,000 is $140,000. Thus, Cost X is approximately $140,000 in every quarter. The small variation is reasonably attributable to rounding because the percentages are presented to only one decimal place. A fixed cost remains constant in total over the relevant range of activity, while its percentage of output or cost per unit changes inversely as activity changes. Here, as output value declines, Cost X represents an increasing percentage of that output, which is the expected pattern for a fixed cost. This cost-behavior distinction is fundamental to planning, budgeting, performance analysis, and evaluating how changes in operating volume affect financial results. See OpenStax, Cost Behavior and AccountingCoach, Cost Behavior.

QUESTION NO: 25

Which of the following is accurate regarding help desk service providers?

A. Performance results, deficiencies, and remediation should not be used as criteria for ongoing vendor evaluation.

B. Turn-around time cannot always be defined for each level of service in complex environments.

C. Ongoing monitoring procedures that measure and compare actual performance to the expected service-level parameters must be set by the service provider.

D. Any problems troubleshooting can be categorized as a help desk service.

ANSWER: B

Explanation:

Turn-around time cannot always be defined for each level of service in complex environments. is accurate because a help desk can establish target response and resolution times for common, well-defined incidents, but some requests cannot be assigned a reliable fixed completion period in advance. Complex incidents may require detailed diagnosis, coordination with multiple internal teams or external suppliers, investigation of an unknown root cause, change approval, or restoration of an interdependent service. These factors make the ultimate time to resolve uncertain even when the service provider has clear obligations to acknowledge, prioritize, communicate about, and escalate the ticket.

A well-designed service-level agreement therefore distinguishes measurable commitments, such as availability, initial response time, update frequency, and escalation procedures, from resolution objectives that may be conditional on incident severity, dependencies, and the information available. This approach gives the organization meaningful performance criteria while recognizing that complex troubleshooting often develops as evidence is gathered. NIST's supply-chain guidance emphasizes defining requirements and continuously managing supplier performance and dependencies, which supports using realistic, measurable service expectations rather than assuming every outcome can be precisely timed. See NIST SP 800-161 Rev. 1 and NIST guidance on service providers.

QUESTION NO: 26

According to Porter's model of competitive strategy, which of the following is a generic strategy?

1 Differentiation.

2) Competitive advantage.

3) Focused differentiation.

4) Cost focus.

A. 2 only

B. 3 and 4 only

C. 1, 3, and 4 only

D. 1, 2, 3, and 4

ANSWER: C

Explanation:

1, 3, and 4 only is correct because Porter's generic-strategy framework identifies differentiation and cost leadership as the principal sources of competitive advantage, combined with either a broad industry scope or a narrow target segment (focus). Differentiation means creating offerings perceived as distinctive by customers. When this differentiation approach is directed at a narrow market segment, it is commonly termed focused differentiation (or differentiation focus). Similarly, when a business seeks the lowest-cost position within a narrowly defined segment, it is pursuing cost focus. These focused variants apply the same fundamental strategic choices to a particular buyer group, product line, or geographic market rather than the industry as a whole. "Competitive advantage" is the outcome a successful generic strategy is intended to produce, rather than itself being one of the generic strategies. Porter presents the relationship between competitive advantage and competitive scope in his foundational work, Competitive Advantage: Creating and Sustaining Superior Performance. The framework remains a core strategic-analysis tool for evaluating how an organization intends to achieve a defensible position in its chosen market; see also the Harvard Business School Institute for Strategy and Competitiveness overview.

QUESTION NO: 27 - (SIMULATION)

Which of the following is a project planning methodology that involves a complex series ot required simulations to provide information about schedule risk?

ANSWER: See the explanation for the answer

Explanation:

Answer: Monte Carlo simulation (Monte Carlo analysis).

Monte Carlo simulation is a project-planning and risk-analysis technique that runs many iterations using varying assumptions for activity durations, costs, or other uncertain inputs. The results estimate the probability of meeting specific schedule dates and identify schedule risk.

For example, it can show that a project has only a 60% probability of completing by a planned deadline, rather than presenting a single deterministic completion date.

QUESTION NO: 28

In terms of international business strategy, which of the following is true regarding a multi-domestic strategy?

A. It uses the same products in all countries.

B. It centralizes control with little decision-making authority given to the local level.

C. It is an effective strategy when large differences exist between countries.

D. It provides cost advantages, improves coordinated activities, and speeds product development.

ANSWER: C

Explanation:

It is an effective strategy when large differences exist between countries. A multidomestic strategy emphasizes responsiveness to conditions in each national market. Rather than treating all countries as one homogeneous market, the organization allows substantial local adaptation of products, marketing, distribution, and operating decisions. This approach is especially appropriate where consumer preferences, cultural norms, language, regulations, competitive conditions, or distribution systems differ significantly from country to country. Local managers generally need meaningful decision-making authority because they are closer to these market-specific requirements and can tailor the business's offerings and practices accordingly. The strategy therefore seeks to maximize local responsiveness, even when that limits opportunities to standardize activities globally or realize the full scale economies of a single uniform product and centralized operating model. For internal auditors, the decentralized nature of this strategy makes it important to assess whether governance establishes clear global policies and risk tolerances while preserving the local flexibility needed to comply with country-specific laws and serve local customers effectively. The distinction between global integration and local responsiveness is a core framework in international strategy. See OpenStax, International Strategies and Pearson, Global Strategy.

QUESTION NO: 29

Which of the following statements is true regarding partnership liquidation?

A. Operations can continue after the liquidation if all partners agree

B. Partnership liquidation ends both the legal and economic life of an entity

C. Partnership liquidation occurs when there is capital deficiency Stable

D. When a partnership is liquidated, each partner pays creditors from cash received

ANSWER: B

Explanation:

Partnership liquidation ends both the legal and economic life of an entity. Liquidation is the final windup process for a partnership: the partnership stops conducting its ordinary revenue-generating activities, converts noncash assets to cash, settles liabilities with creditors, and distributes any remaining cash to partners in accordance with their capital interests and the partnership agreement. Once this process is completed, the partnership no longer has an ongoing economic purpose or operations; its affairs have been concluded. The legal relationship represented by the partnership is also terminated after the required winding-up and termination steps are completed under applicable partnership law. This distinguishes liquidation from changes in the partner group or other events that may require accounting adjustments while a business continues. In financial-accounting terms, liquidation accounting focuses on realizing assets, paying obligations, and making final distributions rather than measuring results from continuing operations. OpenStax describes partnership liquidation as the process of converting assets to cash, paying creditors, and distributing the residual cash to partners: OpenStax, Partnership Liquidation. Partnership-law concepts concerning winding up and termination are also summarized by the Legal Information Institute.

QUESTION NO: 30

According to IIA guidance, which of the following is a broad collection of integrated policies, standards, and procedures used to guide the planning and execution of a project?

A. Project portfolio.

B. Project development.

C. Project governance.

D. Project management methodologies.

ANSWER: D

Explanation:

Project management methodologies is correct because a project management methodology provides an organized, repeatable framework for directing work throughout a project life cycle. It brings together integrated policies, standards, processes, procedures, tools, and practices that guide how a project is initiated, planned, executed, monitored, controlled, and closed. Using a defined methodology helps project teams apply consistent governance and management discipline, establish roles and decision points, manage scope, schedules, costs, risks, quality, and communications, and produce documentation that supports oversight and assurance activities. From an internal-audit perspective, the methodology also supplies criteria against which project controls and project-management practices can be evaluated. The IIA's Global Technology Audit Guide on auditing project management emphasizes the importance of assessing the project-management framework, including its processes, controls, and governance arrangements, across the project life cycle. Similarly, PMI describes project management as applying knowledge, skills, tools, and techniques through established processes to meet project requirements. A methodology is therefore the broad integrated collection that guides planning and execution rather than merely a single project, development activity, or governance structure. See the IIA's GTAG: Auditing Project Management and PMI's overview of project management.

QUESTION NO: 31

Which of the following statements is true regarding the risks associated with the increased use of smart devices at work?

A. Due to their small size and portability smart devices and their associated data are typically less susceptible to physical loss

B. The Bluetooth and WI-FI features of smart devices enhance the security of data while in transit

C. The global positioning system (GPS) capability of smart devices could be exploited to plan cyberattacks

D. When the user fads to perform jailbreaking or rooting, data security and privacy risks we increased

ANSWER: C

Explanation:

The global positioning system (GPS) capability of smart devices could be exploited to plan cyberattacks. GPS and other location-service data can reveal where a device—and often its user—is located, travels, or routinely works. If such information is exposed through an application, device telemetry, social engineering, insecure configuration, or a compromised device, an attacker can use it for reconnaissance. For example, location patterns may identify a sensitive facility, reveal when personnel are likely to be away from a site, help target individuals with convincing location-themed phishing messages, or support physical intrusion attempts coordinated with cyber activity. This makes location information a security-relevant form of organizational data, rather than merely a personal convenience feature.

Effective mobile-device risk management therefore includes limiting location collection and sharing to a legitimate business need, applying least-privilege permissions, managing devices through enterprise mobile-device controls, keeping device software current, and ensuring personnel understand the sensitivity of location data. NIST's guidance on enterprise mobile-device security identifies the need to manage device capabilities, applications, and data protections throughout the mobile-device lifecycle. The OWASP Mobile Application Security Verification Standard likewise addresses privacy controls and the secure handling of sensitive data by mobile applications. See NIST SP 800-124 Rev. 2 and the OWASP MASVS.

QUESTION NO: 32

Which of the following accounting methods is an investor organization likely to use when buying 40 percent of the stock of another organization?

A. Cost method

B. Equity method

C. Consolidation method

D. Fair value method

ANSWER: B

Explanation:

The equity method is the accounting approach an investor organization is likely to use after acquiring 40 percent of another organization's voting stock. A holding of this size generally gives the investor significant influence over the investee's operating and financial policy decisions, even though it does not necessarily establish control. Under the equity method, the investment is initially recorded at cost. Subsequently, the investor adjusts the investment's carrying amount for its proportionate share of the investee's earnings or losses. The investor also reduces the carrying amount for dividends received, because those dividends represent a distribution of the investee's net assets rather than new income to the investor. Significant influence is presumed under U.S. GAAP when an investor holds 20 percent or more of an investee's voting stock, absent evidence that influence is not present. Thus, a 40 percent ownership interest normally supports use of the equity method, provided the investor does not control the investee. See the Financial Accounting Standards Board's accounting standards resources at FASB Accounting Standards Codification and the U.S. Securities and Exchange Commission's overview of equity-method investments at SEC accounting guidance.

QUESTION NO: 33

An organization is considering mirroring the customer data for one regional center at another center. A disadvantage of such an arrangement would be:

A. Lack of awareness of the state of processing.

B. Increased cost and complexity of network traffic.

C. Interference of the mirrored data with the original source data.

D. Confusion about where customer data are stored.

ANSWER: B

Explanation:

Increased cost and complexity of network traffic is a principal disadvantage of data mirroring between regional centers. Mirroring maintains a duplicate copy of customer data at a separate location to improve availability, resilience, and disaster-recovery capability. To keep the copy usable, the organization must transmit initial data volumes and then continually send changed records, transaction logs, or replication updates across the network. This creates ongoing bandwidth consumption and may require dedicated links, encryption, monitoring, replication software, additional storage, and administration. The architecture also has to manage replication latency, transmission failures, sequencing, reconciliation, and the choice between synchronous replication—where updates wait for the remote copy—and asynchronous replication—where a recovery point gap may exist. These design and operational requirements increase both direct cost and technical complexity, particularly where customer data volumes or transaction rates are high. NIST describes replication as maintaining copies of data at alternate sites for contingency and recovery purposes, while emphasizing the need to plan and test recovery capabilities. The Cybersecurity and Infrastructure Security Agency likewise identifies redundant systems and geographically separate backups as resilience measures that require appropriate implementation and protection. See NIST SP 800-34 Rev. 1 and CISA StopRansomware Guide.

QUESTION NO: 34

A company sells a product for $80 per unit. Variable cost is $50 per unit, and annual fixed costs are $300,000. How many units must the company sell to break even?

A. 6,000 units.

B. 7,500 units.

C. 10,000 units.

D. 16,000 units.

ANSWER: C

Explanation:

10,000 units. is correct because the contribution margin per unit is $30, calculated as the $80 selling price less the $50 variable cost. The break-even volume equals fixed costs divided by contribution margin per unit: $300,000 divided by $30 equals 10,000 units.

At the break-even point, total contribution margin exactly covers fixed costs, resulting in neither profit nor loss. Break-even analysis is useful for evaluating the sensitivity of profitability to changes in sales volume, pricing, variable costs, and fixed-cost commitments. See OpenStax, The Breakeven Point.

QUESTION NO: 35

Which of the following application controls, implemented by management, monitors data being processed to ensure the data remains consistent and accurate?

A. Management trail controls.

B. Output controls.

C. Integrity controls.

D. Input controls.

ANSWER: C

Explanation:

Integrity controls are designed to preserve the completeness, accuracy, consistency, and validity of data throughout processing. In an application, these controls monitor whether data continues to conform to defined rules as it is transformed, stored, transferred, or updated. Examples include validation rules, referential-integrity checks, edit checks, sequence checks, hash totals, reconciliation routines, and exception reporting. Their purpose is not merely to accept data at entry, but to ensure that processing does not create inconsistent records, omit transactions, duplicate information, or corrupt relationships among data elements. This directly supports management's responsibility to maintain reliable information for operational and financial decision-making, while also providing internal audit with evidence that automated processing is controlled. The IIA's Global Internal Audit Standards emphasize evaluating the adequacy and effectiveness of governance, risk management, and control processes, including controls that support the reliability and integrity of information. See the IIA Global Internal Audit Standards. The importance of maintaining information integrity through controls is also reflected in the ISACA COBIT framework, which addresses reliable, secure, and useful information.

QUESTION NO: 36

New data privacy laws require an organization to use collected customer information for me sole purpose of meeting the organization's business requirements. Which of the following best addresses the risk of the organization not complying with this objective?

A. Provide training on social engineering attacks

B. Encrypt the customer information retained by the organization

C. Establish policies that discipline those who misuse customer information

D. Allocate access profiles for each end user of the information

ANSWER: D

Explanation:

Allocate access profiles for each end user of the information best addresses this risk because access profiles can enforce that customer information is available only to personnel whose job responsibilities create a legitimate business need for it. Properly designed role-based access profiles apply least-privilege and need-to-know principles, limiting both the data elements and system functions available to each user. This makes the privacy requirement operational: access is tied to defined business purposes rather than being broadly available for unrelated use. The organization should define roles from its data-processing purposes, approve access through an accountable process, periodically review profile assignments, and promptly remove or amend access when responsibilities change. These practices create preventive evidence that use of personal information is constrained by business requirements. The GDPR purpose-limitation principle requires personal data to be collected for specified, explicit, and legitimate purposes and not further processed incompatibly with those purposes; access controls help implement that restriction in daily operations. See GDPR, Article 5. The importance of access management as a privacy-risk control is also consistent with the NIST Privacy Framework, which supports managing privacy risk through organizational and technical measures.

QUESTION NO: 37

Which of the following is false with regard to Internet connection firewalls?

A. Firewalls can protect against computer viruses.

B. Firewalls monitor attacks from the Internet.

C. Firewalls provide network administrators tools to retaliate against hackers.

D. Firewalls may be software-based or hardware-based.

ANSWER: C

Explanation:

Firewalls provide network administrators tools to retaliate against hackers is false. A firewall is a preventive and detective network-security control: it enforces traffic rules, restricts unauthorized connections, records relevant events, and can generate alerts that support investigation and incident response. Its purpose is to protect the organization's environment by controlling network communications at defined boundaries, not to launch actions against an external source. Appropriate response to suspected hostile activity includes preserving logs and evidence, blocking or restricting traffic, escalating through the organization's incident-response process, and, where appropriate, coordinating with legal counsel, Internet service providers, or law enforcement. Attempting to "retaliate" or hack back can create legal, operational, and evidentiary risks and is not a firewall function. Firewalls may be implemented as hardware appliances, software, or cloud-delivered controls. Depending on their capabilities and configuration, they can also contribute to malware protection by restricting risky traffic or inspecting permitted traffic, but they should be used as part of layered security rather than as the sole malware control. See NIST's guidance on firewall policy and implementation in SP 800-41 Rev. 1 and CISA's incident response resources.

QUESTION NO: 38

When applied to international economics, the theory of comparative advantage proposes that total worldwide output will be greatest when:

A. Each nation's total imports approximately equal its total exports.

B. Each good is produced by the nation that has the lowest opportunity cost for that good.

C. Goods that contribute to a nation's balance-of-payments deficit are no longer imported.

D. International trade is unrestricted and tariffs are not imposed.

ANSWER: B

Explanation:

Each good is produced by the nation that has the lowest opportunity cost for that good. Comparative advantage concerns relative production costs, measured by what a country must forgo to produce one additional unit of a particular good or service. When each nation specializes in goods for which its opportunity cost is lower than that of its trading partners, global resources are allocated toward their relatively most productive uses. This specialization increases the combined quantity of goods and services that can be produced from the world's available labor, capital, technology, and natural resources. Countries can then trade some of their specialized output to obtain other goods, allowing consumption possibilities to expand beyond what each country could achieve through self-sufficiency. The principle does not require a country to be the absolute lowest-cost producer in every sense; the critical comparison is the opportunity cost of one product relative to another within each country. This conclusion is a foundational application of David Ricardo's comparative-advantage model and explains why mutually beneficial trade can occur even when one country is more productive in producing all goods. For further background, see the International Monetary Fund's overview of comparative advantage and the OpenStax discussion of gains from trade.

QUESTION NO: 39

Which of the following cost of capital methods identifies the time period required to recover the cost of the capital investment from the annual inflow produced?

A. Cash payback technique.

B. Annual rate of return technique.

C. Internal rate of return method.

D. Net present value method.

ANSWER: A

Explanation:

Cash payback technique is correct because it measures the payback period: the length of time needed for cumulative cash inflows generated by an investment to equal its initial cash outlay. When annual net cash inflows are uniform, the calculation is generally the initial investment divided by the annual net cash inflow. For example, an investment of $100,000 expected to generate $25,000 of net cash inflow each year has a four-year cash payback period. Where inflows differ by year, the cash flows are accumulated until the original investment has been recovered, including a fraction of a year if necessary.

This method is commonly used as a capital-budgeting screening measure because it focuses directly on investment recovery time and liquidity. It answers the question posed without requiring a discount rate or estimating an investment's return as a percentage. The concept is also widely described as the "payback period." For a concise definition and calculation approach, see Investopedia's Payback Period overview. Additional capital-budgeting context is available from Corporate Finance Institute's Payback Period guide.

QUESTION NO: 40

Which of the following professional organizations sets standards for quality and environmental audits?

A. The Committee of Sponsoring Organizations of the Treadway Commission.

B. The Board of Environmental, Health, and Safety Auditor Certifications.

C. The International Organization of Supreme Audit Institutions.

D. The International Organization for Standardization (ISO).

ANSWER: D

Explanation:

The International Organization for Standardization (ISO) is correct because it develops internationally recognized standards for quality-management and environmental-management systems and provides the principal guidance used when auditing

those systems. ISO 9001 specifies requirements for quality management systems, while ISO 14001 specifies requirements for environmental management systems. Organizations may use these standards to establish controls, demonstrate conformity, and support certification or other assurance activities. ISO 19011, *Guidelines for auditing management systems*, is especially relevant to the question because it sets out guidance for audit principles, audit-program management, audit activities, and auditor competence for management-system audits. Its scope expressly includes quality and environmental management systems, among others. Thus, ISO is the standard-setting body associated with the common framework for conducting quality and environmental audits; accredited certification bodies and qualified auditors use the ISO standards and audit guidance in practice. ISO's official overview of ISO 19011 is available at ISO 19011:2018, and its environmental-management standard is described at ISO 14001 environmental management.

QUESTION NO: 41

Which of the following assumptions regarding cost-volume-profit analysis is true?

A. Costs are affected by changes in activity only.

B. The behavior of costs and revenues is inverse.

C. When more than one type of product is sold, the sales mix changes.

D. Only variable costs have to be classified accurately.

ANSWER: A

Explanation:

"Costs are affected by changes in activity only." is the applicable cost-volume-profit analysis assumption, provided the analysis is performed within the relevant range of operations. Cost-volume-profit analysis models how operating income responds when the level of an activity driver, commonly unit sales volume, changes. For the model to produce meaningful results, unit selling price and unit variable cost are treated as stable, while total fixed costs remain stable over the relevant range. Thus, the analysis attributes changes in total cost to changes in the activity level and relies on a predictable cost behavior pattern. This simplifying assumption allows management and internal auditors to calculate contribution margin, break-even volume, margin of safety, and the expected profit effect of planned changes in sales volume. It also supports sensitivity analysis, such as estimating the volume needed to attain a target profit. The relevant range qualification is important: a major capacity expansion, a new supplier arrangement, or another operational change can alter fixed costs, variable costs, or both, requiring the model inputs to be updated. This treatment of cost behavior is consistent with standard managerial-accounting descriptions of cost-volume-profit analysis. See OpenStax, Cost-Volume-Profit Analysis and AccountingCoach, Break-Even Point and Cost Behavior.

QUESTION NO: 42

Senior management has decided to implement the Three Lines of Defense model for risk management. Which of the following best describes senior management's duties with regard to this model?

A. Ensure compliance with the model.

B. Identify management functions.

C. Identify emerging issues.

D. Set goals for implementation.

ANSWER: A

Explanation:

Ensure compliance with the model is correct because senior management is responsible for putting the organization's risk-management and control arrangements into operation and ensuring that the assigned roles are observed in practice. Under the Three Lines Model, management is accountable for achieving organizational objectives and is responsible for establishing and maintaining appropriate structures and processes for managing operations, risk, and control. This includes

making sure that first-line operational management owns and manages risk in day-to-day activities, while second-line functions provide the relevant expertise, support, monitoring, and challenge. Senior management must therefore ensure that the model is applied consistently and that its roles, accountabilities, reporting relationships, and escalation mechanisms function as intended. This responsibility supports effective governance by providing the governing body with reliable assurance that risks are being managed within the organization's framework and risk appetite. The IIA's model emphasizes that management's role is not merely to design a framework, but to direct resources and activities so that risk management and control responsibilities are carried out. See the IIA's Three Lines Model and its Global Internal Audit Standards for the governance, management, risk, and control context.

QUESTION NO: 43

Which of the following is a logical access control designed to enhance the security of a computer-based application system?

A. User accounts will be locked alter three unsuccessful attempts to access the system

B. Users will not be allowed to use any of their last five passwords to access the system

C. Users will be assigned rights to access the system based on their job responsibilities

D. Users will automatically lose access to the system after 15 minutes of inactivity

ANSWER: C

Explanation:

Users will be assigned rights to access the system based on their job responsibilities is the best answer because it describes role-based access control (RBAC), a core logical access control for application systems. RBAC grants permissions according to defined organizational roles, so a user receives access needed to perform assigned duties rather than broad or individually improvised permissions. This implements the principles of least privilege and need to know, limits opportunities for unauthorized transactions or data viewing, and supports segregation of duties by ensuring that incompatible responsibilities can be assigned to separate roles. Effective RBAC also makes access administration and periodic access reviews more manageable: management can evaluate whether each role's permissions remain appropriate and whether users still need their assigned role as duties change. NIST identifies RBAC as a means of regulating access based on users' roles within an organization and associates it with centrally administered role and permission relationships. This type of authorization directly controls what authenticated users may do within the application, making it a fundamental logical control for protecting application resources. See NIST's Role Based Access Control project and NIST's RBAC models publication.

QUESTION NO: 44

Which of the following are appropriate functions for an IT steering committee?

1) Assess the technical adequacy of standards for systems design and programming.

2) Continually monitor of the adequacy and accuracy of software and hardware in use.

3) Assess the effects of new technology on the organization`s IT operations.

4) Provide broad oversight of implementation, training, and operation of new systems.

A. 1, 2, and 3

B. 1, 2, and 4

C. 1, 3, and 4

D. 2, 3, and 4

ANSWER: D

Explanation:

2, 3, and 4 is correct because an IT steering committee provides governance-level direction and oversight for technology use across the organization. Its remit includes monitoring whether the organization's technology resources remain suitable and reliable for business needs, considering the operational implications, risks, and opportunities introduced by emerging technologies, and maintaining broad oversight as significant systems are implemented and placed into operation. This oversight helps ensure that technology investments, system deployment, user preparation, and ongoing use support organizational strategy and are subject to appropriate governance.

An effective steering committee operates as a cross-functional management forum. It considers priorities, resources, business impacts, major technology risks, and the status of important initiatives. Monitoring the adequacy of technology in use does not require the committee to perform detailed technical testing; rather, it reviews management information, performance indicators, risk reporting, and major issues to determine whether action or escalation is needed. Similarly, its oversight of implementation, training, and operation is broad and strategic, focused on accountability and successful business adoption. The IIA's IT governance guidance discusses governance bodies' responsibilities for aligning IT with organizational objectives and overseeing IT-related value, risk, and performance. See The IIA Global Technology Audit Guides and ISACA COBIT resources.

QUESTION NO: 45

Which of the following is an example of an application system control?

A. Data values fall within a prescribed range.

B. Error listings are generated and promptly remediated.

C. Report distribution is restricted to authorized personnel.

D. Field amounts contain an upper or lower limit.

ANSWER: A

Explanation:

"Data values fall within a prescribed range" is an application system control because it describes an automated input-validation control, commonly called a range check. The application compares an entered value with defined minimum and maximum parameters and accepts, rejects, or flags the value according to those rules. For example, a payroll application can prevent an employee's recorded hours from exceeding a reasonable maximum, or an expense application can flag an amount outside the organization's approved threshold. This control helps preserve the accuracy, completeness, and validity of data before it is used in downstream processing, reporting, or decision-making. Application controls are embedded in, or configured within, a specific business application and are designed to ensure that transactions are processed according to defined business rules. Range validation directly supports that purpose by reducing the risk that erroneous, malformed, or unreasonable data will enter the system. NIST identifies input validation as a key software-security and integrity practice, including checking that input conforms to expected constraints. See NIST SP 800-53, Revision 5 and the OWASP Input Validation guidance.

QUESTION NO: 46

Which of the following activities most significantly increases the risk that a bank will make poor-quality loans to its customers?

A. Borrowers may not sign all required mortgage loan documentation.

B. Fees paid by the borrower at the time of the loan may not be deposited in a timely manner.

C. The bank's loan documentation may not meet the government's disclosure requirements.

D. Loan officers may override the lending criteria established by senior management.

ANSWER: D

Explanation:

Loan officers may override the lending criteria established by senior management most directly increases the risk of poor-quality lending because it permits credit decisions outside the bank's approved risk appetite and underwriting framework. Lending criteria typically establish minimum standards for assessing a borrower's capacity to repay, credit history, collateral, debt levels, and other risk characteristics. When individual officers can bypass these standards without robust, independent approval and documented justification, loans may be originated to borrowers who do not meet the institution's accepted credit-quality threshold. This creates the potential for elevated delinquency, default, loss provisions, and concentrations of unrecognized credit risk. Sound bank governance therefore requires clear credit policies, appropriate delegation of lending authority, segregation between loan origination and independent credit risk review, and effective monitoring of policy exceptions. The Basel Committee's credit-risk principles emphasize that banks should operate under sound, well-defined credit-granting criteria and establish clear processes for approving, amending, renewing, and refinancing credits. The Office of the Comptroller of the Currency likewise describes loan underwriting standards as a fundamental control for safe and sound lending. Basel Committee: Principles for the Management of Credit Risk; OCC Comptroller's Handbook: Credit Underwriting.

QUESTION NO: 47

An internal auditor is evaluating an organization's business continuity management program According to the guidance on IT. which of the following tests would best demonstrate the ability to perform Key processes without significant problems?

A. End-to-end testing

B. IT systems and application walkthrough

C. Tabletop or boardroom-style testing

D. Desk check testing

ANSWER: A

Explanation:

End-to-end testing is the best method to demonstrate that key business processes can actually be performed without significant problems during a disruption. This type of exercise validates the complete process flow, including the people, facilities, technology, applications, data, communications, third-party dependencies, and handoffs required to deliver a critical product or service. Rather than merely confirming that plans exist or that participants understand their roles, it provides practical evidence that the organization can execute recovery procedures and operate priority processes through to their intended outcomes. For an internal auditor, the results can reveal operational bottlenecks, unmet recovery requirements, interface failures, incomplete procedures, and resource constraints that may not be apparent in less comprehensive exercises. A well-designed end-to-end test should use realistic disruption assumptions, define measurable success criteria, document exceptions, and require management to track remediation of issues identified. This aligns with the expectation that business continuity arrangements be exercised and validated at appropriate intervals, with lessons learned incorporated into continual improvement. The NIST contingency-planning guidance describes testing and exercises as essential for validating contingency capabilities and identifying plan weaknesses; see NIST SP 800-34 Rev. 1. Additional business-continuity good practice is available from the ISO 22301 standard overview.

QUESTION NO: 48

Which of the following statements is true regarding reversing entries in an accounting cycled

A. Reversing all previous closing adjustments is a mandatory step in the accounting cycle

B. Reversing entries should be completed at the end of the next accounting period after recording regular transactions of the period

C. Reversing entries are identical to the adjusting entries made in the previous period.

D. Reversing entries are the exact opposite of the adjustments made in the previous period.

ANSWER: D

Explanation:

Reversing entries are the exact opposite of the adjustments made in the previous period. A reversing entry is an optional journal entry recorded at the beginning of a new accounting period to reverse a selected adjusting entry from the end of the preceding period. It uses the same accounts and amounts as the prior adjustment, but switches the debit and credit treatment. For example, if an accrued expense adjustment debited an expense and credited a payable at year-end, the reversing entry debits the payable and credits the expense on the first day of the next period. This approach simplifies recording subsequent routine cash transactions because the normal transaction can be entered without separately identifying the portion related to the prior-period accrual. Reversals are commonly used for accrued revenues, accrued expenses, and certain deferred items when the original transaction will be recorded in the following period. They are not required for every adjusting or closing entry; rather, an organization uses them when they improve processing efficiency and help prevent duplicate recognition. The accounting-cycle context and the purpose of adjusting entries are described in OpenStax's discussion of the adjusting process, while the mechanics of reversing entries are illustrated by LibreTexts' reversing entries guidance.

QUESTION NO: 49

Which of the following application software features is the least effective control to protect passwords?

A. Suspension of user IDs after a user's repeated attempts to sign on with an invalid password.

B. Encryption of passwords prior to their transmission or storage.

C. Forced change of passwords after a designated number of days.

D. Automatic logoff of inactive users after a specified time period of inactivity.

ANSWER: C

Explanation:

Forced change of passwords after a designated number of days is the least effective control because routine, time-based password expiration does not directly prevent password disclosure, interception, replay, or automated guessing. When users must change passwords on an arbitrary schedule, they commonly select predictable variations of prior passwords or weaker passwords that are easier to remember. This behavior can reduce the practical strength of the authentication control rather than improve it. Current password-management guidance favors requiring sufficiently long passwords, screening new passwords against known-compromised or commonly used values, protecting passwords in transit and storage, and requiring a password change when there is evidence of compromise. NIST specifically states that verifiers should not require periodic password changes; instead, changes should be required when compromise is known or suspected. In an internal-audit assessment, the control objective is therefore better met by risk-based credential management and strong technical protections than by an expiration interval alone. See NIST SP 800-63B, Digital Identity Guidelines and CISA guidance on implementing phishing-resistant MFA.

QUESTION NO: 50

Which of the following factors is considered a disadvantage of vertical integration?

A. It may reduce the flexibility to change partners.

B. It may not reduce the bargaining power of suppliers.

C. It may limit the organization's ability to differentiate the product.

D. It may lead to limited control of proprietary knowledge.

ANSWER: A

Explanation:

It may reduce the flexibility to change partners. is correct because vertical integration brings activities that were previously performed by external suppliers, distributors, or other business partners under the organization's ownership or direct control. Although this can improve coordination and reduce dependence on outside parties, it also creates commitment to the acquired or internally developed capability. The organization may have invested substantial capital in facilities, technology, personnel, contracts, and operating processes. Consequently, changing to a different supplier, distributor, technology platform, or channel can become more difficult and costly than it would be when the activity is outsourced or purchased through arm's-length market relationships.

This reduced flexibility is a significant strategic consideration. Market conditions, customer preferences, input prices, and technology can change quickly. A vertically integrated organization may be less able to respond by replacing a partner or switching sources, because it must first address the costs and operational consequences associated with its own integrated operations. Strategic-management guidance recognizes that vertical integration can increase control over stages of the value chain while also increasing investment, organizational complexity, and exposure to the risks of those stages. For background on vertical integration and its strategic role, see Encyclopaedia Britannica's overview of vertical integration and OpenStax's strategic-analysis discussion.

QUESTION NO: 51

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, a multinational organization fills important foreign-unit positions primarily with parent-country nationals. Sending expatriate employees abroad commonly increases total staffing cost because the organization may need to provide relocation support, housing, tax equalization, travel, hardship allowances, and expatriate training in addition to normal compensation. This approach can also create resentment among host-country employees when they perceive that senior roles and advancement opportunities are reserved for personnel from headquarters rather than being available based on local capability. Further, reliance on parent-country assumptions, leadership practices, and decision-making norms can cause cultural myopia: management may insufficiently recognize or adapt to host-country values, market expectations, and business practices. Parent-country nationals, by contrast, generally gain international assignment and development opportunities under this approach, rather than having their career mobility limited. These people-related and cultural effects are material considerations for internal auditors evaluating global talent, governance, operating-model, and human-capital risks. See OpenStax, International Management and SHRM, Managing a Global Workforce.

QUESTION NO: 52

Which of the following best describes the concept of relevant cost?

A. A future cost that is the same among alternatives.

B. A future cost that differs among alternatives.

C. A past cost that is the same among alternatives.

D. A past cost that differs among alternatives.

ANSWER: B

Explanation:

A future cost that differs among alternatives is the correct description of a relevant cost. In managerial decision-making, a cost is relevant only when it will occur in the future and its amount changes depending on which available course of action the organization selects. Because the cost differs across alternatives, it affects the incremental financial consequence of the decision and should be included in the analysis. This concept helps management and internal auditors focus attention on decision-useful information, such as additional materials, labor, capacity-related costs, or avoidable expenditures associated with a particular alternative. Relevant-cost analysis is forward-looking: the decision cannot alter costs already incurred, whereas future differential amounts can be influenced by the choice made. The Institute of Management Accountants describes relevant information for decisions as information involving future costs and revenues that differ between alternatives. This approach supports sound evaluations of choices such as outsourcing versus performing work internally, accepting a special order, replacing equipment, or discontinuing an activity. For further discussion of cost behavior and decision-relevant cost concepts, see the IMA Statements on Management Accounting and the OpenStax managerial accounting materials.

QUESTION NO: 53

Which of the following actions would senior management need to consider as pan of new IT guidelines regarding the organization's cybersecurity policies?

A. Assigning new roles and responsibilities for senior IT management.

B. Growing use of bring your own devices tor organizational matters

C. Expansion of operations into new markets with united IT access

D. Hiring new personnel within the IT department tor security purposes

ANSWER: B

Explanation:

Growing use of bring your own devices tor organizational matters is the appropriate consideration because personally owned smartphones, tablets, and computers accessing organizational data extend the organization’s security boundary beyond devices that it directly procures and configures. Senior management should ensure that cybersecurity policy addresses the governance and risk appetite for personally owned devices, including authorization to connect, device inventory and management, strong authentication, encryption, secure configuration, timely patching, separation or protection of organizational information, monitoring, incident reporting, and secure removal of organizational data when access ends. These requirements should be applied consistently with privacy, legal, and records-management obligations. A growing personally owned-device environment can materially alter the organization’s threat exposure and therefore warrants explicit treatment when cybersecurity guidelines are established or updated. NIST’s guidance on managing enterprise mobile devices emphasizes centrally defined security requirements and lifecycle controls for devices that access enterprise resources. The IIA also describes cybersecurity as a governance issue in which management establishes appropriate risk-management processes and controls. See NIST SP 800-124 Rev. 2, Guidelines for Managing the Security of Mobile Devices and The IIA GTAG: Assessing Cybersecurity Risk.

QUESTION NO: 54

Which of the following statements is true regarding user-developed applications (UDAs)?

A. UDAs are less flexible and more difficult to configure than traditional IT applications.

B. Updating UDAs may lead to various errors resulting from changes or corrections.

C. UDAs typically are subjected to application development and change management controls.

D. Using UDAs typically enhances the organization's ability to comply with regulatory factors.

ANSWER: B

Explanation:

Updating UDAs may lead to various errors resulting from changes or corrections. UDAs, such as spreadsheets, databases, and small workflow tools created by business users, are often changed quickly to meet operational needs. This flexibility is useful, but it also means that a seemingly minor update can alter formulas, logic, links, data ranges, access settings, or embedded macros. If the change is not independently reviewed, tested with representative data, documented, and appropriately approved, it can introduce errors that affect the completeness, accuracy, or reliability of information used in business decisions and financial or regulatory reporting.

The relevant risk is heightened because UDAs may be maintained outside formal IT development processes and can depend heavily on a particular individual’s knowledge. Effective governance therefore applies controls proportionate to the UDA’s risk and criticality, including an inventory, identified ownership, controlled access, version management, backup and recovery arrangements, testing, and documented review of significant changes. Internal audit should assess whether management has identified critical UDAs and implemented controls that make changes traceable and reliable. The IIA’s guidance on this topic is available in GTAG 14: Auditing User-developed Applications. Additional IIA technology guidance is available through the IIA Global Guidance library.