初級資訊安全工程師能力鑑定樣題

科目 1：資訊安全管理概論

單選題 50 題（佔 100%）

A	1. 下列哪一種攻擊手法，主要目的是在破壞「機密性」？ (1) 社交工程 (2) 搜尋引擎攻擊（Google-Hacking） (3) 拒絕服務（Denial-of-Services） (4) 駭客侵入銀行資料庫竄改存款金額 (A) (1), (2) (B) (3), (4) (C) (2), (3), (4) (D) (1), (2), (4)
A	2. 請問「無論是資源、通訊、資料或是資訊等，只能讓經授權的使用者使用」所代表的意義是下列何者？ (A) 機密性 (B) 完整性 (C) 可用性 (D) 可讀性
B	3. 建立資訊系統資料備份機制，與下列何者關聯性最高？ (A) 可歸責性 (B) 可用性 (C) 完整性 (D) 機密性
B	4. 請問系統安全程序、設計、裝置、或內部控制裡的一個瑕疵或缺點，若被運用，會破壞安全性或違背系統安全政策，此為 NIST SP800-30 對下列敘述何者的定義？ (A) 威脅 (B) 弱點 (C) 風險 (D) 衝擊
D	5. 關於文件管制措施，下列敘述何者正確？ (A) 所有制定的 SOP 皆須書面發行 (B) 制定的各項管理制度、程序，不宜以電子檔案公佈 (C) 所制訂管理辦法及作業程序需要被遵守，因此所有人皆可閱讀所有文件 (D) 文件管制宜訂定標準作業程序，以利組織成員遵循
D	6. 關於資訊安全政策的審查，下列敘述何者不正確？

	(A) 資訊安全政策應定期審查 (B) 相關法令有重大變更時，應進行審查 (C) 公司主要營業項目有重大改變時，應進行審查 (D) 資訊安全政策之審查由資訊主管單獨進行即可
B	7. 在資訊安全管理系統（Information Security Management System, ISMS）的維運過程中，「文件化資訊」是必要的要求，下列何者不是所有文件化資訊需確保的事項？ (A) 制訂需要有可識別的方式，例如：標示文件的標題和日期 (B) 發行需要由文件管理人員審查之後，即可對外公佈發行 (C) 在需要時得提供給相關人員 (D) 需要受到適切的保護，以避免不當使用和外洩
C	8. 資訊安全政策是資訊安全管理系統中的最高指導原則，有不可缺少的重要性，下列敘述何者正確？ (A) 滿足相關的要求事項的承諾後，無需持續改善 (B) 在四階管理文件中屬於第二階管理程序文件 (C) 建立的資訊安全政策必須符合組織的目的及資安目標 (D) 屬於內部或機密文件，不可對外公告
A	9. 資訊資產群組化的好處是簡化並縮短資訊資產之風險評鑑時間，減少威脅、弱點的重複判斷。下列何者資訊資產比較不適合群組化為同一類型？ (A) 機房內的所有主機 (B) 同部門的工作電腦 (C) 識別門禁卡 (D) 系統開發規格書
A	10. 進行資產分類為下列哪一種安全控管類型？ (A) 預防性控制（Preventive） (B) 檢測性控制（Detective） (C) 指令性控制（Directive） (D) 糾正性控制（Corrective）
D	11. 資訊資產價值需考量資訊資產的機密性、可用性及完整性，下列何種情況是應該考量提高可用性？ (A) 公司官網遭竄改 (B) 未授權存取人事資料 (C) 電腦安裝免費軟體

	(D) ERP 系統當機
B	12. 關於資訊資產，下列敘述何者不正確？ (A) 資訊資產安全等級之影響評估構面通常至少會包含機密性、完整性等 (B) 資訊資產重要性等級一旦區分完成，之後不需要再重新檢視或變更 (C) 資產分類分級作業通常是為了之後進行風險管控作業所需 (D) 資產標示並不僅限於硬體資產
C	13. 關於資產分類分級，下列敘述何者正確？ (A) 資產評估不需考量資產之完整性、可用性、機密性 (B) 資產分類分級不需考慮產業別差異 (C) 資產分類分級可以做為風險評估重要的依據 (D) CCTV 系統歸在人資行管部門管控，可不列入分類與評估建議
A	14. 關於雲端服務資產識別議題，下列敘述何者有待商榷？ (A) 租賃雲端服務系統，未列會計科目資產，所以不列入資訊資產盤點項目 (B) 雲端服務資料屬於企業組織之資產 (C) 雲端服務系統，仍屬於資產識別需考量之範圍 (D) 法規的適用上，在雲端資訊資產處理方式，各國無一致標準，需審慎使用
B	15. 在進行資產盤點和建立資產清冊時，下列何者不是必要做法？ (A) 資產清冊需要識別與資訊及資訊處理設施有關的資產 (B) 資產清冊需要標示資產購置時的成本和費用 (C) 對已識別的資訊資產，需要指派資產的擁有者 (D) 資產清冊應予文件化
A	16. 風險不可能不存在，面對風險有哪四種處置的方法？ (A) 接受、降低、移轉、避免 (B) 規劃、評估、排序、避免 (C) 面對、處理、解決、接受 (D) 評估、分析、處理、降低
B	17. 假設災難一定會發生（不論機率再低），當災難發生時，為了確保組織在災難發生時有可遵循的作業程序，以降低損失，所以必須要制定哪一種文件？ (A) 風險管理計畫 (B) 緊急應變計畫 (C) 適用性聲明

	(D) 內部稽核計畫
C	18. 為能達成 ERP 系統不中斷的使用要求，資訊單位決定建立 ERP 備援系統，請問這是風險處理哪一種行為？ (A) 風險規避（Avoid） (B) 風險轉嫁（Transfer） (C) 風險降低（Reduce） (D) 風險接受（Accept）
D	19. 關於風險降低，下列敘述何者不正確？ (A) 其方式包括稽查及遵守計畫 (B) 其方式包括處理偶發事故的計畫 (C) 其方式包括找出相較於現有的控制方法，新的控制方法所可能帶來的相對利益 (D) 其方法包括契約的簽訂、保險和機關的結構，如合夥經營和共同投資
C	20. 關於風險處理，下列敘述何者正確？ (A) 只要進行風險處理，就可以消弭所有的風險因子 (B) 風險處理，不需要考慮成本或法規要求 (C) 風險處理後，可能產生新的風險項目或是殘餘風險 (D) 風險處理僅能選擇暫時接受風險，別無他法
B	21. 關於網路及系統存取管理，下列敘述何者不正確？ (A) 系統主機應考量保護機制，如設定在一段時間未操作時即會自動登出的機制 (B) 若因人為因素誤植帳號及密碼，無需保存紀錄檔 (C) 連線的來源位址與目的位址應建立路由（Routing）控管 (D) 管理者應依照使用者身份，控制系統應用程式的存取
D	22. 關於特權管理，下列敘述何者最為正確？ (A) 登入主機應該使用 Administrator or Root 帳號，以利管理相關權限設定 (B) 資料庫管理員除了備份資料外，還需要讀取資料以利調校資料庫效能 (C) 基於代理人機制，系統管理員除了網路管理帳號外也需本機管理帳號 (D) 應該定期審查特權帳號，若有人員離職也須立即審查相關系統帳號
D	23. 為了防止非授權的存取，企業應根據存取控管政策對使用者（包括內、

	外部使用者）存取權限進行管理。下列何者較無關於管理存取權限？ (A) 定期變更密碼 (B) 定期審查使用者存取權限 (C) 保留存取紀錄 (D) 資料備份
C	24. 您是資訊業務承辦人員，當您有特殊業務需求進行存取敏感性資料時，需要獲得存取許可，即使您有資料存取權限，還需要提出資料存取的理由。上述說明主要為？ (A) 職務區隔（Segregation of Duties） (B) 最小權限原則（Principle of Least Privilege） (C) 必要知道原則（Need-to-know Principle） (D) 以角色為基礎的存取控制（Role-based Access Control, RBAC）
D	25. 關於權限管理，下列敘述何項較不適？ (A) 採購人員擁有採購系統新增、編修、存檔的權限，但無刪除權限 (B) 總經理只擁有採購系統所有模組的查詢權限 (C) 總經理將採購系統最高管理者的帳號密碼，存放於保險箱未使用，另外使用其他帳號登入系統 (D) 資訊主管的系統帳號已是採購系統管理者，因此無須監控其系統操作行為
A	26. 常見的密碼驗證攻擊中，以下何種方法「不是」透過反覆嘗試密碼的方式破解密碼？ (A) 雜湊注入（Pass-the-Hash） (B) 暴力攻擊（Exhaustive Search Attack） (C) 字典攻擊（Dictionary Attack） (D) 猜測攻擊（Guessing Attack）
A	27. 使用者在選定密碼時需注意避免太容易被攻擊者破解，請比較下面四組密碼，指出何組密碼較不容易遭到攻擊者破解？ (A) qwA$c&1!e (B) password (C) 12345678 (D) abcd0229
C	28. 我們常使用密碼來做為認證身份的主要方式，關於密碼強度，下列敘述何者不正確？ (A) 符合密碼複雜性原則可增強密碼強度 (B) 對於複雜程度相同的密碼而言，長度較長的密碼安全度較短密碼

	為高 (C) 密碼複雜性原則不包含數字 (D) 密碼複雜性原則不包含圖片
B	29. 為強化身份認證機制，我們常會使用雙因素認證機制，請問下列何種組合並不屬於雙因素認證的定義？ (A) 密碼（Password） + RFID 感應卡（如悠遊卡） (B) RFID 感應卡 + 自然人憑證 IC 卡 (C) 自然人憑證 IC 卡 + 指紋 (D) 指紋 + 密碼
D	30. 下列何者非單一登入（Single Sign-On, SSO）的優點？ (A) 集中權限控管 (B) 降低不同的帳號密碼組合的困擾 (C) 減少重新輸入密碼的程序 (D) 簡訊認證
B	31. 關於 Kerberos，下列敘述何者不正確？ (A) 針對個人通信安全，可進行身份認證 (B) 是一種非對稱金鑰管理機制來進行金鑰管理的系統 (C) 可採複合 Kerberos 伺服器和缺陷認證機制來補救 (D) 具備加密機制，可保護資料完整性
C	32. 關於設計網際網路服務使用者身分驗證機制的考量因素，下列何者不正確？ (A) What you know？使用者所記住的身分內容，如：個人識別名稱及對應的密碼 (B) What you have？使用者所擁有之認證裝置，如：金融卡、智慧卡 (C) Who you are？使用者所扮演的角色：如：學代、班聯會主席？ (D) What you are？使用者擁有之特徵，如：指紋、虹膜
D	33. 請問在系統服務裡，關於身分驗證，下列敘述何者正確？ (A) 只要通過身分驗證，就可以暢行無阻。 (B) 身分驗證後，即是擁有最高權限。 (C) 身分驗證後，所有的使用行為都是適合理的，不需要軌跡。 (D) 依照最小權限原則，劃分給予適當的權限控管。
C	34. 中華民國目前使用自然人憑證，做為民眾於網路應用時之合法身份識別依據。關於自然人憑證，下列敘述何者不正確？ (A) 自然人憑證是基於 PKI（Public Key Infrastructure）架構下之應用 (B) 自然人憑證在網路上使用時，其代表申請人之身分識別上具有法律效力 (C) 自然人憑證申請一次永久有效，無需換發

	(D) 自然人憑證於網路上的相關應用具有不可否認性
C	35. 關於營運持續管理處理策略之選擇，下列敘述何者不正確？ (A) 轉移風險（Transfer） (B) 避免風險（Avoid） (C) 調整風險（Adjust） (D) 接受風險（Accept）
D	36. 依據「行政院國家資通安全會報通報及應變作業流程」，判定事故影響等級時，應評估資安事故造成之機密性、完整性以及可用性衝擊，下列何者非 4 級事件？ (A) 國家機密資料遭洩漏 (B) 關鍵資訊基礎設施系統或資料遭嚴重竄改 (C) 關鍵資訊基礎設施運作遭影響或系統停頓，無法於可容忍中斷時間內回復正常運作 (D) 機關業務系統或資料遭嚴重竄改
B	37. 將不同的設備或不同時間的日誌進行比對，強化判斷是否為真正資安事件之動作，稱之為？ (A) 根因分析（Root Cause Analysis） (B) 關聯分析（Correlation） (C) 暫時解決方案（Workaround） (D) 升級（Escalation）
C	38. 請問下列何者可以確定為資安事故（Security Incident）？ (A) 防毒軟體成功地更新了病毒碼 (B) 監控系統出現「硬碟使用量超過 80%」的訊息 (C) 執行 google 蒐尋，發現結果出現有公司機密文件 (D) 設備廠商進入機房維修
D	39. 企業委託信賴的第三方團隊，對企業網路目標範圍進行安全性評估，找出存在的弱點或錯誤安全設定問題；並藉此瞭解員工對各種攻擊異常事件的反應。該進行哪種測試？ (A) 原始碼測試(Source Code Review) (B) 壓力測試(Stress Testing) (C) 迴歸測試（Regression Testing） (D) 滲透測試(Penetration Test)
D	40. 您是資安專家，希望能估計營運可承受之最長中斷時間（Maximum Tolerable Period of Disruption），而您最有可能從下列何者取得？ (A) 平衡計分卡（Balanced Score Card）

	(B) 風險估算（Risk Evaluation） (C) 恢復點目標（Recovery Point Objective） (D) 營運衝擊分析（Business Impact Analysis）
D	41. 公司或組織願意提供資源建立 Hot Site 即時備援系統，下列何者是較不可能的原因？ (A) 營業項目有法規的要求 (B) 為了符合所訂定的資訊安全目標 (C) 與客戶訂定的合約條款要求 (D) 客戶在公司提供的服務資源上，建立重要機密的管理系統
D	42. 針對相同資料，請問下列三種備份方式，依其執行備份所需的時間，由大到小排列為下列何者？甲：完整備份（Full Backup） 乙：增量備份 （Incremental Backup） 丙：差異備份 （Differential Backup）？ (A) 甲>乙=丙 (B) 甲<丙<乙 (C) 甲=乙>丙 (D) 甲>丙>乙
C	43. 關於復原的目標時間（Recovery Time Objective），下列敘述何者正確？ (A) 實際系統復原的時間 (B) 系統無法復原的時間 (C) 發生災難後，預計完成系統復原的時間 (D) 發生災難後，預計系統可能中斷的時間
A	44. 下列何者非現代常用的備份媒體？ (A) 磁片 (B) 磁帶 (C) 光碟 (D) 外接硬碟
A	45. 智慧財產權（Intellectual Property Rights）是指由人類思想、智慧、創作而產生具有財產價值的產物。下列何者不屬於智慧財產權？ (A) 肖像權 (B) 專利權 (C) 著作權 (D) 營業秘密法
C	46. 商標註冊後，商標註冊人享有商標專用權，圖形為 『®』，表示某個商標經過註冊，並受法律之保護。關於商標與專利，下列敘述何者不正確？ (A) 專利需要具有發明、新型及新式樣等 (B) 商標是一個圖樣，或文字，或符號，或顏色，或聲音 (C) 德國愛迪達公司控告美國威名百貨銷售的佩雷斯運動鞋有三條

	線，是非法使用其『愛迪達』專利權 (D) 專利權是對發明授予的權利，對專利權人之發明予以保護，保護權利在一段期間內有效，一般期限為 20 年
B	47. 下列何者不是展現保護智慧財產權的良好做法？ (A) 建立銷毀軟體或是轉讓給他人的政策 (B) 允許暫時超過軟體授權內的使用人數上限 (C) 將合法授權的軟體光碟複製一份作為備用 (D) 妥善保存軟體光碟的授權書和啓用碼
B	48. 根據我國內部稽核協會所訂定之「內部稽核與職業道德規範」，認為內部稽核人員應遵守四大原則，下列何者未包含在其中？ (A) 誠正 (B) 節省 (C) 客觀 (D) 保密
B	49. 下列稽核的程序活動中，何者較為優先？ (A) 評估內部控制之有效性 (B) 規劃稽核目標及範圍 (C) 營運活動的觀察 (D) 準備稽核報告
A	50. 下列何種權利必須到經濟部智慧財產局申請，才可享有？ (a)專利權(b)商標權(c)著作權 (A) (a)(b) (B) (a)(c) (C) (b)(c) (D) (a)(b)(c)