113 年度第 1 次 資訊安全工程師能力鑑定 中級試題

科目：I21 資訊安全規劃實務

考試日期： 113 年 4 月 13 日

單選題 15 題，複選題 5 題，題組題 5 題（佔 100%）

C	1. 服務組織控制報告（Service Organization Controls，SOC Report）為美國會計師協會（AICPA）所訂定之報告形式，有 SOC1、SOC2 與 SOC3 等三種，其目的是透過獨立會計師審查以說明組織所提供服務之安全控管現況、程度及有效性。請問下列何種報告最適合發布給一般大眾閱讀的？ (A) SOC1 (B) SOC2 (C) SOC3 (D) SOC1 及 SOC2
	2. 智慧型物聯網（IoT）設備於進入歐盟市場之時，應該要遵循下列何項歐盟新發布的法案，以完成應遵循的安全責任及義務事項，以避免高額的罰鍰(如 1,500 萬歐元)？ (A) NIS2 Directive（歐盟第 2022/2555 號《於歐盟實施高度共通程度之資安措施指令》） (B) Cybersecurity Resilience Act（《資通安全韌性法案》） (C) NIS Directive（《網路與資訊系統安全指令》） (D) Cybersecurity Act, Regulation 2019/881（《資通訊安全法案》） 答案為 Cyber Resilience Act
B	3. 公司建置資訊安全管理系統時，下列何者並「不」是主要考慮的因素？ (A) 適用的法令法規 (B) 資訊安全主管的專長 (C) 客戶與合約的資訊安全要求 (D) 所屬主管機關的資訊安全要求
A B D 或 A D	4. 某公司建置的測試區域遭受駭客入侵，導致重要客戶資料外流。以下哪些選項可作為前述資安問題的改善措施？ (A) 避免使用真實資料做為測試資料 (B) 強化防火測試區防火牆管理 (C) 在公司測試系統輸入重要客戶資料

	(D) 將測試區與公司正式區實施安全、明確之區隔
B	5. 【題組 1】情境如附圖所示，關於建置組織內資訊安全管理系統需參考的關注方要求，下列敘述何者錯誤？ 某 A 公司內部已開始實施 ISO 27001 資訊安全管理系統，建置時需要考量內部與外部議題，及關注方要求，其產出相關資訊也已有紀錄留存。 (A) 建置組織內資訊安全管理系統時，關注方亦包含相關適用法規要求 (B) 個人資料保護法屬於電腦處理相關行業才須遵守的法規 (C) 主管機關也為組織建置資訊安全管理系統的關注方 (D) 組織有合約規範的供應商，也為組織內建置資訊安全管理系統的關注方
C	6. 【題組 1】情境如附圖所示，關於資通安全責任等級分級辦法，下列敘述何者正確？ 某 A 公司內部已開始實施 ISO 27001 資訊安全管理系統，建置時需要考量內部與外部議題，及關注方要求，其產出相關資訊也已有紀錄留存。 (A) 資通安全管理法規範公務機關及特定非公務機關之資通安全責任等級，分為 A 至 D 級 (B) 公務機關應每三年核定其所屬機關資通安全責任等級 (C) 公務機關其負責業務有涉及國家機密，其資通安全責任等級即為 A 級 (D) 各公務機關未維運自行或委外開發之資通系統者，其資通安全責任等級為 C 級
A	7. 【題組 1】情境如附圖所示，關於組織建置資訊安全管理系統的法規遵循性敘述，下列何者錯誤？ 某 A 公司內部已開始實施 ISO 27001 資訊安全管理系統，建置時需要考量內部與外部議題，及關注方要求，其產出相關資訊也已有紀錄留存。 (A) 組織識別適用所在地之法規為主，不予以考量營業據點所在其他國家相關的法規事項 (B) 智慧財產權為所有組織皆須遵守的法規 (C) 客戶提供之紀錄，亦須予以授權保護，以免違反與客戶合約要求

	(D) 個人隱私資訊的法規，需將資料會傳遞的國家法規皆予以納入
A B D	8. 【題組 1】情境如附圖所示，下列哪些是組織建置資訊安全管理系統決定實施範圍需要考量的項目？ 某 A 公司內部已開始實施 ISO 27001 資訊安全管理系統，建置時需要考量內部與外部議題，及關注方要求，其產出相關資訊也已有紀錄留存。 (A) 會影響組織實施資訊安全管理系統時的內部與外部議題 (B) 組織關注方有關資訊安全管理系統實施的要求事項 (C) 與組織實施資訊安全管理系統，範圍內有委外給供應商的活動，可以不予納入 (D) 與客戶合約要求的系統範圍，應納入資訊安全管理系統範圍考量
C	9. 一個要導入 ISO 27001 的組織，為了降低組織資產未經授權或誤用的機會，下列何種措施較「無法」避免？ (A) 職務區隔 (B) 職務輪調 (C) 資產清冊 (D) 存取控制政策
B	10. 關於政府零信任（Zero Trust）網路之敘述，下列何項正確？ (A) 政府推動零信任網路是由國家通訊傳播委員會推動主導 (B) 政府零信任網路包含身分鑑別、設備鑑別及信任推斷等 3 大核心機制 (C) FIDO2 無密碼雙因子驗證滿足零信任網路要求 (D) 持續掌握設備健康管理即滿足設備鑑別要求
C	11. 關於「資料」存取的控制方法，「不」包括下列何者？ (A) 強制存取控制（Mandatory Access Control，MAC） (B) 存取控制清單（Access Control List，ACL） (C) 隨機存取控制（Randomly Access Control，RAC） (D) 角色基準存取控制（Role-based Access Control，RBAC）
B	12. 關於「身分驗證管理」相關控制措施的敘述，下列哪些正確？

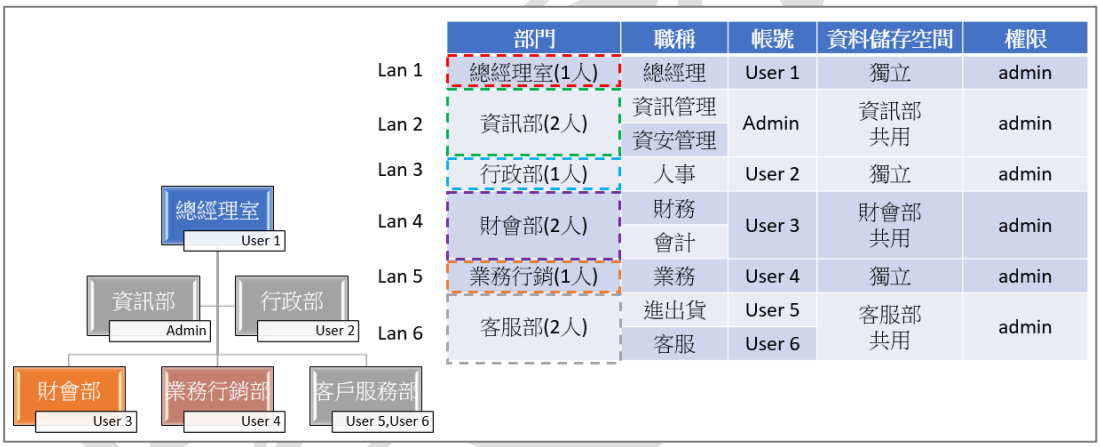
C D	(A) 使用預設密碼登入系統時，於登入後無需立即變更 (B) 應具備帳戶鎖定機制，例如：帳號登入進行身分驗證失敗達五次後，至少十五分鐘內不允許該帳號繼續嘗試登入 (C) 已逾期之臨時或緊急帳號應刪除或禁用 (D) 使用密碼進行驗證時，應強制最低密碼複雜度
A	13. 【題組 2】情境如附圖所示，為了避免該公司所保有的會員個人資料遭受內部未經授權的存取，因此公司資安長（老闆）要求資訊部評估採取適切的控制措施，以降低個人資料外洩風險的發生，試問資訊部對於會員個人資料遭受內部未經授權存取的風險所採取之控制措施，下列敘述何者錯誤？ A 公司為一新創之電子商務股份有限公司(登記資本額為新臺幣一千萬元以上之股份有限公司)，主要業務係以會員制的方式於網路上蒐集、處理與利用會員之個人資料進行販售露營相關之商品為目的，公司組織包含總經理室（老闆）、資訊部（資訊管理作業）、業務部（含進出貨、客服作業）、行政部（含會計、財務、人事作業）。 (A) 採用圖靈驗證碼（Captcha）控制措施，以識別該身分於存取系統或資源時的權限 (B) 採取權限管理之控制措施，以確保每個使用者僅能存取其需要的資源與功能防止越權存取 (C) 採取存取紀錄監控與審查，以確保及時發現異常之系統存取活動 (D) 採取桌面淨空政策，以避免遭受未經授權存取之風險
B	14. 【題組 2】情境如附圖所示，為了強化該公司對於會員個人資料保護的作為，資安長（老闆）要求資訊部重新評估公司整體資訊安全相關作為，以降低整體營運上之風險，試問資訊部對於整體資訊安全強化所採取之作為，下列敘述何者錯誤？

	A 公司為一新創之電子商務股份有限公司（登記資本額為新臺幣一千萬元以上之股份有限公司），主要業務係以會員制的方式於網路上蒐集、處理與利用會員之個人資料進行販售露營相關之商品為目的，公司組織包含總經理室（老闆）、資訊部（資訊管理作業）、業務部（含進出貨、客服作業）、行政部（含會計、財務、人事作業）。 (A) 採取邊界防禦評估，包含防火牆、入侵偵測/防禦系統（IDS/IPS）與網路安全設備等，以防止未經授權之存取 (B) 採用防毒軟體進行身分驗證及授權管理評估 (C) 採取應用程式保護評估，包含弱點掃描、滲透測試以及源碼檢測等 (D) 採取資料保護評估，包含機密等級識別、資料加密傳書、存取控制等
A	15. 【題組 2】情境如附圖所示，依據 A 公司現行事業之經營模式，試問若要滿足個人資料保護相關之法規範要求，下列敘述何者錯誤？ A 公司為一新創之電子商務股份有限公司（登記資本額為新臺幣一千萬元以上之股份有限公司），主要業務係以會員制的方式於網路上蒐集、處理與利用會員之個人資料進行販售露營相關之商品為目的，公司組織包含總經理室（老闆）、資訊部（資訊管理作業）、業務部（含進出貨、客服作業）、行政部（含會計、財務、人事作業）。 (A) 依據 A 公司個人資料蒐集、處理與利用之目的，對於會員個人資料蒐集之特定目的項目與類別可包含〇四〇行銷（包含金控共同行銷業務）、C〇〇一識別個人者、C 一一一 健康紀錄等 (B) 在實施個人資料之蒐集前應向潛在客戶告知包含一、A 公司名稱；二、蒐集之目的；三、個人資料之類別；四、個人資料利用之期間、地區、對象及方式；五、當事人依第三條規定得行使之權利及方式；六、當事人得自由選擇提供個人資料時，不提供將對其權益之影響

(C) 應採行適當之安全措施，防止個人資料被竊取、竄改、毀損、滅失或洩漏，包含採取技術上及組織上之措施

(D) 依據網際網路零售業及網際網路零售服務平台業個人資料檔案安全維護計畫及業務終止後個人資料處理作業辦法制定個人資料檔案安全維護計畫及業務終止後個人資料處理方法之訂定、修正及執行

B C D 16. 【題組 2】情境如附圖所示，為了因應日益成長的網路業務，A 公司決定擴大規模，將原本會計與財務作業由行政部獨立出來，進出貨與客服作業由業務部獨立出來，資訊部由原本資訊管理作業增加資安業務，因此 A 公司的新組織架構如附圖所示。試問依據新的組織架構，下列哪些規劃措施較「不」符合資安管理要求？



	部門	職稱	帳號	資料儲存空間	權限
Lan 1	總經理室(1人)	總經理	User 1	獨立	admin
Lan 2	資訊部(2人)	資訊管理 資安管理	Admin	資訊部 共用	admin
Lan 3	行政部(1人)	人事	User 2	獨立	admin
Lan 4	財會部(2人)	財務 會計	User 3	財會部 共用	admin
Lan 5	業務行銷(1人)	業務	User 4	獨立	admin
Lan 6	客服部(2人)	進出貨 客服	User 5 User 6	客服部 共用	admin

(A) 依據部門屬性切分網段隔離

(B) 全組織人員之權限均為 admin

(C) 資訊部人員共用 Admin 帳號

(D) 財會部人員共用 User 3 帳號

D 17. 關於端點偵測及回應（Endpoint Detection and Response，EDR）的作用敘述，下列何者較「不」正確？

(A) 記錄所有端點上發生的活動和事件

(B) 分析事件以偵測可疑行為

(C) 可協助使用者快速回應安全事件

(D) 能夠完全防止所有端點安全事件發生

A 18. 規劃網路安全架構時，下列何項措施能「較有效」的保護資料的機密性？

	(A) 資料傳輸加密 (B) 強化防火牆設置 (C) 定期資料備份 (D) 內部網路隔離
A	19. 「資通威脅情資」(Cyber Threat Intelligence，CTI）是指蒐集、分析和處理有關網宇威脅行為和漏洞的資訊，以幫助組織瞭解資安威脅的狀況，主動做好威脅應對和預防措施，以保護組織的營運，並降低事件所造成的衝擊影響。若以提供高階主管的 CTI 類型應選擇下列何項較為合適？ (A) Strategic（戰略型） (B) Tactical（戰術型） (C) Technical（技術型） (D) Operational（操作型）
A B D	20. 規劃系統安全架構時可採取之控制措施，下列敘述哪些「有誤」？ (A) 使用單一的帳號名稱及密碼 (B) 無須定期檢視防火牆規則 (C) 定期執行漏洞掃描並修補漏洞 (D) 開放不必要的伺服器連接埠
C	21. 【題組 3】情境如附圖所示，該公司主要是遭受下列何種攻擊？

【aespa 貨車租賃公司網路攻擊事件說明】

親愛的會員您好：

「aespa 貨車」官方網站於 113 年 1 月 7 日下午 18~22 時、113 年 1 月 14 日凌晨 2~5 時分別遭到駭客以不同技術手法進行網路攻擊，經本公司阻擋後，發現均屬惡意人士自不明來源取得會員之手機號碼及該號碼於其他平台慣用密碼，藉此嘗試登入「aespa 貨車」會員帳號。經分析，此次駭客攻擊，應屬駭客按上述帳號密碼於「aespa 貨車」官網循正常路徑進行會員登入，大量攻擊取得資料，全臺共計 19,876 筆會員帳號遭駭客登入，並盜取電子票證卡號及其駕駛紀錄，「aespa 貨車」已主動變更遭惡意登入之會員密碼，並發簡訊通知上述會員變更密碼。為抵禦駭客可能再次發動攻擊，「aespa 貨車」於 113 年 1 月 14 日關閉會員登入功能，將全會員強制登出，完成修改密碼強度規則及新增防堵機器人之驗證功能後，於 113 年 1 月 15 日下午 3 時恢復開放會員登入功能，全會員需先以「忘記密碼」功能重新設定密碼（新密碼須包含 8 至 20 碼英文大小寫與數字），並建議勿採用生日、電話號碼或與其他平台相同等較易遭人破解之密碼作為新密碼。

針對此事件，「aespa 貨車」已通報政府相關主管機關、通知會員及提供資訊予檢調單位進行調查，並依照「aespa 貨車」已通過驗證之 ISO27001 資訊安全標準及 BS 10012 個資管理標準，進行全面系統潛在風險盤查，及提升系統防禦能力。

(A) 分散式阻斷服務（DDoS）攻擊
(B) 中間人攻擊（Man-in-the-middle attack）
(C) 憑證填充（Credential Stuffing）攻擊
(D) 表頭攻擊（host header attack）

A 22. 【題組 3】情境如附圖所示。承上題，關於該項攻擊敘述，下列何項錯誤？

【aespa 貨車租賃公司網路攻擊事件說明】

親愛的會員您好：

「aespa 貨車」官方網站於 113 年 1 月 7 日下午 18~22 時、113 年 1 月 14 日凌晨 2~5 時分別遭到駭客以不同技術手法進行網路攻擊，經本公司阻擋後，發現均屬惡意人士自不明來源取得會員之手機號碼及該號碼於其他平台慣用密碼，藉此嘗試登入「aespa 貨車」會員帳號。經分析，此次駭客攻擊，應屬駭客按上述帳號密碼於「aespa 貨車」官網循正常路徑進行會員登入，大量攻擊取得資料，全臺共計 19,876 筆會員帳號遭駭客登入，並盜取電子票證卡號及其駕駛紀錄，「aespa 貨車」已主動變更遭惡意登入之會員密碼，並發簡訊通知上述會員變更密碼。為抵禦駭客可能再次發動攻擊，「aespa 貨車」於 113 年 1 月 14 日關閉會員登入功能，將全會員強制登出，完成修改密碼強度規則及新增防堵機器人之驗證功能後，於 113 年 1 月 15 日下午 3 時恢復開放會員登入功能，全會員需先以「忘記密碼」功能重新設定密碼（新密碼須包含 8 至 20 碼英文大小寫與數字），並建議勿採用生日、電話號碼或與其他平台相同等較易遭人破解之密碼作為新密碼。

針對此事件，「aespa 貨車」已通報政府相關主管機關、通知會員及提供資訊予檢調單位進行調查，並依照「aespa 貨車」已通過驗證之 ISO27001 資訊安全標準及 BS 10012 個資管理標準，進行全面系統潛在風險盤查，及提升系統防禦能力。

(A) 主要目的在癱瘓網路服務
(B) 使用自動化的方式嘗試登入網路服務
(C) 使用其他服務外洩的帳號密碼
(D) 此攻擊有效的可能原因是人們重複使用帳號密碼

C 或 A

23. 【題組 3】情境如附圖所示。承上題，該公司最「不」可能會有下列何項法律問題？

【aespa 貨車租賃公司網路攻擊事件說明】

親愛的會員您好：

「aespa 貨車」官方網站於 113 年 1 月 7 日下午 18~22 時、113 年 1 月 14 日凌晨 2~5 時分別遭到駭客以不同技術手法進行網路攻擊，經本公司阻擋後，發現均屬惡意人士自不明來源取得會員之手機號碼及該號碼於其他平台慣用密碼，藉此嘗試登入「aespa 貨車」會員帳號。經分析，此次駭客攻擊，應屬駭客按上述帳號密碼於「aespa 貨車」官網循正常路徑進行會員登入，大量攻擊取得資料，全臺共計 19,876 筆會員帳號遭駭客登入，並盜取電子票證卡號及其駕駛紀錄，「aespa 貨車」已主動變更遭惡意登入之會員密碼，並發簡訊通知上述會員變更密碼。為抵禦駭客可能再次發動攻擊，「aespa 貨車」於 113 年 1 月 14 日關閉會員登入功能，將全會員強制登出，完成修改密碼強度規則及新增防堵機器人之驗證功能後，於 113 年 1 月 15 日下午 3 時恢復開放會員登入功能，全會員需先以「忘記密碼」功能重新設定密碼（新密碼須包含 8 至 20 碼英文大小寫與數字），並建議勿採用生日、電話號碼或與其他平台相同等較易遭人破解之密碼作為新密碼。

針對此事件，「aespa 貨車」已通報政府相關主管機關、通知會員及提供資訊予檢調單位進行調查，並依照「aespa 貨車」已通過驗證之 ISO27001 資訊安全標準及 BS 10012 個資管理標準，進行全面系統潛在風險盤查，及提升系統防禦能力。

(A) 資通安全管理法
(B) 個人資料保護法
(C) 公司法
(D) 上市上櫃公司資通安全管控指引

A B D

24. 【題組 3】情境如附圖所示。承上題，下列哪些安全管制措施，能減低此項攻擊成功的機率？

【aespa 貨車租賃公司網路攻擊事件說明】

親愛的會員您好：

「aespa 貨車」官方網站於 113 年 1 月 7 日下午 18~22 時、113 年 1 月 14 日凌晨 2~5 時分別遭到駭客以不同技術手法進行網路攻擊，經本公司阻擋後，發現均屬惡意人士自不明來源取得會員之手機號碼及該號碼於其他平台慣用密碼，藉此嘗試登入「aespa 貨車」會員帳號。經分析，此次駭客攻擊，應屬駭客按上述帳號密碼於「aespa 貨車」官網循正常路徑進行會員登入，大量攻擊取得資料，全臺共計 19,876 筆會員帳號遭駭客登入，並盜取電子票證卡號及其駕駛紀錄，「aespa 貨車」已主動變更遭惡意登入之會員密碼，並發簡訊通知上述會員變更密碼。為抵禦駭客可能再次發動攻擊，「aespa 貨車」於 113 年 1 月 14 日關閉會員登入功能，將全會員強制登出，完成修改密碼強度規則及新增防堵機器人之驗證功能後，於 113 年 1 月 15 日下午 3 時恢復開放會員登入功能，全會員需先以「忘記密碼」功能重新設定密碼（新密碼須包含 8 至 20 碼英文大小寫與數字），並建議勿採用生日、電話號碼或與其他平台相同等較易遭人破解之密碼作為新密碼。

針對此事件，「aespa 貨車」已通報政府相關主管機關、通知會員及提供資訊予檢調單位進行調查，並依照「aespa 貨車」已通過驗證之 ISO27001 資訊安全標準及 BS 10012 個資管理標準，進行全面系統潛在風險盤查，及提升系統防禦能力。

(A) 對用戶宣導避免使用與其他服務相同之密碼
(B) 使用多因子驗證機制（Multi-Factor Authentication）
(C) 將對外網路服務主機設置於防火牆的 DMZ（Demilitarized Zone）區
(D) 使用一次性密碼

C 25. 關於風險管理流程之敘述，下列何者錯誤？
(A) 有些辨識出的風險經過分析與評估之後，可以考量接受該風險
(B) 風險處理的成本與風險的嚴重性可能沒有直接關係
(C) 通過 ISO 27001 驗證之公司，進行風險評鑑時，必須通過 ISO 31000 風險管理系統驗證
(D) 決定處理風險優先項目，是依據風險分析與評估後，所判斷的風險嚴重性做為依據

B 26. 如附圖所示，依據 ISO/CNS 31010 當資通安全主管決定利用「後果

	/機率矩陣」模型完成以資通資產（Asset）為基礎的風險評鑑。附圖中的哪些項目比較能夠說明該方式可能會得到的結果？ 1. 復原時間目標（RTO） 2. 受到影響的可能性（likelihood） 3. 影響程度（Impact） 4. 營運持續（Continuity）策略 5. 營運復原（Recovery）策略 6. 風險處置事項 (A) 1、2、3 (B) 2、3、6 (C) 3、4、5 (D) 1、4、5、6
A	27. 風險分析的其中一個用以詮釋量化計算公式，包含「單一損失預期值」（Single Loss Expectancy，SLE）、「年度發生比率」（Annual Rate of Occurrence，ARO）、和「年度損失預期值」（Annual Loss Expectancy，ALE），請問三者的關係為下列何項？ (A) ALE= ARO*SLE (B) ARO= ALE*SLE (C) ALE= ARO/SLE (D) ARO= SLE/ALE
C D	28. 如附圖所示，委外廠商的滲透測試人員在與客戶接洽之前，會在工作說明書（SOW）訂定附圖中的規定並由客戶完成審核。而根據 SOW 所呈現的資訊，下列哪些行為會較容易被視為該廠商人員具有「不道德」的風險行為？ 「網路架構圖、邏輯和實體資產清單、以及員工姓名均應視為客戶機密資料，參與專案完成結案後，滲透測試人員將透過加密協議向客戶的資訊安全長（CISO）提交檢測結果，隨後即利用安全資料抹除方式，處理所有該案相關的作業紀錄（含檢測結果）。」 (A) 使用合法軟體授權之滲透測試工具，進行安全查核和檢視 (B) 利用公鑰加密技術以確保檢測結果在檢測作業完成後，能妥適安全地交付 CISO

	(C) 未能將發現的重要漏洞報告及討論，以滿足客戶的高階領導團隊的安全需求 (D) 使用客戶所屬 IP 位址，至地下駭客論壇或暗網查找技術文件或工具
C D	29. 【題組 4】情境如附圖所示，請問在 A 企業位於英國的電子商務平台發生駭客入侵事故，下列應變與處理程序哪些正確？ A 企業為一總部在台灣的股票上市公司，為國際知名的電子商務平台，主要業務包括企業對企業（B2B）及企業對個人（B2C）及消費者對消費者（C2C）的電子商務活動，員工超過 50,000 人，擁有 1,000 個據點及超過 2,000 部的伺服器及 300 座的機房，服務對象包括美國、英國、歐盟、俄羅斯、中國大陸、日本、韓國、台灣等等。在安全佈署上，除了每部服務主機建置防火牆外，亦佈署入侵防禦系統（Intrusion Prevention System，IPS），所有的存取控制以及安全性 Log 都收容到位於台灣的資訊安全監控中心（Security Operation Center，SOC）內的安全性資訊與事件管理系統（SIEM）中進行關聯資料分析，並且建立了完善的事件管理與追蹤系統。日前 A 企業位於英國的電子商務平台發生駭客入侵事故導致英國地區客戶超過 1,000 萬筆個人資料外洩，公司決定全公司各據點導入資訊安全管理系統（ISMS）及個人資料保護系統（PIMS）並於半年內完成。 (A) 依資通安全管理法規定於 2 小時之內通報目的事業主管機關 (B) 依一般資料保護規範（GDPR）規定於 1 週內通報個資外洩 (C) 應該至公開資訊觀測站發佈重大訊息 (D) 發佈的程序應遵循 A 企業訂定的相關程序進行處理
C	30. 【題組 4】情境如附圖所示，請問在進行風險識別作業時，對於本類型的跨國企業以何種方式進行風險識別較「不」合適？ A 企業為一總部在台灣的股票上市公司，為國際知名的電子商務平台，主要業務包括企業對企業（B2B）及企業對個人（B2C）及消費者對消費者（C2C）的電子商務活動，員工超過 50,000 人，擁有 1,000 個據點及超過 2,000 部的伺服器及 300 座的機房，服務對象包括美國、英國、歐盟、俄羅斯、中國大陸、日本、韓國、台灣等等。在安全佈署上，除了每部服務主機建置防火牆外，亦佈署入侵防禦系統（Intrusion Prevention System，IPS），所有的存取控制以及安全性 Log 都收容到位於台灣的資訊安全監控中心（Security Operation Center，SOC）內的安全性資訊與事件管理系統（SIEM）中進行關聯資料分析，並且建立了完善的事件管理與追蹤系統。日前 A 企業位於英國的電子商務平台發生駭客入侵事故導致英國地區客戶超過 1,000 萬筆個人資料外洩，公司決定全公司各據點導入資訊安全管理系統（ISMS）及個人資料保護系統（PIMS）並於半年內完成。

	(A) 以資產為基礎的風險識別 (B) 以事件為基礎的風險識別 (C) 以教材範本進行風險識別 (D) 以人員為基礎的風險識別
B	31. 【題組 4】情境如附圖所示，請問於 A 企業於歐盟內系統據點執行的資訊安全管理系統（ISMS）及個人資料保護管理系統（PIMS），執行下列選項較為適當？ A 企業為一總部在台灣的股票上市公司，為國際知名的電子商務平台，主要業務包括企業對企業（B2B）及企業對個人（B2C）及消費者對消費者（C2C）的電子商務活動，員工超過 50,000 人，擁有 1,000 個據點及超過 2,000 部的伺服器及 300 座的機房，服務對象包括美國、英國、歐盟、俄羅斯、中國大陸、日本、韓國、台灣等等。在安全佈署上，除了每部服務主機建置防火牆外，亦佈署入侵防禦系統（Intrusion Prevention System，IPS），所有的存取控制以及安全性 Log 都收容到位於台灣的資訊安全監控中心（Security Operation Center，SOC）內的安全性資訊與事件管理系統（SIEM）中進行關聯資料分析，並且建立了完善的事件管理與追蹤系統。日前 A 企業位於英國的電子商務平台發生駭客入侵事故導致英國地區客戶超過 1,000 萬筆個人資料外洩，公司決定全公司各據點導入資訊安全管理系統（ISMS）及個人資料保護系統（PIMS）並於半年內完成。 (A) 資訊安全風險評鑑（ISRA）及營運衝擊評鑑（BIA） (B) 資訊安全風險評鑑（ISRA）及資料保護衝擊評鑑（DPIA） (C) 環境影響評鑑（EIA）及營運衝擊評鑑（BIA） (D) 環境影響評鑑（EIA）及資訊安全風險評鑑（ISRA）
C	32. 【題組 4】情境如附圖所示，A 企業欲針對此次在英國的電子商務平台，所發生的大量客戶個資外洩事件進行風險處理，請問下列何風險處理方式較「不」適當？

	A 企業為一總部在台灣的股票上市公司，為國際知名的電子商務平台，主要業務包括企業對企業（B2B）及企業對個人（B2C）及消費者對消費者（C2C）的電子商務活動，員工超過 50,000 人，擁有 1,000 個據點及超過 2,000 部的伺服器及 300 座的機房，服務對象包括美國、英國、歐盟、俄羅斯、中國大陸、日本、韓國、台灣等等。在安全佈署上，除了每部服務主機建置防火牆外，亦佈署入侵防禦系統（Intrusion Prevention System，IPS），所有的存取控制以及安全性 Log 都收容到位於台灣的資訊安全監控中心（Security Operation Center，SOC）內的安全性資訊與事件管理系統（SIEM）中進行關聯資料分析，並且建立了完善的事件管理與追蹤系統。日前 A 企業位於英國的電子商務平台發生駭客入侵事故導致英國地區客戶超過 1,000 萬筆個人資料外洩，公司決定全公司各據點導入資訊安全管理系統（ISMS）及個人資料保護系統（PIMS）並於半年內完成。 (A) 電子商務平台個人資料去識別化 (B) 落實資料庫加密以避免未經授權的存取 (C) 採用 SSL3.0 的傳輸加密 (D) 採用多因子身份認證（MFA）
B 或 D	33. 有關資訊安全之風險處理，下列何項敘述「有誤」？ (A) 應依據風險評估準則與導致該等風險之事故情境之關係，訂定優先序之風險清單 (B) 風險處理時若已選擇降低風險，則無需進行風險處理計畫 (C) 風險處理應由高風險項目優先處理 (D) 對於所識別出之風險，只要經過風險處理後所剩下來的殘餘風險即可
B	34. A 銀行風險評估後，決定不使用雲端廠商提供之服務，此項屬下列何項風險回應措施？ (A) 風險緩解（Risk mitigation） (B) 風險避免（Risk avoidance） (C) 風險保留（Risk retention） (D) 風險分擔（Risk sharing）
D	35. 有關風險處理目的之敘述，下列何項正確？ (A) 風險處理之目的係選擇並實施識別風險的選項 (B) 風險處理之目的係選擇並實施評估風險的選項 (C) 風險處理之目的係選擇並實施分析風險的選項

	(D) 風險處理之目的係選擇並實施處理風險的選項
B D	36. 關於「風險」與「風險管理」的敘述，下列哪些正確？ (A) 風險是外部威脅利用弱點對內部資產造成衝擊的可能性 (B) 通常風險管理都會以 ISO/IEC 27005 風險管理指引作為參考 (C) 風險分析可依可用性、完整性、機密性加以質化後，決定風險等級 (D) 進行風險識別須包含威脅識別與弱點識別
B	37. 【題組 5】情境如附圖所示。請問應該選用下列何項由 ISP 業者提供的服務型防護機制，較能有效地減緩攻擊及其所帶來的影響？ 您是 Quick GO 公司的資安官，負責 Quick GO 公司整體資安管理制度（含資通安全風險）的規劃、執行及監控。該公司目前已建置一個線上購物網站，每一年經由該網站完成的交易收入金額達 500 萬元（占公司全部盈收的 70%）。 但近年遭受到全球分散式阻斷服務(DDoS)攻擊的損失，經評估後預期每年約為 100,000 元，身為 Quick GO 公司資安官的您，在導入某一項防禦機制後，預估年度的損失值將降為 30,000 元，但該機制的季度服務費用 20,000 元。 (A) 網路存取控制（NAC） (B) 網路流量清洗服務（Flow Cleaning） (C) 蜜罐誘捕系統（Honey Pot） (D) 入侵偵測系統（IDS）
C	38. 【題組 5】情境如附圖所示。承上題，單以營業損失而言，該項防禦機制一年能為 Quick GO 降低多少金額？ 您是 Quick GO 公司的資安官，負責 Quick GO 公司整體資安管理制度（含資通安全風險）的規劃、執行及監控。該公司目前已建置一個線上購物網站，每一年經由該網站完成的交易收入金額達 500 萬元（占公司全部盈收的 70%）。 但近年遭受到全球分散式阻斷服務(DDoS)攻擊的損失，經評估後預期每年約為 100,000 元，身為 Quick GO 公司資安官的您，在導入某一項防禦機制後，預估年度的損失值將降為 30,000 元，但該機制的季度服務費用 20,000 元。

	(A) 10,000 元 (B) 80,000 元 (C) 70,000 元 (D) 30,000 元
B	39. 【題組 5】情境如附圖所示。承本題組第一題，該項防禦機制於每一年能夠為 Quick GO 公司創造的價值為何？ 您是 Quick GO 公司的資安官，負責 Quick GO 公司整體資安管理制度（含資通安全風險）的規劃、執行及監控。該公司目前已建置一個線上購物網站，每一年經由該網站完成的交易收入金額達 500 萬元（占公司全部盈收的 70%）。 但近年遭受到全球分散式阻斷服務(DDoS)攻擊的損失，經評估後預期每年約為 100,000 元，身為 Quick GO 公司資安官的您，在導入某一項防禦機制後，預估年度的損失值將降為 30,000 元，但該機制的季度服務費用 20,000 元。 (A) 負 20,000 元 (B) 負 10,000 元 (C) 20,000 元 (D) 50,000 元
A B C	40. 【題組 5】情境如附圖所示。有關 DDoS 攻擊的防禦機制，除本題組第一題的服務型機制外，還可以在建置下列哪些設備或服務，以減輕攻擊所造成的影響？ 您是 Quick GO 公司的資安官，負責 Quick GO 公司整體資安管理制度（含資通安全風險）的規劃、執行及監控。該公司目前已建置一個線上購物網站，每一年經由該網站完成的交易收入金額達 500 萬元（占公司全部盈收的 70%）。 但近年遭受到全球分散式阻斷服務(DDoS)攻擊的損失，經評估後預期每年約為 100,000 元，身為 Quick GO 公司資安官的您，在導入某一項防禦機制後，預估年度的損失值將降為 30,000 元，但該機制的季度服務費用 20,000 元。 (A) 建置網頁型防火牆（WAF）系統 (B) 建置「內容傳遞網路」（Content Delivery Network, CDN） (C) 建置「負載平衡伺服器」（Server Load Balancer）

	(D) 建置資料外洩防護（DLP）系統