Topic 1, Exam Pool A

Question: 1

An IT balanced scorecard is the MOST effective means of monitoring:
A. governance of enterprise IT.
B. control effectiveness.
C. return on investment (ROI).
D. change management effectiveness.

Answer: A

Explanation:

An IT balanced scorecard is a strategic management tool that aligns IT objectives with business goals and measures the performance of IT processes using key performance indicators (KPIs). It is the most effective means of monitoring governance of enterprise IT, which is the process of ensuring that IT supports the organization’s strategy and objectives. Governance of enterprise IT covers aspects such as IT value delivery, IT risk management, IT resource management, and IT performance measurement. An IT balanced scorecard can help monitor these aspects and provide feedback to improve IT governance. Reference: ISACA Frameworks: Blueprints for Success, CISA Review Manual (Digital Version)

Question: 2

When reviewing an organization's information security policies, an IS auditor should verify that the policies have been defined PRIMARILY on the basis of:
A. a risk management process.
B. an information security framework.
C. past information security incidents.
D. industry best practices.

Answer: A

Explanation:

Information security policies are high-level statements that define the organization's approach to protecting its information assets from threats and risks. They should be based primarily on a risk management process, which is a systematic method of identifying, analyzing, evaluating, treating, and monitoring information security risks. A risk management process can help ensure that the policies are aligned with the organization's risk appetite, business objectives, legal and regulatory requirements, and stakeholder expectations. An information security framework is a set of standards, guidelines, and best practices that provide a structure for implementing information security policies. It can support the risk management process, but it is not the primary basis for defining the policies. Past information security incidents and industry best practices can also provide valuable inputs for defining the policies, but they are not sufficient to address the organization's specific context and needs. Reference: Insights and Expertise, CISA Review Manual (Digital Version)

Question: 3

Which of the following would be an IS auditor's GREATEST concern when reviewing the early stages of a software development project?

A. The lack of technical documentation to support the program code

B. The lack of completion of all requirements at the end of each sprint

C. The lack of acceptance criteria behind user requirements.

D. The lack of a detailed unit and system test plan

Answer: C

Explanation:

User requirements are statements that describe what the users expect from the software system in terms of functionality, quality, and usability. They are essential inputs for the software development process, as they guide the design, implementation, testing, and deployment of the system. Therefore, an IS auditor's greatest concern when reviewing the early stages of a software development project would be the lack of acceptance criteria behind user requirements. Acceptance criteria are measurable conditions that define when a user requirement is met or satisfied. They help ensure that the user requirements are clear, complete, consistent, testable, and verifiable. Without acceptance criteria, it would be difficult to evaluate whether the system meets the user expectations and delivers value to the organization. Technical documentation, such as program code, is usually produced in later stages of the software development process. Completion of all requirements at the end of each sprint is not mandatory in agile software development methods, as long as there is a prioritized backlog of requirements that can be delivered incrementally. A detailed unit and system test plan is also important for ensuring software quality, but it depends on well-defined user requirements andacceptance criteria. Reference: Information Systems

Acquisition, Development & Implementation, CISA ReviewManual (Digital Version)

Question: 4

Which of the following is the BEST data integrity check?
A. Counting the transactions processed per day
B. Performing a sequence check
C. Tracing data back to the point of origin
D. Preparing and running test data

Answer: C

Explanation:

Data integrity is the property that ensures that data is accurate, complete, consistent, and reliable throughout its lifecycle. The best data integrity check is tracing data back to the point of origin, which is the source where the data was originally created or captured. This check can verify that data has not been altered or corrupted during transmission, processing, or storage. It can also identify any errors or discrepancies in data entry or conversion. Counting the transactions processed per day is a performance measure that does not directly assess data integrity. Performing a sequence check is a validity check that ensures that data follows a predefined order or pattern. It can detect missing or out-of-order data elements, but it cannot verify their accuracy or completeness. Preparing and running test data is a testing technique that simulates real data to evaluate how a system handles different scenarios. It can help identify errors or bugs in the system logic or functionality, but it cannot ensure data integrity in production environments. Reference: Information Systems Operations and Business Resilience, CISA Review Manual (Digital Version)

Question: 5

Spreadsheets are used to calculate project cost estimates. Totals for each cost category are then keyed into the job-costing system. What is the BEST control to ensure that data is accurately entered into the system?
A. Reconciliation of total amounts by project
B. Validity checks, preventing entry of character data
C. Reasonableness checks for each cost type
D. Display the back of the project detail after the entry

Answer: A

Explanation:

Reconciliation of total amounts by project is the best control to ensure that data is accurately entered into the job-costing system from spreadsheets. Reconciliation is a process of comparing two sets of data to identify any differences or discrepancies between them. By reconciling the total amounts by project from spreadsheets with those from the job-costing system, any errors or omissions in data entry can be detected and corrected. Validity checks are controls that verify that data conforms to predefined formats or ranges. They can prevent entry of character data into numeric fields, but they cannot ensure that the numeric data is correct or complete. Reasonableness checks are controls that verify that data is within expected or acceptable limits. They can detect outliers or anomalies in data, but they cannot ensure that the data matches the source. Display back of project detail after entry is a control that allows the user to review and confirm the data entered into the system. It can help reduce human errors, but it cannot guarantee that the data is accurate or consistent with the source. Reference: Information Systems Operations and Business Resilience, CISA Review Manual (Digital Version)