M2_2 風險管理

風險管理(RiSK management):一般觀念

A	1.	下列何者為資訊安全風險管理的要求？ (A) 資訊安全風險評鑑過程，以識別與機密性、完整性及可用性相關聯之風險 (B) 需有一位風險管理主管 (C) 相關之風險計算需納入年度預期損失的程序 (D) 需取得資產擁有者對資訊安全風險處理計畫之核准
C	2.	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
C	3.	19. 某公司的派工系統，原先未在高風險資產項目中，但近一年來接連遇到幾次服務中斷事件，造成極大的損失，若要重新檢視該公司資產風險評鑑要素，下列何者「不」是適當的考量項目？ (A) 資訊資產重要性 (B) 資訊資產威脅 (C) 資訊資產殘值 (D) 資訊資產脆弱點
A	4.	關於風險評鑑與風險處理，下列敘述何者正確？ (A) 經過風險評鑑，低風險或處理成本過高的風險項目，可能會被組織選擇接受 (B) 風險評鑑可以百分百找出可能的風險項目，並且進行風險處置 (C) 風險處理可以百分百消除風險項目，確保資訊安全 (D) 風險處理後，組織就不再需要進行風險評鑑作業

風險評鑑（Risk Assessment）

D	5.	關於風險評鑑（Risk Assessment），下列敘述何者較「不」正確？ (A) 是一種風險管理的機制 (B) 是將預估的風險和已知風險準則進行比較的過程 (C) 目的是決定可接受風險的程度 (D) 目的是將可接受的風險與主要風險分開，並移除殘餘風險
D	6.	關於風險評鑑管理程序，下列敘述何者較「不」正確？ (A) 建立全景係界定風險評鑑範圍 (B) 詳細風險評鑑包括風險識別、風險分析與風險評估 (C) 風險處理若符合風險處理準則，則進入風險接受階段

		(D) 風險評鑑若不符合風險評鑑準則，則進入風險溝通階段
D	7.	關於風險評鑑管理程序，下列敘述何者「不」正確？ (A) 建立全景係界定風險評鑑範圍 (B) 詳細風險評鑑包括風險識別、風險分析與風險評 估 (C) 風險處理若合意，則進入風險接受階段 (D) 風險評鑑若不合意，則進入風險溝通階段
D	8.	下列何者「不」屬於風險評鑑之範圍及執行步驟？ (A) 風險分析 (B) 防護措施的選擇 (C) 風險接受 (D) 營運持續計畫
C	9.	下列何者「不」是風險評鑑過程中主要的活動？ (A) 風險鑑別 (B) 風險分析 (C) 風險處理 (D) 風險評估
A	10.	關於風險辨識（Risk Identification），下列敘述何者正確？ (A) 是發掘可能發生風險之事件及其發生之原因和方式 (B) 是組織進行風險評鑑、分析與評估的整體流程 (C) 是理解風險本質並且決定風險等級的流程 (D) 是比較風險分析結果與風險準則來決定風險或嚴重程度是否為可接受的流程
C	11.	在資安風險管理過程中，關於風險識別（Risk Identification）應包括的 工作項目，下列何者較「不」正確？ (A) 識別威脅（Threat） (B) 識別脆弱點（Vulnerability） (C) 識別風險等級（Risk Level） (D) 識別資產（Asset）
D	12.	在資訊安全管理系統（Information Security Management System, ISMS） 中，風險識別「不」含下列何者？ (A) 識別各項資產的脆弱性 (B) 分析資安事故或事件對組織帶來的衝擊程度 (C) 評估環境或新技術帶來的威脅 (D) 建議購買軟硬體設備清單
D	13.	關於風險分析，下列敘述何者較「不」正確？ (A) 風險分析的目的是找出風險發生的可能性 (B) 風險分析用於評估風險等級 (C) 風險分析可分析事件發生的影響性 (D) 風險分析會影響風險準則的訂定
A	14.	風險分析所使用的方法，除了「定量法（Quantitative Method）」之外， 還可以採用下列何種方法？ (A) 定性法 (B) 類比法 (C) 平均法 (D) 參數法
A	15.	在風險評鑑的過程，對於衝擊所造成的損失，不以金錢來計算，而改採 用「極小、較小、中等、較大、巨大」的方式來表達，屬於下

		列何種 方法？ (A)定性法 (B) 類比法 (C) 定量法 (D) 參數法
D	16.	關於風險評估（Risk Evaluation），下列敘述何者正確？ (A) 是識別風險來源、事件、發生的原因，與可能產生的後果 (B) 是組織進行風險評鑑、識別、分析的整體流程 (C) 是理解風險本質並且決定風險等級的流程 (D) 是比較風險分析結果與風險準則來決定風險或嚴重程度是否為可接受的流程
C	17.	若在執行定期風險評鑑進入尾聲時發現一項新的風險議題，下列何者較「不」適當？ (A) 將該風險議題納入此次風險評鑑，一併完成評鑑 (B) 針對該風險議題額外執行風險評鑑並出具報告 (C) 因定期風險評鑑有完成期限，故對此風險議題不做處理 (D) 先初步評估該風險議題是否有重大影響，若無重大影響則於事後再進行完整評估
C	18.	執行定期風險評鑑進入尾聲時，發現一項新的風險議題，下列何者較 「不」適當？ (A) 將該風險議題納入此次風險評鑑，一併完成評鑑 (B) 針對該風險議題額外執行風險評鑑並出具報告 (C) 因定期風險評鑑有完成期限，故對此風險議題不做處理 (D) 先初步評估該風險議題是否有重大影響，若無重大影響則於事後再進行完

風險處理(Risk treatment)

C	19.	下列何者「不」是風險處理的選項？ (A) 風險降低 (B) 風險轉移 (C) 風險忽略 (D) 風險接受
D	20.	下列何者「不」是風險評鑑後，對於風險事項的處理方式？ (A) 風險規避 (B) 風險移轉 (C) 風險控制 (D) 風險再評鑑
D	21.	下列何者「不」是選擇風險處理對策時的主要考量因素？ (A) 法令法規 (B) 實施成本 (C) 利害相關者的感知 (D) 短期內可達成
C	22.	當進行風險評估，發現機密資料外洩風險是組織內部最大之風險時，組織進行了相對應之風險處理方法，其中包含了購買資料外洩保險，此為下列何種風險處理方式？ (A) 風險接受 B) 風險降低 C) 風險轉移 D) 風險避免
C	23.	若公司為資訊資產購買保險，當資訊安全事件發生時，所造成的損失由保險公司理賠，此種風險處置策略屬於下列何者？ (A) 風險接受 (B) 風險降低 (C) 風險移轉 (D) 風險避免

A	24.	關於風險改善計畫，下列敘述何者較「不」正確？ (A) 風險改善計畫不可變更 (B) 風險改善計畫應有期限 (C) 風險改善計畫完成後，應評估成效 (D) 風險改善計畫應針對超過可接受風險項目進行處置
B	25.	某公司之風險評鑑發現，公司全球網站設置於內部網路，將增加外部入侵內部網路的風險，下列何者是「迴避」（Avoid）上述風險的作法？ (A) 將網站改設置於公司內防火牆的非交戰區（Demilitarized zone, DMZ） (B) 將網站改設置於外部租用空間 (C) 增設網路監控設施，加強入侵監控機制 (D) 將網站設置於內部獨立網段
A	26.	發生資安事件攻擊時，若其損失在組織可容忍範圍，可採取下列何種風險處置策略？ (A) 風險接受（Acceptance） (B) 風險降低（Reduction） (C) 風險移轉（Transfer） (D) 風險避免（Avoidance）
D	27.	公司機房重地購買地震險或火險，此行為屬於下列何種風險處理方式？ (A) 風險接受（Acceptance） (B) 風險規避（Avoidance） (C) 風險降低（Reduction） (D) 風險移轉（Transfer）
B	28.	下列何者的處理方式無法降低風險？ (A) 風險避免(Risk avoidance) (B) 風險保留(Risk retention) (C) 風險修改(Risk modification) (D) 風險分擔(Risk sharing)
D	29.	為了降低風險，下列何者最「不」是實施風險控制措施 的考量因素？ (A) 法規要求與限制 (B) 組織的目標與規範 (C) 實施的可能成本 (D) 資訊資產類別
A	30.	21. 下列敘述何者符合風險移轉？ (A) 投保機房火險 (B) 建立備援網路系統 (C) 停止網路平台交易業務 (D) 增加開啟系統權限的簽核流程
D	31.	24. 關於風險降低（Reduction），下列敘述何者「不」正確？ (A) 其方式包括日常稽核遵守控制程度 (B) 其方式包括處理偶發事故的計畫 (C) 其方式包括找出相較於現有的控制方法，新的控制方法所可能帶來的相對利益 (D) 其方法包括契約的簽訂、保險和機關的結構，如合夥經營和共同投資
A	32.	為避免機房在一樓會有淹水的風險，而將機房搬到較高樓層，請問這是何種風險處理行為？

		(A) 風險規避（Avoidance） (B) 風險移轉（Transfer） (C) 風險降低（Reduction） (D) 風險接受（Acceptance）
C	33.	23. 關於風險規避（Risk Avoidance），下列敘述何者「不」正確？ (A) 決定不涉入風險處境 (B) 決定退出風險處境 (C) 通常不考量主管機關的影響，而會有躲避風險的傾向 (D) 會造成不願面對風險或淡化處理風險所需要的成本

殘餘風險 Residual Risk

D	34.	下列何者是「殘餘風險」（Residual Risk）的敘述？ (A) 單位可以承受的風險 (B) 沒有被識別的風險 (C) 已經被識別，但是沒有指定處置方法的風險 (D) 執行風險處理措施後，還殘留下來的風險
D	35.	關於殘餘風險（Residual Risk），下列敘述何者正確？ (A) 單位可以承受的風險 (B) 沒有被識別的風險 (C) 已經被識別，但是沒有指定處置方法的風險 (D) 執行風險處理措施後，還殘留下來的風險