

範疇 1—電腦稽核程序(14%)

按照電腦稽核標準，提供稽核服務，以協助組織保護和控制資訊系統。

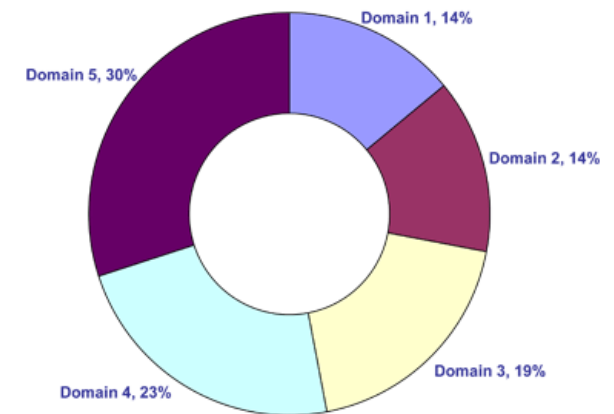
工作說明

- 發展及建置一個以風險為基礎之電腦稽核策略以遵循電腦稽核標準與確保其包含關鍵的範圍。
- 進行具體稽核計畫以確定資訊系統受到保護、控制與提供組織價值。
- 依照資訊稽核標準、指引與最佳實務進行稽核以符合稽核計畫的目標。
- 與利害關係人溝通新出現問題、潛在風險及稽核結果。
- 建議組織有關實施風險管理與控制的做法，並持續保持獨立性。

知識範疇

- 瞭解 ISACA 電腦稽核與確認的標準、指引、工具、技術、職業道德和其他適用之標準。
- 瞭解稽核環境下風險評鑑的概念、工具與技術。
- 瞭解資訊系統的控制目標和相關控制措施。
- 瞭解稽核計畫和稽核專案管理技術。
- 瞭解企業基本流程(如：採購、薪資、應付帳款、應收帳款)中有關 IT 的知識。
- 瞭解適用的法律與法規，與其影響範圍、證據搜集、保存與稽核頻率。
- 瞭解搜集證據的技術(如：觀察、調查、檢查、訪談、資料分析)並實際用於搜集、保存與保護稽核證據。

CISA Certification Job Practice Areas by Domain



- 瞭解不同的抽樣方法論。
 - 瞭解報告與溝通的技術。(如：促進、談判、解決衝突、報告的結構)
 - 瞭解稽核品質保證系統與框架。
-

範疇 2—資訊治理與管理(14%)

提供必要的領導力、組織結構和流程使能達到組織目標與支持其策略。

工作說明

- 評估資訊治理架構的成效以確認其決策、方向和績效是否支持組織的策略與目標。
- 評估資訊組織結構與人力資源(員工)管理是否支持組織的策略和目標。
- 評估資訊的策略，包含：資訊方向和策略的發展、核准、建置和維護流程與組織策略和目標的一致性。
- 評估組織的資訊政策、標準、程序和它的發展、核准、建置、維護、監控流程是否支持資訊策略和遵循規範和法規需求。
- 評估品質管理系統的適當性，在符合成本效益的方式下是否支持組織的策略和目標。
- 評估資訊管理和監控的控制項(如：持續監控、品質保證)符合組織的政策、標準和程序。
- 評估資訊資源的投入、使用和配置方式(包含：優先順序的標準)與組織策略和目標相符。
- 評估資訊承攬合約的策略、政策與合約管理做法是否支持組織的策略和目標。
- 評估風險管理做法以確認組織的資訊相關風險是否被妥善的管理。
- 評估監控和確保的做法以確認董事會及高階管理階層收到充份與即時的資訊績效訊息。

- 評估組織的營運持續計畫以確認組織在資訊服務中斷時的基本營運持續能力。

知識範疇

- 瞭解資訊治理、管理、安全和控制框架與其相關的標準、指引和實務。
- 瞭解組織的資訊策略、政策、標準、程序與每一必要元素的目的。
- 瞭解組織結構和與資訊相關的角色與職責。
- 瞭解資訊策略、政策、程序的發展、建置和維護的流程。
- 瞭解組織的技術方向、資訊架構和其設定長遠戰略方向的影響。
- 瞭解相關法律、法規和行業標準對組織的影響。
- 瞭解品質管理系統。
- 瞭解成熟度模型的運用。
- 瞭解最佳化技術的流程。
- 瞭解資源投資與分配的做法，包含：優先順序的標準(如：組合管理、價值管理、專案管理)。
- 瞭解資訊供應商的選擇、合約管理、關係管理與績效監控流程，其中包含與第三方外包的關係。
- 瞭解企業風險管理。
- 瞭解資訊績效監控和報告的做法。(如：平衡計分卡、關鍵績效指標[KPI])
- 瞭解資訊人力資源(員工)管理做法用於施行營運持續計畫。
- 瞭解營運衝擊分析(BIA)與營運持續計畫的相關性。
- 瞭解發展和維護營運持續計畫與測試方法的標準和程序。

範疇 3—資訊系統的取得、發展、建置(19%)

確保資訊系統的取得、發展、測試及建置實務符合組織的策略與目標。

工作說明

- 評估業務需求所建議投入資訊系統的取得、發展、維護和淘汰是否符合企業目標。
- 評估專案管理做法與控制是否符合企業成本效益需求的考量並管理了組織的風險。
- 實施檢視以確定專案進度是否依照計畫進行，並有足夠的相關文件和報告證明。
- 評估資訊系統的需求、取得、發展及測試的控制面向符合組織政策、標準、程序與適用外部的需求。
- 評估資訊系統實施與轉移到正式環境的準備作業，是否符合專案可交付成果、控制與組織的需求。
- 進行系統建置後的審查，確認是否符合專案可交付成果、控制與組織需求。

範疇 3—知識範疇

- 瞭解效益實現的作法。(如：可行性研究、企業案例、總擁有成本[TCO]、投資回報率[ROI])
- 瞭解專案治理的機制。(如：指導委員會、專案監督委員會、專案管理辦公室)
- 瞭解專案管理控制框架、實踐與工具。
- 瞭解專案中風險管理的做法。
- 瞭解與資訊結構相關的資料、應用及技術。(如：分散式應用系統、以網頁為基礎的應用系統、網路服務、多層次應用系統)

- 瞭解取得資訊系統的做法。(供應商評估、供應商管理與託管)
 - 瞭解需求分析與管理的做法。(如：需求驗證、追溯、差異分析、弱點管理、安全需求)
 - 瞭解專案成功標準與風險。
 - 瞭解控制目標和技術以確保交易資料的完整性、準確性、有效性與授權的交易和資料。
 - 瞭解系統發展方法論和工具，包含它的長處和弱點。(如：敏捷開發法、雛型法、快速應用開發[RAD]、物件導向設計技術)
 - 瞭解資訊系統開發的測試方法論和實踐做法。
 - 瞭解與資訊系統發展有關的組態與發布管理。
 - 瞭解系統轉移、基礎設施佈署的做法、資料轉換工具、技術與程序。
 - 瞭解系統建置後的目標審查與做法。(如：專案結案、控制實行，效益實現，績效評估)
-

範疇 4—資訊系統的營運、維護及支持(23%)

確保資訊系統的營運、維護及支持流程符合組織的策略與目標。

工作說明

- 定期審查資訊系統以確認是否持續符合組織目標。
- 評估服務等級管理的做法以確認內外部提供之服務等級已被定義及管理。
- 評估第三方管理的做法以確認由提供商遵循的控制等級符合組織之預期。
- 評估系統與使用者的程序以確認被排程和未排程的流程已完成管理。

- 評估資訊系統維護流程以確認其控制的有效性與持續性支持組織目標。
- 評估數據管理的做法以確認其完整性與資料庫的最佳化。
- 評估使用容量與效能的監控工具和技術以確認資訊服務是否符合組織目標
- 評估問題和事件管理的做法以確認事件、問題或錯誤已即時紀錄、分析和解決。
- 評估變更、組態和發布管理的做法以確認對於組織正式環境的排程和未排程的變更得到充分的控制與紀錄。
- 評估是否有足夠的備份和復原準備以確認所需的資料可獲得處理。
- 評估組織的災難復原計畫以確認災難事件發生時資訊處理能力的回復可被啟用。

知識範疇

- 瞭解在服務等級協議中對服務等級管理的做法與其要素。
- 瞭解監控第三方遵循組織內部控制的技術。
- 瞭解系統和使用者程序已被排程和未排程之流程所管理。
- 瞭解硬體、網路元件、系統軟體和資料庫管理系統的相關技術概念。
- 瞭解確保系統介面完整性的控制技術。
- 瞭解軟體授權與盤存的作法。
- 瞭解系統恢復的工具與技術。(如：硬體容錯、單點故障消除、叢集)
- 瞭解資料庫管理的作法。
- 瞭解容量規劃和相關的監控工具與技術。
- 瞭解系統效能監控流程、工具和技術。(如：網路分析、系統使用率報告、負載平衡)

- 瞭解問題與事件管理的做法。(如：服務台、問題升級處理程序、追蹤)
 - 瞭解對正式系統和(或)基礎設施之排程與未排程之管理程序，包含變更、組態、發布和修補補丁的管理做法。
 - 瞭解資料備份、儲存、維護、保留和恢復的做法。
 - 瞭解災難復原相關的法規、法律、合約與保險議題。
 - 瞭解營運衝擊分析[BIA]與災難復原計畫間之關係。
 - 瞭解災難復原計畫的發展與維護。
 - 瞭解備援場所的類型與方法並用於監控合約協議。(如：熱備援、暖備援、冷備援)
 - 瞭解災難復原計畫實行的程序。
 - 瞭解災難復原測試的方法。
-

範疇 5—資訊資產的保護(30%)

確保組織的安全政策、標準、程序和控制足以保證資訊資產的機密性、完整性與可用性。

工作說明

- 評估資訊安全政策、標準和程序的完整性與是否與普遍接受的做法一致。
- 評估系統設計、建置、監控和邏輯安全控制，以驗證資訊的機密性、完整性和可用性。
- 評估資料分類過程和流程的設計、建置和監控符合組織的政策、標準、程序且適用外部的需求。
- 評估實體存取與環境控制的設計、建置、監控以確認資訊資產已被充份保護。

- 評估用於資訊資產儲存、恢復、轉換、處理的流程與程序。(如：備份裝置、異地儲存、硬拷貝/資料列印、軟拷貝/媒體)以確保資訊資產已充份保護。

知識範疇

- 瞭解安全控制的設計、建置和監控技術，其中包含：安全意識方案。
- 瞭解安全事件監控與回應的相關流程。(如：問題升級處理程序、緊急事件回應小組)
- 瞭解資料邏輯存取控制的識別、授權和對於使用者授權的功能與資料的限制。
- 瞭解軟、硬體(如：應用程式、作業系統)和資料庫管理系統相關的安全控制。
- 瞭解虛擬化系統相關的風險和控制。
- 瞭解網路安全組態、建置、營運和維護的控制。
- 瞭解電腦網路和網際網路的安全設備、通訊埠與技術。
- 瞭解資訊安全攻擊手法和技術。
- 瞭解偵測工具和控制技術。(如：惡意程式、病毒偵測、間諜軟體)
- 瞭解安全測試技術。(如：入侵測試、弱點掃描)
- 瞭解資料外洩相關的風險與控制。
- 瞭解加密相關的技術。
- 瞭解公開金鑰基礎建設(PKI)元件和數位簽章技術。
- 瞭解與點對點計算、即時通訊、網頁技術相關的風險與控制。(如：社群網路、留言板、部落格)
- 瞭解使用移動和無線裝置的風險和控制。

- 瞭解語音通訊安全。(如：交換機[PBX]、網路電話[VoIP])
- 瞭解依數位證據調查中證據保存的技術與流程。(如：IT、流程、證據保管之連續性)
- 瞭解資料分類標準和配套的程序。
- 瞭解實體存取控制的識別、授權和限制與對於使用者授權設備的限制。
- 瞭解環境保護裝置與配套措施。
- 瞭解敏感性資訊資產儲存、恢復、轉換、處理的流程與程序。