M1_2 資訊安全管理系統（Information Security Management System, ISMS）

B	1.	關於資訊安全管理系統（Information Security Management System, ISMS），下列敘述何者較「不」正確？ (A) 瞭解組織資訊安全要求，建立資訊安全之政策與目標的需求 (B) 基於主觀的量測，並且持續改善 (C) 監視與審查資訊安全管理系統（ISMS）的績效與有效性 (D) 在組織的運作中實作與運作各項控制措施，並管理組織的資訊安全風險
C	2.	資訊安全管理系統（Information Security Management System, ISMS）是在於管理面的要求，藉由審查機制、事件的回應及內部稽核來預防資訊安全事件或是降低其損失的風險，請問下列敘述何者「不」正確？ (A) 需要管理階層的承諾及提供相關支援，表達對資訊安全管理系統的支持 (B) 採用規劃（Plan）、執行（Do）、檢查（Check）及行動（Act）等四個階段的改進流程進行 (C) 資訊安全目標無需具體量化，導入解決方案、強化資訊安全防護為指導方針 (D) 內部稽核的成果報告需要在管理審查會議中進行檢討
D	3.	關於資訊安全管理系統（Information Security Management System, ISMS），下列敘述何者較「不」正確？ (A) 導入資訊安全管理系統可以保護組織資訊資產的安全 (B) 要建立良好的資訊安全管理系統，需要制度面與技術面互相配合 (C) 最高管理階層的參與及支持是成功建立資訊安全管理系統的重點之一 (D) 在建立組織資訊安全管理系統的活動中，識別弱點會優先於識別資訊資產
B	4.	導入資訊安全管理系統（Information Security Management System, ISMS），第三方驗證單位是依據下列何種 ISO 標準進行驗證？ (A) ISO/IEC 27000 :2013 (B) ISO/IEC 27001 :2013 (C) ISO/IEC 27002 :2013 (D) ISO/IEC 27003 :2013
B	5.	下列何者是國際標準組織（International Organization for Standardization, ISO）將資訊安全管理系統（Information Security Management System, ISMS）制定的資訊安全第三方驗證標準？ (A) ISO 27000 (B) ISO 27001 (C) ISO 27002 (D) ISO 27005
B	6.	若要實施資訊安全管理系統（Information Security Management

		System, ISMS），第三方驗證公司是依據下列何種 ISO 標準進行驗證？ (A) ISO/IEC 27000 :2013 (B) ISO/IEC 27001 :2013 (C) ISO/IEC 27002 :2013 (D) ISO/IEC 27003 :2013
C	7.	建立或導入資訊安全管理系統（Information Security Management System, ISMS）時，最重要的第一個步驟是下列何者？ (A)資訊資產分級與盤點造冊 (B)資訊安全教育訓練 (C)界定資訊安全管理系統的範圍 (D)實施必要的控制措施
C	8.	建立或導入資訊安全管理系統（Information Security Management System, ISMS）時，最重要的第一個步驟為下列何者？ (A)資訊資產清冊盤點 (B)資訊安全滲透測試 (C)資訊安全管理系統範圍的決定 (D)實施必要的控制措施
C	9.	建立資訊安全管理系統（Information Security Management System, ISMS）時，下列何者「最」常由管理階層執行？ (A) 撰寫資訊安全政策 (B) 執行風險分析與評鑑 (C) 決定可接受風險等級 (D) 擔任教育訓練講師
C	10.	高階管理階層（資安長）在資訊安全管理系統中所展現 領導與承諾，「不」包含下列何項？ (A) 確保建立的資訊安全政策及資訊安全目標，必須 與組織發展方向相容 (B) 整合人員、組織及提供所需的支援，確保資訊安 全管理系統的要求 (C) 向組織內部所有人員說明資訊安全產品的設定 (D) 確保資訊安全管理系統達成預期的成效
A	11.	關於資訊安全管理系統（Information Security Management System, ISMS） 中的實體控制措施，下列敘述何者「不」正確？ (A) 設立訪客櫃台，為了表示友善，訪客可以自由進出辦公區域 (B) 劃分安全區域，設定門禁管理 (C) 進出機房重地除了需刷卡外，還需要留下詳細的進出記錄 (D) 沒有被授權的人員，不應該進入管制區域
A	12.	請問 ISO/IEC 27001 指導組織用下列何種方法來持續改善資訊安全管理系統(Information Security Management System, ISMS)活動，以落實控制措施之實施？ (A) P（規劃）→D（執行）→C（檢查）→A（行動） (B) D（執行）→P（規劃）→C（檢查）→A（行動） (C) C（檢查）→D（執行）→P（規劃）→A（行動） (D) A（行動）→D（執行）→C（檢查）→P（規劃）
C	13.	在建置與運作資安系統時，常用戴明循環(Deming Cycle)協助管理，下列何項是戴明循環(Deming Cycle)正確的順序？

		(A) Plan – Act – Do – Check (B) Do – Check – Plan – Act (C) Plan – Do – Check – Act (D) Act – Check – Do – Plan
B	14.	資訊安全管理系統(Information Security Management System, ISMS)中的風險評估(Risk Assessment)作業，屬於規劃（Plan）、執行(Do)、檢查(Check)及行動(Act)循環中的哪一部分？ (A) 規劃(Plan) (B) 執行(Do) (C) 檢查(Check) (D) 行動(Act)
B	15.	組織已開始著手進行資訊資產之盤點、建立清冊，並實施風險評鑑作 業，請問此作業屬於 PDCA 循環之何者階段？ (A) P(Plan) (B) D(Do) (C) C(Check) (D) A(Act)
B	16.	資訊安全管理系統（Information Security Management System, ISMS）採用 PDCA 循環的概念，下列何者「不」包含在此流程中？ (A) 高階管理審查會議 (B) 業務達成率審查 (C) 內部稽核執行 (D) 災難復原計畫演練
B	17.	資訊安全管理系統遵照計畫（Plan）、執行（Do）、檢查 （Check）及行動（Act）等四個程序，不斷的改進。請問「建立及執行管理程序」是屬於下列哪一個程序？ (A) 計畫（Plan） (B) 執行（Do） (C) 查核（Check） (D) 行動（Act）
C	18.	可建議發出 ISO 27001 通過驗證的國際證書，為下列何者？ (A) 第一方稽核 (B) 第二方稽核 (C) 第三方稽核 (D) 第四方稽核
C	19.	下列何種稽核可做出建議 ISO 27001 通過驗證發出證書？ (A) 第一方（First Party）稽核 (B) 第二方（Second Party）稽核 (C) 第三方（Third Party）稽核 (D) 第四方（Fourth party）稽核
C	20.	在進行資安內部稽核時，下列何者「不」是組織應該採取的做法？ (A) 由稽核小組規劃和建立內部稽核的計畫 (B) 在稽核計畫中定義稽核的範圍和準則 (C) 為確保稽核專業度，由資訊人員稽核其所負責的資訊系統 (D) 在完成稽核之後，將稽核結果報告給相關管理階層