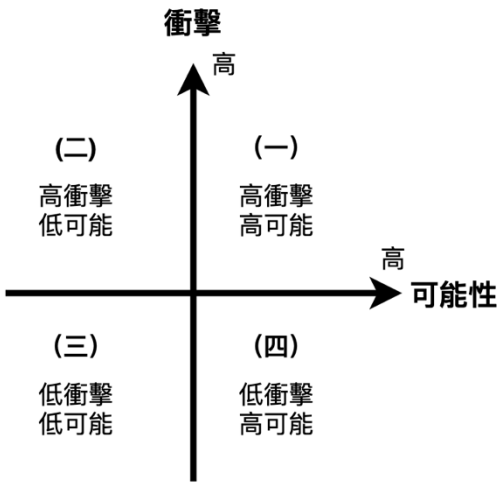
110 年度中級資訊安全工程師能力鑑定試題

科目 1：資訊安全規劃實務
考試日期：110 年 9 月 25 日　　第 1 頁，共 13 頁

單選題 15 題，複選題 5 題，題組題 5 題（佔 100%）

C	1. 下列何者最能說明系統角色權限存取控制（Role-Based Access Control, RBAC）？ (A) 允許系統管理者決定誰能不能夠存取相關資源 (B) 採用集中存取控制方法，系統管理者可不需要依使用者部門來進行存取控制設定 (C) 可依據系統使用者的工作任務，設定與變更人員操作存取權限，也可於使用人員任務異動時撤銷不需要的授權功能 (D) 主要作為執行企業資訊系統的安全策略、資安標準和作業管理指南
D	2. 公司指派專人負責去回收櫃檯的新客戶個人資料表，裝箱並貼上封條後，再由該專人將這些資料開車運送到 3 公里之外的無人庫房存放，請問上述情境主要違反下列資訊安全管理的何項原則？ (A) 最小權限（Least Privilege） (B) 僅知原則（Need to Know） (C) 定期權限審查（Periodically Access Rights Review） (D) 職務區隔（Segregation Of Duties）
A	3. 關於資訊安全事故管理，下列敘述何者「不」正確？ (A) 系統管理人員於組織內發現駭客侵害行為，為避免擴大危害，應自行調整流程，先處置並降低影響後再通報 (B) 可建立網站資安事故的通報平台，鼓勵外部人員（使用者、客戶）進行資訊安全事故通報 (C) 應加入條文要求委外廠商即時回報該公司所發現之資安事故或案件，以利組織迅速回應 (D) 針對員工所通報之資訊安全事件，組織除即時處置外，也需評鑑其是否為資安事故；若為事故則需分析其成因並取得改善方式，以降低再度發生之可能性
C	4. 電子郵件常用的數位簽章（Digital Signature），其目的是保護下列哪些資訊安全要素？ (A) 機密性（Confidentiality）與完整性（Integrity） (B) 完整性（Integrity）與可用性（Availability） (C) 完整性（Integrity）與不可否認性（Non-Repudiation） (D) 機密性（Confidentiality）與不可否認性（Non-Repudiation）
C	5. 下列何種組合「不」屬於多因子驗證（Multi-factor Authentication）？ (A) Smart Card, PIN (B) Password, OTP (C) Password, Username

	(D) Fingerprint, PIN
B	6. 在資訊安全模型(Security Models)中，關於自主存取控制(Discretionary Access Control, DAC)，下列敘述何者「不」正確？ (A) 定義於可信任計算機系統評估準則（Trusted Computer System Evaluation Criteria, TCSEC） (B) 依據事前定義（Pre-defined）主體（Subject）的安全等級和被存取物件（Object）機敏等級來決定是否可以存取 (C) 傳統 Unix 系統的使用者（Users）、群組（Groups）以及其它使用者（Other）的讀-寫-執行（Read-Write-Execute）管控，即為 DAC 的一種實作 (D) 有特定權限的主體（Subject）可將存取權限授予其他主體
A B C D	7. 依據資通安全責任等級分級辦法，對於組織的資通安全責任等級共可區分為 A 級、B 級、C 級、D 級及 E 級，當組織業務涉及公務機關捐助或研發之敏感科學技術資訊之安全維護及管理事項之情形者，其資通安全責任等級應為下列何者？ (A) A 級 (B) B 級 (C) C 級 (D) D 級
D	8. 關於監控中心（Security Operations Center, SOC）的發展與建置規劃，下列敘述何者「不」正確？ (A) SOC 建置重點於主動化、自動化、智能化，主要的關鍵技術是巨量資料分析與機器學習的導入 (B) SOC 核心三元素為：人員、程序、科技，而科技的導入在於輔助人員依相關作業程序完成任務 (C) SOC 提供監控與管理資訊安全系統與設備、執行定期網路安全掃描、防火牆、防毒系統之架設、設定與管理等服務 (D) SOC 工作包含應用程式碼的解析、程式壓力測試與報告
B	9. 關於風險評鑑（Risk Assessment），下列敘述何者「不」正確？ (A) 風險評鑑可以參考 ISO/IEC 31010:2019 (B) 根據風險評鑑的結果，可能有幾種決策：避免、分擔、降低、拒絕等四種處理風險方式 (C) 風險評鑑流程可以提供企業一套有系統、可量化的方式進行評估 (D) 風險評鑑結果可讓企業決定要對這樣的風險做什麼處置或防護來降低該風險，或降低該風險造成的影響
C	10. 下列何者是進行定性（Qualitative）風險分析使用的方法？ (A) 資產產值

	(B) 發生次數 (C) 風險矩陣 (D) 損失金額
D	11. 關於風險接受（Risk Acceptance），下列敘述何者「不」正確？ (A) 在風險影響與處理對策之間取得平衡，決定組織可接受之風險值 (B) 高於可接受的風險值，應優先控管或處理 (C) 用於決定是否接受某風險 (D) 風險控制措施即是緩解風險的途徑
B	12. 實施風險控制措施（Risk Control）的目的為下列何者？ (A) 消除風險並消除損失的可能性 (B) 降低風險並減少損失的可能性 (C) 消除風險並減少損失的可能性 (D) 降低風險並消除損失的可能性
D	13. 如附圖所示，若將風險情境分為四個象限，關於四個風險處理的選擇，下列何者敘述較適切？  (A) 象限(一)：避免（Avoid），象限(二)：降低（Reduce） (B) 象限(二)：降低（Reduce），象限(四)：分擔（Sharing） (C) 象限(三)：分擔（Sharing），象限(四)：避免（Avoid） (D) 象限(一)：避免（Avoid），象限(二)：分擔（Sharing）
D	14. 網站遭遇入侵行為時，關於採取之風險應變處置及改善，下列敘述何者較「不」適當？ (A) 用防火牆或網站應用程式防火牆（Web Application Firewall, WAF）先暫時將此風險做偵測跟阻擋 (B) 採用弱點掃描工具或滲透測試服務驗證是否完成修補 (C) 使用原始碼檢測確認是否有其他類似弱點 (D) 先將網站備份，再進行資料復原作業

C	15. 某公司員工數約 5,000 人，所有員工皆配備一台筆記型電腦，每台筆記型電腦價值：30,000 元，若筆記型電腦遺失，價值將 100%受損，今年公司遺失數量 5 台筆電，請問年度損失期望值（Annualized Loss Expectancy）為下列何者？ (A) 15,000 元 (B) 300,000 元 (C) 150,000 元 (D) 30,000 元
A B C	16. 根據 ISO/IEC 27001:2013，在資訊安全管理系統實施時，下列哪些是要求要留下文件化資訊紀錄的項目？（複選） (A) 資訊安全政策的規範 (B) 風險評鑑與風險處理的過程與結果 (C) 資訊安全目標的內容與監督量測的結果 (D) 實施資訊安全管理系統的優點
B C D	17. 關於多層次縱深防禦（Diversity and Defense-in-Depth），下列敘述哪些較正確？（複選） (A) 以勒索病毒破壞為例，因無絕對解決方案，故沒有多層次防禦的相關機制 (B) 多層次縱深防禦就是利用多層次的防禦技術來阻絕不同類型的攻擊 (C) 多層次縱深防禦架構會涵蓋：管理、實體裝置、技術三個控制層面來達成安全管理的目標 (D) 多層次縱深防禦機制可達到嚇阻（Deter）、偵測（Detect）、延遲（Delay）、禁制（Deny）的效果
A B D	18. 某公司共有 500 名員工，在疫情期間啟用遠距在家上班的應變計畫，關於遠距上班，下列敘述哪些較正確？（複選） (A) 在規劃遠距上班方案時，應滿足同時上線及可由外部連入公私單位內部之線路頻寬大小 (B) 需要注意虛擬私人網路（Virtual Private Network, VPN）設備負載連線數，以及是否需要擴充更多 VPN 設備，而 VPN 設備亦必須修補其韌體漏洞 (C) 使用第三方視訊會議系統，應嚴守不將機敏性資訊貼附在討論群組，但可將機密性資料上傳到不被信任的雲端空間 (D) VPN 連入後，應以職務區隔（Segregation of Duties, SOD）及零信任原則開通員工使用資訊系統與服務之權限，並搭配監控機制確保機密資料不會外洩
A	19. 關於資產威脅實施風險處理流程，下列哪些為風險分擔（Risk Sharing）

C	的方法？（複選） (A) 將風險分擔給委外的廠商 (B) 藉由加強控制風險的措施，而將該風險威脅發生機率降低 (C) 將此威脅造成的風險，向保險公司買保險 (D) 藉由針對該威脅增加控制流程，而將該風險影響降低
A B D	20. 某公司規劃成立新的國際數據資訊中心（International Data Corporation, IDC），委請外包廠商針對風險評估與分析結果提出建議調整方案，關於外包廠商提出之建議，下列敘述哪些較「不」合適？（複選） (A) 建議設計柴油發電機組與 UPS 電池室於地下室，並設有排煙口於一樓停車場旁，降低噪音與空汙問題 (B) 建議在 12 頂樓設有一台水冷式冷氣機 (C) 建議機房採指紋門禁管制進出電動門 (D) 建議消防氣體採二氧化碳氣體，當火災發生時會緊閉機房，噴射滅火氣體
	（題組 1） A 集團是全球知名飯店集團，目前在全球超過 120 個國家，擁有約 6 千家旅館，旅館遍及亞洲、美洲、歐洲等地，並於 2016 年收購位於美國紐約的 BB 酒店。 在 2018 年，BB 酒店房務系統遭駭客入侵造成 3 億多筆個資資料外洩，已知外洩資料中，包含客戶的姓名、通訊地址、電話號碼、電子信箱、護照號碼、出生日期、性別等資料。 經查發現，這並不是 BB 酒店第一次遭駭客入侵而外洩客戶資料，早在 2014 年，BB 酒店就曾發生過客戶個資外洩事件。
C	21. 題組背景描述如附圖。請問 BB 酒店 2018 年的資料外洩事件，是否會受歐盟依一般資料保護規範（General Data Protection Regulation, GDPR）裁罰？ (A) 不會，GDPR 對於總部不在歐盟成員國的企業沒有司法管轄權 (B) 不會，由於系統遍及全世界，應由聯合國進行裁罰 (C) 會，由於系統內包含大量的歐盟成員國公民資料，且 BB 酒店亦有設置在歐盟內 (D) 不一定，因 BB 酒店在本案也是受害者
D	22. 題組背景描述如附圖。A 集團在併購前 BB 酒店前未確認 BB 酒店於 2014 年已發生過訂房系統個資外洩，請問 A 集團可能違反下列何種原則？ (A) 僅知原則（Need to Know）

	(B) 僅用原則（Need to Use） (C) 適度關注（Due Care） (D) 盡職調查（Due Diligence）
D	23. 題組背景描述如附圖。BB 酒店洩漏的個資還包含客戶信用卡資訊，根據發卡銀行要求，下列何種個人資訊最不應被儲存？ (A) 信用卡用戶姓名（Name） (B) 信用卡有效期限（Expire Date） (C) 信用卡號碼（Card Number） (D) 信用卡安全碼（Security Code）
C	24. 題組背景描述如附圖。A 集團在事前投保網通保險（Cyber Insurance），可使損失有效降低，關於網通保險，下列敘述何者「不」正確？ (A) 屬於風險處理中的風險分擔（Risk Sharing） (B) 可將處理事發後的成本納入保單範圍 (C) 可將商譽損失納入保單範圍 (D) 可將後續訴訟成本納入保單範圍
	（題組 2） 實務上，資訊安全架構規劃並不侷限在網路（Network Security）與端點（End-Point）的安全架構，亦包含實體安全（Physical Security）架構、軟體開發（Software Development）安全架構、服務（Service）環境安全架構、以及專案資訊系統（Information System）安全架構、資訊安全制度（含維運作業）架構…等 若您為 IC 設計公司的資安工程師，負責端點（End Point）安全架構，舉凡 PC、Laptop、Printer、Server、FAX、Copy Machine、Smartphone 等都是端點及其附屬周邊（USB、Bluetooth、紅外線）都有控管記錄或禁用。 公司已嚴格控管網路、電子郵件發送、禁止攜入手機、儲存裝置與 Wi-Fi，印表機等輸出裝置都有備份紀錄外且採用金屬保密紙，無法連接外部網路，外接儲存裝置與讀卡機也禁用，出入口亦都有金屬探測門檢查，全公司電腦採用 Windows OS，因為 IC 設計仍會用命令列介面（Command-Line Interface, CLI）形式操作第三方客戶提供的 Linux 開發板，但卻出現公司研發機密資料外洩給競爭對手事件，請就上述情境回答下列問題。
C	25. 題組背景描述如附圖。請問下列哪些可能是您沒顧慮到因而導致資料外洩的原因？ (A) 透過電子郵件將資料寄出 (B) 透過 USB 外接儲存裝置 (C) 透過開發板上 SD 卡，將開發板模擬成網卡

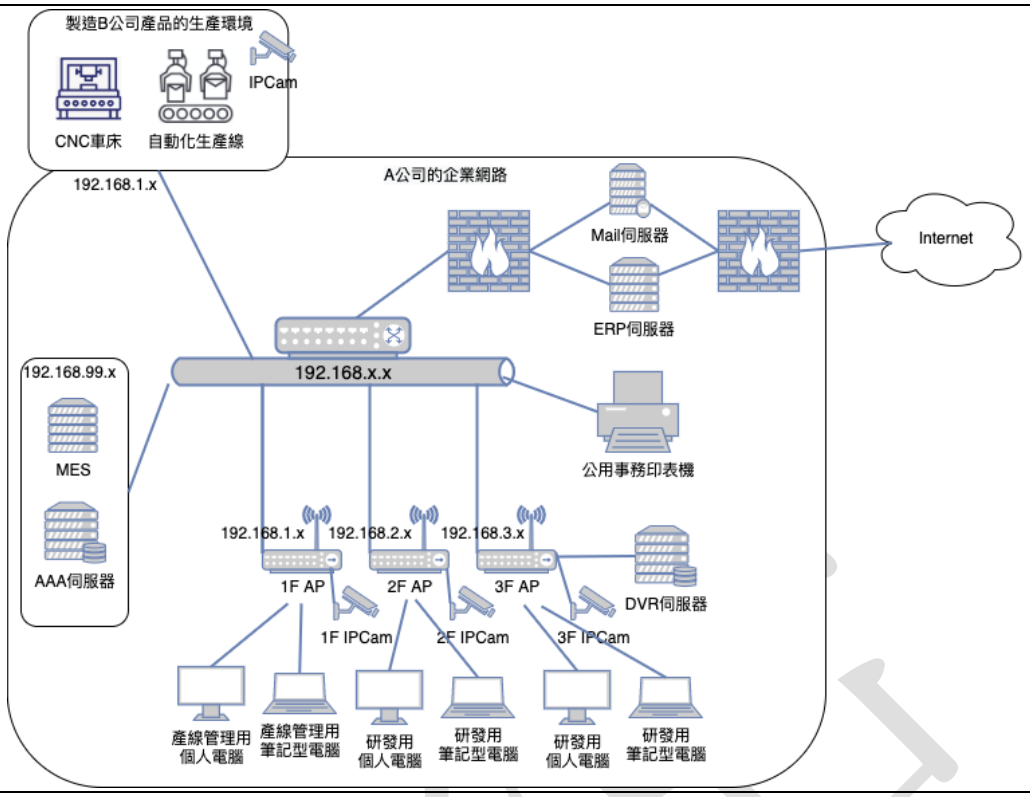
	(D) 透過手機拍照
D	26. 題組背景描述如附圖。承上題，您在資料外洩事件後進行資安事件鑑識工作，透過公司已安裝本機型的資料外洩防護（Data Loss Prevention, DLP）系統，發現外洩的研發檔案、端點電腦的檔案之人為操作皆有管控並留下紀錄，對於檔案及目錄的新增、開啟、刪除、更名、列印甚至權限變更亦都有啟用管控機制、稽核紀錄，未見到任何寫出到 USB 與外接儲存裝置的軌跡紀錄。請問下列哪些可能是您沒顧慮到而導致資料外洩到競爭對手公司的原因？ (A) 缺乏列印成 pdf 管控設計 (B) 缺乏滑鼠拖拉檔案管控記錄 (C) 缺乏檔案寫出寫入記錄 (D) 缺乏命令列介面（Command-Line Interface, CLI）指令行為（SSH, Telnet）記錄
B	27. 題組背景描述如附圖。若您於事件結束後，轉換工作擔任某系統整合商（System Integration, SI）資安工程師，近期公司承接政府一級單位某資訊系統建置案，政府一級單位皆通過 ISO/IEC27001 認證，並在需求建議書（Request for Proposal, RFP）文件中要求：(1)在系統上線前與保固期間該專案軟體必須每季通過 OWASP Top 10 安全檢測、(2)相關程式源碼必須通過白箱檢測、(3)系統上線前應修補與提出對應防護機制，來完成硬體、作業系統、Web Service（如：IIS7, Tomcat, WebLogic）漏洞、(4)上線後還需經過第三方滲透測試。若您要進行安全技術作業來滿足上述軟體開發安全架構、服務環境安全架構需求，下列敘述何者「不」正確？ (A) 建議該單位通過 OWASP Top 10 安全檢測，通常可採用安全測試工具，如：Acunetix、WebInspect (B) 可採用白箱檢測（white-box testing），又稱源碼分析（Source Code Analysis）工具，可以分析已經 Compile 後的執行檔程式，如：Fortify、IDA Pro (C) 在 Web 服務的防護對策，建議該單位採購網站應用程式防火牆（Web Application Firewall, WAF）來進行過濾攔阻攻擊行為，而 WAF 有軟體式與硬體式規格 (D) 在滲透檢測（Penetrant Testing, PT）作業上，因為已經是上線對外服務的系統，在滲透攻入成功後，應嚴守不破壞該資訊系統程式與資料
C	28. 題組背景描述如附圖。承上題，該資訊系統已經上線進入維運階段，通常需求建議書（Request for Proposal, RFP）會要求該專案保有 10%~15%新功能擴充設計的條款，以滿足該資訊系統對外服務實際需

	要。維運階段必須有一個功能版本與上線系統功能一致的測試系統網站，來驗證維運時期的新增程式功能。軟體開發工程師必須將新開發程式放上該測試網站，提供政府一級單位（甲方）進行驗證，驗證通過後更新到正式系統。當您在面對維運階段的資訊安全制度（含維運作業）架構時，下列敘述何者正確？ (A) 該測試系統應對外開放，以利甲方進行測試驗證 (B) 軟體開發工程師開發好程式後，應放在測試系統提供測試，不需要再進行黑白箱檢測 (C) 測試系統上的測試資料，必須是經過甲方同意後的混淆假資料 (D) 甲方在測試系統驗證完成後，對該系統進行程式更新，此時不需要進行任何 ISMS 安全變更程序
	（題組 3） C 公司已投入電子商務 2 年，雖然疾情對既有傳統商務有些微影響，但是整體電子商務營運仍持續成長，並且已達到必須增建機房設施與系統容量之際，身為資訊部門的主管，您必須要在擴充資訊系統之際，同時規劃兼顧提昇系統資訊安全的任務，請就上述情境回答下列問題。
B	29. 題組背景描述如附圖。關於 CNS 27001 資訊安全管理系統與 CNS 27002 資訊安全控制措施作業規範，下列何者「不」是 C 公司啟動資訊安全管理系統最須優先處理的作業？ (A) 建立管理框架，於組織內啟動及控制資訊安全之實作 (B) 識別既有電子商務系統風險，確保相關資訊受到適切等級的保護 (C) 於最高層級上定義資訊安全管理政策，明列組織管理資安目標之作業，並由管理階層核准 (D) 依據營業要求及相關法規，提供資訊安全之管理指導方針及支持
B	30. 題組背景描述如附圖。關於資訊安全管理系統(Information Security Management System, ISMS)提供的風險評鑑方法，藉由資產分類，並判斷其價值與重要性，作出弱點及威脅分析，進行風險分析、風險評估及風險處理的規劃流程，對 C 公司而言，在企業有限的資源下，下列何者在風險控管處理上較「不」適切？ (A) 根據風險評估與業務營運衝擊做出的決定相關資安資源投入的多寡 (B) 風險評估完成後，所有風險項目必須擬訂風險改善計畫，明定管理階層的責任範圍與一般步驟處理 (C) 由風險值之高低決定風險控管之優先順序，風險處理對策應採取適當的控制措施與風險避免的方法，以達到降低風險發生機率或影響程度 (D) 極度危險的風險，就需要立即採取行動，高度危險的風險，管理

	階層需督導所屬研擬計畫並提供資源，但是發生機率低的項目可以採用風險分擔模式
A B D	31. 題組背景描述如附圖。依據行政院技術服務中心 109 年第 4 季資通安全技術報告，統計分析現況資安威脅發現，以「非法入侵」（占 56.39%）類型為主，排除綜合類型「其他」外，其次分別為「設備問題」（占 12.78%）」與「網頁攻擊（占 6.77%）」為主要通報類型。請問下列哪些作為可以大幅減少 C 公司電子商務的資安威脅？（複選） (A) 建立完整的帳號管理與密碼規範，並重新檢視各系統所有使用的操作權限，將權限設定最小化強化帳密管理 (B) 確認做好 DMZ 區域與內網安全存取管理，將網頁服務與資料庫分區管理，減少交易資料與個資洩漏 (C) 電子商務軟體進行軟體弱點掃瞄，且針對程式弱點進行網頁程式修改，減少商業邏輯漏洞 (D) 結合 IPS 入侵防禦系統、WAF 應用程式防火牆、AV 防毒系統、郵件防護系統建構多層次防禦架構
C	32. 題組背景描述如附圖。營運持續管理的資訊安全構面在於防治營運活動的中斷，保護重要營運過程不受重大資訊系統失效或災害的影響，並確保及時的回復，關於營運持續，下列敘述何者較「不」正確？ (A) 依據 ISO/IEC 27001 規範提出組織持續營運所需的資訊與資訊安全要求、並識別能導致營運過程中斷的事件，以及它們對資訊安全的衝擊與後果 (B) 遵循 ISO/IEC 27001，組織應考量多重備援之方案，規劃資訊處理設施之可用性的相關控制措施 (C) 參閱 ISO 22301 營運持續管理系統的框架，組織擬訂之營運持續計劃（Business Continuity Plan, BCP）應必須包含：計劃啟動條件、緊急應變程序、減災程序、後撤及召回程序、維護時程表、定期演練以及教育訓練等相關作業 (D) 組織發展與執行 BCP 持續營運計劃時，除關鍵活動中斷或設備障礙需於必要時間內恢復營運，也應定期測試與更新，以確保持續的適當性、充分性、及有效性
	（題組 4） D 公司主要業務為提供客戶雲端存儲服務，基於對客戶的保障，已通過 ISO/IEC 27001 驗證，並訂定資安政策及資安目標，其中一項資安目標為提供客戶存儲服務系統，中斷服務不可超過 4 小時，因此相關系統及環境皆依此標準建置。 2020 年初，因疫情影響，公司評估此為重大事件，發現先前制定的分艙分

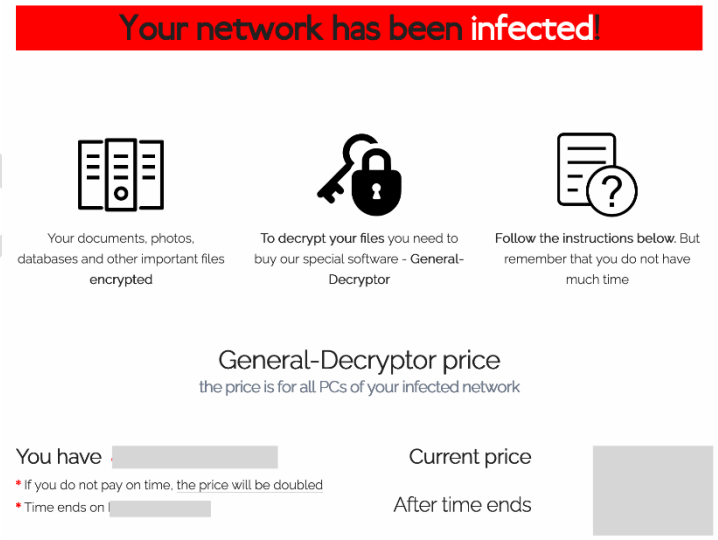
	流計畫不足以因應現況，故決議導入居家辦公系統，以便在公司受到疫情影響無法進入公司辦公時，能有效維運存儲服務系統，不中斷對客戶的服務，並於同年 4 月完成系統建置，讓系統維運及公司人員可透過此系統進入公司內網進行工作並對客戶提供服務。 因 D 公司因應得宜，受到某重要客戶青睞，於 2020 年 6 月與該重要客戶簽約提供資料存儲服務，合約中載明系統中斷不可超過 1 小時，公司評估未來營運成長需求，決定對提供客戶存儲服務之系統，設置異地備援之存儲服務系統，且主機房存儲服務系統中斷時，可自動切換至異地存儲服務系統，以避免區域性災難與滿足客戶要求。
B C D	33. 題組背景描述如附圖。D 公司因疫情影響，決議導入居家辦公系統，依據 ISO/IEC 27001 之規範，下列哪些行為是 D 公司應進行之事項？（複選） (A) 新系統導入後，須重新申請 ISO/IEC 27001 之驗證 (B) 審查資安政策確認其合宜性 (C) 針對此變化進行風險評估 (D) 審查與訂定並執行遠距工作的政策及支援之安全措施
B D	34. 題組背景描述如附圖。資訊單位負責導入居家辦公系統，進行系統安全評估時，評估考量項目應包括下列哪些評估事項：1.功能性需求評估、2.供應商評估、3.系統安全性評估、4.容量管制評估 (A) 123 (B) 234 (C) 12 (D) 34
C	35. 題組背景描述如附圖。若 D 公司決定要符合合約所述的系統維運規格，下列哪些備援模式及敘述為較可行之方案：1.Cold Site（冷備援）、2.Warm Site（暖備援）、3.Hot Site（熱備援）、4.異地備援系統設置於隔壁棟大樓、5.異地備援系統設於與公司所在地不同縣市 (A) 1234 (B) 2345 (C) 35 (D) 235
A	36. 題組背景描述如附圖。若建議異地備援機制後，仍因相關風險事件發生，D 公司進行居家辦公時，提供客戶之存儲服務系統仍出現中斷超過 1 小時的現象。請問造成上述中斷 1 小時的原因可能為下列何者？1.機房發生事故，機房內所有系統中斷超過 2 小時、2.居家辦公系統未設置系統災害復原計畫，導致居家辦公系統無法及時啟動異地備援機

	制、3.主機房之存儲服務系統當機無法使用、4.居家辦公系統及機房內之存儲服務系統同時中斷超過 2 小時 (A) 14 (B) 123 (C) 1234 (D) 234
	（題組 5） A 公司為先進資通訊產品代工製造商，為台灣股票公開發行公司，接受美國知名大廠 B 公司委託代為生產 B 公司所研發與設計商品，為了保護 B 公司的產品設計的機密與安全，A 公司在與 B 公司的製造的合約中，有嚴格的保密條款要求不得以任何型式洩露 B 公司的任何有關他們設計的產品資訊。A 公司也向 B 公司宣稱所有 B 公司委託生產製造的生產線皆採用獨立的生產線及網路實體隔離不與 Internet 連接（如下圖）。 B 公司生產環境的廠區 24 小時全面監控 IPCam 將錄影資訊留存於 A 公司的 DVR 伺服器中，保存 6 個月之久，所有的管理帳中集中於 AAA 伺服器中，由專人管理，絕對安全可靠。 此外，為方便管理 B 公司產線共用 A 公司的製造執行系統 MES（Manufacturing Execution System），提供自動化的製造排程與即時的圖表式看板供產線管理人員及 B 公司相關人員即時監控實際的生產狀況，如有任何異常立即排除。



D

37. 題組背景描述如附圖。某日 A 公司員工發現收到附圖的電子郵件勒索信，請問 A 公司是受到下列何組織/集團的加密勒索？



(A) Revil

(B) Conti

(C) DoppelPaymer

(D) 無法確認是否真的是加密勒索

C

38. 題組背景描述如附圖。承上題，依據「臺灣證券交易所股份有限公司對有價證券上市公司重大訊息之查證暨公開處理程序」新修訂的條文，第四條第一項第二十六款所述「發生災難、集體抗議、罷工、環境污

	染、資通安全事件或其他重大情事...」的規定，下列敘述何者較為正確？ (A) 此為臺灣證券交易所股份有限公司的內部規範，不需要依規定進行訊息揭露 (B) 只要是資通安全事件，皆應依規定發佈重大訊息 (C) 應進一步評估是否構成造成公司重大損害或影響，再確認是否需公開揭露 (D) 重大訊息揭露與否屬於內部控制範疇無需進行資訊揭露
A B	39. 題組背景描述如附圖。關於本題組的敘述與網路架構圖進行資訊安全風險的評估，下列敘述哪些較為正確？（複選） (A) 代 B 公司生產環境的網路的區隔可能較不完整 (B) A 公司內部的網路隔離較為薄弱 (C) ERP 系統放置於 Internet DMZ 區較不適宜，應與圖中的 MES 放置於同網段最為安全 (D) A 公司的研發電腦網路與 B 公司生產環境網路無法互通
A	40. 題組背景描述如附圖。若要強化 A 公司的工控製造資通安全管理，應導入下列何種標準較為合適？ (A) IEC 62443-2-1 (B) IEC 62443-2-4 (C) ISO/IEC 27701 (D) BS 10012