風險管理測驗 1

C	1.	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
ABD	2. 複選	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
C	3.	關於風險管理，下列敘述何者較「不」正確？ (A) 應依照風險改善計畫的期限，執行改善作業 (B) 執行完風險改善計畫後，應進行風險再評鑑作業 (C) 當時間已遠超過風險改善計畫期限時，仍應持續執行原訂風險改 善計畫 (D) 針對超過風險胃納（Risk Appetite）的項目，應提出風險改善計畫
D	4.	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
B C D	5. 複選	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

A B D	6. 複 選	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？ (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
A	7.	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	8.	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)
A	9.	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，下列何種處理較無法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) 導入自動化資料庫稽核管理工具
A B C	10. 複 選	某公司從事國際型科技大廠組裝代工業務，在合作業務上，嚴禁將未上市產品資訊外洩，包含：未上市產品間諜照、設計圖…等，相關資訊檔案讀取使用僅限制公司少數高階技術人員可以讀

		取，不能外洩到公司以外其他地方使用。關於上述狀況，下列風險管理敘述何者正確？ (A) 公司與員工間簽屬相關保密協定與同意限制規範，並進行必要技 術管制手段，如：手機必須放置在公司設定手機電腦保管區、嚴 禁拍照裝置與私人電腦攜入公司廠區 (B) 對公司電腦，限制外接儲存裝置的存取、電腦畫面擷取、與工具 軟體使用限制，以降低公司機密資料外洩風險 (C) 公司成立相對應資安防護措施，如：防止駭客入侵竊取、電子郵 件的附件過濾、對公司內外流量封包監控 (D) 公司不應限制禁止員工上網，這是員工午休時基本人權權利
A B D	11. 複 選	「某政府一級單位官網，交付政府維運機房代管，要求服務層級協議 （Service Level Agreement, SLA）99.999%服務水平，監測發現該政府 官網，固定在每週日，半夜 12:00 會自動停止服務 30 分鐘。該事件已經持續半年才被發現，在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。」 下列哪些選項屬於合適的風險處置措施？ (A) 問題經半年才被發現，表示目前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，就可以知道系統服務層級協議狀態與降低中斷服務 的風險 (B)在 Web root 目錄出現 Lcx.exe，確定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 (C) 以 99.999%服務層級協議來看，本次事件長達半年，以一年 365 天計算仍符合 99.999%服務層級協議 (D)必須依規定進行通報，例如：「國家資通安全通報應變網站」進行通報