112 年度第 2 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

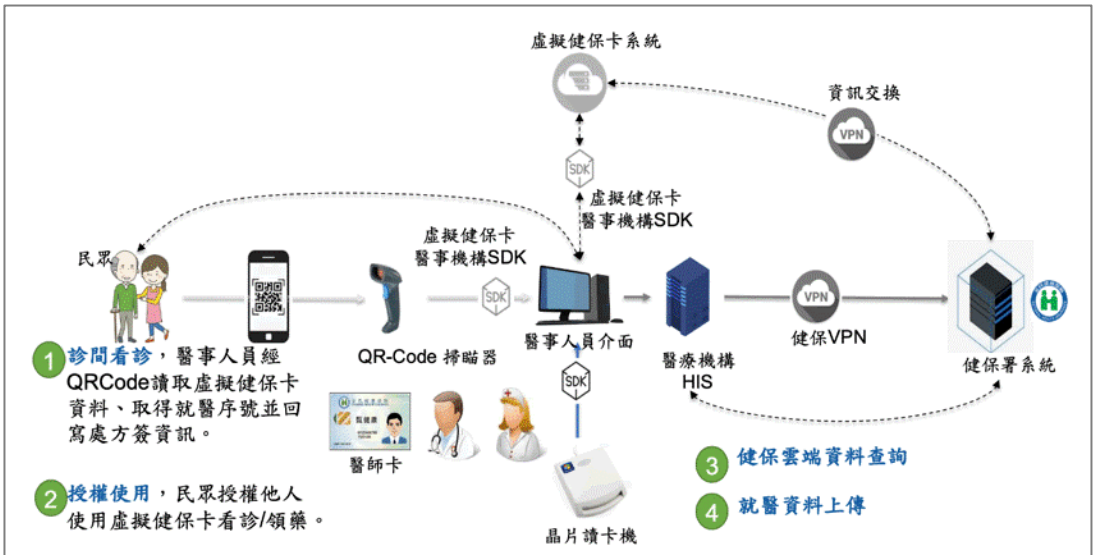
考試日期： 112 年 8 月 12 日

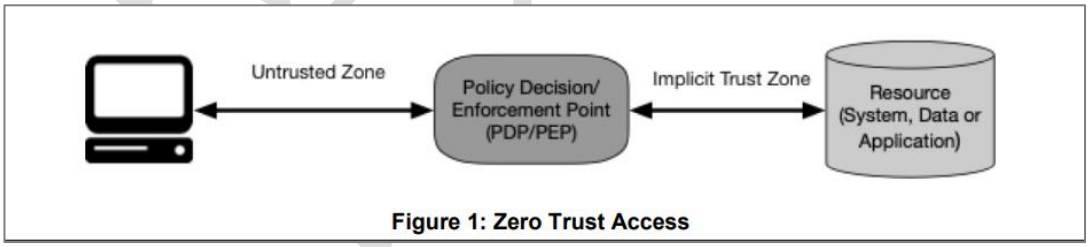
單選題 15 題，複選題 5 題，題組題 5 題（佔 100%）

C	1. 下列何項系統建置規劃並「不」是以可用性作為主要之考量基準？ (A) 建置伺服器負載平衡系統 (B) 重要資料導入高可用性（High Availability）系統 (C) 建置資料加密管理系統 (D) 使用針對重要系統建置即時備援機制
D	2. 下列何者「不」是 ISO/IEC 27001:2013 標準中「資訊安全風險評鑑」所要求組織應進行的事項？ (A) 建立風險接受準則 (B) 識別資訊安全風險 (C) 評估資訊安全風險 (D) 以最高標準處理資訊安全風險
C	3. 近年來，民間企業數位網通服務應用加驟，讓企業的資安單位從原本的支援角色轉變為重要的策略單位，而資訊安全「管理」更拉高至「治理」位階，下列哪一項可以作為企業治理資訊安全的框架及指引？ (A) ISO/IEC 27004 (B) ISO/IEC 27011 (C) ISO/IEC 27014 (D) ISO/IEC 27017
A B D	4. Z 公司為台灣上市櫃公司，主要營業項目 3C 消費性用品零售商並於實體店面及網路直接銷售給一般消費者，公司營運據點遍及歐洲及台灣。該公司並已通過 ISO 27001 驗證，請問下列哪些法規為該公司目前所必須遵守之法令規範？（複選） (A) 個人資料保護法（中華民國） (B) 上市上櫃公司資通安全管控指引（中華民國） (C) 資通安全管理法（中華民國） (D) 歐盟一般資料保護規則（General Data Protection Regulation，GDPR）

	【題組 1】 有一個在我國立案的公司，以下簡稱廠商 A，其主要營業範圍為生產某零組件，銷售予下游廠商，經其加工形成產品，才銷售予最終使用者。廠商 A 非常重視環境保護及生產品質，本身已具備 ISO 9001、ISO 14001 及 ISO 27001 等認證。廠商 A 其主要的客戶（下游廠商 B）因其主要產品銷往歐洲，故其在供應商合約中要求，除 ISO 生產品質及環保的相關認證外，供應商亦需符合 GDPR 的法律規定及通過 BS10012 的驗證。
C	5. 【題組 1】情境如附圖所示，請問廠商 A 在要符合廠商 B 合約要求的前提下，下列相關認證「不」是其需優先考慮具備的項目？ (A) ISO 9001 (B) ISO 14001 (C) ISO 27017 (D) BS 10012
D	6. 【題組 1】情境如附圖所示，請問廠商 A 已於 2 年前取得 ISO 27001: 2013 的認證，在保持認證資格的前提下，請問下列措施何者「不」合適？ (A) 定期實施內部稽核 (B) 每 3 年更新證照 (C) 因應新版本 ISO 27001:2022 推出，規劃相關升級（轉版）事宜 (D) 於明年認證期滿後，再重新驗證
A	7. 【題組 1】情境如附圖所示，請問廠商 A 在上個月進行例行的 ISO 27001 內部稽核時，發現員工缺乏對社交攻擊的認知，請問下列措施何者「不」合適？ (A) 「員工缺乏對社交攻擊的認知」為可接受之風險 (B) 進行相關員工教育訓練，讓員工了解社交攻擊 (C) 以模擬釣魚郵件對內部員工進行點擊測試用來評估教育訓練後的成效 (D) 重新評估「員工缺乏對社交攻擊的認知」可能產生

	的影響
B C D	8. 【題組 1】情境如附圖所示，廠商 A 在規畫新的客戶資料系統時，基於資安及個資等法規、認證之要求，請問應採取下項那些措施？（複選） (A) 儘可能蒐集客戶所有的資料項目作為行銷使用 (B) 系統流程中納入取得當事人同意確認 (C) 僅蒐集必要的最小資料集合 (D) 提供當事人修正的管道
B	9. 如要實施多層次防禦，下列何種措施最為合適？ (A) 在個人電腦安裝防毒軟體 (B) 運用不同網路區段，隔離不同用途的設備，並分別進行相關流量過濾措施 (C) 依照各別使用者，建立各自的電腦帳號 (D) 於作業系統中啟用檔案存取記錄，保留資料存取的相關記錄
B	10. 關於身分識別與存取管理（Identity and Access Management，IAM）的敘述，下列何者正確？ (A) 管理網路防火牆的設定 (B) 控制使用者對系統或資源的存取權限 (C) 監控網路流量與入侵偵測 (D) 保護敏感資料的傳輸
C	11. 關於職務區隔（Segregation of Duties，SOD）的說明，下列何者正確？ (A) 可以促進內部員工合作和溝通 (B) 可以確保資訊系統的可用性 (C) 可以減少內部詐欺行為或誤用之風險 (D) 可以簡化組織的工作流程
A B C D	12. 關於權限管理的說明，下列哪些正確？（複選） (A) 一旦使用者通過身份驗證後，系統會根據其授權層級與角色來分配相應的權限

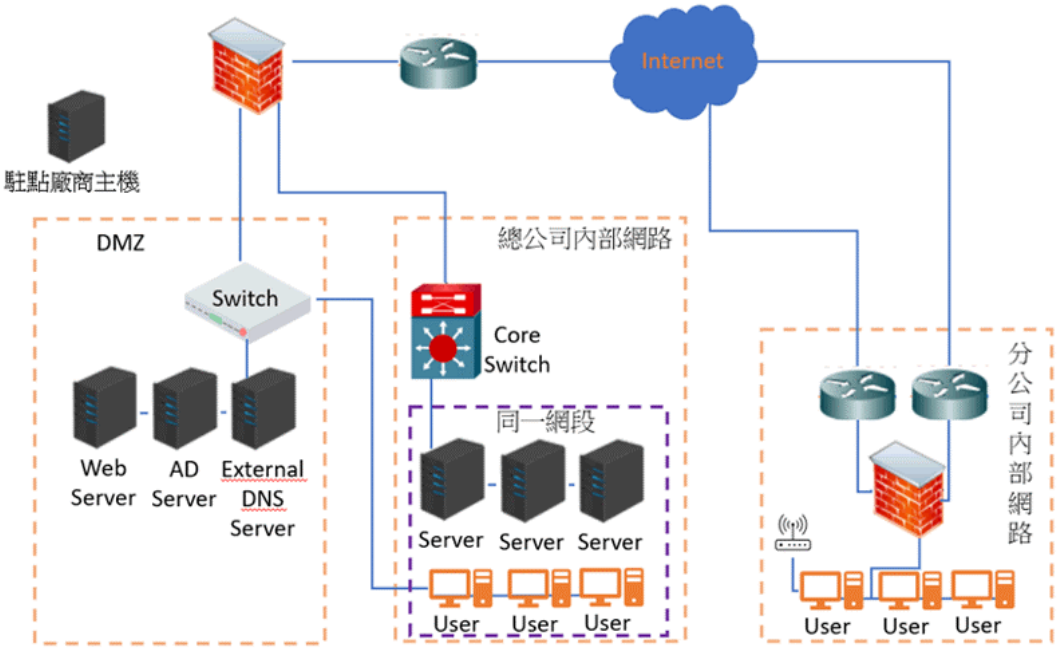
	(B) 可以確保每個使用者僅能存取其需要的資源或功能 (C) 能夠防止越權存取 (D) 可以透過以角色為基礎的存取控制（Role-based access control，RBAC）實作
	【題組 2】  健保署自民國 93 年全面換發健保晶片卡取代原先健保紙卡，配合行政院推動行動生活、智慧醫療政策推動規劃虛擬健保卡（架構與流程如下圖），推動「居家醫療」、「遠距醫療」、「視訊診療」三大場域全面推展以虛擬健保卡就醫，民眾虛擬健保卡手機端 QR 碼的有效時間為 5 分鐘，軟體讀取完成 QR 碼後可保存 1 小時。若有以下狀況虛擬健保卡 QR 碼將於該電腦失效： 1.電腦或虛擬健保卡控制軟體重新啟動。 2.同台電腦讀取不同人虛擬健保卡 QR Code。 3.同台電腦讀取同一人不同虛擬健保卡 QR Code。 4.該民眾虛擬健保卡 QR Code 由其他電腦或裝置讀取成功。 然而擴大的虛擬健保卡仍可能有安全的風險需要加以謹慎考量。
C	13. 【題組 2】情境如附圖所示，請問醫事人員經過讀取虛擬健保卡 QR 碼，再由醫事人員在 HIS 系統透過虛擬健保卡系統至健保署系統查詢資料，主要在強化下列何項程序？ (A) 識別（Identification） (B) 驗證（Authentication） (C) 授權（Authorization） (D) 稽核（Audit）
C	14. 【題組 2】情境如附圖所示，請問下列何者「不」是採用虛

	擬健康保卡的優點？ (A) 強化遠距醫療的安全與認證機制 (B) 避免未經授權的資料存取 (C) 強化實體健保卡的安全 (D) 落實健保資料使用的可歸責性
A	15. 【題組 2】情境如附圖所示，請問虛擬健保卡手機端 QR 碼的內容可能包含下列何項？ (A) 存取資料的符記（Token） (B) 持卡人的照片 (C) 持卡人的帳號及密碼 (D) 持卡人的生日
A B	16. 【題組 2】情境如附圖所示，請問透過虛擬健保卡機制的建置與運用，可能有的風險/問題有下列哪些？（複選） (A) 增加攻擊向量 (B) 與實體卡片資料同步的問題 (C) 帳號密碼的濫用 (D) 使實體健保卡的安全機制更容易被破解
C	17. 如附圖所示，關於 NIST SP 800-207 零信任架構（Zero Trust Architecture）的抽象模型敘述，下列何項錯誤？  Figure 1: Zero Trust Access (A) 政策決策點（Policy Decision Point，PDP）/政策落實點（Policy Enforcement Point，PEP）須適當判斷主體是否可存取資源 (B) 零信任（Zero Trust）提供準則與概念，可使 PDP/PEP 移動並貼近資源 (C) PDP/PEP 已提供一系列控制，因此通過 PEP 的流量便能取得最高層級信任

	(D) 隱式信任區（Implicit Trust Zone）：區域中實體至少達到最後 PDP/PEP 的信任等級
C	18. 關於網路規劃的敘述，下列何項較「不」安全？ (A) 對外服務的伺服器，設置於防火牆的 DMZ 區 (B) 外部分支機構須以 VPN 連入公司內網 (C) 將所有使用者與伺服器置於同一網段 (D) 使用入侵防護系統（IPS）協助維護內部網路安全
C	19. 關於系統災害復原規劃的敘述，下列何項錯誤？ (A) 恢復點目標（RPO）的設定應考量資料備份頻率 (B) 最大可中斷時間（MTD）的設定，應符合組織所訂定之可用性的資安目標 (C) 恢復時間目標（RTO）之設定與最大可中斷時間（MTD）無關 (D) 營運衝擊分析（BIA）可協助評估各個系統的重要性
A C D	20. 端點偵測與回應（Endpoint Detection and Response，EDR）係指可偵測並調查主機以及端點上的一些可疑活動，並透過自動化方式通知資安團隊進行快速回應的資安措施，關於 EDR 所提供的主要功能的敘述，下列哪些正確？（複選） (A) 主動監控端點，並針對具有威脅跡象的活動收集資料 (B) 對蒐集的主機弱點執行分析，以識別是否有任何未知的威脅模式 (C) 針對所有已識別威脅產生自動回應，以移除或遏止威脅 (D) 利用分析和鑑識工具，針對可能導致其他可疑活動的已識別威脅執行研究

【題組 3】

某公司高層要求內部資訊人員重新調整公司內部資訊系統、網路架構以及資安管理架構與程序等相關事宜之規劃，為避免因 ISP 業者之網路可用性遭受破壞，造成該公司對外業務運作遭受影響，故資訊人員所規劃出之網路架構如下所示：



C 21. 【題組 3】情境如附圖所示，請問避免因 ISP 業者之網路可用性遭受破壞，造成該公司對外業務運作遭受影響，下列改善方式何者正確？

(A) 總公司網路架構已區分為內部網路與 DMZ 區，甚為妥適亦無任何改善空間

(B) 可增購另一路由器當做備援設備

(C) 可增購另一 ISP 業者之備援網路

(D) 可增購另一網路交換器當作備援設備

A 22. 【題組 3】情境如附圖所示，請問若要避免遭受勒索軟體病毒大規模攻擊的事件發生在公司內部網路的資訊設備上，下列何項控制措施錯誤？

(A) 內部網路增購 L3 交換器

(B) 安裝防毒軟體

(C) 定期更新病毒碼

(D) 實施內部網路之網路區隔，例如依據內部組織別或

	功能別切分 VLAN
B	23. 【題組 3】情境如附圖所示，公司因某業務委外作業，必須允許委外駐點人員可以攜帶資訊設備至總公司內部進行作業。請問資訊人員對於此委外廠商主機攜入總公司內部之風險控管，下列敘述何者較為「不妥」？ (A) 要求僅能於總公司 DMZ 區作業 (B) 要求僅能於分公司內部網路作業 (C) 要求該委外廠商主機應安裝防毒軟體並更新病毒碼至最新 (D) 要求該委外廠商主機應將系統修補更新至最新狀態
A B C D	24. 【題組 3】情境如附圖所示，有關存取控制面向之風險，下列敘述哪些正確？（複選） (A) AD Server 配置於 DMZ 區，容易導致公司重要網域資訊遭受來自外部之攻擊 (B) 分公司內部網路 User 電腦連接未納管的無線 AP 使用，容易導致外部未經授權存取內部網路資源之風險 (C) 總公司內部網路 User 電腦連接 DMZ 區 Switch 使用，可能遭受來自於 DMZ 區未經授權存取內部網路資源之風險 (D) 總公司內部網路之 Server 以及 User 端並未進行網路切割，容易導致因 User 端所產生之風險直接影響 Server 端
B	25. 與資訊安全風險評估相關議題的敘述，下列何者較為正確？ (A) 需先進行風險評估，再將風險評鑑適用的準則予以建立 (B) 風險評估會依照風險分析的結果，安排其風險處理的優先順序 (C) 風險評鑑的順序，是先執行風險識別、再進行風險評估、風險分析

	(D) 在風險評估的過程中，無需識別風險的擁有者
B	26. 下列何者「不」屬風險管理架構的參考指引？ (A) NIST Cybersecurity Framework（CSF） (B) ISO/IEC 27035 (C) ISO/IEC 31000 (D) NIST SP 800-37
D	27. 關於資訊資產價值計算之因子，下列敘述何者錯誤？ (A) 包含該資產之機密性因子在內 (B) 包含該資產之完整性因子在內 (C) 包含該資產之可用性因子在內 (D) 包含該資產之購買金額因子在內
A B C	28. 依照我國《行政院及所屬各機關風險管理及危機處理作業原則》之規定，下列哪些作業事項屬於風險辨識（Identification）及評估（Evaluation）階段？（複選） (A) 建立、審視風險圖像（Profile） (B) 發掘相關風險資料 (C) 分析風險 (D) 布建控制措施（Controls）
	【題組 4】 A 公司主要業務係為客戶提供客製化軟體系統之開發、維護以及主機代管服務，因為甲客戶（資通安全管理法規範對象）要求 A 公司於承接委託方所委託之系統平台開發業務（委託業務費用為新台幣一仟萬元整，部分系統係利用第三方公司所開發之系統）時，公司應有 ISO 27001 資訊安全管理制度之導入並適用於全公司人員，以確保委託方所委託業務之資訊安全獲得保障。
A B C	29. 【題組 4】情境如附圖所示，A 公司為滿足甲客戶要求，正評估導入 ISO 27001 資訊安全管理制度之範圍。試問 A 公司針對導入範圍評估過程與結果之敘述，下列哪些正確？（複選） (A) 將甲客戶的需求與期望納入利害關係方議題調查過程 (B) 將 A 公司高層對於組織內部資訊安全的需求與期望

	納入利害關係方議題調查過程 (C) 將 A 公司軟體系統之開發、維護之業務活動納入 ISO 27001 資訊安全管理制度之導入範圍 (D) 將 A 公司主機代管服務之業務活動排除納入 ISO 27001 資訊安全管理制度之導入範圍
D	30. 【題組 4】情境如附圖所示，A 公司為了執行軟體系統之開發、維護業務活動內有關資訊資產的風險管理事項，因此實施了一系列的有關作為。試問有關作為之敘述，下列何者錯誤？ (A) 針對軟體系統之開發、維護業務活動內包含人員、軟體、硬體、服務與資訊類的資訊資產實施盤點，並計算其資產價值 (B) 針對每一資訊資產識別出該資產的弱點與面臨之威脅，並考量風險發生後對組織造成之衝擊以計算該資訊資產之風險值 (C) 對於不可接受之風險採取相應之控制措施進行處理，以降低其風險至可接受程度 (D) 依據所採取之控制措施結果，於適用性聲明排除資訊系統獲取、開發及維護之適用
C	31. 【題組 4】情境如附圖所示，為了滿足資通安全管理法有關公務機關或特定非公務機關，於資通安全管理法適用範圍內，委外辦理資通系統之建置、維運或資通服務之提供，應考量受託者之專業能力與經驗、委外項目之性質及資通安全需求，選任適當之受託者，並監督其資通安全維護情形之要求，因此 A 公司與甲客戶均實施了一系列有委外選任與監督責任之要求作為。試問有關 A 公司與甲客戶所實施之作為，下列何者較「不」適當？ (A) A 公司實施包含受託業務相關活動在內之有關資訊資產進行風險評鑑 (B) 甲客戶定期以稽核方式確認 A 公司對於受託業務之執行情形

	(C) 甲客戶委託 A 公司對該委託業務之資通系統實施安全性檢測 (D) A 公司標示非自行開發之內容與其來源及提供授權證明
C	32. 【題組 4】情境如附圖所示，近期 A 公司為了確保能如期如質的完成受託業務，增設系統開發人員的職缺並導入系統開發的安全控制措施。試問有關 A 公司所實施之作為，下列何者較「不」適宜？ (A) 針對 A 公司軟體系統之開發、維護業務活動實施風險評鑑 (B) 針對新進系統開發人員實施資通安全教育訓練 (C) 採用未驗證的第三方套件 (D) 導入安全軟體發展生命週期（Secure Software Development Life Cycle，SSDLC）
A	33. 關於風險處理的敘述，下列何者正確？ (A) 風險可接受準則需先定義清楚，風險評鑑結果超過此準則就必須進行風險處理，以降低風險 (B) 風險處理須實施的控制措施，皆必須參考 ISO 27001 的附錄 A (C) 風險處理計畫及殘餘風險的結果，須由資產擁有者確認 (D) 風險處理後所剩餘的風險必須為零
C	34. 關於必須進行風險評估的狀況，下列敘述何者錯誤？ (A) 依據 ISMS（Information Security Management System）要求，必須定期施行風險評估 (B) 決定到美國設立新的工廠，將公司研發團隊遷往美國 (C) 一般員工國外旅遊 (D) 將本地端所有資訊系統密遷到 Azure 雲端服務
C	35. 某作業流程經過風險評估（Assessment）後的固有風險值，遠低於所設定的可接受風險水準時，下一步行動方案，下列

	何者較「不」適當？ (A) 檢視剩餘風險的水準 (B) 向管理階層報告合規結果 (C) 實施控制措施再降低風險 (D) 持續監控作業流程的變化
C D	36. X 公司與 Y 公司進行網路服務業務合作之風險超過公司所設定之風險胃納（Risk appetite）。X 公司最後決定與 Y 公司進行合作，下列哪些項目是合適的風險回應選擇？（複選） (A) 風險規避（Risk avoidance） (B) 風險保留（Risk retention） (C) 風險緩解（Risk mitigation） (D) 風險分擔（Risk sharing）
	【題組 5】 T 公司為資本額超過百億以上之股票上市電子公司，日前剛完成風險評估作業，發現 5 個高風險事項、10 個中風險事項，以及多個低風險事項。依照公司所訂定之風險管理辦法，高風險事項必須規劃風險改善對策，並具以執行。
C	37. 【題組 5】情境如附圖所示，T 公司未聘雇資安長亦無專責資安管理單位，初步評估為中風險事項。後來經過內部討論時，公司治理主管要求將其調整為高風險事項，請問此項調整「最」可能的原因為何？ (A) 資訊安全為各界重視項目，各項資安措施皆應以最高標準要求 (B) 公司人員編制設有資安長之職位，但尚未招聘專業主管 (C) 法令法規要求 (D) 去年執行風險評鑑時，此項目亦列為中風險事項
D	38. 【題組 5】情境如附圖所示，風險評鑑發現的 5 個高風險事項，皆與公司目前最主要之業務或主要作業流程相關，請問下列何項風險回應是公司最「不」可能選擇執行的項目？ (A) 增加相關控制作業以降低風險 (B) 購置保險，降低公司可能的損失

	(C) 尋求合格之外部合作廠商，將風險降低至可接受水準 (D) 結束該項業務，避免承擔風險
C	39. 【題組 5】情境如附圖所示，公司風險評鑑後發現，其中一個高險事項去年度亦列為高風險事項。請問發生此現象最可能的原因（請見附圖二）為下列何項？ 附圖二 1. 風險項目所處環境發生變動 2. 遵循之相關法規今年已有更新 3. 去年度選擇接受風險，故次一年度風險評鑑時會再次出現 4. 執行風險回應後，未確認風險已有效改善 (A) 123 (B) 234 (C) 124 (D) 12
A B C	40. 【題組 5】情境如附圖所示，公司高層評估未來業務模式後，已決定將主要營運系統架設置雲端以利各地公司協同作業，並已編列預算執行此項。此次風險評估亦將公司內部缺乏建置雲端系統之軟硬體列為高風險事項。請問下列哪些內容是公司可能的風險回應？（複選） (A) 尋找符合公司要求之雲端服務廠商，共同合作完成公司要求 (B) 尋找專業 SI 廠商，由其協助規劃系統轉移至雲端提供服務 (C) 增聘相關專業人員、購買相關軟體及硬體設施，並規劃增設合格機房，自行完成公司要求 (D) 由於初步估計所需經費約超過已編列預算 5%，因此將要求公司停止此項變更