112 年度第 1 次 資訊安全工程師能力鑑定 中級試題

科目 1：I21 資訊安全規劃實務

考試日期： 112 年 4 月 8 日

單選題 15 題，複選題 5 題，題組題 5 題（佔 100%）

D	1. X 公司為在中華民國註冊登記之公司，該公司將於 2023 年導入資安管理制度，並預計於 2024 年第一季通過國際資安驗證，請問下列何項制度最適合 X 公司做為導入資訊安全管理制度依循之參考？ (A) ISO/IEC 27001 : 2013 (B) ISO/IEC 27004 : 2016 (C) ISO/IEC 20000-1 : 2018 (D) ISO/IEC 27001 : 2022
B	2. 在 ISO 系列的 ISMS 標準中，下列何者與電信產業資訊安全管理最有關聯？ (A) ISO / IEC 27010 (B) ISO / IEC 27011 (C) ISO / IEC 27015 (D) ISO 27799
C	3. 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》第九條之一第二項規定，以及金融監督管理委員會 110 年 12 月 28 日金管證審字第 11003656544 號函釋，上市（櫃）公司實收資本額達新台幣 100 億元以上時，應於民國 111 年 12 月 31 日前，完成哪些資訊安全單位及人員的設置？ 1.資訊安全長；2.資安專責單位；3.資安專責人員(至少 3 名)；4.資安專責人員(至少 2 名)；5.資安專責單位主管 (A) 1、3、5 (B) 1、4、5 (C) 1、2、4、5 (D) 1、2、3、5
B C	4. 常見的資訊安全標準中，下列哪些標準可以為個人資訊保護或隱私資訊管理提供指引？ (A) ISO 27001 (B) ISO 27701 (C) BS 10012

	(D) IEC 62443
	【題組 1】 A 公司為某先進產品的製造商，該公司主要據點 B 與 C 分散在國內兩地，距離約 20 km，其主要客戶位於歐洲地區，該公司十分重視資訊安全及品質管理，先前已通過 ISO 9001、ISO 27001 及 ISO 27701 等相關標準的驗證。據點 B 主要主要包含的業務與技術服務部門，據點 C 主要包含管理部門、資訊部門及相關研發、製造部門。
D	5. 【題組 1 背景描述如附圖】該公司據點 B 與據點 C 兩地的通訊，在成本考量下，最終分別租用業者 D 的網際網路接取服務，以連接網際網路（Internet）。近日業務部門的印表機突然印出紙本的勒索信，信中表示該公司的電腦已被駭客組織 E 入侵，需支付高額的金錢，否則將進一步把公司的電腦資料加密。經調查後發現，業務部門為了方便業務人員從公司外部直接列印資料，而私自將該部門的印表機設定使用公有 IP（Public Internet Protocol），且部門中的其他電腦皆位於啟用 NAT（Network Address Translation）功能的防火牆後方，請問最有可能被入侵的網路節點？ (A) 據點 C 中資訊部門的電腦 (B) 據點 B 中業務部門的電腦 (C) 據點 B 中技術服務部門的電腦 (D) 印表機遭惡意濫用
C	6. 【題組 1 背景描述如附圖】為符合業務部門員工從公司外部列印資料的需求，下列何種解決方案，可以不需在印表機設定公有 IP（Public Internet Protocol）的前提下達成此需求？ (A) WAF（Web Application Firewall） (B) IDS（Intrusion Detection System） (C) VPN（Virtual Private Network） (D) EDR（Endpoint Detection and Response）
B	7. 【題組 1 背景描述如附圖】因該公司是某先進產品的製造商，若要進一步強化該公司製造場域部分的資訊安全（Operational Technology），宜再導入下列何種標準驗證較為

	合適？ (A) BS 10012 (B) IEC 62443-2-1 (C) IEC 62443-2-4 (D) ISO/IEC 27001
A C	8. 【題組 1 背景描述如附圖】公司希望其服務提供商，亦具備相關的工業控制系統資訊安全能力。從流程（Process）認證而言，可以進行下列哪兩種標準的認證？ (A) IEC 62443-2-4 (B) IEC 62443-3-3 (C) IEC 62443-2-3 (D) IEC 62443-4-2
A	9. 組織擬採取「存取控制」構面之控制措施，確保組織所保有的資通系統之安全防護，請問關於控制措施的敘述，下列何項錯誤？ (A) 遠端存取時使用者之權限檢查作業應於使用者端完成 (B) 超過組織所許可之閒置時間或可使用期限時，系統自動將使用者登出 (C) 採最小權限原則，僅允許使用者依組織任務及業務功能，完成指派任務所需之授權存取 (D) 遠端存取之來源應為組織已預先定義及管理之存取控制點
A	10. 一個通過 ISO 27001:2013 驗證的組織，在內部稽核活動中，發現已離職員工的帳號仍沒有停用，且進一步追查存取紀錄時，發現其在離職後，仍有登入存取部門共用資料夾的行為。請問對於該組織上述的狀況，下列何項敘述最為合適？ (A) 該組織可能未落實使用者存取管理之程序 (B) 該組織可能未落實資產處置之程序 (C) 該組織可能未落實實體及環境安全之程序 (D) 該組織可能已落實存取控制政策

C	11. 在存取控制上，零信任（Zero Trust）是一個重要課題。關於零信任的敘述，下列何者較「不」適當？ (A) 零信任依循「永不信任，一律驗證」的原則 (B) 推動零信任，企業可能需要重新評估每項資產的保護方式 (C) 零信任倚重於最大特權原則等治理政策 (D) 是 Forrester 的 John Kindervag 首次創造的一個名詞
A C D	12. 從 ISO 27001:2022 附錄 A「參考控制目標及控制措施」中，下列哪些是「實體控制措施」相關的規範或控制措施？ (A) 實體進入控制措施 (B) 遠端工作應提出申請 (C) 維護設備，以確保其持續之可用性及完整性 (D) 未經事前授權，不得將設備、資訊帶出場域外
	【題組 2】 某公司資訊系統管理人員發現該公司 SQL Server 有些異常現象發生，經檢視相關 SQL Server 之紀錄檔之後，並未發現足以支撐該管理人員對此異常現象發生原因之推論，惟該管理人員可以判斷的是，這個異常現象應該是人為的因素比較大，因此，管理人員為了確認 SQL Server 異常現象的發生是其所判斷的「人為因素」所產生。
B	13. 【題組 2 背景描述如附圖】此因素仍然可能持續發生，下列何項措施較有助於釐清以下議題？ (A) 防火牆設定阻擋 TCP 21 埠 (B) 安裝資料庫稽核工具 (C) 安裝防毒軟體 (D) 重新設定路由器之路由表
D	14. 【題組 2 背景描述如附圖】該管理人員安裝網路封包側錄器後，對該 SQL Server 持續側錄了一整晚的網路封包，隔天進公司針對所側錄下來的網路封包進行分析，發現在網路封包內容顯示了有一個來自 210.34.17.8 的 IP 位址在深夜的時候連接至公司內部該資料庫主機（TCP 3389 埠以及 TCP 1433

	埠）。請問下列敘述何者較為適當？ (A) 外部人員使用 VNC 軟體進行連線 (B) 外部人員使用虛擬私有網路（Virtual Private Network, VPN）連接內部網路 (C) 外部人員使用虛擬私有網路（Virtual Private Network, VPN）連接 SQL Server (D) 外部人員使用 Remote Desktop Protocol（RDP）連接內部網路設備
D	15. 【題組 2 背景描述如附圖】當管理人員分析網路封包，發現來自於外部的 IP 位址在深夜的時候連接至該公司的內部網路，並進入該 SQL Server 下了一些破壞性的 Command，因此，就將先前封存的網路封包帶至公司附近的警察局進行報案，而受理的警察在第二天，就將案發當天深夜從外部 IP 位址連接至該公司內部網路 SQL Server 進行破壞的案件當事人找到，並確認了案件當事人為該公司最近離職的 MIS 經理。請問對於警察為什麼可以在短短的時間內就可以找到案件當事人的敘述，下列何者最「不」可能？ (A) 因為網路封包的內容有案件當事人進入 SQL Server 使用的帳號 (B) 因為網路封包的內容有案件當事人進入 SQL Server 使用的外部 IP 位址 (C) 因為網路封包的內容有案件當事人進入 SQL Server 的 MFA Token (D) 因為網路封包的內容有案件當事人在 SQL Server 所下的 Command
A B D	16. 【題組 2 背景描述如附圖】公司高層因為此一資安事件進行了事後的檢討，要求必須降低此一資安事件發生之風險，以防止類似案再次發生，請問下列哪些是正確的控制措施？ (A) 建立內部資訊安全管理制度並發布與確實施行 (B) 對於離職人員應及時將其所使用之帳號停用或刪除

	(C) 重新調整防火牆政策以阻擋所有對資料庫的連線 (D) 進行內部資訊安全教育訓練與資安意識宣導
A	17. 某公司新增了一業務型態，員工（20 員，每員配置筆電乙部以及隨身硬碟乙顆）必須至客戶端長期駐點處理有關受託業務，並於客戶端透過網際網路連線回公司內部網路處裡公司相關業務，為了降低此一新增業務型態所衍伸出來的資安風險，該公司正評估採取有效的控制措施來降低此風險，請問下列控制措施何項較無法降低此風險？ (A) 網站應用程式防火牆（Web Application Firewall, WAF） (B) 端點偵測及應變機制（Endpoint Detection and Response, EDR） (C) 虛擬私有網路（Virtual Private Network, VPN） (D) 防毒軟體（Antivirus Software）
B	18. OWASP Top 10:2021 所發布之 A04:2021-Insecure Design 主要是呈現出許多不同的弱點，代表著「缺乏或無效的控制設計」，試問下列對於預防 A04:2021-Insecure Design 發生的控制措施何者較「不」適當？ (A) 建立與使用安全開發生命週期並且協同應用程式安全的專業人士來評估與設計安全與隱私相關的控制措施 (B) 建立與使用第三方的開源函式庫，或是使用已完成的元件 (C) 使用威脅建模在關鍵的認證、存取控制、商業邏輯與關鍵缺陷上 (D) 撰寫單元測試與整合測試來驗證所有的關鍵流程對威脅建模都有抵抗
D	19. 關於 NIST SP 800-207 零信任架構（Zero Trust Architecture, ZTA）的基本規則敘述，下列何項錯誤？ (A) 所有的通訊都需被保護，無論其所在之網路位置

	(B) 須觀察與量測所擁有資產與相關資產，其完整性與安全態勢 (C) 運算服務（Computing Service）和資料來源（Data Sources）皆可視為資源 (D) 應先蒐集資產、網路架構等現狀，建立資產清冊
B C D	20. 關於 NIST SP 800-207 零信任架構（Zero Trust Architecture, ZTA）的邏輯元件敘述，下列哪些正確？ (A) 威脅情資（TI）來源：提供外部資訊給政策落實點（PEP），以進行存取決策 (B) 持續診斷緩解（CDM）系統：收集資產目前狀態，並套用更新至設定與軟體元件 (C) 公鑰基礎設施（PKI）：系統產生給資源、服務與應用程式之憑證，並進行紀錄 (D) 安全資訊事件管理（SIEM）系統：收集以安全為主的資訊，並用於日後分析
	【題組 3】 某醫療機構日前發生多起駭客入侵事件，經查發現其行動式醫療車及行動加護病房的雲端即時監護系統皆遭到駭客入侵，駭客並且透過遠端設定改變點滴流速超出原本設定的 50 倍。為了解決行動式醫療設備及雲端監護系統的安全，該機構規劃導入零信任架構（Zero Trust Architecture）強化存取控制，解決行動式醫療車及行動加護病房的雲端即時監護系統。
B	21. 【題組 3 背景描述如附圖】請問該醫療機構導入零信任（Zero Trust）優先進行的工作為下列何項？ (A) 建立零信任架構 (B) 瞭解現行的架構、設備與流程 (C) 建立政策決策點（Policy Decision Point, PDP） (D) 建立政策落實點（Policy Enforcement Point, PEP）
C	22. 【題組 3 背景描述如附圖】請問在建置行動式醫療車及行動加護病房的雲端即時監護系統的零信任，下列何者「不」是

	零信任（Zero Trust）架構的原則？ (A) 不管與哪個網路位置的裝置通訊都需確保安全 (B) 對於個別企業資源的存取要求，應以連線為基礎去判斷是否許可 (C) 所有的資料、設備與運算服務，都要被當作是主體（Subject） (D) 所有的資源的身分鑑別與授權機制，都要依監控結果動態決定
B	23. 【題組 3 背景描述如附圖】關於建置行動式醫療車及行動加護病房雲端即時監護系統的零信任架構與角色敘述，下列何者錯誤？ (A) 政策引擎（Policy Engine, PE）與政策管理者（Policy Administrator, PA）位於政策決策點（Policy Decision Point, PDP）中 (B) 政策落實點（Policy Enforcement Point, PEP），可以是網路防火牆或監視系統 (C) 持續診斷與緩解系統（Continuous Diagnostics and Mitigation, CDM）的工作是持續收集企業數位資產的狀況，以作為政策引擎（Policy Engine, PE）評估放行與否的參考 (D) 信賴評估演算法可以是條件（Criteria-based）為基礎或以分數（Score-based）為基礎
A B C	24. 【題組 3 背景描述如附圖】導入零信任架構時，可能面臨的威脅挑戰有下列哪些？ (A) 網路的可視性 (B) 帳密被盜/內部威脅 (C) 遭遇 DoS 阻斷服務或網路中斷 (D) 可建立動態存取政策的控管
C	25. 與資訊安全風險分析相關議題的敘述，下列何者錯誤？ (A) 主管機關公文來函要求事項，可納入風險分析的參

	考 (B) 法律法規適用的要求事項，可納入風險分析的參考 (C) 客戶合約的要求，可以不用納入風險分析的參考 (D) 組織本身內部與外部的議題，可納入風險分析的參考
C	26. 關於風險分析與評估之敘述，下列何者錯誤？ (A) 公司最好至少每年定期執行一次風險評鑑 (B) 公司營運重大改變時，應進行風險評鑑 (C) 重大風險項目完成風險回應後，不需進行風險再評估 (D) 進行風險分析與評估前，應先了解相關背景資訊（例如：法規要求、技術環境…）
D	27. ISO/IEC 27005 於 2022 年 10 月發布最新版本，該版本與 2008 年版本的差異之一為風險識別的方式，其中 2008 年版為：基於_____；2022 年版增加了：基於_____。 (A) 事件（event）；資產（asset） (B) 威脅（threat）；事件（event） (C) 資產（asset）；風險（risk） (D) 資產（asset）；事件（event）
A B D	28. 關於風險分析及風險評估議題的敘述，下列哪些正確？ (A) 風險評估的過程，須將目前已實施的措施結果納入考量 (B) 風險分析時產出的後果與可能性的評估方式應定義清楚 (C) 風險識別僅需將與機密性有關風險識別清楚 (D) 以風險評鑑工具直接執行的過程與結果皆須留存紀錄
	【題組 4】 A 公司年初導入 ISO 27001 資訊安全管理制度，並參考 ISO 31000 風險架構制度訂定風險管理辦法及相關程序。公司亦順利於年底取

	得驗證通過，驗證過程稽核員於風險管理過程出具一項次要缺失，主因為 A 公司於年度風險評鑑過程，風險項目量化數值計算錯誤，但不影響風險排序以及後續選擇風險進行回應之作業。
C	29. 【題組 4 背景描述如附圖】ISO 31000 風險管理架構所述簡要列示如後：1.風險回應、2.建立全景、3.風險分析及評估、4.風險辨識，以及貫穿於整個風險管理流程之「監督與覆核」、「溝通及協商」。請問上述 1~4 項風險管理流程的正確順序為下列何項？ (A) 1234 (B) 4321 (C) 2431 (D) 4231
C	30. 【題組 4 背景描述如附圖】請問 A 公司是否必須要重新進行年度風險評鑑作業，其原因為下列何項？ (A) 是，因為此為外部稽核缺失 (B) 是，因為必須以此做為矯正預防措施之處理方式 (C) 否，僅需修正量化計算結果，因為不影響風險評鑑之結果 (D) 否，因為此項缺失並非主要缺失，不須立即於期限內回應驗證單位
B	31. 【題組 4 背景描述如附圖】公司取得 ISO 27001 驗證不久之後，即因違反法令規定收到政府機關之處罰，且該項法令規定並未被公司所關注。請問依照前述之風險管理流程，此問題應該在下列何項階段即被關注？ (A) 風險辨識 (B) 建立全景 (C) 風險回應 (D) 風險分析及評估
A B C	32. 【題組 4 背景描述如附圖】導入 ISO 27001 後，A 公司評估資安市場商機龐大，擬開發以 AES 512 加密技術之資安產品，並將主要目標市場設定為：美國、中國、日本、韓國、台灣。

	公司已瞭解此為重大事項，要求風險部門啟動風險評估作業，下列哪些項目是風險評估過程應被關注的事項？ (A) 法律法規 (B) 公司資本 (C) 技術 (D) 評估者之偏好
C	33. 關於風險處理的敘述，下列何者錯誤？ (A) 風險處理計畫是定義行動並實施所需的控制，以降低無法接受風險的管理文件 (B) 風險處理計畫中要考量風險處理之優先順序 (C) 風險處理計畫如果完成時間較長，如需導入工具，可以先以接受該高風險處理 (D) 風險處理計畫中，所需資源及交付事項，皆須完整計畫考量
D	34. 關於風險評估準則的敘述，下列何者錯誤？ (A) 組織應定義用於評估風險重要性的準則 (B) 不同組織可能採用不同的方法跟準則 (C) 這些準則應反映組織的價值觀、目標和資源 (D) 風險評估準則應與組織的管理政策可以不一致
C	35. ISO/IEC 27002 於 2022 年 2 月發布最新版本，該版本與 2013 年版本的差異之一，是增加控制措施的屬性標籤，其中一項是「類別」，共有預防、偵測與矯正等 3 項，請問系統資料備份比較偏向下列哪一類型？ (A) 預防（Preventive） (B) 偵測（Detective）及矯正 (C) 矯正（Corrective） (D) 預防及偵測
A B D	36. 關於風險處理相關議題的敘述，下列哪些正確？ (A) 制定資訊安全目標，可依據風險處理的實施狀況來量化其達成結果

	(B) 風險處理的計畫，需細部描述其內容，包含實施內容及相關負責人員等 (C) 風險處理的方式必須以修正風險的選項處理 (D) 風險分析結果可能性高、衝擊大的可考量選用避免風險
	【題組 5】 風險管理是資訊安全的核心，對於風險的識別、策略面對於風險的危險的計算均來自於有效的風險管理。 您是一位資訊安全管理人員，公司的資訊資產無論是管理、技術或營運都須由你來進行規畫，你發現由人事單位所執行的 EIP（Enterprise Information Portal）開發一案，承辦廠商無法提出任何技術性檢測報告，上線進入測試階段時，你發現該站台上有非常嚴重的 SQL Injection、XSS、CSRF…等網站應用程式弱點，你試圖要透過合約中規範開發廠商基於安全性問題，必須提供無償 20%程式碼修改的服務。 但基於你於此類技術性風險識別後，發現此類問題為非常低級錯誤，但在現在階段進行修補曠日廢時，而 CEO 要求你針對此類風險進行評估，必須避免重複花費，且可接受採用現有公司防護資訊設備進行保護。 經過盤點，你基於一個月內能進行降低風險的解決方案包含： 1. 將該 EIP 納入網站應用程式防火牆保護，可提供 60%的防護效益 2. 要求乙方應對安全性問題提出改善計劃，但需三個月的時間 3. 另外尋求外包資源針對發現的資安問題進行修補，需額外花費超過本案 50%的金額 4. 透過 MSSP（Managed Security Service Provider）提供監控 EIP 服務即早預警入侵事件，需額外花費本案 25%的費用 5. 設定網站伺服器平台提供過濾 URI（Uniform Resource Identifier）字串功能，可提供 85%的防護效益
B	37. 【題組 5 背景描述如附圖】CEO 表示，現階段已經進入測試階段，無法提供更多的預算進行防護，乙方回覆修改程式碼需要至少三個月，且會超過 20%的修改比例，CEO 需要你規劃最佳成本效益（Cost Effective），下列何項可以進行暫時性保護，並爭取廠商修復時間？

	(A) 導入其它雲端流量清洗服務 (B) 選擇設定網站伺服平台提供過濾 URI 字串功能，以提供 85%的防護效益 (C) 選擇透過 MSSP 提供監控 EIP 服務即早預警入侵事件 (D) 選擇納入網站應用程式防火牆保護
C	38. 【題組 5 背景描述如附圖】風險處理實務中，針對定量分析（Quantitative），可以計出精準的風險危害程度，計算出可被度量的數值，一般來說，它是金錢的單位，要計算出一年內單一風險因子對於資訊資產產生單一危害。經過評估，本項網站弱點資產價值為 120 萬元，已識別出有 3 個可利用的弱點，可取得網站上所有員工的個人資料，無論其弱點的多寡，其危害網站 40%的價值，該 EIP 網站並未被公開於網路上，但在過去此類內部網站弱點被利用一年內約有 12%的弱點被利用，請問其年損失期望計算下列何者正確？ (A) 120 萬 * 3 * 40% * 12% (B) (120 萬 * 3 * 40%) － (120 萬 * 12%) (C) (120 萬 * 40%) * 12% (D) (120 萬 * (40%/3) * 12
C	39. 【題組 5 背景描述如附圖】CEO 所要求的風險處理原則，是在選擇控制措施前必須先考量到成本效益（Cost Effective），因此第一步就是金錢利益分析（Cost/Benefit Analysis），計算出保護措施的總價值，這類的風險處理稱之為降低風險。請問下列何項降低風險的敘述最為適當？ (A) 風險處理必須降到為零為止 (B) 透過一系列的控制措施，將衝擊降到可以被規避為止 (C) 選擇投入最少花費的控制措施，將風險降至擁有者（Owner）可接受為止 (D) 投入降低風險比例最大的控制措施，將風險降至接

	近零為止
AC	40. 【題組 5 背景描述如附圖】因人事單位發包的員工入口網弱點事件，發現公司內部的系統發包規範未有一個有效的管理規範，以導致本項問題，在公司組織內無設置 CIO/CISO 及資安專責人員的制度，造成資訊安全問題層出不窮，因此公司決定要導入資訊安全管理系統制度進行管理，目前已完成資訊資產盤點，透過內部議題討論後發現，除了無資安專責人員以外，亦無有效管控資安風險的資訊資產。請問下列哪些可以有效的提升這些資訊軟體取得之前的安全強度？ (A) 建立合約範本，將相關檢測需求明文規範 (B) 定期執行已發包專案合約內容審查 (C) 設立資安專責單位並將相關需求交由該專責單位查驗 (D) 驗收後定期執行各項檢測並要求廠商辦理技術移轉教育訓練