

## 2011 年 5 月 CISA 认证考试新增中文模擬題

對於一個獨立的小型商業計算環境而言，下列哪一種安全控制措施是最有效的？

選項:

- A、對電腦使用的監督
- B、對故障日誌的每日檢查
- C、電腦存儲介質存話加鎖的櫃中
- D、應用系統設計的獨立性檢查

標準答案:A

一旦業務功能發生變化，已列印的表格和其他備用資源都可能要改變。下面哪一種情況構成了對組織的主要風險？

選項:

- A、在異地存儲的備用資源詳細目錄沒有及時更新
- B、在備份電腦和恢復設備上存儲的備用資源詳細目錄沒有及時更新
- C、沒有對緊急情況下的供應商或備選供應商進行評估，不知道供應商是否還在正常營業
- D、過期的材料沒有從有用的資源中剔除

標準答案:C

以下哪一項屬於所有指令均能被執行的作業系統模式？

選項:

- A、問題
- B、中斷
- C、監控
- D、標準處理

標準答案:B

企業將其技術支持職能（help desk）外包出去，下面的哪一項指標納入外包服務等級協定（SLA）是最恰當的？

選項:

- A、要支援用戶數

- B、首次請求技術支持，即解決的（事件）百分比
- C、請求技術支援的總人次
- D、電話回應的次數

標準答案:B

IS 審計師檢查組織的資料檔案控制流程時，發現交易事務使用的是最新的檔，而重啓動流程使用的是早期版本，那麼，IS 審計師應該建議：

選項:

- A、檢查根源程式文檔的保存情況
- B、檢查資料檔案的安全狀況
- C、實施版本使用控制
- D、進行一對一的核查

標準答案:C

將輸出結果及控制總計和輸入資料及控制總計進行匹配可以驗證輸出結果，以下哪一項能起上述作用？

選項:

- A、批量頭格式
- B、批量平衡
- C、資料轉換差錯糾正
- D、對列印池的訪問控制

標準答案:B

審計客戶/伺服器資料庫安全時，IS 審計師應該最關注於哪一方面的可用性？

選項:

- A、系統工具
- B、應用程式生成器
- C、系統安全文檔
- D、訪問存儲流程

標準答案:A

測試程式變更管理流程時，IS 審計師使用的最有效的方法是：

選項:

- A、由系統生成的資訊跟蹤到變更管理文檔
- B、檢查變更管理文檔中涉及的證據的精確性和正確性

- C、由變更管理文檔跟蹤到生成審計軌跡的系統
- D、檢查變更管理文檔中涉及的證據的完整性

標準答案:A

分散式環境中，伺服器失效帶來的影響最小的是：

選項:

- A、冗余路由
- B、集群
- C、備用電話線
- D、備用電源

標準答案:B

實施防火牆最容易發生的錯誤是：

選項:

- A、訪問列表配置不準確
- B、社會工程學會危及口令的安全
- C、把 modem 連至網路中的電腦
- D、不能充分保護網路和伺服器使其免遭病毒侵襲

標準答案:A

為確定異構環境下跨平臺的資料訪問方式，IS 審計師應該首先檢查：

選項:

- A、業務軟體
- B、系統平臺工具
- C、應用服務
- D、系統開發工具

標準答案:C

資料庫規格化的主要好處是：

選項:

- A、在滿足用戶需求的前提下，最大程度地減小表內資訊的冗餘（即：重複）
- B、滿足更多查詢的能力
- C、由多張表實現，最大程度的資料庫完整性

D、通過更快地資訊處理，減小反應時間

標準答案:A

以下哪一種圖像處理技術能夠讀入預定義格式的書寫體並將其轉換為電子格式？

選項:

- A、磁墨字元識別（MICR）
- B、智慧語音識別（IVR）
- C、條碼識別（BCR）
- D、光學字元識別（OCR）

標準答案:D

代碼簽名的目的是確保：

選項:

- A、軟體沒有被後續修改
- B、應用程式可以與其他已簽名的應用安全地對接使用
- C、應用（程式）的簽名人是受到信任的
- D、簽名人的私鑰還沒有被洩露

標準答案:A

檢查用於互聯網 Internet 通訊的網路時，IS 審計應該首先檢查、確定：

選項:

- A、是否口令經常修改
- B、客戶/伺服器應用的框架
- C、網路框架和設計
- D、防火牆保護和代理伺服器

標準答案:C

企業正在與廠商談判服務水準協定（SLA），首要的工作是：

選項:

- A、實施可行性研究
- B、核實與公司政策的符合性
- C、起草其中的罰則
- D、起草服務水準要求

標準答案:D

電子商務環境中降低通訊故障的最佳方式是：

選項:

- A、使用壓縮軟體來縮短通訊傳輸耗時
- B、使用功能或消息確認（機制）
- C、利用包過濾防火牆，重新路由消息
- D、租用非同步傳輸模式（ATM）線路

標準答案:D

以下哪一項措施可最有效地支持 24/7 可用性？

選項:

- A、日常備份
- B、異地存儲
- C、鏡像
- D、定期測試

標準答案:C

某製造類公司欲建自動化發票支付系統，要求該系統在復核和授權控制上花費相當少的時間，同時能識別出需要深入追究的錯誤，以下哪一項措施能最好地滿足上述需求？

選項:

- A、建立一個與供應商相聯的內部客戶機用及伺服器網路以提升效率
- B、將其外包給一家專業的自動化支付和賬務收發處理公司
- C、與重要供應商建立採用標準格式的、電腦對電腦的電子業務文檔和交易處理用 EDI 系統
- D、重組現有流程並重新設計現有系統

標準答案:C

以下哪一項是圖像處理的弱點？

選項:

- A、驗證簽名
- B、改善服務
- C、相對較貴
- D、減少處理導致的變形

標準答案:C

某 IS 審計人員需要將其微機與某大型機系統相連，該大型機系統採用同步塊資料傳輸通訊，而微機只支援非同步 ASCII 字元資料通訊。為實現其連通目標，需為該 IS 審計人員的微機增加以下哪一類功能？

選項:

- A、緩衝器容量和平行埠
- B、網路控制器和緩衝器容量
- C、平行埠和協定轉換
- D、協定轉換和緩衝器容量

標準答案:D

為了確定哪些用戶有權進入享有特權的監控態，IS 審計人員應該檢查以下哪一項？

選項:

- A、系統訪問日誌檔
- B、被啟動的訪問控制軟體參數
- C、訪問控制違犯日誌
- D、系統配置檔中所使用的控制選項

標準答案:D

在審查一個大型資料中心期間，IS 審計人員注意到其電腦操作員同時兼任備份磁帶管理員和安全管理員。以下哪一種情形應在審計報告中視為最為危險的？

選項:

- A、電腦操作員兼任備份磁帶庫管理員
- B、電腦操作員兼任安全管理員
- C、電腦操作員同時兼任備份磁帶庫管理管理員和安全管理員
- D、沒有必要報告上述任何一種情形

標準答案:B

以下哪一種系統性技術可被財務處理公司用來監控開支的構成模型並鑒別和報告異常情況？

選項:

- A、神經網路

- B、資料庫管理軟體
- C、管理資訊系統
- D、電腦輔助審計技術

標準答案:A

大學的 IT 部門和財務部（FSO，financial services office）之間簽有服務水準協定（SLA），要求每個月系統可用性超過 98%。財務部後來分析系統的可用性，發現平均每個月的可用性確實超過 98%，但是月末結賬期的系統可用性只有 93%。那麼，財務部應該採取的最佳行動是：

選項:

- A、就協定內容和價格重新談判
- B、通知 IT 部門協議規定的標準沒有達到
- C、增購電腦設備等（資源）
- D、將月底結賬處理順延

標準答案:A

在檢查廣域網（WAN）的使用情況時，發現連接主伺服器 and 備用資料庫伺服器之間線路通訊異常，流量峰值達到了這條線路容量的 96%。IS 審計師應該決定後續的行動是：

選項:

- A、實施分析，以確定該事件是否為暫時的服務實效所引起
- B、由於廣域網（WAN）的通訊流量尚未飽和，96%的流量還在正常範圍內，不必理會
- C、這條線路應該立即更換以提升其通訊容量，使通訊峰值不超過總容量的 85%
- D、通知相關員工降低其通訊流量，或把網路流量大的任務安排到下班後或清晨執行，使 WAN 的流量保持相對穩定

標準答案:A

以下哪一類設備可以延伸網路，具有存儲資料幀的能力並作為存儲轉發設備工作？

選項:

- A、路由器
- B、網橋
- C、中繼器
- D、閘道

標準答案:B

在評估電腦預防性維護程式的有效性和充分性時，以下哪一項能為 IS 審計人員提供最大的幫助？

選項:

- A、系統故障時間日誌
- B、供應商的可靠性描述
- C、預定的定期維護日誌
- D、書面的預防性維護計畫表

標準答案:A

用於監聽和記錄網路資訊的網路診斷工具是：

選項:

- A、線上監視器
- B、故障時間報告
- C、幫助平臺報告
- D、協議分析儀

標準答案:D

對以下哪一項的分析最有可能使 IS 審計人員確定有未被核准的程式曾企圖訪問敏感資料？

選項:

- A、異常作業終止報告
- B、操作員問題報告
- C、系統日誌
- D、操作員工作日程安排

標準答案:C

有效的 IT 治理要求組織結構和程式確保

選項:

- A、組織的戰略和目標包括 IT 戰略
- B、業務戰略來自於 IT 戰略
- C、IT 治理是獨立的,與整體治理相區別
- D、IT 戰略擴大了組織的戰略和目標

標準答案:D

品質保證小組通常負責：

選項:

- A、確保從系統處理收到的輸出是完整的
- B、監督電腦處理任務的執行
- C、確保程式、程式的更改以及存檔符合制定的標準
- D、設計流程來保護資料，以免被意外洩露、更改或破壞

標準答案:C

組織內資料安全官的最為重要的職責是：

選項:

- A、推薦並監督資料安全政策
- B、在組織內推廣安全意識
- C、制定 IT 安全政策下的安全程式/流程
- D、管理物理和邏輯訪問控制

標準答案:A

企業打算外包其資訊安全職能,那麼其中的哪一項職能不能外包,只能保留在企業內?

選項:

- A、公司安全策略的記賬
- B、制訂公司安全策略
- C、實施公司安全策略
- D、制訂安全堆積和指導

標準答案:A

在小型組織內，充分的職責分工有些不實際，有個員工兼職作電腦操作員和應用程式師，IS 審計師應推薦如下哪一種控制，以降低這種兼職的潛在風險？

選項:

- A、自動記錄開發（程式/文檔）庫的變更
- B、增員，避免兼職
- C、建立適當的流程/程式，以驗證只能實施經過批准的變更，避免非授權的操作

D、建立阻止電腦操作員更改程式的訪問控制

標準答案:C

一旦組織已經完成其所有關鍵業務的業務流程再造（BPR），IS 審計人員最有可能集中檢查：

選項:

- A、BPR 實施前的處理流程圖
- B、BPR 實施後的處理流程圖
- C、BPR 專案計畫
- D、持續改進和監控計畫

標準答案:B

某零售企業的每個出口自動到銷售定單進行順序編號。小額定單直接在出口處理，而大額定單則送往中心生產機構。保證所有送往生產機構的定單都被接收和處理的最適當的控制是：

選項:

- A、發送並對賬交易數及總計
- B、將資料送回本地進行比較
- C、利用奇偶檢查來比較資料
- D、在生產機構對銷售定單的編號順序進行追蹤和計算

標準答案:A

以下哪一項資料庫管理員行為不太可能被記錄在檢測性控制日誌中？

選項:

- A、刪除一個記錄
- B、改變一個口令
- C、洩露一個口令
- D、改變訪問許可權

標準答案:C

IS 戰略規劃應包含：

選項:

- A、制定的硬體採購規格說明
- B、未來業務目標的分析
- C、專案開發的（啓動和結束）日期

D、IS 部門的年度預算（目標）

標準答案:B

達到評價 IT 風險的目標最好是通過

選項:

- A、評估與當前 IT 資產和 IT 專案相關的威脅
- B、使用過去公司損失的實際經驗來確定當前的風險
- C、流覽公開報導的可比較組織的損失統計資料
- D、流覽審計報告中涉及的 IT 控制薄弱點

標準答案:A

在確認是否符合組織的變更控制程式時，以下 IS 審計人員執行的測試中哪一項最有效？

選項:

- A、審查軟體遷移記錄並核實審批情況
- B、確定已發生的變更並核實審批情況
- C、審核變更控制文檔並核實審批情況
- D、保證只有適當的人員才能將變更遷移至生產環境

標準答案:B

以哪項功能應當由應用所有者執行，從而確保 IS 和最終用戶的充分的職責分工？

選項:

- A、系統分析
- B、資料訪問控制授權
- C、應用編程
- D、資料管理

標準答案:B

在以下何種情況下應用系統審計蹤跡的可靠性值得懷疑？

選項:

- A、審計足跡記錄了用戶 ID
- B、安全管理員對審計文件擁有唯讀許可權

- C、日期時間戳記錄了動作發生的時間
- D、用戶在糾正系統錯誤時能夠修正審計蹤跡記錄

標準答案:D

對於資料庫管理而言，最重要的控制是：

選項:

- A、批准資料庫管理員（DBA）的活動
- B、職責分工
- C、訪問日誌和相關活動的檢查
- D、檢查資料庫工具的使用

標準答案:B

IT 治理的目標是保證 IT 戰略符合以下哪一項的目標？

選項:

- A、企業
- B、IT
- C、審計
- D、財務

標準答案:A

資料編輯屬於：

選項:

- A、預防性控制
- B、檢測性控制
- C、糾正性控制
- D、補償控制

標準答案:A

業務流程再造（BPR）專案最有可能導致以下哪一項的發生？

選項:

- A、更多的人使用技術
- B、通過降低資訊技術的複雜性而大量節省開支
- C、較弱的組織結構和較少的責任
- D、增加的資訊保護（IP）風險

標準答案:A

IS 審計師發現不是所有雇員都瞭解企業的資訊安全政策。IS 審計師應當得出以下哪項結論：

選項:

- A、這種缺乏瞭解會導致不經意地洩露敏感資訊
- B、資訊安全不是對所有只能都是關鍵的
- C、IS 審計應當為那些雇員提供培訓
- D、該審計發現應當促使管理層對員工進行繼續教育

標準答案:A

資料管理員負責：

選項:

- A、維護資料庫系統軟體
- B、定義資料元素、資料名及其關係
- C、開發物理資料庫結構
- D、開發資料字典系統軟體

標準答案:B

許多組織強制要求雇員休假一周或更長時間，以便：

選項:

- A、確保雇員維持生產品質，從而生產力更高
- B、減少雇員從事不當或非法行為的機會
- C、為其他雇員提供交叉培訓
- D、消除當某個雇員一次休假一天造成的潛在的混亂

標準答案:B

對 IT 部門的戰略規劃流程/程式的最佳描述是：

選項:

- A、依照組織大的規劃和目標，IT 部門或都有短期計畫，或者有長期計畫
- B、IT 部門的戰略計畫必須是基於時間和基於項目的，但是不會詳細到能夠確定滿足業務要求的優先順序的程式
- C、IT 部門的長期規劃應該認識到組織目標、技術優勢和規章的要求
- D、IT 部門的短期規劃不必集成到組織的短計畫內，因為技術的發展對 IT 部門的規劃的推動，快於對組織計畫的推動

標準答案:C

開發一個風險管理程式時進行的第一項活動是：

選項:

- A、威脅評估
- B、資料分類
- C、資產盤點
- D、並行模擬

標準答案:C

在審核某業務流程再造（BPR）專案時，以下審計人員要評價的專案中哪一項最重要？

選項:

- A、被撤銷控制的影響
- B、新控制的成本
- C、BPR 專案計畫
- D、持續改進和監控計畫

標準答案:A

資料庫管理員負責：

選項:

- A、維護電腦內部資料的訪問安全
- B、實施資料庫定義控制
- C、向用戶授予訪問許可權
- D、定義系統的資料結構

標準答案:B

IS 審計師復核 IT 功能外包合同時，應當期望它定義：

選項:

- A、硬體設置
- B、訪問控制軟體
- C、知識產權
- D、應用開發方法論

標準答案:C

IS 審計師發現被審計的企業經常舉辦交叉培訓，那麼需要評估如下哪一種風險？

選項:

- A、對某個技術骨幹的過分依賴
- B、崗位接任計畫不適當
- C、某個人知道全部系統的細節
- D、運營中斷

標準答案:C

應用系統開發的責任下放到各業務基層，最有可能導致的後果是

選項:

- A、大大減少所需資料通訊
- B、控制水準較低
- C、控制水準較高
- D、改善了職責分工

標準答案:B

可以降低社交工程攻擊的潛在影響的是：

選項:

- A、遵從法規的要求
- B、提高道德水準
- C、安全意識計畫（如：促進安全意識的教育）
- D、有效的績效激勵政策

標準答案:C

企業資源規劃中的總帳設置功能允許設定會計期間。對此功能的訪問被授予財務、倉庫和訂單錄入部門的用戶。這種廣泛的訪問最有可能是因為：

選項:

- A、經常性地修改會計期間的需要
- B、需要向關閉的會計期間過入分錄
- C、缺乏適當的職責分工政策和步驟
- D、需要創建和修改科目表及其分配

標準答案:C

IT 治理確保組織的 IT 戰略符合於：

選項:

- A、企業目標
- B、IT 目標
- C、審計目標
- D、控制目標

標準答案:A

以下哪一項最好地描述了企業生產重組（ERP）軟體的安裝所需要的文檔？

選項:

- A、僅對特定的開發
- B、僅對業務需求
- C、安裝的所有階段必須進行書面記錄
- D、沒有開發客戶特定文檔的需要

標準答案:C

實施下面的哪個流程，可以幫助確保經電子資料交換（EDI）的入站交易事務的完整性？

選項:

- A、資料片斷計數內建到交易事務集的尾部
- B、記錄收到的消息編號，定期與交易發送方驗證
- C、為記賬和跟蹤而設的電子審計軌跡
- D、已收到的確認的交易事務與發送的 EDI 消息日誌比較、匹配

標準答案:A

評估資料庫應用的便捷性時，IS 審計師應該驗證：

選項:

- A、能夠使用結構化查詢語言（SQL）
- B、與其他系統之間存在資訊的導入、導出程式
- C、系統中採用了索引（Index）
- D、所有實體（entities）都有關鍵名、主鍵和外鍵

標準答案:A

以下哪一項有利於程式維護？

選項:

- A、強內聚/松耦合的程式
- B、弱內聚/松耦合的程式
- C、強內聚/緊耦合的程式
- D、弱內聚/緊耦合的程式

標準答案:A

軟體發展項目中納入全面品質管制（TQM，total quality managemnet）的主要好處是：

選項:

- A、齊全的文檔
- B、按時交付
- C、成本控制
- D、最終用戶的滿意

標準答案:D

隨著應用系統開發的進行,很明顯有數個設計目標已無法實現最有可能導致這一結果的原因是：

選項:

- A、用戶參與不足
- B、項目此理早期撤職
- C、不充分的品質保證（QA）工具
- D、沒有遵從既定的已批准功能

標準答案:A

一個通用串列匯流排（USB）埠：

選項:

- A、可連接網路而無需網卡
- B、用乙太網適配器連接網路
- C、可代替所有現存的連接
- D、連接監視器

標準答案:B

集線器（HUB）設備用來連接：

選項:

- A、兩個採用不同協定的 LANs

- B、一個 LAN 和一個 WAN
- C、一個 LAN 和一個 MAN（城域網）
- D、一個 LAN 中的兩個網段

標準答案:D

對於確保非現場的業務應用開發的成功，下面哪一個是最佳選擇？

選項:

- A、嚴格的合同管理實務
- B、詳盡、正確的應用需求規格說明
- C、認識到文化和政治上差異
- D、注重現場實施後的檢查

標準答案:B

審計軟體採購的需求階段時，IS 審計師應該：

選項:

- A、評估專案時間表的可行性
- B、評估廠商建議的品質程式
- C、確保採購到最好的套裝軟體
- D、檢查需求規格的完整性

標準答案:D

為評估軟體的可靠性，IS 審計師應該採取哪一種步驟？

選項:

- A、檢查不成功的登陸嘗試次數
- B、累計指定執行週期內的程式出錯數目
- C、測定不同請求的反應時間
- D、約見用戶，以評估其需求所滿足的範圍

標準答案:B

IS 審計人員在應用開發專案的系統設計階段的首要任務是：

選項:

- A、商定明確詳盡的控制程式
- B、確保設計準確地反映了需求
- C、確保初始設計中包含了所有必要的控制
- D、勸告開發經理要遵守進度表

標準答案:C

企業最終決定直接採購商業化的套裝軟體，而不是開發。那麼，傳統的軟體發展生產週期（SDLC）中設計和開發階段，就被置換為：

選項:

- A、挑選和配置階段
- B、可行性研究和需求定義階段
- C、實施和測試階段
- D、（無，不需要置換）

標準答案:A

在審核組織的系統開發方法學時，IS 審計人員通常首先執行以下哪一項審計程式？

選項:

- A、確定程式的充分性
- B、分析程式的效率
- C、評價符合程式的程度
- D、比較既定程式和實際觀察到的程式

標準答案:D

用戶對應用系統驗收測試之後，IS 審計師實施檢查，他（或她）應該關注的重點

選項:

- A、確認測試目標是否成文
- B、評估用戶是否記載了預期的測試結果
- C、檢查測試問題日誌是否完整
- D、確認還有沒有尚未解決的問題

標準答案:D

IS 審計師正在檢查開發完成的專案，以確定新的應用是否滿足業務目標的要求。下面哪類報告能夠提供最有價值的參考？

選項:

- A、用戶驗收測試報告
- B、性能測試報告

- C、開發商與本企業互訪記錄（或社會交往報告）  
D、穿透測試報告

標準答案:A

TCP/IP 協定簇包含的面向連接的協定處於：

選項:

- A、傳輸層  
B、應用層  
C、物理層  
D、網路層

標準答案:A

如果已決定買進軟體而不是內部自行開發，那麼這一決定通常發生於：

選項:

- A、專案需求定義階段  
B、專案可行性研究階段  
C、專案詳細設計階段  
D、專案編程階段

標準答案:B

接收 EDI 交易並通過通訊介面站（stage）傳遞通常要求：

選項:

- A、轉換和拆開交易  
B、選擇驗證程式  
C、把資料傳遞給適當的應用系統  
D、建立一個記錄接收審計日誌的點

標準答案:B

假設網路中的一個設備發生故障，那麼在下哪一種局域網結構更容易面臨全面癱瘓？

選項:

- A、星型  
B、匯流排  
C、環型  
D、全連接

標準答案:A

通過評估應用開發專案，而不是評估能力成熟度模型（CMM），IS 審計師應該能夠驗證：

選項:

- A、可靠的產品是有保證的
- B、程式師的效率得到了提高
- C、安全需求得到了規劃、設計
- D、預期的軟體程式（或流程）得到了遵循

標準答案:D

組織要捐贈一些本單位的舊電腦設備給希望小學，在運輸這些捐贈品之前應該確保：

選項:

- A、電腦上不曾保存機密資料
- B、受捐的希望小學簽署保密協議
- C、資料存儲的介質是徹底空白的
- D、所有資料已經被刪除

標準答案:C

在契約性協議包含源代碼第三方保存契約(escrow)的目的是：

選項:

- A、保證在供應商不存在時源代碼仍然有效
- B、允許定制軟體以滿足特定的業務需求
- C、審核源代碼以保證控制的充分性
- D、保證供應商已遵從法律要求

標準答案:A

專案開發過程中用來檢測軟體錯誤的對等審查活動稱為：

選項:

- A、仿真技術
- B、結構化走查
- C、模組化程式設計技術
- D、自頂向下的程式構造

標準答案:B

對於測試新的、修改的或升級的系統而言，為測試其（處理）邏輯，創建測試資料時，最重要的是：

選項:

- A、為每項測試方案準備充足的資料
- B、實際處理中期望的資料表現形式
- C、按照計畫完成測試
- D、對實際資料進行隨機抽樣

標準答案:B

在審計系統開發專案的需求階段時，IS 審計人員應：

選項:

- A、評估審計足跡的充分性
- B、標識並確定需求的關鍵程度
- C、驗證成本理由和期望收益
- D、確保控制規格已經定義

標準答案:D

以下哪一項面向物件的技術特徵可以提高資料的安全級別？

選項:

- A、繼承
- B、動態倉庫
- C、封裝
- D、多態性

標準答案:C

軟體發展的瀑布模型，用於下面的哪一種情況時最為適當的？

選項:

- A、理解了需求，並且要求需求保持穩定，尤其是開發的系統所運行的業務環境沒有變化或變化很小
- B、需求被充分地理解，專案又面臨工期壓力
- C、專案要採用面向物件的設計和編程方法
- D、項目要引用新技術

標準答案:A

獲得優質軟體的最佳途徑是：

選項:

- A、通過徹底的測試
- B、發現並快速糾正編程錯誤
- C、根據可用時間和預算決定測試的數量
- D、在整個專案過程中應用定義良好的流程和結構化的審核

標準答案:D

資訊系統不能滿足用戶需求的最常見的原因是：

選項:

- A、用戶需求頻繁變動
- B、對用戶需求增長的預測不準確
- C、硬體系統限制了併發用戶的數目
- D、定義系統時用戶參與不夠

標準答案:D

用於 IT 開發專案的業務模式（或業務案例）文檔應該被保留，直到：

選項:

- A、系統的生命週期結束
- B、項目獲得批准
- C、用戶驗收了系統
- D、系統被投入生產

標準答案:A

以下哪一項是採用原型法作為系統開發方法學的主要缺點？

選項:

- A、用戶對專案進度的期望可能過於樂觀
- B、有效的變更控制和管理不可能實施
- C、用戶參與日常專案管理可能過於廣泛
- D、用戶通常不具備足夠的知識來幫助系統開發

標準答案:A

制定基於風險的審計戰略時,IS 審計師應該實施風險評估,以確定:

選項:

- A、已經存在減免風險的控制
- B、找到了弱點和威脅
- C、已經考慮到審計風險
- D、實施差異分析是適當的

標準答案:B

使用統計抽樣流程有助於最小化:

選項:

- A、抽樣風險
- B、檢測性風險
- C、固有風險
- D、控制風險

標準答案:B

以下哪種抽樣方法對符合性測試最有用?

選項:

- A、屬性抽樣
- B、變數抽樣
- C、分層單位平均估算法
- D、差值估計法

標準答案:A

通用審計軟體(GAS)的主要用途是:

選項:

- A、測試程式中內嵌的控制
- B、測試對資料的非授權訪問
- C、為審計資料精選資料
- D、降低對(交易)事務判斷的需要

標準答案:C

測試程式的更改時,以下哪項是最適合作為總體來抽取樣本?

選項:

- A、測試庫清單

- B、原程式清單
- C、程式更改需求
- D、生產用程式庫清單

標準答案:D

在審查定義 IT 服務水準的程序控制時，資訊系統審計師最有可能先與下列哪種人面談：

選項:

- A、系統編程人員
- B、法律顧問
- C、業務單位經理人員
- D、應用編程人員

標準答案:C

以下哪項應是 IS 審計師最為關注的:

選項:

- A、沒有報告網路被攻陷的事件
- B、未能就企業闖入事件通知執法人員
- C、缺少對操作許可權的定期檢查
- D、沒有就闖入事件告之公眾

標準答案:A

使用集成測試系統(ITF,或譯為:整體測試)的最主要的缺點是需要:

選項:

- A、將測試資料孤立於生產資料之外
- B、通知用戶,讓他們調整輸出
- C、隔離特定的主文件記錄
- D、用單獨的檔收集事務和主文件記錄

標準答案:A

在建立連續線上監控系統時，IS 審計師首先應該識別：

選項:

- A、合理的目標下限
- B、組織中高風險領域
- C、輸出檔的位置和格式

D、帶來最大潛在回報的應用程式

標準答案:B

審計章程應該:

選項:

- A、是動態的並且經常修訂以適應技術和審計職業的變化
- B、消除表述經管理當局授權以復核並維護內控制度的審計目標
- C、明文規定設計好的審計程式,以達成預定審計目標
- D、概述審計職能的權力、範圍和責任

標準答案:D

IS 審計師參與應用系統開發,他們從事以下哪項可以導致獨立性的減弱.

選項:

- A、對系統開發進行了復核
- B、對控制和系統的其他改進提出了建議
- C、對完成後的系統進行了獨立評價
- D、積極參與了系統的設計和完成

標準答案:D

IS 審計師應該能識別並評估各種風險及潛在影響。以下哪項風險與繞過授權程式（後門）有關？

選項:

- A、固有風險
- B、檢測性風險
- C、審計風險
- D、錯誤風險

標準答案:A

制訂基於風險的審計程式時,IS 審計師最可能關注的是:

選項:

- A、業務程式/流程
- B、關鍵的 IT 應用
- C、運營控制
- D、業務戰略

標準答案:A

在不熟悉領域從事審計時，IS 審計師首先應該完成的任務是：

選項:

- A、為涉及到的每個系統或功能設計審計程式
- B、開發一套符合性測試和實質性測試
- C、收集與新審計專案相關的背景資訊
- D、安排人力與經濟資源

標準答案:C

內部審計部門,從組織結構上向財務總監而不是審計委員會報告,最有可能:

選項:

- A、導致對其審計獨立性的質疑
- B、報告較多業務細節和相關發現
- C、加強了審計建議的執行
- D、在建議中採取更對有效行動

標準答案:A

審計章程的主要目的是：

選項:

- A、把組織需要的審計流程記錄下來
- B、正式記錄審計部門的行動計畫
- C、為審計師制定職業行為規範
- D、描述審計部門的權力與責任

標準答案:D

確保審計資源在組織中發揮最大價值的首要步驟應該是:

選項:

- A、規劃審計工作並監控每項審計的時間花費
- B、培訓資訊系統審計師掌握公司中使用的最新技術
- C、基於詳細的風險評估制定審計計畫
- D、監控審計進展並實施成本控制

標準答案:C

如下哪一類風險是假設被檢查的方面缺乏補償控制:

選項:

- A、控制風險
- B、檢查風險
- C、固有風險
- D、抽樣風險

標準答案:C

風險分析的關鍵要素是:

選項:

- A、審計計畫
- B、控制
- C、脆弱點
- D、責任

標準答案:C

對於抽樣而言,以下哪項是正確的?

選項:

- A、抽樣一般運用於與不成文或無形的控制相關聯的總體
- B、如果內部控制健全,置信系統可以取的較低
- C、通過儘早停止審計測試,屬性抽樣有助於減少對某個屬性的過量抽樣
- D、變數抽樣是估計給定控制或相關控制集合發生率的技術

標準答案:B

資料庫管理系統套裝軟體不可能提供下面哪一種訪問控制功能?

選項:

- A、用戶對欄位數的訪問
- B、用戶在網路層的登錄
- C、在程式級的身份驗證
- D、在交易級的身份驗證

標準答案:B

電腦舞弊行為可以被以下哪一條措施所遏制?

選項:

- A、準備起訴

- B、排斥揭發腐敗內幕的雇員
- C、忽略了司法系統的低效率
- D、準備接收系統缺乏完整性所帶來的風險

標準答案:A

IS 審計師檢查企業的生產環境中的主機和客戶/伺服器體系之後。發現的哪一種漏洞或威脅需要特別關注？

選項:

- A、安全官兼職資料庫管理員
- B、客戶/伺服器系統沒有適當的管理口令/密碼控制
- C、主機系統上運行的非關鍵應用沒有納入業務持續性計畫的考慮
- D、大多數局域網上的檔伺服器沒有執行定期地硬碟備份

標準答案:B

數位簽名可以有效對付哪一類電子資訊安全的風險？

選項:

- A、非授權地閱讀
- B、盜竊
- C、非授權地複製
- D、篡改

標準答案:D

能夠最佳地提供本端伺服器上的將處理的工資資料的訪問控制的是：

選項:

- A、將每次訪問記入個人資訊（即：作日誌）
- B、對敏感的交易事務使用單獨的密碼/口令
- C、使用軟體來約束授權用戶的訪問
- D、限制只有營業時間內才允許系統訪問

標準答案:C

E-MAIL 軟體應用中驗證數位簽名可以：

選項:

- A、幫助檢查垃圾郵件（spam）
- B、實現保密性
- C、加重閘道伺服器的負載

D、嚴重降低可用的網路帶寬

標準答案:A

下面哪一種情況可以使資訊系統安全官員實現有效進行安全控制的目的？

選項:

- A、完整性控制的需求是基於風險分析的結果
- B、控制已經過了測試
- C、安全控制規範是基於風險分析的結果
- D、控制是在可重複的基礎上被測試的

標準答案:D

每感染一個檔就變體一次的惡意代碼稱為：

選項:

- A、邏輯炸彈
- B、隱秘型病毒
- C、特洛伊木馬
- D、多態性病毒

標準答案:D

通常，駭客使用如下哪一種攻擊手段時，會引起對互聯網站點的分散式拒絕服務攻擊（DDos）？

選項:

- A、邏輯炸彈
- B、網路釣魚
- C、間諜軟體
- D、特洛伊木馬

標準答案:D

為保證主記錄中的關鍵字段已被正確更新，最好採用下列哪一種辦法？

選項:

- A、欄位檢查
- B、求和校驗與控制
- C、合理性檢查
- D、審查事前和事後的維護報告

標準答案:D

下列哪一組高層系統服務可以提供對網路的訪問控制  
選項:

- A、訪問控制列表和訪問特權
- B、身份識別和驗證
- C、認證和鑒定
- D、鑒定和保證

標準答案:B

企業裏有個混合訪問點不能升級其安全強度，而新的訪問點具有高級無線安全特性。IS 審計師建議用新的訪問點替換老的混合訪問點，下面哪一個選項支援 IS 審計師的建議的理由最為充分？

選項:

- A、新的訪問點具有更高的安全強度
- B、老的訪問點性能太差
- C、整個企業網路的安全強度，就是其最為薄弱之處的安全強度
- D、新的訪問點易於管理

標準答案:C

檢查入侵監測系統(IDS)時,IS 審計師最關注的內容是:

選項:

- A、把正常通訊識別為危險事件的數量(誤報)
- B、系統沒有識別出的攻擊事件
- C、由自動化工具生成的報告和日誌
- D、被系統阻斷的正常通訊流

標準答案:B

銀行的自動櫃員機(ATM)是一種專門用於銷售點的終端，它可以：

選項:

- A、只能用於支付現金和存款服務
- B、一般放置在入口稠密的場所以威懾盜竊與破壞
- C、利用保護的通訊線進行資料傳輸
- D、必須包括高層的邏輯和物理安全

標準答案:D

下面哪一種日誌檔有助於評估電腦安全事例的危害程度？

選項:

- A、聯絡日誌
- B、活動日誌
- C、事件日誌
- D、審計日誌

標準答案:C

下面哪一種說法的順序正確？

選項:

- A、脆弱性導致了威脅，然後威脅導致了風險
- B、風險導致了威脅，然後威脅導致了脆弱性
- C、脆弱性導致了風險，然後風險導致了威脅
- D、威脅導致了脆弱性，然後脆弱性導致了風險

標準答案:A

下列哪一種行為是互聯網上常見的攻擊形式？

選項:

- A、查找軟體設計錯誤
- B、猜測基於個人資訊的口令
- C、突破門禁系統闖入安全場地
- D、種植特洛伊木馬

標準答案:D

內聯網（Intranet）可以建立在一個組織的內部網路上，也可以建互聯網（internet）上，上面哪一條針對內聯網的控制在安全上是最弱的？

選項:

- A、用加密的通道傳輸資料
- B、安裝加密路由器
- C、安裝加密防火牆
- D、對私有 WWW 伺服器實現口令控制

標準答案:D

在一個無線局域網環境下，能用來保證有效資料安全的技術是哪一種？

選項:

- A、消息鑒定碼和無線變頻收發儀
- B、在不同的通道傳輸資料和消息鑒定碼
- C、在不同的通道傳輸資料和加密
- D、加密和無線變頻收發儀

標準答案:C

下面哪一種類型的反病毒軟體是最有效的？

選項:

- A、掃描
- B、活動監測
- C、完整性檢查
- D、種植疫苗

標準答案:C

消息在發送前，用發送者的私鑰加密消息內容和它的哈希（hash,或譯作：雜選、摘要）值，能夠保證：

選項:

- A、消息的真實性和完整性
- B、消息的真實性和保密性
- C、消息的完整性和保密性
- D、保密性和防抵賴性

標準答案:A

對每個字元和每一幀都傳輸冗餘資訊，可以實現對錯誤的檢測和校正，這種方法稱為：

選項:

- A、回饋錯誤控制
- B、塊求和校驗
- C、轉發錯誤控制
- D、迴圈冗餘校驗

標準答案:C

實施安全政策時,落實責任控制是很重要的一方面,在控制系統用戶的責任時下面哪一種情況有效性是最弱的?

選項:

- A、審計要求
- B、口令
- C、識別控制
- D、驗證控制

標準答案:B

最有效的防病毒控制是:

選項:

- A、在郵件伺服器上掃描 e-Mail 附件
- B、使用無毒的、清潔的、正版的光碟恢復系統
- C、卸掉軟碟驅動器
- D、附有每日更新病毒庫功能的線上病毒掃描程式

標準答案:D

拒絕服務攻擊損害了下列哪一種資訊安全的特性?

選項:

- A、完整性
- B、可用性
- C、機密性
- D、可靠性

標準答案:B

下列哪一種情況會損害電腦安全政策的有效性?

選項:

- A、發佈安全政策時
- B、重新檢查安全政策時
- C、測試安全政策時
- D、可以預測到違反安全政策的強制性措施時

標準答案:D

組織的安全政策可以是廣義的，也可以是狹義的，下面哪一條是屬於廣義的安全政策？

選項:

- A、應急計畫
- B、遠端辦法
- C、電腦安全程式
- D、電子郵件個人隱私

標準答案:C

在傳輸模式中，使用封裝的安全載荷(ESP, Encapsulating Security Payload)協議比認證頭(AH)協議更有優勢，原因是 ESP：

選項:

- A、提供了無連接的完整性
- B、能驗證資料來源
- C、帶有防重放服務
- D、具備保密性

標準答案:D

在對資料中心進行審計時,審計師應當檢查電壓調整器是否存在,以保證:

選項:

- A、保護硬體設備免受浪湧損害
- B、如果主電力被中斷,系統的完整性也可以得到維護
- C、如果主電力被中斷,可以提供即時的電力供應
- D、保護硬體設備不受長期電力波動的影響

標準答案:A

下面哪一種小程序式(Applet)入侵類型會使組織面臨系統運行中斷的最大威脅？

選項:

- A、在客戶機上放置病毒程式
- B、能記錄用戶擊鍵行為，收集口令的小程式
- C、從網下載的能讀硬碟檔的代碼
- D、可以從客機建立網路連接的小程式

標準答案:D

虛擬專用網（VPN）提供以下哪一種功能？

選項:

- A、對網路嗅探器隱藏資訊
- B、強制實施安全政策
- C、檢測到網路錯誤和用戶對網路資源的濫用
- D、制定訪問規則

標準答案:A

基本的電腦安全需求不包括下列哪一條：

選項:

- A、安全政策和標識
- B、絕對的保證和持續的保護
- C、身份鑒別和落實責任
- D、合理的保證和連續的保護

標準答案:B

公共密鑰體系（PKI）的某一組成要素的主要功能是管理證書生命週期，包括證書目錄維護，證書廢止列表維護和證書發佈這個要素是：

選項:

- A、證書機構（CA）
- B、數字簽名
- C、證書實踐聲明
- D、註冊機構（RA）

標準答案:D

非授權用戶或外部人員（例如駭客）可以通過公共電話撥入網路，不斷地嘗試系統代碼、用戶身份識別碼和口令來獲得對網路的訪問許可權。這種“暴力破解”的方法一般在什麼情況下有效？

選項:

- A、非授權用戶在嘗試一定數量的口令猜測後，會被系統自動斷開
- B、使用常用字符和個人相關資訊作為口令
- C、用戶身份識別碼和口令有各種大量的可能性組合
- D、所有登錄企圖被記錄下來，並妥善保護

標準答案:B

下面哪一種方法在保護系統免受非授權人員的訪問時可以提供最高級安全？

選項:

- A、加密
- B、電話回叫或撥號回叫系統
- C、含有個人身份識別碼的磁卡
- D、用戶身份別碼和口令

標準答案:A

為保證正常運行的電腦系統能被連續使用，用戶支援服務是很重要的，下面哪一種情況與用戶支援服務比較接近？

選項:

- A、事件處理能力
- B、配置管理
- C、存儲介質控制
- D、系統備份

標準答案:A

無線局域網比有線局域網在哪方面具有更大的風險？

選項:

- A、偽裝和修改/替換
- B、修改/替換和設備失竊
- C、竊聽和偽裝
- D、竊聽和盜竊設備

標準答案:B

軟體編程人員經常會生成一個直接進入程式的入口，其目的是進行調試和（或）日後插入新的程式碼。這些入口點被稱為：

選項:

- A、邏輯炸彈
- B、蠕蟲
- C、陷門
- D、特洛伊木馬

標準答案:C

下面哪一種安全技術是鑒別用戶身份的最好的方法？

選項:

- A、智能卡
- B、生物測量技術
- C、挑戰--回應權杖
- D、用戶身份識別碼和口令

標準答案:B

對公司內部網路實施滲透測試時，如下哪一種方法可以確保網路上的測試人始終不被發覺？

選項:

- A、使用現有的檔伺服器或網域控制器的 IP 位址發起測試
- B、每掃描幾分鐘暫停一會兒，以避免達到或超過網路負載極限
- C、在沒有人登陸的夜間實施掃描
- D、使多種掃描工具，多管齊下

標準答案:B

哪一個最能保證來自互聯網 internet 的交易事務的保密性？

選項:

- A、數字簽名
- B、數位加密標準（DES）
- C、虛擬專用網（VPN）
- D、公鑰加密（Public Key encryption）

標準答案:D

虛擬專用網（VPN）的資料保密性，是通過什麼實現的？

選項:

- A、安全介面層（SSL，Secure Sockets Layer）
- B、網路隧道技術（Tunnelling）
- C、數字簽名
- D、網路釣魚

標準答案:B

下面的哪一種反垃圾過濾技術可以最大程度地避免正常的、長度不定的、內容裏存在多處垃圾郵件關鍵字的電子郵件被識別為垃圾郵件？

選項:

- A、啓發式的過濾技術
- B、基於簽名的檢查
- C、模版匹配
- D、基於統計（學）的貝葉斯判斷（Bayesian）

標準答案:D

下面哪一種屬於網路上的被動攻擊？

選項:

- A、消息篡改
- B、偽裝
- C、拒絕服務
- D、流量分析

標準答案:D

網路上資料傳輸時，如何保證資料的保密性？

選項:

- A、資料在傳輸前經加密處理
- B、所有消息附加它哈希值
- C、網路設備所在的區域加強安全警戒
- D、電纜作安全保護

標準答案:A

生物測試安全控制設備的最佳量化性能測量指標是：

選項:

- A、錯誤拒絕率
- B、錯誤接受率
- C、平均錯誤率
- D、估計錯誤率

標準答案:C

下面哪一條措施不能防止資料洩漏？

選項:

- A、數據冗餘
- B、數據加密
- C、訪問控制
- D、密碼系統

標準答案:A

軟體的盜版是一個嚴重的問題。在下面哪一種說法中反盜版的政策和實際行為是矛盾的？

選項:

- A、員工的教育和培訓
- B、遠距離工作（Telecommuting）與禁止員工攜帶工作軟體回家
- C、自動日誌和審計軟體
- D、政策的發佈與政策的強制執行

標準答案:B

如果一台可攜式電腦丟失或被盜，管理人員最關注的是機密資訊是否會暴露。要保護存放在可攜式電腦上的敏感資訊，下面哪一條措施是最有效的和最經濟的？

選項:

- A、用戶填寫情況簡要介紹
- B、簽署確認用戶簡要介紹
- C、可移動資料存儲介質
- D、在存儲介質上對資料檔案加密

標準答案:C

IS 審計師檢查日誌檔中的失敗登陸的嘗試，那麼，最關注的帳號是：

選項:

- A、網路管理員
- B、系統管理員
- C、資料管理員
- D、資料庫管理員

標準答案:B

長遠來看，最有可能改善安全事件反應程式的選項是：

選項:

- A、通盤檢查事件反應程式和流程
- B、事件反應小組的事後檢查、回顧
- C、對用戶不斷地安全培訓
- D、記錄對事件的反應過程

標準答案:B

下面哪一種關於安全的說法是不對的？

選項:

- A、加密技術的安全性不應大於使用該技術的人的安全性
- B、任何電子郵件程式的安全性不應大於實施加密的電腦的安全性
- C、加密演算法的安全性與密鑰的安全性一致
- D、每個電子郵件消息的安全性是通過用標準的非隨機的密鑰加密來實現

標準答案:D

在公共密鑰加密系統中，註冊中心（RA，Registration Authority）負責：

選項:

- A、驗證證書請求相關的資訊
- B、驗證所必需的屬性，並生成密鑰（指密鑰對）之後發放證書
- C、對消息進行數位簽名，以實現防抵賴的特性
- D、登記簽名的消息，保護它避免抵賴

標準答案:A

下面哪一種方式，能夠最有效的約束雇員只能履行其分內的工作？

選項:

- A、應用級訪問控制
- B、數據加密
- C、卸掉雇員電腦上的軟碟和光碟驅動器
- D、使用網路監控設備

標準答案:A

一家 B2C 電子商務網站的資訊安全程式要求能夠監測和預防駭客的活動，一時有可疑行為即警示系統管理員。下面的哪個系統元件可以實現這個目標？

選項:

- A、入侵監測系統（IDS）
- B、防火牆

- C、路由器
- D、不對稱加密

標準答案:A

跨國公司的 IS 經理打算把現有的虛擬專用網（VPN，virtual private network）升級，採用通道技術使其支援語音 IP 電話（VOIP，voice-over IP）服務，那麼，需要首要關注的是：

選項:

- A、服務的可靠性和品質（Qos,quality of service）
- B、身份的驗證方式
- C、語音傳輸的保密
- D、資料傳輸的保密

標準答案:A

建立資料所有權關係的任務應當是下列哪一種人的責任？

選項:

- A、職能部門用戶
- B、內部審計人員
- C、資料處理人員
- D、外部審計人員

標準答案:A

重新配置下列哪一種防火牆類型可以防止內部用戶通過檔傳輸協議（FTP）下載檔？

選項:

- A、電路閘道
- B、應用閘道
- C、包過濾
- D、遮罩式路由器

標準答案:B

下面哪一種安全措施可以允許調查人員有足夠的反應時間？

選項:

- A、阻止
- B、檢測

- C、拖延
- D、拒絕

標準答案:C

處理電腦犯罪事件需要運用管理團隊的方法，下面哪一個角色的職責是明確的？

選項:

- A、經理
- B、審計人員
- C、調查人員
- D、安全負責人

標準答案:A

從電腦安全的角度看，下面哪一種情況是社交工程的一個直接的例子：

選項:

- A、電腦舞弊
- B、欺騙或脅迫
- C、電腦偷竊
- D、電腦破壞

標準答案:B

在業務連續性計畫（BCP）中，下面哪個求救電話目錄是最重要的？

選項:

- A、先聯繫設備供應商和電力、通訊等資源
- B、先聯繫保險公司
- C、先聯繫人力仲介公司
- D、已排定優先順序的聯絡表（緊急救援電話表）

標準答案:D

在提供備份電腦設備方面，下面哪一種情況是成本最低的？

選項:

- A、互助協議
- B、共用設備
- C、服務機構
- D、公司擁有的鏡像設備

標準答案:A

業務連續性計畫（BCP）的哪個部分，是企業 IS 部門的主要責任？

選項:

- A、制定業務連續性計畫
- B、選定、批准業務連續性計畫的相關戰略
- C、遇災報警
- D、災後恢復 IS 系統和資料

標準答案:D

審計涵蓋關鍵業務領域的災難恢復計畫時，IS 審計師發現該計畫沒有包括全部系統。那麼，IS 審計師最為恰當的處理方式是：

選項:

- A、推遲審計，直到把全部系統納入 DRP
- B、知會領導，並評估不包含所有系統所帶來的影響
- C、中止審計
- D、按照現有的計畫所涵蓋的系統和範圍繼續審計，直到全部完成

標準答案:B

一個組織的資料中心的成本是 10000000 美元，實際遭受損失的機率是萬分之一。資料中心登記在冊的價值是 5000000 美元。在零利潤現價交易條件下，這個組織需要付給保險公司的最小保險費是多少？

選項:

- A、1000 美元
- B、10000 美元
- C、5000 美元
- D、500 美元

標準答案:A

局域網環境下與大型電腦環境下的本地備份方式有什麼主要區別？

選項:

- A、主要結構
- B、容錯能力
- C、網路拓撲
- D、局域網協定

標準答案:B

根據組織業務連續性計畫的複雜程度，可以建立多個計畫來滿足業務連續和災難恢復的各方面。在這種環境下，有必要：

選項:

- A、每個計畫都與其他計畫相協調
- B、所有計劃都整合到一個計畫中
- C、每個計畫都獨立於其他計畫
- D、指定所有計劃實施的順序

標準答案:A

在災難發生期間，下列哪一種應用系統應當首先被恢復？

選項:

- A、總賬系統
- B、供應鏈系統
- C、固定資產系統
- D、客戶需求處理系統

標準答案:D

關於冷站的電腦設備的組成，下面哪一種說法不正確？

選項:

- A、加熱系統，濕度控制和空調設備
- B、CPU 和其他電腦設備
- C、電源連接
- D、通訊連接

標準答案:B

由於資料檔案的損壞，存儲在異地備份設備上的資訊經常要恢復到本地站點（主電腦）上去，能快速簡易地從備份站點傳送所需備份資訊到本地主電腦設備上去的機制稱為：

選項:

- A、特殊急件信差
- B、常規急件信差
- C、電子保險庫
- D、特殊信使

標準答案:C

一家大型銀行實施 IT 審計的過程中，IS 審計師發現許多業務應用沒有執行正規的風險評估，也沒有確定其重要性和恢復時間上的要求。那麼，這些暴露的銀行風險是：

選項:

- A、業務連續性計畫（BCP）可能沒有與銀行各應用被破壞的風險相對應
- B、業務連續計畫（BCP）可能沒有包含所有相關應用，因此，在範圍上不完整
- C、領導或許沒有正確認識災難對業務的影響
- D、業務連續性計畫（BCP）或許缺少有效的業務所有者關係

標準答案:A

微型電腦上的軟體和資料是否要保存到異地備份站點主要取決於：

選項:

- A、訪問的簡便性
- B、風險評估
- C、完備的標籤
- D、完備的文檔

標準答案:B

企業目前磁帶備份，每週一次全備份、每日一次增量備份的策略。最近，企業領導把磁帶備份流程中增加了向磁片備份的步驟。這種做法之所以恰當，是因為：

選項:

- A、它支援非現場存儲的快速合成備份
- B、向磁片備份的速度遠快于向磁帶備份
- C、隨著技術的進步，不再需要磁帶庫
- D、資料保存在磁片上，其可靠性高於磁帶存儲

標準答案:A

審計 BCP 時，IS 審計師發現儘管所有部門都位於同一棟大樓裏，各部門還是制定了本部門的 BCP。IS 審計師建議將各 BCP 協調統一起來，那麼，首先要統一的是：

選項:

- A、疏散和撤離計畫

- B、恢復的優先順序
- C、備份存儲 (Backup storages)
- D、電話表 (Call tree)

標準答案:A

制訂業務連續性計畫時，下面哪一類工具可以用於瞭解各企業的業務流程？

選項:

- A、業務連續性自我審計
- B、資源恢復分析
- C、風險評估
- D、差異分析

標準答案:C

制訂業務連續性計畫的第一步，也是必不可少的一步是：

選項:

- A、根據風險將應用系統分類
- B、羅列出所有資產的清單
- C、完整地記錄所有災難
- D、軟體和硬體的可用性

標準答案:A

下面哪一條是資訊系統審計師主要考慮的問題？

選項:

- A、備份站點是否有一個“誘捕陷阱”
- B、備份站點是否有安全保衛人員
- C、備份站點與主站點間是否有一段合理的距離
- D、備份站點是否是一個服務機構

標準答案:C

IS 審計師發現企業的業務連續性計畫中選定的備用處理設施的處理能力只能達到現有系統的一半。那麼，他/她該怎麼做？

選項:

- A、無需做什麼。因為只有處理能力低於正常的 25%，才會嚴重影響企業的生存和備份能力

- B、找出可以在備用設施使用的應用，其他業務處理採用手工操作，制訂手工流程以備不測
- C、找出所有主要的應用，確保備用設施可以運行這些應用
- D、建議相關部門增加備用設施投入，使其能夠處理 75%的正常業務

標準答案:C

在制定災難恢復與應急計畫時，下面哪一種情況不是正確的考慮？

選項:

- A、對應急計畫測試與維護應當是一個持續過程
- B、在異地恢復站點恢復系統處理能力時要用到的所有資源與材料應當是可獲得的
- C、所有相對不重要的工作沒有必要恢復
- D、在多個站點的環境下，應當為每一個電腦中心制定一份單獨的恢復計畫

標準答案:C

能涵蓋損失的最好的保險單類型是：

選項:

- A、基本保險單
- B、擴展保險單
- C、特殊的涵蓋所有風險的保險單
- D、與風險類型相稱的保險

標準答案:D

下面哪一種情況可以稱為“災難恢復計畫”的最後手段？

選項:

- A、與恢復中心的一份合同
- B、恢復中心的一份能力演示
- C、對恢復中心的走訪
- D、一份保險單

標準答案:D

如下哪一種情況下，網路資料管理協定（NDMP）可用於備份？

選項:

- A、需要使用網路附加存儲設備（NAS）時
- B、不能使用 TCP/IP 的環境中

- C、需要備份舊的備份系統不能處理的檔許可時
- D、要保證跨多個資料卷的備份連續、一致時

標準答案:A

當一個組織在選擇異地備份供應商時，對資訊系統審計師來說，下列哪一種情況是最少考慮的？

選項:

- A、供應商保密存儲介質的責任
- B、供應商的保險範圍及對員工的擔保
- C、要求同一個人一直保管存儲介質
- D、請求和接收貨物的程式和緊急情況下的處理方式

標準答案:C

IS 審計師發現被審計的企業，各部門均制訂了充分的業務連續性計畫（BCP），但是沒有整個企業的 BCP。那麼，IS 審計師應該採取的最佳行動是：

選項:

- A、各業務部門都有適當的 BCP 就夠了，無需其他
- B、建議增加、制訂全企業的、綜合的 BCP
- C、確定各部門的 BCP 是否一致，沒有衝突
- D、建議合併所有 BCP 為一個單獨的全企業的 BCP

標準答案:C

應急計畫能應對下列哪一種威脅？

選項:

- A、物理威脅和軟體威脅
- B、軟體威脅和環境威脅
- C、物理威脅和環境威脅
- D、軟體威脅和硬體威脅

標準答案:C

一聲火災蔓延到一個組織的機房場地，這個組織損失了所有的電腦系統。從前，這個組織最應該做的是：

選項:

- A、為冷站備份方式作戰計畫

- B、為互助協議作計畫--與其他相同的組織協商互為備份
- C、為熱站備份方式作計畫--使一切設備與資料準備就緒
- D、為異地存儲設備作每日備份

標準答案:D

當獲得高層管理人員對災難恢復計畫的支持和制定計劃所需資源的授權後，選擇起草計畫的人應當具有以下哪一種能力：

選項:

- A、具有與資訊系統相關的作業系統、資料庫和通訊的技術知識
- B、具有硬體和軟體供應商諮詢背景
- C、具有在相同行業中的客戶諮詢經驗
- D、具有組織的全局觀點和認識所有災難後果的能力

標準答案:D