2022 iPAS 資訊安全管理概論(初級) #112147

1. 使用專用帳號及密碼登入 CRM（Customer Relationship Management）系統，主要是基於下列何種原則？（A）可靠性（B）可用性（C）機密性（D）完整性
2. 高階管理階層（資安長）在資訊安全管理系統中所展現領導與承諾，「不」包含下列何項？（A）確保建立的資訊安全政策及資訊安全目標，必須與組織發展方向相容（B）整合人員、組織及提供所需的支援，確保資訊安 全管理系統的要求（C）向組織內部所有人員說明資訊安全產品的設定（D）確保資訊安全管理系統達成預期的成效
3. 請問資訊安全的定義是下列何項最正確？（A）保護資訊資產的機密性與完整性（B）保護資訊資產的完整性與可用性（C）保護資訊資產的機密性與可用性（D）保護資訊資產的機密性、完整性與可用性
4. 請問下列哪一種攻擊手法，最主要目的是讓合法授權的 使用者無法使用系統或網路資源？（A）社交工程（Social Engineering）（B）蠕蟲（Worm）（C）暴力破解(Brute-Force Attack)（D）拒絕服務(Denial-of-services)
5. 資訊安全管理系統遵照計畫(Plan)、執行(Do)、檢查（Check)及行動(Act)等四個程序，不斷的改進。請問「建立及執行管理程序」是屬於下列哪一個程序？（A）計畫（Plan）（B）執行（Do）（C）查核（Check）（D）行動（Act）
6. 下列何者「不」屬於特種個資？（A）性生活（B）病歷（C）健康檢查（D）指紋
7. 關於公務員假借職務上之權力、機會或方法，犯個人資料保護法所訂之罪者，加重刑罰的比例為下列何項？（A）加重其刑至五分之一（B）加重其刑至四分之一（C）加重其刑至三分之一（D）加重其刑至二分之一
8. 關於公務機關未遵守資通安全管理法規定的敘述，下列何者正確？（A）應按其情節輕重，依相關規定按次處新臺幣十萬 元以上一百萬元以下罰鍰（B）應按其情節輕重，依相關規定按次處新臺幣三十萬元以上五百萬元以下罰鍰（C）應按其情節輕重，依相關規定予以懲戒或懲處（D）應按其情節輕重，依相關規定按次處新臺幣三萬元以上五十萬元以下罰鍰
9. 關於資通安全管理法對於委託機關於委外辦理資通系統 之建置、維運或資通服務之提供，選任及監督受託者時，應注意「適任性查核」的敘述，下列何者錯誤？（A）應查核有無曾犯洩密罪，或於動員戡亂時期終止前，犯內亂罪、外患罪，經判刑確定，或通緝有案 尚未結案（B）應查核有無曾犯洩密罪，或於動員戡亂時期終止後，犯內亂罪、外患罪，經判刑確定，或通緝有案尚未結案（C）應查核有無曾受到外國政府之利誘、脅迫，從事不 利國家安全或重大利益情事（D）應查核有無曾受到大陸地區、香港或澳門政府

之利 誘、脅迫，從事不利國家安全或重大利益情事

10. 當某關鍵基礎設施提供者之核心業務資訊遭受嚴重之洩漏時，該關鍵基礎設施提供者就該資通安全事件通報的敘 述，下列何者錯誤？ (A) 知悉資通安全事件後應於一小時內進行資通安全事 件之通報 (B) 通報內容應包含為因應該事件所採取之措施 (C) 應於知悉該事件後三十六小時內完成損害控制或復 原作業 (D) 完成損害控制或復原作業候應持續進行事件之調查及處理並於二個月內送交調查處理及改善報告
11. 公務或非公務機關在進行個人資料蒐集時，應明確告知當事人事項，請問其告知內容「不」包含下列何項？ (A) 個人資料蒐集的目的 (B) 個人資料的類別 (C) 個人資料儲存方式 (D) 個人資料利用的期間與地區
12. 下列何者「不」屬於個人資料？ (A) 以直接方式識別該個人之資料 (B) 以間接方式識別該個人之資料 (C) 公司營業據點的地址 (D) 個人的出生年月日
13. 個人資料保護法主要是保護下列何種隱私？ (A) 資訊隱私 (B) 身體隱私 (C) 決定權隱私 (D) 物理空間隱私
14. 關於組織所擁有之較常見的資產分類，下列敘述何者錯誤？ (A) 可區分為資訊類資產 (B) 可區分為軟體類資產 (C) 可區分為韌體類資產 (D) 可區分為硬體類資產
15. 關於實施「資訊分類」作業主要目的之敘述，下列何者最正確？ (A) 防止儲存在媒體的資訊被經授權的移除 (B) 防止儲存在媒體的資訊被經授權的揭露 (C) 確保組織重要的資訊受到適切等級的保護 (D) 確保公開的資訊受到適切等級的保護
16. 關於資訊資產控管原則，下列敘述何者正確？ (A) 關鍵系統設備不需建立備援機制 (B) 網路設備不用建立備用系統 (C) 個人使用之套裝軟體，其存取權限的賦予，應與使 用者的角色與職責相符 (D) 公開資料未經權責主管之授權核可，禁止複製
17. 通常資訊類的資產分級，可區分為公開、內部使用以及密 級等三種，關於資訊類資產分級為「密級」之敘述，下列 何者錯誤？ (A) 若流傳至組織外部，不會對組織造成任何有形或無形的傷害 者 (B) 資料外洩可能造成個人與組織之困擾，造成聲譽受損或財務損失者 (C) 含有病例、醫療、基因、性生活、健康檢查及犯罪前科等之個人資料之資訊，僅有經過授權之人員始得存取者 (D) 含有可直接或間接識別特定個人之未公開個人資料
18. 關於紙本類之資訊資產保護原則，下列敘述何者最「不」正確？ (A) 內部使用級之紙本類資訊資產，於保管人員暫時離開座位時，不得置於開放空間處 (B) 內部使用級之紙本類資訊資產，於保管人員長時間離開座位時，應放置於上鎖空間或上鎖櫃並隨時上鎖 (C) 密級之紙本類資訊資產，於保管人員暫時離開座位時，得置於開放空間處 (D) 密級之紙本類資訊資產，於保管人員進出上鎖空間或借用上鎖櫃之鑰匙時應作成紀錄

19. 關於資產盤點之執行方式，下列敘述何者最「不」正確？（A）所有軟體類資產之盤點可藉由軟體掃描工具來輔助執行（B）所有硬體類資產之盤點可藉由軟體掃描工具來輔助執行（C）所有資訊類資產之盤點可藉由檔案搜尋工具來輔助執行（D）所有人員類資產之盤點可藉由組織架構與業務職掌表來輔助執行
20. 資訊安全管理系統（Information Security Management System, ISMS）中，電力供應是屬於下列何種資產類型？（A）服務資產（B）資訊資產（C）硬體資產（D）軟體資產
21. 下列敘述何者符合風險移轉？（A）投保機房火險（B）建立備援網路系統（C）停止網路平台交易業務（D）增加開啟系統權限的簽核流程
22. 關於風險評鑑管理程序，下列敘述何者「不」正確？（A）建立全景係界定風險評鑑範圍（B）詳細風險評鑑包括風險識別、風險分析與風險評 估（C）風險處理若合意，則進入風險接受階段（D）風險評鑑若不合意，則進入風險溝通階段
23. 下列何者的處理方式無法降低風險？（A）風險避免(Risk avoidance)（B）風險保留(Risk retention)（C）風險修改(Risk modification)（D）風險分擔(Risk sharing)
24. 為了降低風險，下列何者最「不」是實施風險控制措施的考量因素？（A）法規要求與限制（B）組織的目標與規範（C）實施的可能成本（D）資訊資產類別
25. 下列何者是「殘餘風險」(Residual Risk）的敘述？（A）單位可以承受的風險（B）沒有被識別的風險（C）已經被識別，但是沒有指定處置方法的風險（D）執行風險處理措施後，還殘留下來的風險
26. 無人看守設備（Unattended Equipments），如系統主機、無人看管的通訊設備，皆存在著可能被錯誤使用、竊取的風險。下列何者較「無」關於無人看守設備應注意事項？（A）若為封閉場所，可以加裝門鎖保護（B）若為開放場所，可以加裝監視器加以監控（C）加裝滅火器（D）設定螢幕保護或使用密碼
27. 公司 ERP（Enterprise Resource Planning）系統針對不同職務功能給予不同權限的目地，與下列何項關聯性較 高？（A）機密性、完整性（B）可用性、完整性（C）機密性、可用性（D）機密性、可用性、完整性
28. 門禁卡與機房進出需要特定密碼控制實體出入，是下列哪一個目的？（A）偵測性（B）指導性（C）預防性（D）嚇阻性
29. 關於特權帳號管理與控制中需要特別注意的項目，下列何者錯誤？（A）特權帳號登入時間、頻繁次數（B）留下詳細的必要軌跡，每日進行盤點與稽核（C）使用雙授權的管理機制，增加控制點（D）避免特權帳號分散，帳號密碼應該共用，便於管理
30. 以現行科技發展而言，下列何種生物特性較「不」適合拿來作為身份鑑別使

用？（A）指紋（B）虹膜（C）臉部特徵（D）身高

31. 關於生物辨識錯誤型態的敘述，下列何者正確？（A）錯誤接受（False Acceptance）發生時，會拒絕正確使用者進入（B）交叉錯誤率（Crossover Error Rate, CER）發生時為第一型錯誤率等於第二型錯誤率（C）對存取控制來說第一型錯誤發生時比第二型錯誤 嚴重（D）視網膜與虹膜辨識的 CER 最高

32. 如附圖所示，使用帳號及通關密碼（Password）來登入資訊系統，為了確保安全起見，必須採取何項措施？（A）(1)、(2)、(3)（B）(1)、(2)、(4)（C）(1)、(3)、(4)（D）(2)、(3)、(4)

(1)密碼長度不宜太短 (2)不可以使用懶人密碼，例如 1234 (3)系統管理員統一設定帳號密碼並不允許更改密碼 (4)使用者離職後，其登入全線必須立即停止

33. 關於 AD（Active Directory）與 LDAP（Light-weighted Data Access Protocol）兩者比較的敘述，下列何者正確？（A）AD 是用來交談的協議，也就是目錄資料的協議 規範（B）LDAP 是一目錄服務，通過 IP 協議提供訪問控制 和維護分布式資訊（C）AD 網域的基本物件包含了 Domain Controllers、 Computers、Builtin、Users（D）LDAP 提供唯讀型網域控制站的網域控制站角色

34. 某位安全性分析師負責整合企業的單一登入（Single Sign-On, SSO）解決方案，解決方案需要採用開放性的標準，並且在許多不同網頁應用程式間交換認證及授權訊息，下列何者為分析師最應提出的建議方案？（A）RADIUS（B）SAML（C）TACACS +（D）XTACACS

35. 公司的簽到系統是採用動態行為特徵「簽名辨識」(在電子筆上加裝感應器)，但某日員工 Alex 因為慣用右手受傷，改用左手簽名，卻一樣可以通過辨識簽到系統，請問安全管理人員得知此狀況後，該如何處理？（A）將簽到系統的敏感度調高，以降低錯誤拒絕率（False Rejection Rate）（B）將簽到系統的敏感度調低，以提高錯誤拒絕率（False Rejection Rate）（C）將簽到系統的敏感度調高，以降低錯誤接受率（False Acceptance Rate）（D）將簽到系統的敏感度調低，以提高錯誤接受率（False Acceptance Rate）

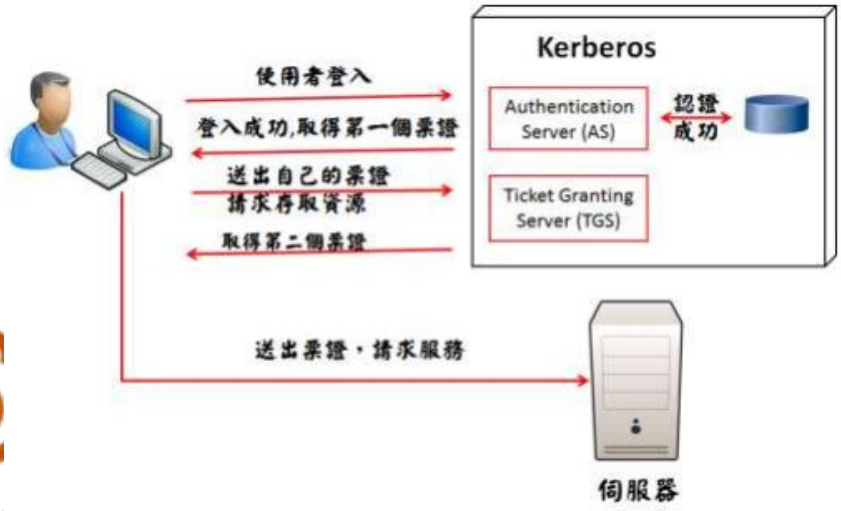
36. 關於密碼學(Cryptography)所能達成之主要目的，下列何項錯誤？（A）機密性（confidentiality）（B）完整性（Integrity）（C）可用性（Availability）（D）不可否認性（Non-Repudiation）

37. 關於金鑰生命週期管理（Key Management Lifecycle），於儲存階段之最佳實務的敘述，下列何項錯誤？（A）金鑰不應以明文形式（Plaintext）進行儲存（B）金鑰若留存於系統記憶體（Memory）中，其暫存特 性能達成保護目的（C）金鑰離線儲存須以「金鑰加密密鑰」(Key Encryption Keys）加

密保護 (D) 金鑰應儲存於密碼庫 (Cryptographic Vault)，如：硬體安全模組 (HSM, Hardware Security Module)

38. 量子電腦運算 (Quantum Computing) 技術日益成熟，其 對於現代密碼學影響的敘述，下列何項錯誤？ (A) 非對稱密碼學(Asymmetric Cryptography) 可被有效破解 (B) 對稱式密碼學 (Symmetric Cryptography) 面臨巨大 風險而需全數汰換 (C) 後量子密碼學 (Post-Quantum Cryptography) 可抵抗量子電腦運算優勢 (D) CRYSTALS-Kyber, FALCON, Classic McEliece 皆為 後量子密碼學演算法

39. 附圖為 Kerberos 的簡略認證過程，圖中使用者取得的二個票證(Tickets)，依序分別為下列何種票證？(A) Ticket-granting Ticket (TGT)、Service Ticket (ST) (B) Service Ticket (ST)、Ticket-granting Ticket (TGT) (C) Master Ticket (MT)、Service Ticket (ST) (D) Client Ticket (CT)、Server Ticket (ST)



40. 下列何種機制「不」可用於加密及解密？ (A) AES (Advanced Encryption Standard) (B) DES (Data Encryption Standard) (C) RSA (Rivest-Shamir-Adleman) (D) MD5 (Message-digest algorithm)

41. 關於安全事件管理的敘述，下列何者錯誤？ (A) 藉由完整的資安管理制度密切掌握重要服務的日誌現況 (B) 良好的安全資訊與事件管理機制應達到法規遵循以及威脅管理兩個主要目標 (C) 風險矩陣:定義事件類別風險係數及設備服務重要性賦予資產價值 (D) OSSIM 是一個常見商業化之安全資訊管理系統

42. 依據「資通安全事件通報及應變辦法」，主管機關於接獲通報後，若判定為 1 級或 2 級事件，應於幾小時內完 成審核？ (A) 2 小時 (B) 4 小時 (C) 8 小時 (D) 12 小時

43. 常常聽到不同設備集中管理的資安事件整合系統 SIEM，SIEM 的原文為下列何項？ (A) Security Information and Event Management (B) System Incident and Escalation Management (C) Server Integration and Event

Management (D) System Integration and Escalation Management

44. 若為重大資訊安全事件，於處理完畢且獲得妥善控制 後，為落實預防管理及確保資訊安全事件不再重複發生，必須研析問題發生之原因，該由下列何者指派專人 召集相關單位召開資訊安全事件檢討會議？ (A) 資安事件處理小組組長 (B) 資訊安全工程師 (C) 資訊安全長 (D) 資安稽核組長

45. 關於企業組織遭遇 DoS 或 DDoS 攻擊的常見特徵，下 列何者錯誤？ (A) 網路頻寬滿載 (B) 網通設備或防火牆不堪負載 (C) 電腦與伺服器作業系統或服務超載 (D) 網站內容只有影片無法播放

46. 公司採單次租賃方式建立熱備援測試站點，並定期進行災害復原計畫測試，每次測試完成後，在離開測試的熱 備援站點前，應先確定下列何項活動？ (A) 執行管理審查會議，提供測試建議報告給供應商 (B) 確定測試中殘餘的風險與需修正的步驟 (C) 清理熱備援站點內公司的所有測試資料 (D) 執行根本原因分析，確定測試評估報告

47. 下列何種情況，最應該建立線上即時備援系統？ (A) 承諾客戶須提供 7*24*365 的不中斷線上平台服 務 (B) 公司資安目標要求，非電信商因素網路中斷不可 超過 2 小時 (C) 營運衝擊分析結果，ERP 系統評估為具有高衝擊性 (D) 風險評估結果，防火牆被列入高風險項目

48. 營運持續的過程中，在(甲)備援中心將重要服務回復 至最低可接受水準，與最後於(乙)原地重建之階段。其重啟服務順序應為下列何項？ (A)(甲)(乙)都先回復最重要系統 (B) (甲)最重要系統先回復 (乙)最重要系統最後才回復 (C) (甲)最重要系統最後才回復 (乙)最重要系統 先回復 (D) (甲)(乙)最重要系統都最後才回復

49. 下列何者是組織建立備援機制的首要步驟？ (A) 建立相關備援機制的政策 (B) 建立多個位於不同地點的機房 (C) 購置最新的網路安全設備 (D) 購置最新的主機監視系統

50. 下列何者「不」是營運持續性的相關用語？ (A) 交叉錯誤率 (Crossover Error Rate, CER) (B) 營運衝擊分析 (Business Impact Analysis, BIA) (C) 復原時間目標 (Recovery Time Objective, RTO) (D) 最大可容忍中斷時間 (Maximum Tolerable Downtime, MTD)