

# 112 年度第 1 次 資訊安全工程師能力鑑定 初級試題

科目 1：I11 資訊安全管理概論

考試日期：112 年 6 月 3 日

第 1 頁，共 12 頁

## 單選題 50 題（佔 100%）

A	1. 下列何者為資訊安全的「機密性」之定義？ (A) 確保資訊不會被揭露或被未經授權的個人、實體和流程所取得 (B) 確保資訊的正確和完全性 (C) 確保資訊在需要時可被存取和使用 (D) 確保資訊在傳輸過程中已確認兩方的身分和合法性
D	2. 關於文件管制措施，下列敘述何者正確？ (A) 所有制定的 SOP 皆須以書面發行 (B) 制定的各項管理制度、程序，不宜以電子檔案公佈 (C) 所制訂相關作業程序必須以四階文件來發行 (D) 文件管制宜制定標準作業核可及發行流程，以利組織成員遵循
C	3. 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，無需定期審查目前要求 (B) 資訊安全政策不一定須由最高管理階層審核 (C) 建立的資訊安全政策必須與組織的目的及資安目標相容一致 (D) 屬於內部或機密文件，不可對外公告
B	4. 駭客侵入銀行資料庫竄改存款金額，主要在破壞資訊系統의何種特性？ (A) 機密性（Confidentiality） (B) 完整性（Integrity） (C) 可用性（Availability） (D) 可靠性（Accountability）
B	5. 請問在資訊安全管理系統中的風險評鑑（Risk Assessment）作業，是在 Plan（規劃）、Do（執行）、Check（檢查）、Act（改善）循環中的那一部分？

# 112 年度第 1 次 資訊安全工程師能力鑑定 初級試題

科目 1：I11 資訊安全管理概論

考試日期：112 年 6 月 3 日

第 2 頁，共 12 頁

	(A) Plan（規劃） (B) Do（執行） (C) Check（檢查） (D) Act（改善）
A	6. 關於個人資料蒐集之特定目的消失或期限屆滿時之作為，下列何者錯誤？ (A) 應主動停止蒐集該個人資料 (B) 應主動停止處理該個人資料 (C) 應主動停止利用該個人資料 (D) 應主動刪除該個人資料
B	7. 關於資通安全管理法所定義「公務機關」的敘述，下列何者正確？ (A) 依法行使公權力之軍事機關 (B) 依法行使公權力之中央機關、地方機構 (C) 依法行使公權力之情報機關 (D) 政府捐助並依法行使公權力之財團法人
C	8. 立案於我國的 A 公司主要營業活動市場位於中華人民共和國及新加坡並將以 ISO 27001 架構公司之資訊安全管理系統，下列何項要求在其架構資訊安全管理系統時，並非優先考量項目？ (A) ISO 27001：2022 (B) 個人資料保護法（中華民國） (C) 歐盟一般資料保護法規（General Data Protection Regulation, GDPR） (D) 網路安全法（中華人民共和國）
C	9. 依據民國 110 年 12 月發布的「公開發行公司建立內部控制制度處理準則」，附圖中哪些事項的設置，為各類級公開發行公司皆應於所定期限內如實完成的共通事項？

# 112 年度第 1 次 資訊安全工程師能力鑑定 初級試題

科目 1：I11 資訊安全管理概論

考試日期：112 年 6 月 3 日

第 3 頁，共 12 頁


	<div> 1. 資訊安全長  2. 資安專責單位  3. 資安專責人員（至少 1 名）  4. 資安專責人員（至少 2 名）  5. 資安專責單位主管 </div> <p>(A) 1、2、4 (B) 2、3 (C) 3 (D) 4</p>
D	<p>10. 下列何者「不」是個人資料保護法中，當事人對於個人資料的權利？</p> <p>(A) 查詢或請求閱覽 (B) 請求補充或更正 (C) 請求刪除 (D) 請求永久保留</p>
D	<p>11. 中華民國「營業祕密法」所稱之營業祕密，係指方法、技術、製程、配方、程式、設計或其他可用於生產、銷售或經營之資訊，其所必須符合之要件，下列敘述何項錯誤？</p> <p>(A) 非一般涉及該類資訊之人所知者 (B) 因其秘密性而具有實際或潛在之經濟價值者 (C) 所有人已採取合理之保密措施者 (D) 資訊洩漏將造成公司損失者</p>
B	<p>12. 下列何者屬於中華民國「個人資料保護法」第 6 條規範中的「特種個人資料」？</p> <p>(A) 身分證統一編號 (B) 基因 (C) 生物特徵 (D) 血統</p>
C	<p>13. 如附圖所示，依照創用 CC (Creative Commons) 授權的規定，下列何種使用方式違反附圖中授權標示的規定？</p>

# 112 年度第 1 次 資訊安全工程師能力鑑定 初級試題

科目 1：I11 資訊安全管理概論

考試日期： 112 年 6 月 3 日

第 4 頁，共 12 頁

	 <p>(A) 使用者必須按照著作人或授權人所指定的方式，表彰其姓名</p> <p>(B) 使用者將該素材用於公益的用途上</p> <p>(C) 使用者將該素材用於商業廣告上</p> <p>(D) 使用者重製、散布、傳輸著作時，亦不得修改該著作</p>
D	14. 在公司資產管理中，為達成識別組織之資產並定義適切之保護責任，應優先建議採取下列何種控制措施？ (A) 金鑰管理 (B) 懲處過程 (C) 變更管理 (D) 資產盤點
D	15. 關於可移除式媒體(如：USB 隨身碟)，下列敘述何者較「不」適當？ (A) 所有可移除式媒體依製造商的規格要求，儲存於安全的環境 (B) 針對儲存於可移除式媒體上的敏感資料進行加密 (C) 不再需要使用可移除式媒體時，將所儲存的資料徹底移除 (D) 不將可移除式媒體登載於資產清冊上，以減少資料遺失的機會
A	16. 關於紙本類之資訊資產標示原則，下列敘述何者最「不」適當？ (A) 內部使用級之紙本類資訊資產標示原則可為無需標示 (B) 內部使用級之紙本類資訊資產標示原則可為使用不透明卷宗 (C) 密級之紙本類資訊資產標示原則可為文件首頁標明機密等級或使用紅色卷宗

# 112 年度第 1 次 資訊安全工程師能力鑑定 初級試題

科目 1：I11 資訊安全管理概論

考試日期：112 年 6 月 3 日

第 5 頁，共 12 頁

	(D) 密級之紙本類資訊資產標示原則可為文件封面標明機密等級或使用紅色卷宗
A	17. 關於資產盤點之程序，下列敘述何者最適當？ (A) 可由組織個別之業務活動流程開始進行盤點 (B) 應由資訊類資產開始進行盤點 (C) 應由軟體類資產開始進行盤點 (D) 應由硬體類資產開始進行盤點
A	18. 關於資訊資產盤點作業的描述，下列何者「不」最適當？ (A) 資訊資產盤點即是資訊設備盤點 (B) 資訊資產盤點在確認資產的使用狀況 (C) 資訊資產盤點應考量全面性 (D) 資訊資產盤點應確認資產的可用性
B	19. 關於資產分類分級的敘述，下列何者錯誤？ (A) 建立資訊資產清冊，並定期清查資訊資產 (B) 資訊資產不須指派人員負責管理事宜 (C) 人員異動或離職前，須確實移交所保管之相關資訊資產 (D) 資訊資產報廢時，應依資產類別循相關安全程序辦理銷毀
C	20. 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
C	21. 當進行風險評估，發現機密資料外洩風險是組織內部最大之風險時，組織進行了相對應之風險處理方法，其中包含了購買資料外洩保險，此為下列何種風險處理方式？ (A) 風險保留 (Risk Retention) (B) 風險降低 (Risk Reduction) (C) 風險轉移 (Risk Transfer)

# 112 年度第 1 次 資訊安全工程師能力鑑定 初級試題

科目 1：I11 資訊安全管理概論

考試日期：112 年 6 月 3 日

第 6 頁，共 12 頁

	(D) 風險避免 (Risk Avoidance)
A	22. 風險評鑑 (Risk Assessment) 後的風險處理方式有以下哪幾種方法？ (A) 接受、降低、轉移、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
A	23. 關於風險評鑑 (Risk Assessment) 的敘述，下列何者較正確？ (A) 應建立一套適用於全公司 (組織) 之準則 (B) 不同類別被評鑑項目，無須依不同類別區分風險 (C) 可接受風險一定要在風險評鑑前先決定 (D) 風險改善計畫，執行單位應再選擇是否需執行
D	24. 關於風險轉移 (Risk Transfer) 的敘述，下列何者「不」正確？ (A) 藉由其他的團體，來承擔或分擔部份的風險 (B) 當風險全部或部分被轉移時，可能會遭遇新的風險 (C) 將風險轉移給其他團體時，可以降低風險對自身的影響 (D) 可以有效減低風險發生的機率
C	25. 下列何者「不」是風險處理的選項？ (A) 風險降低 (Risk Reduction) (B) 風險轉移 (Risk Transfer) (C) 風險忽略 (Risk Neglect) (D) 風險保留 (Risk Retention)
B	26. 關於存取控制 (Access control) 的描述，下列何者錯誤？ (A) 存取者向受保護資源進行存取操作的控制管理 (B) 未被授權者，可透過系統管理員，取得未被授權的資源 (C) 存取控制包含了認證、授權以及稽核 (D) 現實生活中門禁系統也是一種存取控制的表現



# 112 年度第 1 次 資訊安全工程師能力鑑定 初級試題

科目 1：I11 資訊安全管理概論

考試日期：112 年 6 月 3 日

第 7 頁，共 12 頁

C	27. 在自由決定存取控制（Discretionary Access Control, DAC）環境中，以下哪個角色被授權向其他人授予資訊存取權限？ (A) 資安經理 (B) 部門經理 (C) 資料擁有者 (D) 執行長（CEO）
D	28. 最常見的身分驗證方式是「帳號密碼」的驗證，請問下列措施中何者無法提升安全性？ (A) 要求定期修改密碼 (B) 採用動態密碼 (C) 規範高強度密碼長度與複雜度 (D) 密碼統一並共用
A	29. 在存取控制（Access Control）中，提到存取控制系統能夠達到的 AAA 機制，請問這 3 個 A「不」包含下列何者？ (A) Availability (B) Accounting (C) Authentication (D) Authorization
C	30. 下列關於存取控制的作法，何者較「不」正確？ (A) 應訂定資訊存取控制政策，並文件化公告 (B) 存取控制規範，需符合資料保護法令與契約規定 (C) 為了能快速進行除錯，存取記錄應開放給所有工程人員存取 (D) 資訊存取控制規範，應依照人員的工作與職務分別訂定
D	31. 為避免職務及責任範圍衝突，應採取下列何者控制措施？ (A) 強化密碼管理 (B) 日誌管理 (C) 資訊之分級 (D) 職責區隔

# 112 年度第 1 次 資訊安全工程師能力鑑定 初級試題

科目 1：I11 資訊安全管理概論

考試日期：112 年 6 月 3 日

第 8 頁，共 12 頁

C	32. 下列何者為使用持有物（Something You Have）進行身分驗證（Authentication）？ (A) 密碼 (B) 指紋 (C) 個人識別證 (D) 簽名
B	33. 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) 網路存取應設定設備來源位置與目的位置 (D) 管理者應依照使用者身份，控制系統應用程式的存取權限
B	34. 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，下列何者最相關？ (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
D	35. 憑證記載了個人資料、公開金鑰、憑證單位名稱、數位簽章、以及憑證有效期限及用途等資訊，下列何者「不」是憑證的特性？ (A) 機密性（Confidentiality） (B) 不可否認性（Non-Repudiation） (C) 身分識別（Authentication） (D) 可用性（Availability）
B	36. 關於目前尚未被公開有碰撞攻擊（Collision attack）威脅之雜湊函式（Hash functions）類型，下列敘述何者正確？ (A) SHA-1



# 112 年度第 1 次 資訊安全工程師能力鑑定 初級試題

科目 1：I11 資訊安全管理概論

考試日期：112 年 6 月 3 日

第 9 頁，共 12 頁

	<p>(B) SHA-2</p> <p>(C) MD5</p> <p>(D) CRC-32</p>
A	<p>37. 關於非對稱式密碼學 (Asymmetric cryptography) 的敘述，下列何項錯誤？</p> <p>(A) 私鑰 (Private-key) 僅能用於解密訊息</p> <p>(B) 私鑰可用於產生數位簽章 (Digital signatures)</p> <p>(C) 公鑰 (Public-key) 可用於加密訊息</p> <p>(D) 也稱作公鑰密碼學 (Public-key cryptography)</p>
A	<p>38. 關於雙重要素驗證 (Two-factor authentication, 2FA) 的敘述，下列何者錯誤？</p> <p>(A) 指的是登入帳戶時需要提供多個驗證因素，通常是三個或更多。除了密碼外，其他驗證因素可能包括短信驗證碼、生物識別、硬體安全鑰匙、安全問題、行為分析等</p> <p>(B) 郵件釣魚攻擊，攻擊者可以進行釣魚攻擊，試圖騙取您的 2FA 代碼，以進入您的帳戶</p> <p>(C) 使用安全性低的第三方服務來實現 2FA 可能會導致安全漏洞，讓攻擊者入侵您的帳戶</p> <p>(D) 當使用第三方應用程式進行 2FA 驗證時，攻擊者可能通過偽造應用程式來竊取您的 2FA 代碼，以進入您的帳戶</p>
B	<p>39. 密碼學身分認證的三個因素：所知之事 (something you know)、所持之物 (something you have)、所具之形 (something you are)。下列何項為所持之物認證因素？</p> <p>(A) 指紋</p> <p>(B) 晶片卡</p> <p>(C) 密碼</p> <p>(D) 臉型</p>
A	<p>40. 假設有兩金鑰，金鑰 A 用來將明文 x 變成密文 y，而金鑰 B</p>

# 112 年度第 1 次 資訊安全工程師能力鑑定 初級試題

科目 1：I11 資訊安全管理概論

考試日期：112 年 6 月 3 日

第 10 頁，共 12 頁

	<p>用來將密文 <math>y</math> 變成明文 <math>x</math>，當金鑰 A 與金鑰 B 是同一把金鑰時，請問他最有可能是下列何種加密演算法？</p> <p>(A) AES (B) RSA (C) ECC (D) SHA</p>
D	<p>41. 關於資訊安全事件的通報，下列敘述何者正確？</p> <p>(A) 如果只是觀察到可疑的資訊安全弱點，不須通報，以免耗用太多資源</p> <p>(B) 如果是人為的錯誤，不須即時通報，可再觀察後續結果</p> <p>(C) 如果看到應用系統存取違反的狀況，系統會主動發出通知，可以不用即時通報</p> <p>(D) 除了組織員工，所有與資訊安全有關會接觸到的約聘人員，也要求如果觀察到可疑事件亦須及時通報</p>
A	<p>42. 下列何者較「不」是持續營運資料備份的考量項目？</p> <p>(A) 場地大小 (B) 存放位置 (C) 成本高低 (D) 安全性</p>
B	<p>43. 關於營運衝擊分析及災害復原計畫應考慮項目，下列敘述何者最「不」正確？</p> <p>(A) 復原至最小營運水準所需之員工、技術、設施及服務所需之時間</p> <p>(B) 損害程度之等級不包括收入損失、附加成本、商譽損失、喪失競爭優勢等</p> <p>(C) 最小營運水準所需之人員、系統軟體及硬體及交通等，皆為須考量之資源</p> <p>(D) 復原時間是完全復原至原服務水準所需之員工、技</p>

# 112 年度第 1 次 資訊安全工程師能力鑑定 初級試題

科目 1：I11 資訊安全管理概論

考試日期： 112 年 6 月 3 日

第 11 頁，共 12 頁

	術、設施及服務所需之時間
A	<p>44. 資訊安全事故發生後，證據蒐集的相關敘述，下列何者較正確？</p> <p>(A) 組織可考量與數位證據控管有關的工具導入，以確保對數位證據的有效保存</p> <p>(B) 於資訊安全事故發生後，若需要針對證據予以鑑識，一旦超過組織之權限，即無法提供使用</p> <p>(C) 若資訊安全事故涉及法律議題相關，證據保存存在困難程度，所以無法實施控管</p> <p>(D) 資訊安全事故的發生會揭露內部的問題，所以不適合文件化太過詳細</p>
C	<p>45. 如附圖所示，資訊安全事件處理的正確步驟順序為下列何項？</p> <div style="border: 1px solid black; padding: 5px; margin: 10px 0;"> <p>A. 分析問題，設法找出問題發生的根本問題</p> <p>B. 以隔離的方式降低問題造成的損失</p> <p>C. 偵測問題後，做簡單的分類與報告</p> <p>D. 將狀況復原並記錄處理的步驟，做為未來處理類似事件的參考</p> </div> <p>(A) ABCD</p> <p>(B) ACBD</p> <p>(C) CBAD</p> <p>(D) DBCA</p>
C	<p>46. 營運持續性計畫（Business Continuity Plan, BCP）實務上通常多久須測試一次？</p> <p>(A) 在所有稽核活動前</p> <p>(B) 執行一次確認有效性即可</p> <p>(C) 至少每年一次</p> <p>(D) 只有當異地備份改變時</p>
B	<p>47. 營運衝擊分析最主要的目的為何？</p> <p>(A) 進行風險分析</p> <p>(B) 確認重要流程的最大可承受中斷時間</p> <p>(C) 記錄結果，並提出改正措施</p>

# 112 年度第 1 次 資訊安全工程師能力鑑定 初級試題

科目 1：I11 資訊安全管理概論

考試日期：112 年 6 月 3 日

第 12 頁，共 12 頁

	(D) 確認殘餘風險
C	48. 關於資料備份的敘述，下列何者正確？ (A) 因為資源設備的限制，無須進行回復測試 (B) 備份儲存媒體上的資料可永久保存 (C) 備份媒體儲存的地點，需考量主要地點發生災難時，不會被波及的場域 (D) 因為備份工具每天皆會啟動進行備份，所以若當日無法備份完成，隔日成功即可
B	49. 若是 A 公司不能接受重要系統中斷超過 1 小時，下列何項異地備援方式最適合該公司？ (A) 冷備援 (B) 熱備援 (C) 溫備援 (D) 機房內自主備援
C	50. X 公司對於電子郵件系統可用性目標設定為不得中斷超過一天，在制定該系統災害復原計畫時，關於此公司復原時間目標（Recovery Time Objective, RTO）的設定，下列何項最適當？ (A) RTO 設定為二天 (B) RTO 設定為一週 (C) RTO 設定為 20 小時 (D) 在制定災害復原計畫時，不需考慮 RTO