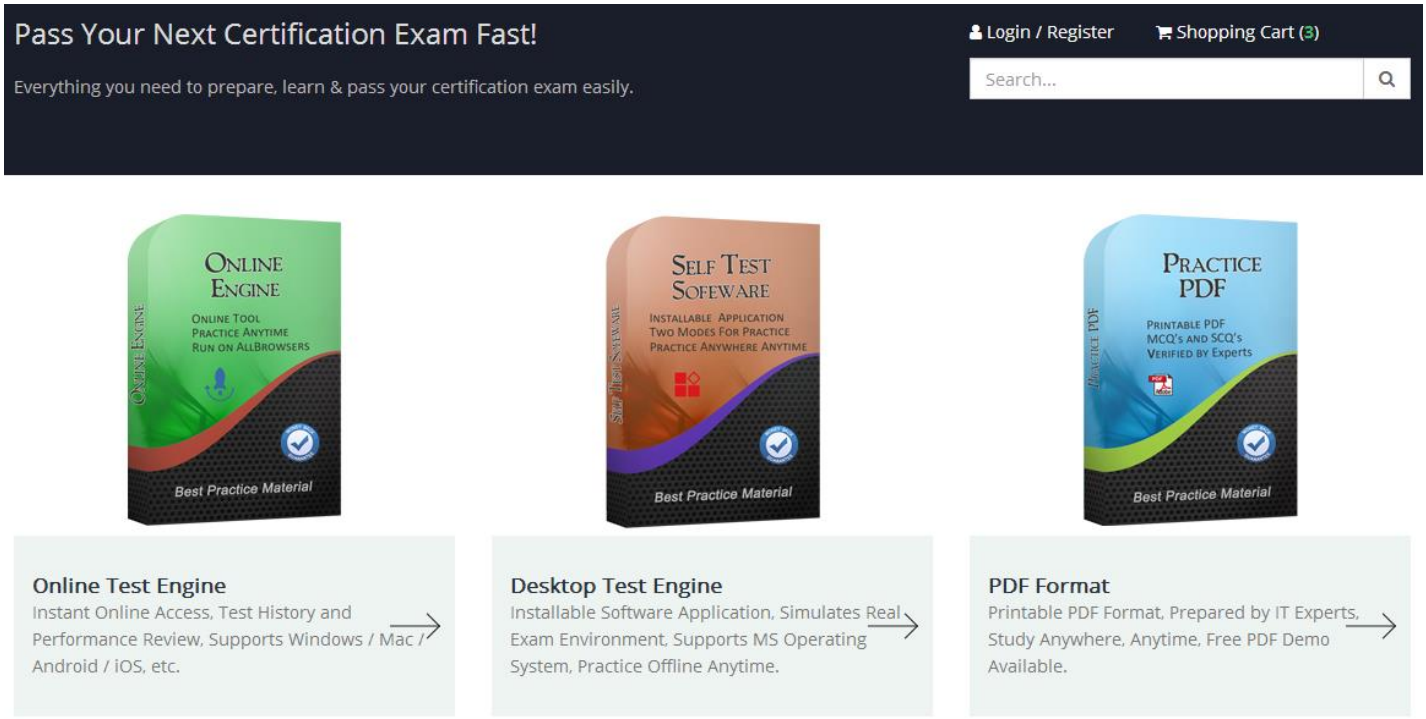
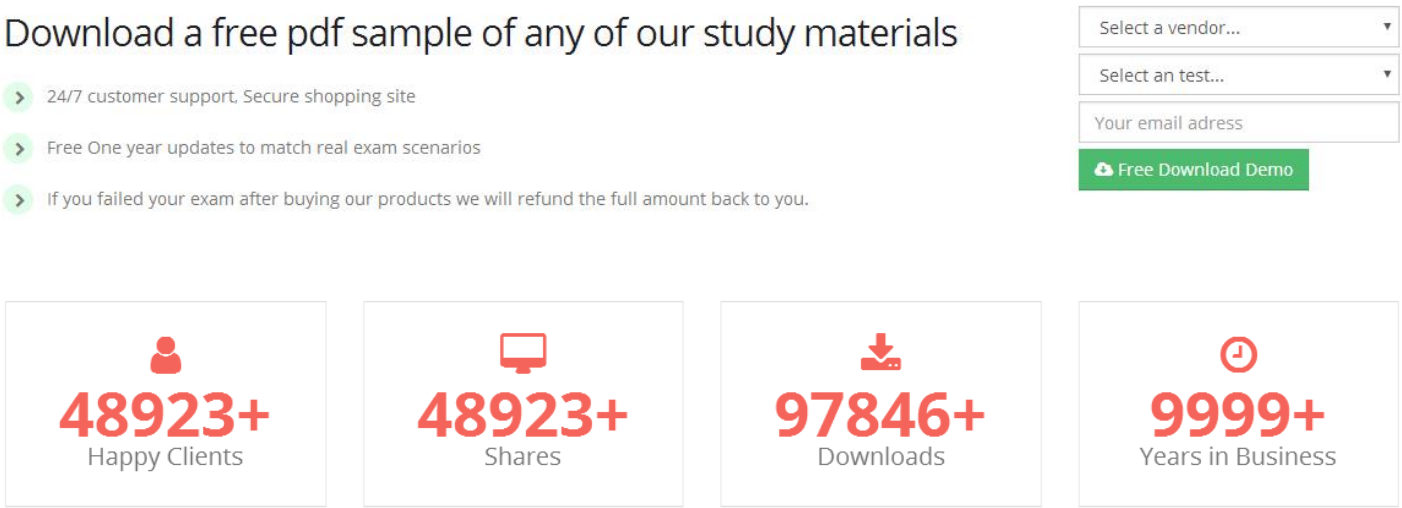
ExamcollectionPass





http://www.examcollectionpass.com/

Everything you need to prepare, learn & pass your certification exam easily.

Exam : **CISA-Deutsch**

Title : Certified Information Systems Auditor (CISA Deutsch Version)

Vendor : ISACA

Version : DEMO

QUESTION NO: 1
Eine Bank hat geringfügige Änderungen am Computerprogramm zur Zinsberechnung vorgenommen. Welche der folgenden Methoden liefert den stärksten Beweis dafür, ob die Zinsberechnungen korrekt sind?
A. Überprüfung des Quellcodes
B. Parallele Simulation mit Audit-Software
C. Manuelle Überprüfung einer Stichprobe der Ergebnisse
D. Überprüfung der Ergebnisse der Qualitätssicherungsprüfung (QS).
Answer: B
Explanation:
Parallel simulation involves running the same data through two systems and comparing the results1. In this case, the bank's data would be processed using both the modified interest calculation program and an audit software. The results from both systems would then be compared to check for discrepancies1. This technique provides strong evidence of the correctness of interest calculations as it directly tests the program's output against a known and trusted output1. While source code review23, manual verification of a sample of results4567, and review of QA test results8910 can also provide valuable insights, they do not offer the same level of direct, comparative evidence as parallel simulation1.
References:
Parallel simulation in IT testing - Universal CPA Review
5 code review best practices - Work Life by Atlassian
How to Make Good Code Reviews Better - Stack Overflow
Guidelines for the validation and verification of quantitative and qualitative test methods - Mathematics LibreTexts Method Validation and Verification - University of Utah Sample Procedure for Method Validation - NIST Method validation and verification - CFS Goo d Practices for Quality Assurance Reviewers: Assessing Evidence of Supervisory Review - IGNET How do quality assurance engineers test calculations? - Software Quality Assurance and Testing Stack Exchange Quality Assurance/Quality Control (QA/QC) Plan and Procedures - UNFCCC

QUESTION NO: 2
Welche der folgenden Methoden liefert die zuverlässigsten Prüfungsnachweise?
A. Anfrage
B. Bestätigung des Managements
C. Wiederholung der Kontrollen
D. Beobachtung
Answer: C
Explanation:
The best answer is C. Re-performance of controls.
Under ISACA audit principles, evidence obtained directly by the auditor is generally more reliable than evidence provided by management or gathered indirectly. Re-performance allows the auditor to independently execute the control or procedure and verify whether it works as intended, making it stronger than inquiry, observation, or management attestation. Option A is the least reliable because inquiry depends on what people say. Option B is

stronger than simple inquiry but still relies on management representation. Option D can be useful, but observation only shows what happened at a point in time and may not prove consistent operation. Re-performance gives the auditor the highest level of assurance because the evidence is generated through the auditor's own independent work.
References (Official ISACA):
ISACA, Follow-Up Audits and Follow-Up Process: The Auditor's Impact Litmus Tool ISACA, The Top-Five Audit Essentials for Driving Efficiency and Value

QUESTION NO: 3
Ein neues Systementwicklungsprojekt hinkt einem kritischen Implementierungstermin hinterher. Welche der folgenden Aktivitäten ist die wichtigste?
A. Dokumentieren Sie die Verbesserungen in letzter Minute
B. Führen Sie ein Vorimplementierungsaudit durch.
C. Benutzerakzeptanztests (UAT) durchführen
D. Stellen Sie sicher, dass der Code überprüft wurde.
Answer: A
Explanation:
Performing user acceptance testing (UAT) is the most important activity before implementing a new system, as it ensures that the system meets the user requirements and expectations, and that it is free of major defects. Documenting last-minute enhancements, performing a pre-implementation audit, and ensuring that code has been reviewed are also important activities, but they arenot as critical as UAT. References: CISA Review Manual (Digital Version), Chapter 4, Section 4.2.2

QUESTION NO: 4
Welcher der folgenden Aspekte ist beim Patchen geschäftskritischer Anwendungsserver gegen bekannte Sicherheitslücken am wichtigsten?
A. Patches werden in einer Testumgebung implementiert, bevor sie in die Produktionsumgebung eingeführt werden.
B. Netzwerk-Schwachstellenscans werden nach der Implementierung von Patches durchgeführt.
C. Schwachstellenanalysen werden regelmäßig nach festgelegten Zeitplänen durchgeführt.
D. Rollen und Verantwortlichkeiten für die Implementierung von Patches werden definiert
Answer: A
Explanation:
The most important consideration for patching mission critical business application servers against known vulnerabilities is A. Patches are implemented in a test environment prior to rollout into production. This is because patching mission critical business application servers involves a high level of risk and complexity, and requires careful planning and testing before applying the patches to the live environment. Patches may introduce new bugs, errors, or conflicts that could affect the functionality, performance, or security of the application servers, and cause system downtime, data loss, or business disruption1. Therefore, it is essential to implement patches in atest environment first, where the patches can be verified and validated for their effectiveness and compatibility, and any issues or defects can be identified and resolved before they impact the production environment2.

QUESTION NO: 5
Bei der forensischen Untersuchung eines Cyberangriffs mit Bezug auf Kreditkartendaten ist Folgendes am wichtigsten sicherzustellen:
A. Angemessene Kartensicherheitsfunktionen sind aktiviert.
B. Die Zahlungsplattformen des Unternehmens sind blockiert.
C. Die ordnungsgemäße Nachweiskette wird aufrechterhalten.
D. Alle Mitarbeiter der Zahlungskartenabteilung werden befragt.
Answer: C
Explanation:
In forensic investigations,maintaining a proper chain of custodyiscriticalto ensuring that evidence is admissible in court and has not been altered.
Option A (Incorrect):Activatingsecurity features(e.g., encryption or tokenization) is apreventive measurebut does not aid in investigating the attack.
Option B (Incorrect):Blocking payment platforms may be necessary fordamage control, but it does not ensure a properinvestigation.
Option C (Correct):Thechain of custodyensures thatevidence remains intact, can betraced, and islegally validfor prosecution. This is the most critical aspect of forensic investigations.
Option D (Incorrect):Interviewing staff may provide insights, but without properevidence handling, the investigation's integrity is at risk.
Reference:ISACA CISA Review Manual -Domain 5: Protection of Information Assets-Coversforensic investigations, evidence handling, and legal compliance.

QUESTION NO: 6
Welche der folgenden Maßnahmen würde das Risiko der Nichtverfügbarkeit der Anwendungsprogrammierschnittstelle (API) am besten reduzieren?
A. Einrichtung dedizierter Server für eingehende API-Anfragen
B. Implementierung eines kontinuierlichen Integrations- und Bereitstellungsprozesses
C. Durchführung regelmäßiger Belastungstests
D. Begrenzung der Anzahl eingehender Anfragen
Answer: D
Explanation:
Limiting the rate of incoming requests, known as rate limiting, helps prevent API overloading by controlling the number of requests a client can make within a specific timeframe. This measure protects the API from being overwhelmed, ensuring better availability and performance. While dedicated servers, continuous integration/deployment, and stress testing contribute to overall system robustness, rate limiting directly addresses the risk of unavailability due to excessive or malicious traffic.
References:
ISACA CISA Review Manual, 28th Edition, Chapter 4: Information Systems Operations and Business Resilience.

QUESTION NO: 7
Ein IT-Auditor kann die Auswirkungen von Systemausfällen auf das Geschäft am besten wie folgt beurteilen:

A. Bewertung der Nutzerzufriedenheit.
B. Befragung des Sicherheitsadministrators.
C. Analyse von Wartungsprotokollen der Ausrüstung.
D. Überprüfung der vom System generierten Protokolle.
Answer: C

QUESTION NO: 8
Im Rahmen der Reaktion auf eine Prüfung äußert der Geprüfte Bedenken hinsichtlich der Empfehlungen und zögert, diese umzusetzen. Welche der folgenden Vorgehensweisen ist für den IT-Prüfer die beste?
A. Die Antwort des Auditierten akzeptieren und zusätzliche Tests durchführen.
B. Schlagen Sie vor, einen externen Berater mit der Durchführung einer Ist-Analyse zu beauftragen.
C. Führen Sie weitere Gespräche mit dem Auditierten, um einen Risikominderungsplan zu entwickeln.
D. Einen Abschlussbericht erstellen, ohne die Stellungnahme des Geprüften aufzunehmen.
Answer: C
Explanation:
Collaborative discussions help address the auditee ' s concerns, find mutually agreeable solutions, and create buy-in for implementing improvements.
References
ISACA CISA Review Manual (Current Edition) - Chapters on audit reporting and communication Auditing Standards - Emphasize the importance of understanding and addressing auditee concerns.

QUESTION NO: 9
Welche der folgenden Optionen ermöglicht am besten einen Nutzenrealisierungsprozess für ein Systementwicklungsprojekt?
A. Die Kennzahlen für das Projekt wurden vor Projektbeginn ausgewählt.
B. Das Projektbudget umfasst die Kosten für die Durchführung des Projekts sowie die mit der Lösung verbundenen Kosten.
C. Die Schätzungen des geschäftlichen Nutzens basieren auf ähnlichen, bereits abgeschlossenen Projekten.
D. Die Kennzahlen werden unmittelbar nach der Implementierung des Projekts ausgewertet.
Answer: A
Explanation:
A benefits realization process is a systematic way of identifying, defining, planning, tracking and realizing the benefits from a project or program. Benefits are the measurable improvements that result from the delivery of project outputs and outcomes. Benefits realization management (BRM) is the practice of ensuring that benefits are derived from outputs and outcomes.
One of the best practices for BRM is to select metrics for the project before it begins. Metrics are the indicators that measure the performance and value of the project and its benefits. By selecting metrics in advance, the project team can align the project objectives with the

expected benefits, establish a baseline for comparison, and monitor and evaluate the progress and results of the project. Metrics also help to communicate the value of the project to stakeholders and justify the investment.
The other options are not as effective as selecting metrics before the project begins. Project budget is an important factor for BRM, but it does not enable the benefits realization process by itself. It only reflects the costs of executing the project and delivering the solution, not the benefits or value that are expected from them. Estimates of business benefits are useful for planning and forecasting, but they are not sufficient for BRM. They need to be validated by actual data and evidence from similar projects or other sources. Metrics are evaluated after the project has been implemented, but this is only one part of the benefits realization process. BRM requires continuous monitoring and evaluation throughout the project life cycle and beyond, to ensure that benefits are sustained and optimized.
References:
ISACA, CISA Review Manual, 27th Edition, 2019, p. 3261
PMI, Benefits Realization Management: A Practice Guide, 20192
APM, What is benefits management and project success?, 20213

QUESTION NO: 10
Ein IT-Prüfer entdeckt eine schwerwiegende Sicherheitslücke in einem öffentlich zugänglichen Webserver, der zur Abwicklung von Online-Kundenzahlungen verwendet wird. Der IT-Prüfer sollte ZUERST

A. Die Ausnahme in einem Prüfbericht dokumentieren.

B. Sicherheitsvorfallberichte prüfen.

C. kompensierende Kontrollmechanismen identifizieren.

D. Benachrichtige den Prüfungsausschuss.

Answer: C
Explanation:
The first action that an IS auditor should take when finding a high-risk vulnerability in a public-facing web server used to process online customer payments is to identify compensating controls. Compensating controls are alternative or additional controls that provide reasonable assurance of mitigating the risk of exploiting the vulnerability. The IS auditor should assess the effectiveness of the compensating controls and determine whether they reduce the risk to an acceptable level. If not, the IS auditor should recommend remediation actions to address the vulnerability. Documenting the exception in an audit report is an important action, but it should not be the first action, as it does not address the urgency of the situation. Reviewing security incident reports is a useful action, but it should not be the first action, as it does not provide assurance of preventing future incidents. Notifying the audit committee is a necessary action, but it should not be the first action, as it does not involve taking any corrective measures. References:
CISA Review Manual, 27th Edition, pages 295-2961
CISA Review Questions, Answers and Explanations Database, Question ID: 260

QUESTION NO: 11
Eine Firewall zwischen internen Netzwerksegmenten verbessert die Sicherheit und reduziert das Risiko durch:

A. Alle Pakete, die Netzwerksegmente durchlaufen, werden analysiert.
B. Überprüfung des gesamten Datenverkehrs zwischen Netzwerksegmenten und Anwendung von Sicherheitsrichtlinien
C. Überwachung und Berichterstattung über Sitzungen zwischen Netzwerkteilnehmern
D. Sicherstellen, dass auf allen verbundenen Systemen geeignete Sicherheitskontrollen aktiviert sind.
Answer: B
Explanation:
A firewall between internal network segments improves security and reduces risk by inspecting all traffic flowing between network segments and applying security policies. This will prevent unauthorized or malicious access, data leakage, or network attacks from compromising the network resources or data. Logging all packets passing through network segments may provide audit trails and evidence, but not prevent or mitigate security incidents. Monitoring and reporting on sessions between network participants may help to identify anomalous or suspicious activities, but not block or filter them. Ensuring all connecting systems have appropriate security controls enabled may enhance the overall network security posture, but not isolate or segregate different network segments.
References: Info Technology and Systems Resources | COBIT, Risk, Governance ... - ISACA, section "Book COBIT 2019 Design Guide: Designing an Information and Technology Governance Solution | Digital | English"

QUESTION NO: 12
Welche der folgenden Möglichkeiten ist die BESTE Methode, um sicherzustellen, dass Zahlungstransaktionsdaten nur den entsprechenden Benutzern zugänglich sind?
A. Implementierung der Zwei-Faktor-Authentifizierung
B. Beschränkung des Zugriffs auf Transaktionen mithilfe von Netzwerksicherheitssoftware
C. Implementierung rollenbasierter Zugriffskontrolle auf Anwendungsebene
D. Verwendung eines einzigen Menüs für sensible Anwendungstransaktionen
Answer: C
Explanation:
The best way to ensure payment transaction data is restricted to the appropriate users is implementing role- based access at the application level. Role-based access is a method of access control that assigns permissions or privileges to users based on their roles or functions within an organization or system. Role-based access can help ensure that payment transaction data is restricted to the appropriate users, by allowing only authorized users who have a legitimate need orpurpose to access or use the payment transaction data, and preventing unauthorized or unnecessary access or use by other users. Implementing two-factor authentication is a possible way to enhance the security and verification of user identities, but it is not the best way to ensure payment transaction data is restricted to the appropriate users, as it does not define what permissions or privileges users have on the payment transaction data. Restricting access to transactions using network security software is a possible way to protect the network communication and transmission of payment transaction data, but it is not the best way to ensure payment transaction data is restricted to the appropriate users, as it does not specify what actions or operations users can perform on

the payment transaction data.
Using a single menu for sensitive application transactions is a possible way to simplify the user interface and navigation of payment transaction data, but it is not the best way to ensure payment transaction data is restricted to the appropriate users, as it does not limit what users can access or use the payment transaction data.

QUESTION NO: 13
Welche der folgenden Empfehlungen eines IT-Auditors ist die BESTE, um eine Organisation vor Angriffen zu schützen, wenn ihr Dateiserver für externe Benutzer zugänglich sein muss?
A. Erzwingt eine sichere Tunnelverbindung.
B. Interne Firewalls verbessern.
C. Eine entmilitarisierte Zone (DMZ) einrichten.
D. Implementieren Sie ein sicheres Protokoll.
Answer: C
Explanation:
A demilitarized zone (DMZ) is a network segment that is separated from the internal network and the external network, such as the internet, by firewalls or other security devices. A DMZ provides an extra layer of security for the organization's internal network by isolating the servers and services that need to be accessible to external users, such as a file server, from the rest of the network. A DMZ also prevents external users from accessing the internal network directly, as they have to go through two firewalls to reach it. Therefore, setting up a DMZ is an IS auditor's best recommendation to protect anorganization from attacks when its file server needs to be accessible to external users12.
The other possible options are:
Enforce a secure tunnel connection: This means that the organization requires external users to establish a secure and encrypted connection, such as a virtual private network (VPN), to access its file server. This can provide some level of security and privacy for the data transmission, but it does not protect the file server or the internal network from attacks if the connection is compromised or if the external users are malicious. Therefore, enforcing asecuretunnel connection is not an IS auditor's best recommendation to protect an organization from attacks when its file server needs to be accessible to external users3.
Enhance internal firewalls: This means that the organization improves the security and performance of its internal firewalls, which are devices that filter and control the network traffic between different segments of the network. This can provide some level of protection for the internal network from unauthorized or malicious access, but it does not protect the file server or the external network from attacks if the file server is exposed to the internet or if the external network is compromised. Therefore, enhancing internal firewalls is not an IS auditor's best recommendation to protect an organization from attacks when its file server needs to be accessible to external users4.
Implement a secure protocol: This means that the organization uses a secure and standardized protocol, such as Secure File Transfer Protocol (SFTP) or Secure Shell (SSH), to transfer files between its file server and external users. This can provide some level of security and integrity for the data transmission, but it does not protect the file server or the internal network from attacks if the protocol is exploited or if the external users are malicious. Therefore, implementing a secure protocol is not an IS auditor's best recommendation to

protect an organization from attacks when its file server needs to be accessible to external users5. References: 1: What Is a DMZ Network and Why Would You Use It? | Fortinet 2: Demilitarised zone (DMZ) | Cyber.gov.au 3: What Is VPN Tunneling? | Fortinet 4: Firewall - Wikipedia 5: Secure Shell - Wikipedia

QUESTION NO: 14
Ein IT-Auditor untersucht einen kürzlich aufgetretenen Sicherheitsvorfall und stellt fest, dass die Reaktion auf den Vorfall unzureichend war.
Welche der folgenden Erkenntnisse ist als AM kritischsten einzustufen?
A. Die Sicherheitslücke, die den Angriff ermöglichte, wurde nicht identifiziert.
B. Der Angriff wurde nicht automatisch vom Intrusion Detection System (IDS) blockiert.
C. Der Angriff konnte nicht auf die Person zurückgeführt werden, die ihn ausgelöst hat.
D. Es wurde keine angemessene Antwortdokumentation geführt.
Answer: A
Explanation:
The most critical finding for an IS auditor following up on a recent security incident is that the security weakness facilitating the attack was not identified. This finding indicates that the root cause of the incident was not analyzed, and the vulnerability that allowed the attack to succeed was not remediated. This means that the organization is still exposed to the same or similar attacks in the future, and its security posture has not improved. Identifying and addressing the security weakness is a key step in the incident response process, as it helps to prevent recurrence, mitigate impact, and improve resilience.
The other findings are not as critical as the failure to identify the security weakness, but they are still important issues that should be addressed by the organization. The attack was not automatically blocked by the intrusion detection system (IDS) is a finding that suggests that the IDS was not configured properly, or that it did not have the latest signatures or rules to detect and prevent the attack. The attack could not be traced back to the originating person is a finding that implies that the organization did not have sufficient logging, monitoring, or forensic capabilities to identify and attribute the attacker. Appropriate response documentation was not maintained is a finding that indicates that the organization did not follow a consistent and formal incident response procedure, or that it did not document its actions, decisions, and lessons learned from the incident.
References:
ISACA CISA Review Manual 27th Edition (2019), page 254
Incident Response Process - ISACA1
Incident Response: How to Identify and Fix Security Weaknesses

QUESTION NO: 15
Welcher der folgenden Punkte sollte einem IS-Auditor bei der Bewertung des Patch-Management-Programms einer Organisation die größten Sorgen bereiten?
A. Patches werden von mehreren Bereitstellungsservern aus bereitgestellt.
B. Es gibt keinen Prozess, um das Netzwerk nach fehlenden Patches abzusuchen.
C. Patches für Schwachstellen mit mittlerem und niedrigem Risiko werden ausgelassen.
D. Es gibt keinen Prozess, um Server, die nicht gepatcht wurden, unter Quarantäne zu stellen.

Answer: B

QUESTION NO: 16
In welcher Phase des Softwareentwicklungszyklus ist es am besten, die Diskussion über Anwendungskontrollen zu beginnen?
A. Phase der Geschäftsentwicklung, in der die Stakeholder identifiziert werden
B. Die Funktionalitäten des Anwendungsdesignprozesses werden finalisiert.
C. Phase der Benutzerakzeptanztests (UAT), in der Testszenarien entworfen werden
D. Anwendungsentwicklungsphase, in der Algorithmen zur Lösung von Geschäftsproblemen entwickelt werden
Answer: B
Explanation:
The best phase of the software development life cycle to initiate the discussion of application controls is the application design phase when process functionalities are finalized. Application controls are the policies, procedures, and techniques that ensure the completeness, accuracy, validity, and authorization of data input, processing, output, and storage in an application. Application controls help prevent, detect, or correct errors and fraud in software applications. Examples of application controls include input validation, edit checks, reconciliation, encryption, access control, audit trails, etc.
The application design phase is when the software requirements are translated into a logical and physical design that specifies how the application will look and work. This phase is the best time to discuss application controls because it allows the developers to incorporate them into the design specifications and ensure that they are aligned with the business objectives and user needs. By discussing application controls early in the design phase, the developers can also avoid costly rework or changes later in the development process.
The other phases are not as optimal as the application design phase to initiate the discussion of application controls. A. Business case development phase when stakeholders are identified. The business case development phase is when the feasibility, scope, objectives, benefits, risks, and costs of a software project are defined and evaluated. This phase is important for obtaining stakeholder approval and support for the project, but it is too early to discuss application controls in detail because the software requirements and functionalities are not yet clear or finalized. B. User acceptance testing (UAT) phase when test scenarios are designed. The user acceptance testing phase is when the software is tested by the end-users or stakeholders to verify that it meets their expectations and requirements. This phase is too late to discuss application controls because it is near the end of the development process and any changes or additions to the application controls would require retesting and revalidation of the software. C. Application coding phase when algorithms are developed to solve business problems. The application coding phase is when the software design is translated into executable code using programming languages and tools. This phase is not ideal to discuss application controls because it is after the design phase and any changes or additions to the application controls would require redesigning and recoding of the software.
References:
ISACA, CISA Review Manual, 27th Edition, 2019, p. 2471
ISACA, CISA Review Questions, Answers and Explanations Database - 12 Month Subscription2 What Is Application Control? | McAfee3 What Is Application Lifecycle

Management? | Red Hat4

QUESTION NO: 17
Wenn ein IT-Auditor bestätigen muss, dass eine Organisation sensible Informationen auf Datenbankebene verschlüsselt, welche der folgenden Maßnahmen bietet die BESTE Gewissheit?
A. Überprüfung der Laufwerkseinstellungen des Hostservers
B. Überprüfung des Netzwerkverkehrs auf Klartextübertragungen
C. Überprüfung einer Stichprobe kritischer Felder
D. Überprüfung der Verschlüsselungsrichtlinie der Organisation
Answer: C
Explanation:
The best assurance is obtained by verifying a sample of critical fields. If the question is specifically about encryption at the database level, the auditor should test the actual data elements in the database that are expected to be encrypted. ISACA privacy and data-protection guidance discusses encryption of sensitive data fields as a protection mechanism, which supports validating field-level protection directly.
Option C is correct because it provides direct evidence that sensitive database fields are actually encrypted.
This is stronger than reviewing policies or peripheral settings because it tests the implemented control itself.
Option A is incorrect because drive settings usually relate to disk or full-volume encryption on the host server, not necessarily to database-level encryption of specific sensitive fields.
Option B is incorrect because checking network traffic for clear text transmissions only helps verify encryption in transit, not whether the data is encrypted within the database.
Option D is incorrect because a policy only states intent or requirement. It does not prove the database is actually encrypting sensitive fields.
Therefore, C is the best answer because direct verification of sensitive fields provides the strongest assurance that encryption is implemented at the database level.
References (Official ISACA):
ISACA Journal, Practical Data Security and Privacy for GDPR and CCPA - discusses encryption of sensitive client data fields.
ISACA Journal, Privacy-Preserving Analytics and Secure Multiparty Computation - discusses encryption of sensitive data fields throughout the data life cycle.
ISACA, Cloud Data Sovereignty: Governance and Risk Implications of Cross-Border Cloud Storage - distinguishes encryption at rest and in transit, supporting why network checks alone are insufficient for database-level assurance.

QUESTION NO: 18
Welches der folgenden Risiken ist am bedeutendsten, wenn eine Anwendung individuelle Endbenutzerkonten für den Zugriff auf die zugrunde liegende Datenbank verwendet?
A. Es werden mehrere Verbindungen zur Datenbank verwendet, was den Prozess verlangsamt.
B. Benutzerkonten können nach der Kündigung aktiv bleiben.
C. Benutzer können möglicherweise die Anwendungskontrollen umgehen.

D. Die Anwendung erfasst möglicherweise keinen vollständigen Prüfpfad.

Answer: C

Explanation:

The most significant risk when an application uses individual end-user accounts to access the underlying database is that users may be able to circumvent application controls. Application controls are the policies, procedures, and mechanisms that ensure the accuracy, completeness, validity, and authorization of transactions and data within an application. Application controls can include input validation, output verification, processing logic, reconciliation, exception handling, and audit trails. Application controls can help prevent or detect errors, fraud, or unauthorized access or modification of data.

However, if an application uses individual end-user accounts to access the underlying database, it means that the users have direct access to the database without going through the application layer. This can expose the database to potential risks such as:

Users may be able to bypass the application controls and manipulate the data in the database directly using SQL commands or other tools. For example, users may be able to change their own or others' salaries, grades, or balances without proper authorization or validation.

Users may be able to access or disclose sensitive or confidential data that they are not supposed to see or share. For example, users may be able to view other users' personal information, passwords, or credit card numbers.

Users may be able to introduce errors or inconsistencies in the data by entering invalid or incorrect data or by deleting or modifying existing data. For example, users may be able to create duplicate records, break referential integrity, or cause data loss or corruption.

Users may be able to compromise the security and performance of the database by creating unauthorized objects, granting excessive privileges, executing malicious code, or consuming excessive resources. For example, users may be able to create backdoors, viruses, or denial-of-service attacks.

Therefore, using individual end-user accounts to access the underlying database can pose a serious threat to the integrity, confidentiality, availability, and reliability of the data and the application.

The other options are not as significant as option C. Multiple connects to the database are used and slow the process is a performance issue that can affect the efficiency and responsiveness of the application and the database, but it does not necessarily compromise the data quality or security. User accounts may remain active after a termination is a security issue that can increase the risk of unauthorized access or misuse of data by former employees or others who have access to their credentials, but it can be mitigated by implementing proper account management and monitoring processes. Application may not capture a complete audit trail is a compliance issue that can affect the accountability and traceability of transactions and data within the application and the database, but it does not directly affect the data accuracy or protection.

References:

Should application users be database users? - Stack Overflow1

An Approach Toward Sarbanes-Oxley ITGC Risk Assessment - ISACA2

ISACA CISA Certified Information Systems Auditor Exam ... - PUPUWEB3

Why inactive accounts are a security risk | Stratosphere4

QUESTION NO: 19
Welches der folgenden Risiken sollte ein IT-Prüfer als das bedeutendste Risiko im Zusammenhang mit einem neuen Gesundheitsdatensystem betrachten, das ein Altsystem ersetzt?
A. Die Mitarbeiter wurden nicht in den Beschaffungsprozess einbezogen, was bei den Nutzern Widerstand gegen das neue System hervorrief.
B. Die Daten werden nicht korrekt konvertiert, was zu ungenauen Patientendatensätzen führt.
C. Das Implementierungsprojekt hat erhebliche Kostenüberschreitungen erfahren, die die Budgetprognosen überstiegen haben.
D. Das neue System hat Kapazitätsprobleme, was zu langsamen Reaktionszeiten für die Benutzer führt.
Answer: B
Explanation:
The most significant risk associated with a new health records system that replaces a legacy system is data not being converted correctly, resulting in inaccurate patient records. Data conversion is the process of transferring data from one format or system to another. Data conversion is a critical step in implementing a new health records system, as it ensures that the patient data are consistent, complete, accurate, and accessible in the new system. Data not being converted correctly may cause errors, discrepancies, or losses in patient records, which may have serious implications for patient safety, quality of care, legal compliance, and privacy protection. Staff not being involved in the procurement process, creating user resistance to the new system; the deployment project experiencing significant overruns, exceeding budget projections; and the new system having capacity issues, leading to slow response times for users are also risks associated with a new health records system implementation, but they are not as significant as data not being converted correctly.
References: [ISACA CISA Review Manual 27th Edition], page 281.

QUESTION NO: 20
Welches der folgenden Netzwerkkommunikationsprotokolle wird von Netzwerkgeräten wie Routern verwendet, um Fehlermeldungen und Betriebsinformationen zu senden, die den Erfolg oder Misserfolg der Kommunikation mit einer anderen IP-Adresse anzeigen?
A. Transmission Control Protocol/Internet Protocol (TCP/IP)
B. Internet Control Message Protocol
C. Mehrzweck-Transaktionsprotokoll
D. Punkt-zu-Punkt-Tunneling-Protokoll
Answer: B

QUESTION NO: 21
Welcher der folgenden Punkte ist der wichtigste Vorteil der Virtualisierungstechnologie für Unternehmensanwendungen?
A. Stärkere Datensicherheit
B. Bessere Nutzung der Ressourcen

C. Erhöhte Anwendungsleistung

D. Verbesserte Notfallwiederherstellung

Answer: B

Explanation:

The primary advantage of using virtualization technology for corporate applications is to achieve better utilization of resources, such as hardware, software, network and storage. Virtualization technology allows multiple applications to run on a single physical server or device, which reduces the need for additional hardware and maintenance costs. Virtualization technology also enables dynamic allocation and reallocation of resources according to the demand and priority of the applications, which improves efficiency and flexibility. The other options are not the primary advantage of using virtualization technology, although they may be some of the benefits or challenges depending on the implementation and configuration.

References:

ISACA, CISA Review Manual, 27th Edition, chapter 4, section 4.21

ISACA, COBIT 2019 Framework: Introduction and Methodology, section 3.23

QUESTION NO: 22

Welche der folgenden Definitionen ist im Rahmen eines Notfallwiederherstellungsplans (DRP) am wichtigsten?

A. Geschäftskontinuitätsplan (BCP)

B. Testergebnisse für die Wiederherstellung von Sicherungsdaten

C. Eine umfassende Liste von Notfallwiederherstellungsszenarien und Prioritäten

D. Rollen und Verantwortlichkeiten der Mitglieder des Wiederherstellungsteams

Answer: D

Explanation:

The most important thing to define within a disaster recovery plan (DRP) is the roles and responsibilities for recovery team members, as this ensures that everyone knows what to do, who to report to, and how to communicate in the event of a disaster. A business continuity plan (BCP) is a broader document that covers the overall strategy and objectives for maintaining or resuming business operations after a disaster. Test results for backup data restoration are important to verify the integrity and availability of backup data, but they are not part of the DRP itself. A comprehensive list of disaster recovery scenarios and priorities is useful to identify the potential risks and impacts of different types of disasters, but it is not as critical as defining the roles and responsibilities for recovery team members. References: CISA Review Manual (Digital Version), Chapter 4: Information Systems Operations, Maintenance and Service Management, Section 4.3: Disaster Recovery Planning1

QUESTION NO: 23

Ein IT-Auditor prüft das Risikomanagementprogramm einer Organisation. Welcher der folgenden Faktoren sollte der primäre Treiber für die Risikobereitschaft der IT-Abteilung des Unternehmens sein?

A. Strategische Ziele

B. Kapitalrendite (ROI)

C. Kosten für die Implementierung von Kontrollen

D. Wahrscheinlichkeit von Risikoereignissen

Answer: A

Explanation:

An organization ' s IT risk appetite should be primarily driven by its strategic objectives. The risk appetite defines the amount and type of risk the organization is willing to pursue or retain to achieve its goals.

Aligning risk appetite with strategic objectives ensures that risk-taking is consistent with the organization ' s mission and vision. While ROI, cost of controls, and the likelihood of risk events are important considerations in risk management, they are factors evaluated within the context of the overarching strategic objectives.

References:

ISACA CISA Review Manual, 28th Edition, Chapter 2: Governance and Management of IT.

QUESTION NO: 24

In einem Gebiet, das anfällig für unerwartete Stromspitzen ist, welche der folgenden Maßnahmen würde das System am effektivsten schützen?

A. Generator

B. Spannungsregler

C. Schutzschalter

D. Alternative Stromversorgungsleitung

Answer: B

QUESTION NO: 25

Ein Systemadministrator informierte kürzlich den IT-Auditor über mehrere erfolglose Eindringversuche von außerhalb des Unternehmens. Welche der folgenden Maßnahmen ist am effektivsten, um einen solchen Eindringversuch zu erkennen?

A. Regelmäßige Überprüfung der Protokolldateien

B. Konfigurieren des Routers als Firewall

C. Verwendung von Smartcards mit Einmalpasswörtern

D. Installation der biometrischen Authentifizierung

Answer: A

Explanation:

The most effective way to detect an intrusion attempt is to periodically review log files, which record the activities and events on a system or network. Log files can provide evidence of unauthorized access attempts, malicious activities, or system errors. Configuring the router as a firewall, using smart cards with one-time passwords, and installing biometrics-basedauthentication are preventive controls that can reduce the likelihood of an intrusion, but they do not detect it. References: ISACA CISA Review Manual 27th Edition, page 301

QUESTION NO: 26

Welche der folgenden Fragen ist für einen IS-Auditor in der detaillierten Entwurfsphase eines Systementwicklungsprojekts am wichtigsten zu klären?

A. Die Programmierrichtlinien wurden eingehalten.

B. Es wurden Akzeptanzkriterien entwickelt

C. Es wurden Verfahren zur Datenkonvertierung eingerichtet.

D. Der Entwurf wurde von der Geschäftsleitung genehmigt.

Answer: B

Explanation:

The most important thing for an IS auditor to determine during the detailed design phase of a system development project is that acceptance test criteria have been developed. Acceptance test criteria define the expected functionality, performance and quality of the system, and are used to verify that the system meets the user requirements and specifications. The IS auditor should ensure that the acceptance test criteria are clear, measurable and agreed upon by all stakeholders. Program coding standards have been followed is something that the IS auditor should check during the coding or testing phase, not the detailed design phase.

Data conversion procedures have been established or the design has been approved by senior management are things that the IS auditor should verify during the implementation phase, not the detailed design phase. References: ISACA, CISA Review Manual, 27th Edition, 2018, page 323

QUESTION NO: 27

Welches der folgenden Risiken stellt im Hinblick auf die Resilienz das größte Risiko für eine Organisation dar, die ein neues kritisches System implementiert hat?

A. Es wurde keine Geschäftsauswirkungsanalyse (BIA) durchgeführt.

B. Geschäftsdaten werden in der Entwicklungsumgebung nicht bereinigt.

C. Es gibt keinen Plan zur Überwachung von Systemausfallzeiten.

D. Der Prozessverantwortliche hat die Benutzerakzeptanztests (UAT) nicht freigegeben.

Answer: A

Explanation:

Resilience is the ability of an organization to continue to operate effectively during or after a disruptive event. A business impact analysis (BIA) is a key process to identify the critical systems and processes that support the organization's objectives and determine the impact of their disruption. Without a BIA, the organization may not be able to prioritize the recovery of the most important systems and processes, which poses the greatest risk to its resilience. The other options are not as significant as a BIA, as they relate to data quality, system monitoring, and user acceptance testing, which are important but not essential for resilience. References: CISA Review Manual (Digital Version), Domain 4: Information Systems Operations and Business Resilience, Section 4.2 Business Continuity Planning1

QUESTION NO: 28

Welche der folgenden Aussagen ist am besten ein Indikator dafür, dass ein Vorfallmanagementprozess effektiv ist?

A. Verringerte Anzahl der Anrufe beim Helpdesk

B. Verkürzte Zeit für die Störungsbehebung

C. Erhöhte Anzahl der von der IT-Leitung überprüften Vorfälle

D. Erhöhte Anzahl gemeldeter kritischer Vorfälle

Answer: B

QUESTION NO: 29
Ein IT-Auditor erfährt von einer neuen Verordnung, die Strafen basierend auf der Anzahl der Personen vorsieht, deren personenbezogene Daten (PII) durch eine Sicherheitsverletzung offengelegt wurden. Was wäre die beste Empfehlung, um dem Unternehmen zu helfen, die Haftung im Zusammenhang mit einer Verletzung seiner Kundendatenbank zu begrenzen?
A. Datenbanksegmentierung
B. Datenbanknormalisierung
C. Datenbankharmonisierung
D. Datenbankoptimierung
Answer: A
Explanation:
The best recommendation is database segmentation. If liability depends on the number of individuals whose PII is exposed, the organization should reduce the amount of data that could be compromised in any single breach event. Segmenting databases or separating sensitive data domains limits blast radius and can reduce the number of records exposed in a single incident. ISACA guidance supports isolating high-value assets and tightening internal controls as a way to reduce exposure and improve resilience.
Option A is correct because segmentation limits concentration risk. Instead of keeping all customer data in one broadly exposed logical store, segmentation helps confine access and reduce how many records a single compromise can reach. This directly supports limiting breach impact and, in this case, potential liability tied to the number of affected individuals. This conclusion is an inference from ISACA's risk-reduction principles around isolation, exposure control, and documenting exposure.
Option B is incorrect because database normalization improves data structure and reduces redundancy; it is not primarily a breach-liability reduction control.
Option C is incorrect because database harmonization is about consistency or integration across datasets, not limiting exposure in a breach.
Option D is incorrect because database optimization focuses on performance and efficiency, not on minimizing the number of PII records exposed in a security incident.
Therefore, A is the best answer because segmentation is the option that most directly reduces the scope of exposure in a breach and therefore helps limit liability based on affected individuals.
References (Official ISACA):
ISACA, Best Practices for Setting Up a Cybersecurity Operations Center - recommends prioritizing assets and isolating high-value asset networks.
ISACA Journal, Reporting on GDPR Compliance to the Board - emphasizes documenting exposure and relevant risk controls for privacy risk reporting.
ISACA Journal, Practical Data Security and Privacy for GDPR and CCPA - supports governance approaches to limiting privacy exposure. (Referenced conceptually from prior ISACA privacy guidance.)

QUESTION NO: 30
Der Hauptvorteil der Automatisierung von Anwendungstests besteht darin:
A. Testkonsistenz gewährleisten.
B. mehr Flexibilität bieten.

C. Alle manuellen Testprozesse ersetzen.

D. die Zeit für die Codeüberprüfung verkürzen.

Answer: A

Explanation:

The primary benefit of automating application testing is to provide test consistency. Automated testing can ensure that the same test cases are executed in the same manner and order every time, which can improve the reliability and accuracy of the test results. Providing more flexibility, replacing all manual test processes, and reducing the time to review code are possible benefits of automating application testing, but they are not the primary benefit. References:

ISACA, CISA Review Manual, 27th Edition, 2020, p. 3091

ISACA, CISA Review Questions, Answers and Explanations Database - 12 Month Subscription

QUESTION NO: 31

Welche der folgenden Sicherheitsrisiken können durch eine fachgerecht konfigurierte Netzwerk-Firewall reduziert werden?

A. SQL-Injection-Angriffe

B. Denial-of-Service-Angriffe (DoS)

C. Phishing-Angriffe

D. Insiderangriffe

Answer: B

Explanation:

A network firewall is a device or software that monitors and controls the incoming and outgoing network traffic based on predefined rules. A network firewall can help reduce the risk of denial of service (DoS) attacks, which are attempts to overwhelm a system or network with excessive requests or traffic, by filtering or blocking unwanted or malicious packets. A SQL injection attack is a type of code injection attack that exploits a vulnerability in a web application's database query, by inserting malicious SQL statements into the input fields. A phishing attack is a type of social engineering attack that attempts to trick users into revealing sensitive information or installing malware, by sending fraudulent emails or messages that impersonate legitimate entities. An insider attack is a type of malicious activity that originates from within an organization, such as employees, contractors, or partners, who abuse their access privileges or credentials to compromise the confidentiality, integrity, or availability of information systems or data. A network firewall cannot prevent these types of attacks, as they rely on exploiting human or application weaknesses rather than network vulnerabilities.

QUESTION NO: 32

Eine Organisation verfügt sowohl über einen IT-Strategieausschuss als auch über einen IT-Lenkungsausschuss. Bei der Durchsicht der Protokolle des IT-Lenkungsausschusses würde ein IT-Auditor erwarten, Folgendes festzustellen:

A. bewertete den Beitrag der IT zum Geschäftserfolg.

B. beschaffte und ordnete die für die Projekte erforderlichen Ressourcen zu.

C. verglichen Risiko und Rendite von IT-Investitionen.

D. überprüfte die Erreichung des strategischen IT-Ziels.

Answer: B

QUESTION NO: 33

Was ist der wichtigste Befund bei der Überprüfung des Informationssicherheitsmanagements einer Organisation?

A. Kein eigener Sicherheitsbeamter

B. Kein offizieller Träger für das Informationssicherheitsmanagementsystem

C. Keine regelmäßigen Bewertungen zur Identifizierung von Bedrohungen und Schwachstellen

D. Kein Sensibilisierungs- und Weiterbildungsprogramm für Mitarbeiter

Answer: C

Explanation:

The most critical finding when reviewing an organization's information security management is no periodic assessments to identify threats and vulnerabilities. Periodic assessments are essential for ensuring that the organization's information security policies, procedures, standards, and controls are aligned with the current and emerging risks and threats that may affect its information assets. Without periodic assessments, the organization may not be aware of its actual security posture, gaps, or weaknesses, and may not be able to take appropriate measures to mitigate or prevent potential security incidents. No dedicated security officer, no official charter for the information security management system, and no employee awareness training and education program are also findings that may indicate some deficiencies in the organization's information security management, but they are not as critical as no periodic assessments to identify threats and vulnerabilities. References: ISACA CISA Review Manual 27th Edition, page 343.

QUESTION NO: 34

Eine IT-Sicherheitsprüfung deckt Inkonsistenzen bei den Datenschutzbestimmungen in den Verträgen mit Drittanbietern auf. Welche der folgenden Empfehlungen ist am besten geeignet, um diese Situation zu beheben?

A. Verträge mit Drittanbietern, die sensible Daten verarbeiten, aussetzen.

B. Vertragsänderungen für Drittanbieter priorisieren.

C. Überprüfen Sie die Datenschutzbestimmungen, wenn Verträge zur Verlängerung anstehen.

D. Drittanbieter müssen Geheimhaltungsvereinbarungen (NDAs) unterzeichnen.

Answer: B

Explanation:

The best recommendation to address the situation of inconsistencies in privacy requirements across third- party service provider contracts is to prioritize contract amendments for third -party providers. This is because:

Privacy requirements are essential to ensure the protection of personal information and compliance with relevant laws and regulations, such as the GDPR and the CCPA123.

Inconsistencies in privacy requirements can create risks of data breaches, legal liabilities, reputational damage, and consumer distrust for the organization that outsources its data

processing to third-party providers123.
Suspending contracts with third-party providers that handle sensitive data (option A) is not a feasible or effective solution, as it may disrupt the business operations and cause contractual penalties or disputes4.
Reviewing privacy requirements when contracts come up for renewal (option C) is not a proactive or timely approach, as it may leave the organization exposed to privacy risks for a long period of time until the contracts expire4.
Requiring third-party providers to sign nondisclosure agreements (NDAs) (option D) is not a sufficient measure, as NDAs only cover the confidentiality of information, but not other aspects of privacy, such as data minimization, retention, access, deletion, and security4.
Therefore, the best recommendation is to prioritize contract amendments for third-party providers (option B), as this would allow the organization to align the privacy requirements with its own policies and standards, as well as with the applicable laws and regulations. This would also enable the organization to monitor and audit the compliance of third-party providers with the privacy requirements and enforce appropriate remedies or sanctions in case of noncompliance45.
References: 1: Understanding CPRA service provider contract requirements - Transcend 2: What you must know about 'third parties' under GDPR and CCPA 3: Data Privacy Implications for Service Provider and Third-Party Contracts 4: Privacy and outsourcing for businesses - Office of the Privacy Commissioner of Canada 5: Data Security Guidelines for outsourcing and third party compliance - European Union Agency for Network and Information Security

QUESTION NO: 35
Welche der folgenden Aussagen ist für einen IT-Auditor am wichtigsten zu bestätigen, wenn er die Pläne einer Organisation zur Implementierung von Robotic Process Automation (RPA > zur Automatisierung routinemäßiger Geschäftsaufgaben) prüft?
A. Der gesamte Prozess ist verstanden und dokumentiert.
B. Für die relevanten Geschäftsprozesse werden Rollen und Verantwortlichkeiten definiert.
C. Ein Benchmarking-Verfahren mit Branchenkollegen, die RPA einsetzen, wurde abgeschlossen.
D. Eine Aufforderung zur Angebotsabgabe (RFP) wurde an qualifizierte Anbieter herausgegeben.
Answer: A
Explanation:
The most important thing for an IS auditor to confirm when reviewing an organization's plans to implement robotic process automation (RPA) to automate routine business tasks is that the end-to-end process is understood and documented. This is because RPA involves the use of software robots or digital workers to mimic human actions and execute predefined rules and workflows. Therefore, it is essential that the IS auditor verifies that the organization has a clear and accurate understanding of the current state of the process, the desired state of the process, the inputs and outputs, the exceptions and errors, the roles and responsibilities, and the performance measures12. Without a properdocumentation of the end-to-end process, the organizationmay face challenges in designing, developing, testing, deploying, and monitoring the RPA solution3. References: 1: CISA ReviewManual (Digital

Version), Chapter 4: Information Systems Operations and Business Resilience, Section 4.2: IT Service Delivery and Support, page 211 2:CISA Online Review Course, Module 4: Information Systems Operations and Business Resilience, Lesson 4.2: IT Service Delivery and Support 3: ISACA Journal Volume 5, 2019, Article: Robotic Process Automation: Benefits, Risks and Controls