108 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： 108 年 9 月 7 日　　第 1 頁，共 13 頁

單選題 15 題，複選題 5 題，題組題 5 題（佔 100%）

B	1. (單選題) 某中央一級單位通過 ISO/IEC 27001 認證，公務資訊中心位置在台北市中正區。另有對外 7x24x365 Web Based 便民資訊系統與資料庫，以虛擬機制建立在中和機房，關於資訊安全管理建置，下列敘述何者「不」正確？ (A) 該單位資訊中心需定期驗證備份資料，確保資料系統高可用性 (B) 異地備援中心選擇「永和辦公室」主要考量因素是距離近 (C) 建議「異地備援機房建置」參考行政院「電腦機房異地備援機制參考指引」為佳 (D) 便民資訊系統應建立服務層級協議（Service Level Agreement, SLA），資訊系統建立負載平衡，資料庫建立高可用性架構尤佳
D	2. (單選題) 公司在招募新員工時，若打算在網頁上公布錄取榜單，下列敘述何者「不」正確？ (A) 公布招募新進員工之榜單，應先依法取得當事人之書面同意 (B) 自然人之姓名，屬個人資料之範疇，故公布榜單之行為必須符合個資法規範 (C) 若因取得當事人書面同意之作業有窒礙難行之處，採「匿名化」、「去識別化」方式公布榜單，為較適切的作法 (D) 因同名同姓的人很多，若只公告單一項姓名資料，並無法直接識別出本人，不需取得當事人之書面同意
C	3. (單選題) 依據我國《資通安全管理法施行細則》條文中規定，下列何者「不」是資通安全維護計畫應（強制要求）包括的事項？ (A) 核心業務及其重要性 (B) 資通安全政策及目標 (C) 實施安控的作業程序書 (D) 專責人力及經費之配置
D	4. (單選題) 在進行職務規劃時，下列何種情境宜優先考量是否有職務區隔（Segregation Of Duties, SOD）之設計？ (A) 執行資安內部稽核時，業務人員負責查核資訊單位的資安事故通報作業流程 (B) 程式設計人員於程式上架更新時，應在負責更新系統程式的資訊部門待命 (C) 採購人員於向廠商下單訂購前，應在庫存系統確認庫存數量 (D) 人力資源部門主管，負責人資資訊系統之更新與維護

B	5. (單選題) 規劃縱深防禦（Defense in Depth）時，我們常會採用多種不同面向的管控措施（Controls），下列何者屬於預防性存取管控措施（Preventative Access Control）？ (A) 側錄系統（Session recording system） (B) 加密（Encryption） (C) 備份（Backup） (D) 入侵偵測系統（Intrusion detection system）
B	6. (單選題) 關於區塊鏈（Blockchain）技術，下列敘述何者「不」正確？ (A) 原始概念為去中心化的架構設計 (B) 比特幣的 Hash Chain 符合我國電子簽章法中數位簽章的描述 (C) 在實務上不容易竄改交易的內容 (D) 可採用工作量證明加強交易的不可否認性
D	7. (單選題) 關於安全架構規劃實務，下列敘述何者「不」正確？ (A) 企業政府多以租賃影印傳真系統方式提供服務，在年度回收更換影印傳真設備時，應對該設備硬碟暫存區進行清理，或依合約要求廠商硬碟交回租賃方回收銷毀處理 (B) 在公務場域內之公發（務）電腦或行動裝置，應加裝防毒防駭系統加以保護，委外廠商私帶裝置進入公務場域使用，亦需經過防毒掃描後放行 (C) 不論是多協定標籤交換（Multi-Protocol Label Switching, MPLS）或是 Site to Site VPN 所建立外點連線機制，都應建立各段的防火牆機制或網段政策 (D) 企業員工因出差在外連回單位電腦工作，可自行搭建虛擬通道（tunnel）連接公司內電腦與系統
D	8. (單選題) 資訊單位負責導入新 ERP 資訊系統，進行系統安全評估時，評估考量項目應包括下列哪些項目？ 1.系統安全性評估 2.容量管制評估 3.實體環境安全 4.使用者功能性需求評估 (A) 1234 (B) 134 (C) 13 (D) 123

C	9. (單選題) 關於網路區隔，下列敘述何者較「不」可行？ (A) 依安全等級、組織或特定的目的進行區隔 (B) 以實體網路或邏輯網路區隔 (C) 明確的定義無線區域網路的周界（Boundary）並加以控制 (D) 周界使用閘道如防火牆或過濾路由器（Filtering Router）加以控制
A	10. (單選題) 某公司 EIP 系統，建立在 ESXi 5.0 虛擬環境中，EIP 虛擬機硬碟容量 500GB，已經使用 200GB，近期實體硬體主機發生不定時重新開機，屬舊型主機，面板看出燈號已經亮起，卻無相關資訊，最後發現 RAID 卡電池膨脹故障，關於風險處理程序與分析，下列敘述何者較「不」適當？ (A) 應將 ESXi 5.0 系統掛入不同版本的 VCenter 系統中，將其遷移至其他虛擬主機，以確保正常運作 (B) 實體主機面板警示燈號亮起，卻無資訊可分析，應接入 Console 設法連線主機，取出警示錯誤訊息，進行判讀 (C) RAID 卡電池故障，應先將虛擬機移至其他主機後，才能再進行 RAID 卡電池更換 (D) 應先確認相關備份作業是否完成，且可被復原，才進行 EIP 系統遷移
C	11. (單選題) 某機敏單位遷移至公司大樓 23 樓辦公，23 樓只有該部門專用。若從實體安全規劃評估的角度來看，下列敘述何者風險較高？ (A) 該部門屬於機敏單位，且獨立使用 23 樓，建議電梯樓層鎖定，限定只有該部門員工可以抵達 23 樓 (B) 在逃生梯間，應設立充足的監視器與防盜警報機制，防止閒雜人等由逃生梯進入到該樓層 (C) 外來包裹，可以由警衛放行，刷電梯卡直接送至 23 樓 (D) 在 23 樓，應再設立一道門禁關卡，進行人員過濾
A	12. (單選題) M 公司引進最新的科技，大幅度的改善公司重要的資訊系統，雖然功能相同，但效能更快與使用更便利。若從資安的角度來看，下列敘述何者較佳？ (A) 因在重要系統上進行改變，故需要進行風險評估 (B) 因重要系統之更新，其功能相同，故不需要進行風險再評估 (C) 因功能不變，故可視需要調整風險接受度 (D) 因在重要系統上進行改變，故需要進行調整資安政策
A	13. (單選題) 公司網站系統屬於公司門面，網站系統因對外服務，常常成為

	駭客入侵的首要目標，網站風險問題一直居高不下，就有效降低網站風險處理實務，下列敘述何者正確？ (A) 對於公司網站應定期進行網站黑箱檢測以及系統弱點掃描，對其程式碼應進行 Code Review (B) 網站前端呈現與後台管理系統，在資料庫安全設計上，連線 DB 的帳號密碼不需要區隔讀取與寫入刪除資料庫權限區隔 (C) 工程師在系統上直接更新新版程式，將舊版程式改名成 bak 作為歷史留存在上線官網系統中，以便日後改錯後有原始程式碼做修正使用 (D) 網站已經建立網站應用程式防火牆（Web Application Firewall, WAF）系統，其主機作業系統不需要再升級更新
A	14. (單選題) 在網站弱點檢測報告中，發現系統本身有存在 Path Manipulation 問題，可以採取下列何種方案進行修補？ (A) 可以使用白名單路徑跟黑名單危險字串過濾 (B) 可以採用圖像式驗證即可根治 (C) HTML.Encode (D) 採用 Prepare Statement
D	15. (單選題) M 公司位於 Q 大樓一樓，每年的颱風季節，網管人員很擔心相關設備因淹水而損壞，經反映問題給高階主管後，管理階層決定購買相關保險以因應相關的風險。請問上述案例是風險處理中的何種選項？ (A) 風險緩解（Risk Mitigation） (B) 風險接受（Risk Acceptance） (C) 風險規避（Risk Avoidance） (D) 風險轉移（Risk Transference）
ABD	16. (複選題) 關於著作權的說明，下列敘述哪些正確？ (A) 我們常說的版權，其實就是法律上著作 (B) 屬於民事權利 (C) 作品創作完成之著作權取得，需經過主管機關審查批准 (D) 指科學、文學、藝術作品的作者，依法對其作品享有的一系列專有權
BCD	17. (複選題) 某中小企業資訊部門之業務執掌包含程式開發、程式上線、應用程式管理以及資料庫管理等，該公司因故必須縮減資訊部門人力，若您是該企業之資訊部門主管，下列哪些項目之處理較能降低資安風

	險的發生？ (A) 將部分資安工作移轉至其他業務單位 (B) 增加業務活動之監視紀錄 (C) 增加資安稽核頻率 (D) 實施工作輪調
ABC	18. (複選題) 某台灣公司在法國設廠，且帶有業務銷售功能，關於 GDPR 法遵要求，下列敘述哪些正確？ (A) 公司在法國設廠有研發業務中心，在地員工人數超過 400 人，進行在地歐洲各國銷售業務，需要在法國當地設立資料保護長職務（Data Protection Officer, DPO）來負責管控滿足歐盟當地個資隱私保護要求與法律責任 (B) 在銷售相關產品過程中，必須讓歐盟會員國公民，以清楚易懂文字描述讓當事人知道個資蒐集處理利用，獲得當事人「書面」同意 (C) 對歐盟成員國公民，該公民對公司要求撤銷個資蒐集處理利用同意書，可用艱澀法律文書限制撤銷個資程序，來做為後續分析使用 (D) 公司必須建立資安防護手段來確保歐盟公民個資不會外洩，一旦出現個資外洩需要在 36 小時，通知資料保護主管機關（Data Protection Authority）
AB	19. (複選題) 某 AI 開發新創公司規劃在 Microsoft Azure 雲端建立「儲存體」存放公司資料，與美國分公司進行資料分享，希望依賴 Microsoft Azure 既有備份備援機制，並進行相關風險評估與技術應用需求，若從資訊安全管理系統評估提出適宜之備份方案，下列敘述哪些較佳？ (A) 在雲端儲存體服務上 Microsoft Azure 提供本地備援儲存體（Locally-redundant storage, LRS）機制，不需要再建立可讀取備份機制 (B) Microsoft Azure 提供異地備援儲存體（Geo-redundant storage, GRS），可以滿足異地備份安全規定，大幅降地風險，且分屬在不同地區，距離相距 300 公里以上 (C) Microsoft Azure 亦提供更高階讀取權限異地備援儲存體（Read-access geo-redundant storage, RA-GRS），可以提供隨時讀取備份資料機制 (D) Microsoft Azure 所提供 LRS，屬於即時同步備份機制，且備份成三份資料，而 GRS or RA-GRS 則屬於非同步備份機制
AC	20. (複選題)某政府一級單位官網，交付政府維運機房代管，要求服務層級

D	協議（Service Level Agreement, SLA）99.99%服務水平，監測發現該政府官網，固定在每週週一，半夜 12:00 會自動停止服務 30 分鐘。該事件已經持續半年之久，因發生在半夜不易被人員發現。半年後才因民眾發現告知該單位有此問題，風險問題排除過程中：(1) IIS Web Server 都服務正常；(2) MS-SQL 資料庫服務也正常；(3) 防火牆也未變動其政策；(4) 檢查相關排程程有每月一次定期備份檔案到 D 磁碟某目錄；(5) 在檔案異動上發現有多了一個 Lcx.exe 惡意程序放在 Web Root 目錄；若您是該單位 IT 系統維運工程師，若從上述情境選擇合宜的風險處置措施，下列敘述哪些較佳？ (A) 長達半年未發現，是因為缺乏有效監管網站存活狀態，可利用工具建立監控機制，監控 Web Server、URL 連結、資料庫 1433 通訊，就可以知道系統 SLA 狀態與降低中斷服務的風險 (B) 以 99.99%服務水平標準來看，本次事件長達半年，以一年 365 天計算仍符合 99.99%服務水平 (C) 在 Web root 目錄出現 lcx.exe，屬被駭客入侵的資安事件，必須先通知部會主管後，緊急補救風險處理 (D) 必須在「國家資通安全通報應變網站」進行通報
	(題組題 1) 某上櫃企業已通過 ISO/IEC 27001 認證，於某上班日發現公司半數同仁 AD 帳號遭到鎖定，無法使用 AD 帳號密碼登入電腦系統。MIS 進行 AD 解鎖後，同仁隨即再次被鎖定無法登入，慌亂初期 MIS 採取區域性斷網，依然無效。 隨即分析 AD 主機事件記錄，發現都是 Exchange Server 所造成，進一步分析防火牆記錄，發現大量外部 access OWA 的 443 Port 登入失敗，有多個來源遠端攻擊者裝置嘗試入侵 Web Mail 系統失敗，類似「DDoS」與「密碼暴力攻擊」。 MIS 採取緊急應變措施，阻斷相關攻擊者裝置 IP。可是每隔一段時間會自動換成其他國家地區 IP 持續入侵攻擊，MIS 進一步將境外非台 IP 全面禁止，以短暫維持運作。但相關攻擊來源竟轉換台灣地區 IP。 MIS 進一步採取關閉用外部開放使用 Exchange OWA 服務，要求公司外部活動人員須以 VPN 方式，建立裝置放行白名單方式，進行 Exchange 郵件登入作業。而 VPN 依群組方式申請建立不同放行權限，非全面開放。 並對來自台灣的攻擊裝置主機，進行反查，確認其管理公司以及人員，

	進行對主管機關進行資安通報，聯繫該攻擊方 IP 公司進行相關處理。該公司隨即停用該主機，重新安裝，中斷 C&C 在台灣中繼站，國外攻擊者 IP，則以 E-mail 通知，並於事件發生期間，全面中斷境外相關連線，直到改善為止。
A	21. (題組題 1-1，單選題) 上述情境中，關於事件發生當下之敘述，下列何者正確，且符合 ISO/IEC 27001 相關制度？ (A) 依據資安通報流程，應通報「資安官」、「資安主管」告知事件之危害以及可能處置對策 (B) 應要求相關同仁，停止登入，將相關電腦重新安裝作業系統 (C) 通知證交所發布公司重大訊息 (D) 指責委外廠商沒辦理好相關委外工作
AB	22. (題組題 1-2，複選題) 上述情境中，關於問題事件分析、作業規範、以及防護手段，下列敘述哪些正確？ (A) MIS 進行相關處置對策，亦可稱為「緊急應變措施」 (B) MIS 對應措施都必須保留相關需軌跡記錄，如：防火牆記錄、事件記錄、郵件記錄、通報記錄備份以備查，利於後續稽核作業 (C) 這類攻擊模式屬於一種 APT 攻擊行為，是很難防禦的 (D) 這次事件所受到攻擊，應該是針對特定目標人員的入侵攻擊行為
D	23. (題組題 1-3，單選題) 上述情境中，可通報下列何種單位較為合宜？ (A) 通報「行政院資安處」 (B) 通報「資策會資安所」 (C) 通報「工研院資通所」 (D) 通報「TWCERT/CC 台灣電腦網路危機處理暨協調中心」
D	24. (題組題 1-4，單選題) 上述情境中，關於 MIS 在完成事件處置過程中依據之 ISO/IEC 27001 相關制度，下列敘述何者「不」正確？ (A) MIS 需撰寫資安事件報告，作為事件處理記錄 (B) MIS 需執行矯正措施，以利 PDCA 流程管理 (C) MIS 關閉 Exchange OWA 外部服務，需填寫連線申請表單 (D) VPN 服務開啟，只需口頭告知即可
	(題組題 2) A 公司為一中小型 3C 電器設備販售商，服務客群除國內之外（總公司），觸角亦已開拓至歐洲（分公司），目前以 O2O（Online To Offline）營銷模式進行商品販售。 為刺激商品販售動能，該公司於每季均提供會員參加抽獎活動，依據

	抽獎結果以電子郵件方式通知中獎之會員，並將所獲獎品寄送至會員指定之地址。 另該公司為強化各業務活動之效能，因此採購了一批相關軟、硬體設備（軟、硬體設備資料詳如附錄一），以滿足公司自動化與資訊化的作業需求。 附錄一： I. 軟體明細: i. 作業系統 ii. 伺服器軟體 iii. 資料庫軟體 iv. 防毒軟體 v. 客製化 ERP 系統 II. 硬體明細: i. 行政電腦硬體 ii. 伺服器硬體
BC	25. (題組題 2-1，複選題) 上述情境中，關於該公司法務部門新主管為讓公司有關會員的業務活動能符合法律要求，因此提出了幾個供執行業務活動之同仁參考運用的法律規範，下列敘述哪些較正確？ (A) 政府採購法 (B) 個人資料保護法 (C) 一般資料保護規則（General Data Protection Regulation, GDPR） (D) 國家標準制定辦法
B	26. (題組題 2-2，單選題) 上述情境中，關於該公司為避免個資外洩之風險發生，公司高層指派有關部門之同仁針對前述要求進行之處理，下列敘述何者較「不」正確？ (A) 將個資外洩風險轉移至保險公司 (B) 協調會計部門保留預算 (C) 購買資安設備並進行參數之正確設定 (D) 進行個人資料之盤點
D	27. (題組題 2-3，單選題) 上述情境中，關於該公司為強化各業務活動之效能所採購之軟體，下列何者於上線前必須進行原始碼檢測？ (A) 伺服器軟體 (B) 資料庫軟體

	(C) 防毒軟體 (D) 客製化 ERP 系統
A	28. (題組題 2-4，單選題) 承上題，若活動進行中，該公司資安人員發現資料庫遭駭客入侵之處理，下列敘述何者較正確？ (A) 立即依據緊急應變程序進行 (B) 立即關閉資料庫伺服器之電源 (C) 立即通報防毒廠商 (D) 立即登入資料庫採證
	(題組題 3) 超能力公司於年初通過全公司 ISO/IEC 27001 驗證，其中關於系統維運部分的相關政策，要求重要系統中斷時間不得超過 2 小時，所有重要系統及其相關支援環境皆依此標準建立。 超能力公司年中接獲開心買公司重要訂單，由公司負責提供環境建立並維護開心買公司網路訂購系統，並於合約要求該網路訂購系統若因該公司之問題中斷超過 3 分鐘，超能力公司需賠償開心買公司。 超能力公司據此將該系統判定為重要系統，並於既有重要系統支援環境導入此新架設的購物系統，並為該系統在原機房建立備援機制。
AC D	29. (題組題 3-1，複選題) 上述情境中，關於超能力公司將接獲開心買公司訂單並導入新系統視為重大事件，依據 ISO/IEC 27001 之規範，下列哪些是超能力公司應進行之事項？ (A) 重新審查資安政策確認其合宜性 (B) 新系統導入後，須重新申請 ISO/IEC 27001 之驗證 (C) 針對此變化進行風險評估 (D) 對於新系統的導入進行安全性評估及容量管制評估
D	30. (題組題 3-2，單選題) 上述情境中，關於超能力公司依完整評估後決定的備援模式，若從公司管理決策階層的角度來看，下列敘述何者最適當？ (A) 此備援模式不正確，因為未能滿足客戶要求 (B) 此備援模式不正確，因為可能因此而被罰款 (C) 此備援模式正確，因為符合公司的相關政策 (D) 此備援模式正確，因為經過完整評估後確認產生的風險及衝擊在公司可承受範圍
C	31. (題組題 3-3，單選題) 上述情境中，關於超能力公司決定要符合合約所述的系統維運規格，下列何種備援模式最為適合？

(A) Cold Site（冷備援）
(B) Warm Site（暖備援）
(C) Hot Site（熱備援）
(D) 依照題目所述之規劃即可

C

32. (題組題 3-4，單選題) 上述情境中，若超能力公司位於台北市，為降低因地震、颱風等災害造成資訊系統停止運作之風險，公司擬設置第二備援機房，下列何縣市之降低風險效果最差？
(A) 台中市
(B) 雲林縣
(C) 基隆市
(D) 高雄市

(題組題 4)

ABC 公司為了提高資安防護，全公司通過 ISO/IEC 27001 驗證，並「每半年」安排一次後續稽核，以確保證書的有效性。

此次外部稽核派了稽核員 Kelly 負責執行三天的稽核。

受稽的資訊單位主管 Tim 拿出一份資料表，其中部分資料如下：

資產編號	資產名稱	最大可以承受中斷時間 (Max. Tolerable Period of Disruption)	目標回復時間 (Recovery Time Objective)	可用性等級 (四級：極高、高、中、低)
001	線上購務網頁主機 (Web Server)	30 分鐘	20 分鐘	極高
002	線上購物資料庫主機 (DB Server)	30 分鐘	20 分鐘	極高
003	核心交換器 (Core Switch)	60 分鐘	50 分鐘	高
004	辦公室交換機 (Office Switch)	4 小時	3 小時	低
005	對外防火牆 (Firewall)	30 分鐘	20 分鐘	極高

C

33. (題組題 4-1，單選題) 上述情境中，根據 Tim 提供的網路架構圖，ABC 公司將網頁伺服器主機，放於 DMZ（Demilitarized Zone）區，資料庫

	主機放於內網的伺服主機網段（Server Farm），員工電腦使用獨立辦公室網段，上述網段皆透過核心交換器連接，下列何項資產編號的最大可承受中斷時間（Maximum Tolerable Period of Disruption, MTPD）最可能評估錯誤？ (A) 001 (B) 002 (C) 003 (D) 004
C	34. (題組題 4-2，單選題) 上述情境中， Kelly：請問貴公司，在風險評鑑的過程中，若發現有高於可接受風險等級（Acceptable Risk Level）的項目，接下來會怎麼處理? Tim：我們會提出風險處理計劃，執行處理計畫後，再進行風險再評鑑（Re-Assessment），看是否有把風險降到可接受風險等級以下。 關於 Tim 的回答，下列敘述何者正確？ (A) Tim 回答的處理方式沒問題 (B) 有問題，風險再評鑑並不一定需要執行 (C) 有問題，風險再評鑑應在提出風險處理計畫後，即先執行 (D) 有問題，高於可接受風險等級的項目，應先詢問受影響資產的管理單位是否需處理，再決定是否提出風險處理計畫
B	35. (題組題 4-3，單選題) 上述情境中， Kelly 又接著問了下列的問題：請問風險處理，針對衝擊不高（Impact）、發生可能性高（Possibility）且超過可接受風險等級的項目，你們會採取什麼風險處理的對策？ Tim 回答：我們會採取避免/規避（Avoid）的方式，不讓這個可能的項目發生。 關於上述風險處理方式，下列敘述何者正確？ (A) Tim 的回答正確 (B) Tim 的回答不正確，應採用緩解（Modification / Mitigation）的方式 (C) Tim 的回答不正確，應採用移轉（Sharing / Transference）的方式 (D) Tim 的回答不正確，應採用接受（Retention / Acceptance）的方式
A	36. (題組題 4-4，單選題) 上述情境中，

	Kelly：Tim，貴公司的風險管理與營運持續管理執行，似乎將兩個流程整併執行。 Tim：是啊，因為這兩個流程，都需要識別重要的營運服務項目，也需要評鑑可用性的需求，加上營運衝擊分析（Business Impact Analysis）與分析各種事件的風險評鑑（Risk Assessment）的關係也很密切，所以我們是合併在一起執行。 請問 Tim 所提到的 (I)識別重要營運服務項目 (II)營運衝擊分析 (III)風險評鑑，最佳的執行順序為何？ (A) (I)(II)(III) (B) (I)(III)(II) (C) (II)(I)(III) (D) (II)(III)(I)
	(題組題 5) 醫療設備大廠 XYZ 出產的兩款醫療設備，區域醫院 QAZ 為了即時取得醫療資訊，透過網路方式使用這兩款設備，安全廠商 ABC 在區域醫院 QAZ 的安全測試時發現嚴重漏洞，可讓連上同一網路的攻擊者遠端變更系統設定，包括：藥劑、氣體、關閉警鈴和機器數值。但是 XYZ 強調這兩款設備並沒有網路連線能力，僅提供序列埠及 USB 認為漏洞並非出在機器本身，並未發布修補程式。安全廠商 ABC 聲稱雖然這兩款醫療設備本身沒有連網能力，但的確可由 TCP/IP 網路進行連線並下達指令。
C	37. (題組題 5-1，單選題) 上述情境中，主要是運用下列何種設備，使醫院得以利用 TCP/IP 網路連線到 XYZ 公司生產的兩款醫療設備？ (A) 防火牆（Firewall） (B) 網路交換器（Network Switch） (C) 網路終端伺服器（Network Terminal Server） (D) 路由器（Router）
B	38. (題組題 5-2，單選題) 上述情境中，若您是資訊安全顧問，您認為應如何改善整體事件的安全性？ (A) 立即更新這兩款醫療設備的韌體 (B) 建立網路隔離機制，並強化身份認證與存取管控 (C) 建立 VPN 使可以由遠端加密連線至醫療設備 (D) 立即更新這兩款醫療設備的通行碼

C	39. (題組題 5-3，單選題) 上述情境中，醫療設備大廠 XYZ 應該為這個問題負整體責任嗎？ (A) 需要，並應該推出新版韌體進行更新 (B) 需要，應協助解決連網問題 (C) 不需要，但需協助釐清問題並提出安全建議 (D) 不需要，安全廠商 ABC 說法太過牽強
B	40. (題組題 5-4，單選題) 上述情境中，依據我國《資通安全責任分級辦法》，醫院 QAZ 應屬於下列資通安全責任分級的哪一級？ (A) A 級 (B) B 級 (C) C 級 (D) D 級