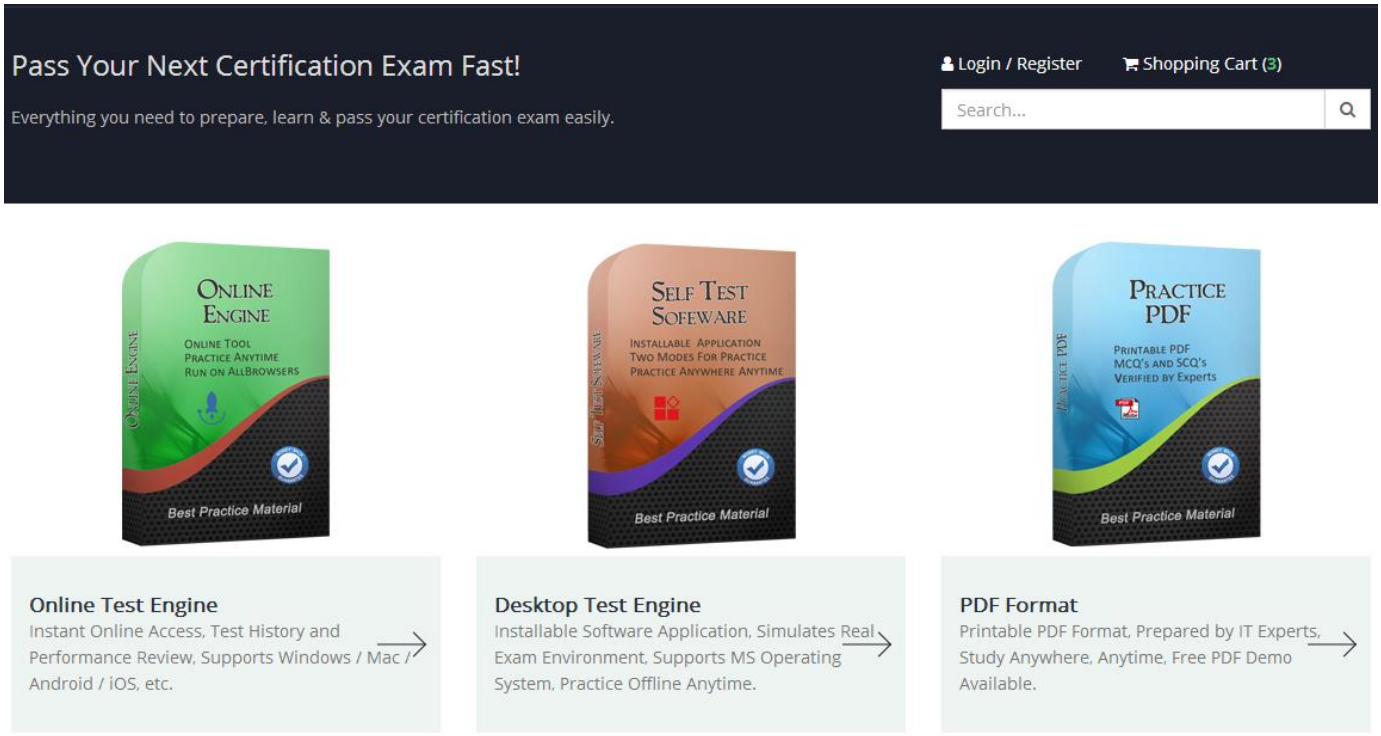
PrepAwayTest



Security & Privacy

We respect customer privacy. We use McAfee's security service to provide you with utmost security for your personal information & peace of mind.

365 Days Free Updates

Free update is available within 365 days after your purchase. After 365 days, you will get 50% discounts for updating.

Money Back Guarantee

Full refund if you fail the corresponding exam in 60 days after purchasing. And Free get any another product.

Instant Download

After Payment, our system will send you the products you purchase in mailbox in a minute after payment. If not received within 2 hours, please contact us.

http://www.prepawaytest.com/

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

Exam : **CISA-CN**

Title : Certified Information Systems Auditor (CISA中文版)

Vendor : ISACA

Version : DEMO

QUESTION NO: 1
一家銀行對利息計算計算機程式進行了微小的改動。下列哪一種方法能提供最有力的證據來確定利息計算是否正確？
A.原始碼審查
B.使用審計軟體進行平行模擬
C.對部分結果進行人工核查
D.品質保證(QA)測試結果審查
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
下列哪一種方法能提供最可靠的審計證據？
A.查詢
B.管理階層證明
C.重新執行控制
D.觀察
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
一個新系統開發專案進度落後，即將面臨關鍵的實施期限。下列哪一項活動最為重要？
A.文件最後時刻的改進
B.執行實施前審計
C.執行使用者驗收測試(UAT)
D.確保程式碼已審核
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
對於修復關鍵業務應用程式伺服器已知漏洞而言，下列哪一項是最重要的考量因素？
A.修補程式在部署到生產環境之前會在測試環境中實作。
B.修補程式實施後會進行網路漏洞掃描。
C.根據既定計畫定期進行漏洞評估。
D.已定義實施補丁的角色和職責。
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
在對涉及信用卡資料的網路攻擊進行取證調查時，下列哪一項最重要？
A.已啟動足夠的卡片安全功能。
B.該公司的支付平台已被封鎖。

C.保持適當的監管鏈。
D.支付卡部門的所有員工都接受了訪談。
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
下列哪項措施最能降低應用程式介面(API)不可用的風險？
A.為傳入的 API 請求建立專用伺服器
B.實施持續整合與部署流程
C.進行定期壓力測試
D.限制傳入請求的速率
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
資訊系統審計員可以透過以下方式最好地評估系統故障對業務的影響：
A.評估使用者滿意度水準。
B.採訪安全管理員。
C.分析設備維護日誌。
D.正在查看系統產生的日誌。
Answer: C

QUESTION NO: 8

作為審計回應的一部分，受審計方對審計建議有疑慮，且不願實施。下列哪一項是資訊系統審計師的最佳因應措施？

A.接受被審計方的答覆並執行額外的測試。

B.建議聘請第三方顧問進行現況評估。

C.與被審計方進一步討論，制定緩解計畫。

D.發布最終報告，但不包含被審計方的意見。

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

下列何者最有利於系統開發專案的效益實現過程？

A.專案指標在專案開始前已選定。

B.專案預算包括執行專案的成本和與解決方案相關的成本。

C.商業效益的估計以先前完成的類似項目為依據。

D.指標在專案實施後立即進行評估。

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
資訊系統審計員在用於處理線上客戶支付的面向公眾的網路伺服器上發現了一個高風險漏洞。資訊系統審計員首先該做什麼？
A.在審計報告中記錄異常情況。
B.審查安全事件報告。
C.辨識補償控制。
D.通知審計委員會。
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
在內部網路段之間設置防火牆，可透過以下方式提高安全性並降低風險：
A.遍歷所有通過網路段的資料包
B.檢查網路段之間所有流量並套用安全策略
C.監控並報告網路參與者之間的會話
D.確保所有連接系統都啟用了適當的安全控制。
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
下列哪一項是確保支付交易資料僅限適當使用者存取的最佳方法？
A.實施雙重認證
B.使用網路安全軟體限制對交易的訪問
C.在應用程式層實現基於角色的存取控制
D.使用單一選單處理敏感應用程式事務
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
當組織的文件伺服器需要對外部使用者開放時，下列哪一項是資訊系統稽核員為保護組織免受攻擊而提出的最佳建議？
A.強制建立安全隧道連線。
B.增強內部防火牆。
C.設立非軍事區(DMZ)。
D.實現安全協定。
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
資訊系統審計員對最近發生的一起安全事件進行跟進，發現事件回應並不充分。
下列哪一項發現最為關鍵？
A.未能發現導致攻擊的安全漏洞。
B.入侵偵測系統(IDS)沒有自動阻止此攻擊。
C.無法追溯攻擊的始發者。
D.未儲存適當的回應文件。
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
對於評估組織補丁管理計畫的資訊系統審計員來說，下列哪一項應該是他們最關注的問題？
A.修補程式從多個部署伺服器進行部署。
B.目前沒有掃描網路以識別缺少修補程式的流程。
C.中低風險漏洞的修補程式被省略。
D.目前沒有針對未打補丁的伺服器進行隔離的流程。
Answer: B

QUESTION NO: 16
在軟體開發生命週期的哪個階段最適合開始討論應用程式控制？
A.商業案例開發階段，此時需要確定利害關係人。
B.應用程式設計階段流程功能已最終確定
C.使用者驗收測試(UAT)階段，此時測試場景已設計完成。
D.應用程式編碼階段，在此階段開發演算法以解決業務問題
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
當資訊系統稽核員需要確認組織是否在資料庫層級對敏感資訊進行加密時，下列何者能夠提供最佳保證？
A.正在檢查主機伺服器的磁碟機設定
B.檢查網路流量中是否有明文傳輸
C.驗證關鍵字段樣本
D.檢視組織的加密策略
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
當應用程式使用個人最終使用者帳戶存取底層資料庫時，下列哪項風險最大？
A.使用了多個資料庫連接，導致處理速度變慢。
B.使用者帳戶在終止後可能仍保持活動狀態。
C.使用者可能能夠繞過應用程式控制。
D.應用程式可能無法擷取完整的稽核追蹤。
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
對於以新的健康記錄系統取代舊系統而言，資訊系統審計師應考慮下列哪項風險最為重大？
A.員工沒有參與採購過程，導致使用者對新系統產生抗拒。
B.資料轉換不正確，導致病患記錄不準確。
C.部署專案嚴重超支，超出預算預期。
D.新系統有容量問題，導致使用者回應時間緩慢。
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
下列哪一種網路通訊協定被路由器等網路設備用於在與另一個 IP 位址通訊時發送錯誤訊息和指示成功或失敗的操作訊息？
A.傳輸控制協定/網際網路協定(TCP/IP)

B.互聯網控制訊息協議
C.多用途交易協議
D.點對點隧道協定
Answer: B

QUESTION NO: 21
使用虛擬化技術開發企業應用程式的主要優勢是什麼？
A.更強大的資料安全性
B.更好地利用資源
C.提升應用程式效能
D.改進的災難復原
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
在災難復原計畫 (DRP) 中，下列哪一項定義最為重要？
A.業務連續性計劃(BCP)
B.備份資料復原測試結果
C.災難復原方案和優先順序的綜合列表
D.恢復團隊成員的角色與職責
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
資訊系統審計員正在審查某組織的風險管理方案。下列哪一項應該是企業IT風險承受能力的主要驅動因素？
A.策略目標
B.投資報酬率(ROI)
C.實施控制的成本
D.風險事件發生的可能性
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
在容易出現電力意外激增的地區，下列哪一項措施能最有效保護電力系統？
A.生成器
B.穩壓器
C.斷路器
D.備用電源線
Answer: B

QUESTION NO: 25
系統管理員最近向資訊系統審計員報告了多次來自組織外部的入侵嘗試，但都沒有成功。下列哪項措施最能有效偵測此類入侵？
A.定期檢視日誌文件
B.將路由器設定為防火牆
C.使用智慧卡與一次性密碼
D.安裝基於生物特徵的身份驗證
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
在系統開發專案的詳細設計階段，資訊系統稽核員最需要確定下列哪一項內容？
A.程序編碼標準已遵循
B.已製定驗收測試標準
C.資料轉換程式已建立。
D.此設計已獲得高階管理人員的批准。
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
就韌性而言，對於實施了新關鍵系統的組織來說，下列哪一項風險最大？
A.尚未進行業務影響分析 (BIA)。
B.開發環境中未對業務資料進行脫敏處理
C.目前沒有監控系統停機時間的計劃
D.流程負責人尚未簽署使用者驗收測試(UAT)協議。
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
下列哪一項最能顯示事件管理流程是有效的？
A.服務台來電數量減少
B.事件解決時間縮短
C.IT 管理階層審查的事件數量增加

D.報告的重大事件數量增加
Answer: B

QUESTION NO: 29
資訊系統審計員了解到一項新規，該規定根據安全漏洞導致個人識別資訊 (PII) 洩露的人數來處以罰款。為了幫助組織最大限度地降低因客戶資訊資料庫外洩而產生的責任，最佳建議是什麼？
A.資料庫分段
B.資料庫規範化
C.資料庫協調
D.資料庫最佳化
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
應用程式測試自動化的主要好處是：

A.提供測試一致性。
B.提供更大的彈性。
C.取代所有手動測試流程。
D.減少程式碼審查時間。
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
透過正確設定網路防火牆可以降低下列哪些安全風險？
A. SQL 注入攻擊
B.拒絕服務 (DoS) 攻擊
C.網路釣魚攻擊
D.內部攻擊
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
一個組織既設有IT策略委員會，也設有IT指導委員會。資訊系統審計員在審查IT指導委員會的會議記錄時，預期會發現該委員會：
A.評估了 IT 對業務的貢獻。
B.取得並分配了專案所需的適當資源。
C.比較了 IT 投資的風險和回報。

D.檢視了策略 IT 目標的實現。
Answer: B

QUESTION NO: 33
在檢視組織的資訊安全管理時，最關鍵的發現是什麼？
A.沒有專門的保安人員
B.資訊安全管理系統沒有正式主席
C.未進行定期評估以識別威脅和漏洞
D.無員工意識訓練與教育計劃
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
資訊系統審計發現第三方服務提供者合約中的隱私要求存在不一致之處。下列哪一項是解決此問題的最佳建議？
A.暫停與處理敏感資料的第三方供應商簽訂合約。
B.優先考慮第三方供應商的合約修改。
C.在合約續約時審查隱私要求。
D.請第三方供應商簽署保密協議(NDA)。
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
在檢視組織實施機器人流程自動化(RPA，用於自動化日常業務任務)的計畫時，資訊系統審計師最需要確認下列哪一項內容？
A.端到端流程已被理解並記錄在案。
B.已為範圍內的業務流程定義了角色和職責。
C.已完成使用 RPA 的行業同業的基準測試。
D.已向合格供應商發出徵求建議書(RFP)。
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