初級資訊安全工程師 能力鑑定樣題

單選題 50 題

B	1. 學生侵入學校的伺服器，偷偷竄改自己的期末考成績。這是破壞了資訊的哪一項特性？ (A) 保密性（Confidentiality） (B) 完整性（Integrity） (C) 可用性（Availability） (D) 責任性（Accountability）
C	2. 組織對外服務之官方網站遭受駭客透過 DDoS 攻擊，請問此為下列哪項遭受破壞？ (A) 機密性 (B) 完整性 (C) 可用性 (D) 可讀性
B	3. 請問下列何項說明內容是關於「可用性」的敘述？ (A) 使用者以專用帳號及密碼登入 ERP 系統 (B) 電信商機房故障，暫時無法使用網路 (C) 親自遞送機密文件給總經理核閱 (D) 出勤系統異常，導致薪資計算錯誤
C	4. 請問下列敘述何者正確？ (A) 衝擊是威脅利用弱點對資產造成風險的可能性 (B) 衝擊是資產利用弱點對威脅造成風險的可能性 (C) 風險是威脅利用弱點對資產造成衝擊的可能性 (D) 風險是資產利用弱點對威脅造成衝擊的可能性
A	5. 下列何項非為成功建立資訊安全管理系統之必要項目？ (A) 導入 ISO 國際標準 (B) 最高管理階層的參與及支持 (C) 組織提供建立資訊安全管理系統（Information Security Management System, ISMS）所需之資源 (D) 確立資訊安全管理的政策及目標
C	6. 在資訊安全管理系統中，進行資安內部查核時，下列敘述何者不正確？ (A) 在查核前擬定稽核計畫 (B) 招開行前會議，說明稽核計畫 (C) 稽核人員可稽核所屬單位，無須具備獨立性 (D) 建立稽核程序書或文件

B	7. 下列何種作為，展現了最高管理階層對資訊安全管理系統（Information Security Management System, ISMS）之領導和承諾？ (A) 確保資訊安全政策和目標需至少維持三年不變 (B) 確保資訊安全的要求已整合至組織的各項作業流程 (C) 確保在未來一年內降低組織的營運成本 (D) 確保適當規劃和制訂完成組織的年度營運計畫
B	8. 資訊安全管理系統的導入，實際執行 PDCA（計畫-執行-檢查-行動）的過程中，不包含下列何者？ (A) 最高管理階層審查會議 (B) 業務部門績效審核 (C) 內部稽核計畫執行 (D) 災害復原計畫演練
D	9. 關於資訊資產之擁有、使用、保管，下列敘述何者正確？ (A) 保管者（Custodian）負責獲得適當的授權，得以檢視、使用、存取或異動資訊資產 (B) 擁有者（Owner）對於資訊資產負有管理的權責，通常由各使用者擔任或其指派之人員擔任 (C) 使用者（User）負責資訊資產的相關處理與保管工作 (D) 為釐清資訊資產之擁有、保管與使用的權責，確保資產由適當的人員保管及使用，應由各部門權責主管指定適當之擁有者、保管者與使用者
C	10. 資產是對組織有價值的任何事物，而資訊也是資產的一種。請問下列何種不是資訊資產？ (A) 員工人事資料 (B) 電腦 (C) 辦公桌 (D) 套裝軟體
C	11. 關於資訊資產分級的目的，下列敘述何者正確？ (A) 確保員工及承包商之相關安全責任 (B) 限制對資訊及資訊處理設施的存取 (C) 確保資產依其對組織之重要性，受到適切等級的保護 (D) 確保運作中系統的完整性
D	12. 在進行資產管理時，下列哪一項應優先建立？ (A) 稽核計畫 (B) 溝通管理 (C) 風險登記表 (D) 資產清冊

D	13. 關於資產分級盤點施作方式，下列敘述何者不正確？ (A) 保管人離職轉移，需要進行相關資產歸戶變更 (B) 異地備援端相關系統，需另標示位置資訊，以為識別 (C) 電腦規格需依據製造商規格項列於資訊紀錄中 (D) 資訊設備送修，無法列入盤點，可以不用處置追蹤
C	14. 下列何者非資產擁有者所負責執行之工作？ (A) 確保資產已盤點並造冊 (B) 確保資產已經適切分級，並實施適當之保護 (C) 確保資產以最低之成本進行採購 (D) 確保資產的銷毀已採取適當之處置程序
C	15. 下列何者為建立組織資訊安全管理系統（Information Security Management System, ISMS）活動中優先於另三項需要進行的任務？ (A) 識別弱點 (B) 識別現有及已規劃之控制措施 (C) 識別資訊資產 (D) 識別威脅
A	16. 如果資訊安全事件的攻擊者的獲益小於成本時，或是預估的損失在組織可以容忍的範圍內，此時可以採取哪一種風險處置策略？ (A) 風險接受 (B) 風險降低 (C) 風險移轉 (D) 風險避免
D	17. 以下何者非風險評鑑後，對於超出風險事項首要處理方式？ (A) 風險規避 (B) 風險轉嫁 (C) 風險控制 (D) 風險再評鑑
C	18. 關於風險分析（Risk Analysis），下列敘述何者不正確？ (A) 在現有的控制方法下，系統性運用有效資訊，以判斷特定事件發生的可能性及其影響的嚴重程度 (B) 將可接受風險與主要風險分開，並提供風險評量所需的資料 (C) 風險分析的步驟之一為畫出風險圖像，依分析資料結果畫出風險圖像，橫軸代表機率，縱軸代表時間 (D) 風險分析的步驟之一為蒐集資訊，包括紀錄經驗、國外的應用、出版文獻、調查與研究、專家判斷、模型應用、實驗及原型

C	19. 關於資訊安全管理系統中的風險處理，下列敘述何者不正確？ (A) 依照風險等級，實施控制措施，降低風險 (B) 可選擇風險轉移；比方購買地震或防火保險 (C) 所有風險都可以選擇直接接受 (D) 移除風險來源
D	20. 下列何者不是定量風險分析中所使用的計算因子？ (A) 年度發生率（Annualized Rate of Occurrence, ARO） (B) 資產價值（Assets Value） (C) 暴露因子（Exposure Factor, EF） (D) 均線（Moving Average, MA）
D	21. 關於存取控制措施，下列敘述何者不正確？ (A) 應建立帳號管理機制，包含帳號之申請、開通、停用及刪除之程序 (B) 組織應在符合資訊存取限制條件下，讓授權的使用者可指派分享的存取權限 (C) 對於每一種允許的遠端存取類型，都應先取得授權，建立使用限制、組態/連線需求及實作指引，並予以文件化 (D) 資訊系統無需對行動裝置之連線要求授權
C	22. 存取控制大概可分為三類，系統、實體與網路存取控制。以下哪種行為是屬於實體存取控制？ (A) 讀取公司郵件 (B) 列印生產報表 (C) 進入機房巡檢 (D) 上網瀏覽新聞
B	23. 新進員工好奇嘗試操作公司資訊系統，發現很多功能都無法使用，但其主管使用時卻無此問題。關於上述情境，最可能發生的原因何？ (A) 系統有缺陷造成 (B) 最小權限原則 (C) 硬碟發生壞軌 (D) 系統感染電腦病毒

C	24. 下列何種權限管理行為較不適當？ (A) 公司負責人擁有 ERP 所有系統的唯讀權限，並另外擁有最高管理者的帳號密碼 (B) 採購主管擁有 ERP 採購系統除單據（紀錄）刪除外的所有權限，並擁有物料庫存數量的查詢權限 (C) 資訊人員擁有 ERP 系統設定權限，並同時擁有 ERP 系統採購單據的新增、編輯、刪除權限 (D) 會計主管擁有 ERP 系統每月結轉權限
B	25. 關於身分認證（Authentication），下列敘述何者正確？ (A) 擁有系統的帳戶與密碼，可以登入電子系統 (B) 確認使用電子身分的是使用者本人的程序 (C) 給予使用者聽、說、讀、寫、執行、刪除等等權限 (D) 留下使用者的使用軌跡，並且自動稽核
A	26. Faker 是公司的資訊人員，主要職責為避免非法存取控制的資安事件發生。請問以下「不是」他應有的作為？ (A) 將多台電腦共用同一組存取密碼 (B) 記錄所有登入的事件 (C) 呼籲同仁在離開電腦時需上鎖 (D) 呼籲同仁切勿將自己的帳戶提供他人使用
B	27. 下列何者不屬於實體控制（Physical Controls）層面？ (A) 門禁系統 (B) 安全政策 (C) 纜線保護 (D) 大樓保全或警衛
D	28. 關於 OTP（One-Time Password）的特性，下列敘述何者不正確？ (A) 不可預測 (B) 使用一次 (C) 不可重複 (D) 能防止釣魚網站
D	29. 身份認證主要是來證明使用者的身份，相關的機制設計主要包含三要素，請問下列何者不包含在其中？ (A) Something you know (B) Something you have (C) Something you are (D) Something you need

A	30. 使用通關密碼或是 PIN 碼來登入資訊系統，這是屬於下列何種身份認證方式？ (A) 所知之事 (B) 所持之物 (C) 所具之形－靜態特徵 (D) 所具之形－動態特徵
D	31. 下列何者不是 Biometric Systems 識別身分驗證技術？ (A) Fingerprint (B) Retina (C) Iris (D) OTP
C	32. 下列哪一個工具無法進行身分認證？ (A) 記名悠遊卡 (B) 信用卡 (C) 超商集點卡 (D) 健保卡
B	33. 某家國防工業公司，員工被要求需使用智慧卡（Smart Card）和個人識別碼（Personal Identification Number, PIN）登入公司資訊系統，請問這家公司使用的是哪一種驗證方法？ (A) 時間基礎的一次密碼（Time-based One-Time Password, TOTP） (B) 多因子認證法（Multifactor） (C) 相互認證法（Mutual Authentication） (D) 聯邦認證法（Federal Authentication）
C	34. 使用帳號及密碼進行身分認證，是時下網路上最常用的方法，破解密碼就可以有效攻擊身分認證，下列何項不是針對破解密碼的攻擊？ (A) 窮舉攻擊（Brute-Force Attack） (B) 字典攻擊（Dictionary Attack） (C) 跨網站指令碼攻擊（Cross-Site Scripting） (D) 網路釣魚網站（Phishing）
C	35. 關於資安事件發生前的預先準備計畫，下列敘述何者不正確？ (A) 應訂定災害預防計畫 (B) 應規劃建置資通安全整體防護環境 (C) 利用防火牆等設備隔離受害主機 (D) 應定期實施安全稽核

D	36. 下列名詞解釋何者不正確？ (A) 年度損失預測值（ALE），一年內預期資產因風險造成之金錢損失 (B) 間接價值（Indirect Value），資訊資產受損或遺失，因置換或回復所估之價值 (C) 社會價值（Societal Value），公眾對於資訊安全事件之對錯判別 (D) 機會價值（Opportunity Value），從特定資安活動取得已知估計正價值
C	37. 依據「行政院國家資通安全會報通報及應變作業流程」，各級政府機關於通報並著手處理資安事件後，若判定為 1 級或 2 級事件，應於幾小時內完成復原或損害管制？ (A) 24 小時 (B) 48 小時 (C) 72 小時 (D) 96 小時
B	38. 請問發生資安事故的第一步驟為何？ (A) 蒐集證據 (B) 記錄 (C) 將系統回復 (D) 檢討原因
C	39. 當組織遇到資訊安全事件時，必須採取正確、有效的處理程序。處理事件的第一步驟是？ (A) 問題隔離 (B) 問題分析 (C) 問題分類 (D) 問題調查
A	40. 您是資安經理，正在分析異地備援的模式，公司將以最低成本考量，您將建議下列何者方案？ (A) 冷備援站（Cold Site） (B) 暖備援站（Warm Site） (C) 熱備援站（Hot Site） (D) 冗餘備援站（Redundancy Site）
D	41. 下列何者與營運持續計畫之規劃的關聯度較低？ (A) 風險評鑑的結果 (B) 可接受 RTO（回復時間目標）、RPO（回復點目標）的標準 (C) 營運衝擊分析的結果 (D) 資訊資產的盤點結果

A	42. 請問同樣的系統資料，採用下列三種備份方式，當要將資料還原時，下列何者執行還原作業所需的時間最長？ 甲：完整備份（Full Backup） 乙：增量備份 （Incremental Backup） 丙：差異備份（Differential Backup） (A) 甲 (B) 乙 (C) 丙 (D) 三者相同
D	43. 下列何者是營運持續管理的國際標準？ (A) ISO 9000 (B) ISO 14000 (C) ISO 20000 (D) ISO 22301
C	44. 在訂定企業營運持續計畫時，下列何者是首要進行的事？ (A) 訂定災難復原計畫（Disaster Recovery Plan, DRP） (B) 執行營運衝擊分析（Business Impact Analysis, BIA） (C) 獲得高階管理階層的支持 (D) 鑑別關鍵性業務
D	45. 先進的網路技術，開啟了個人電腦使用挖掘大量資料的可能性，因此能比過去難以想像的大規模及精準地侵犯個人隱私。下列何者不算個人隱私？ (A) 醫療、健康狀況 (B) 性生活 (C) 財務情況、社會活動 (D) 證件上照片
D	46. 下列何種不是智慧財產相關的法令規範？ (A) 專利法 (B) 著作權法 (C) 商標法 (D) 公司法
B	47. 下列何者不是個人資料的當事人可行使的權利？ (A) 查詢當事人的個人資料 (B) 查詢親友的個人資料 (C) 請求製給複製本 (D) 請求補充或更正

C	48. 請問下列敘述何者不屬於稽核員的主要工作？ (A) 依據稽核規劃與時程執行稽核活動 (B) 在稽核的過程中，紀錄相關發現與待確認事項 (C) 針對前一次稽核活動中的發現事項，規劃並執行相關的矯正預防作為 (D) 在稽核結束會議前，與受稽者再次釐清並確認相關稽核發現事項
A	49. 組織內部的人員擔任稽核人員，進行內部稽核，又稱為？ (A) 第一方稽核 (B) 第二方稽核 (C) 第三方稽核 (D) 驗證稽核
D	50. 請問下列何者不可作為稽核證據？ (A) 受稽人員口述 (B) 檢視紙本紀錄之結果 (C) 利用稽核工作檢測之結果 (D) 稽核人員之主觀判斷
D	51. 下列何者是「機密性」的正確意涵？ (E) 確保被使用的為正確資料，未遭人竄改 (F) 確保網路通訊中的參與者，不會拒絕承認他們的行為 (G) 確保資訊服務隨時可被取用 (H) 防止未經授權的人或系統存取資料或訊息
C	52. 請問「確保已授權之使用者可適時、可靠的存取資料與資源」所代表的意義是下列何者？ (E) 機密性 (F) 完整性 (G) 可用性 (H) 可讀性
B	53. 組織內部某資料庫遭受駭客藉由惡意程式入侵，竊走大量個人資料，請問此為下列哪些特性遭受破壞？ (E) 可用性 (F) 機密性 (G) 完整性 (H) 可讀性
A	54. 關於「識別風險並以定性或定量之方式計算風險值」，是下列何者的敘述？ (A) 風險分析 (B) 風險處理

	(C) 風險轉嫁 (D) 風險降低
C	55. 管理階層的審查作業，是屬於戴明循環（P、D、C、A）的哪個步驟？ (E) 計畫（Plan） (F) 執行（Do） (G) 檢查（Check） (H) 行動（Act）
B	56. 在資訊安全管理中，關於資訊資產的使用，下列敘述何者正確？ (E) 存有資訊資產的設備要汰換時，只需要將機器交給回收廠商即可 (F) 資訊資產攜出，必須經過適當的授權與核可 (G) 印有機敏性資料的文件，集中到大樓回收箱即可 (H) 資訊資產放在 USB 很方便，隨插隨用，訊息交換最直接
C	57. 下列何者不是導入資訊安全管理系統（Information Security Management System, ISMS）的主要目的？ (E) 保護組織資訊資產的安全 (F) 確保資訊系統能夠穩定的運作 (G) 降低企業的營運和人員成本 (H) 避免資料外洩事故的發生
D	58. 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。關於 PDCA 四個程序，下列說明何者不正確？ (E) 計畫（Plan）：依照組織政策，建立必要的資安目標 (F) 執行（Do）：實施此計畫的過程 (G) 檢查（Check）：針對資安目標，確認監督及量測過程，並報告及結果 (H) 行動（Act）：單位執行內部稽核
C	59. 關於資訊資產控管原則，下列敘述何者正確？ (E) 關鍵系統設備不需建立備援機制 (F) 網路設備不用建立備用系統 (G) 個人使用之套裝軟體，其存取權限的賦予，應與使用者的角色與職責相符 (H) 公開資料未經權責主管之授權核可，禁止複製
B	60. 資訊資產分類一般可分為硬體、軟體、資料、文件、人員、服務。請問下列哪一種可分類為服務資產？ (E) 網路設備

	(F) 電力 (G) 請假單 (H) 資訊部門主管
D	61. 關於資訊資產分類的描述，下列敘述何者不正確？ (A) 使資訊資產易於管理 (B) 資產管理者或擁有者應依資產之屬性進行分類 (C) 各組織針對所擁有之資訊資產不同，可能會因定義不同而有不同資訊資產分類 (D) 資訊資產分類定義都是固定的，只能分成四類（資料、軟體、硬體與人員）
A	62. 下列何者負責進行資訊分類的判斷？ (E) 擁有者（Owner） (F) 保管員（Custodian） (G) 資訊安全經理（Information Security Manager） (H) 資訊風險經理（Information Risk Manager）
D	63. 關於資產盤點與汰除事項，下列敘述何者不正確？ (A) 財務重要薪資硬碟故障，除資產變更汰除外，應進行消磁銷毀 (B) 傳真掃描影印事務機舊機報廢，應進行儲存媒體清除 (C) 待汰除設備過多，需要擔心聚合效應（Aggregation Effect） (D) 電腦報廢因整台中古回收價格更高，所以相關硬碟不用額外處理
C	64. 下列何者最適合被指派為資產擁有者？ (E) 資產的採購者 (F) 資產的盤點者 (G) 對資產的使用負有管理責任者 (H) 外包的廠商人員
B	65. 關於組織的資訊資產，下列敘述何者不正確？ (E) 資訊資產包含組織內與資訊活動相關的任何人事物 (F) 資訊資產的擁有者對該資產具有實質的財產權 (G) 資訊安全管理的目的在保護資訊資產的機密性、完整性和可用性 (H) 資訊資產管理對資訊安全而言，其目的在於識別與資訊活動相關的資產，並予以適當的保護
D	66. 對於高等級的衝擊可能會嚴重違背、傷害或阻礙一個組織的使命、聲譽或利益，或者可能會造成人員的死亡或嚴重受傷。此時應該優先考量哪一種風險處置策略？ (E) 風險接受

	(F) 風險降低 (G) 風險移轉 (H) 風險避免
A	67. 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
C	68. 關於風險管理常舉例的「木桶理論」，如何決定一個由長短不同的木板所構成的木桶之「容水量大小」，下列敘述何者正確？ (E) 取決於其中「最長」的那塊木板 (F) 取決於全部木板長度的「平均值」 (G) 取決於其中「最短」的那塊木板 (H) 以上皆非
D	69. 為了降低風險，下列何者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
B	70. 關於風險管理，下列敘述何者不正確？ (E) 管理組織風險，避免風險擴大 (F) 協助組織隱藏風險，避免驗證失效 (G) 協調實作控制風險，降低風險 (H) 尋求備案，以避免意外發生
B	71. 關於存取控制措施，下列敘述何者正確？ (E) 組織建立無線存取資訊系統時，無需取得授權，以快速建立無線存取使用限制、組態/連線需求 (F) 採用最小權限原則時，只允許使用者依據任務和業務功能，完成所需之授權存取 (G) 資訊系統及系統間的資料交換，無需採取強制審查授權，以符合組織的存取控制政策 (H) 作業系統皆無需考慮強制存取控制（Mandatory Access Control, MAC）之架構
C	72. 特權（Privilege）是指使用者對資訊資產擁有特殊的權限。下列何者不是特權使用者？

	(A) 資料庫管理員 (B) 帳號管理員 (C) 文書處理員 (D) 網路管理員
A	73. 「業務承辦人員，不能身兼業務稽核人員」為下列何者的說明？ (A) 職務區隔（Segregation of Duties） (B) 最小權限原則（Principle of Least Privilege） (C) 必要知道原則（Need-to-know Principle） (D) 以角色為基礎的存取控制（Role-based access control, RBAC）
B	74. 關於權限管理，下列做法何者較不適當？ (A) 賦予新到任資訊人員系統權限前，應先經過考核 (B) 由於系統權限設定時已經過核准，故不需定期審查系統權限 (C) 採購助理申請查詢庫存數量權限時，應會簽倉儲主管 (D) 業務助理離職後，系統僅設定停用該員帳號而非刪除帳號
D	75. 下列何者不是資料存取控制的方法？ (A) 強制存取控制（Mandatory Access Control, MAC） (B) 存取控制目錄（Access Control List , ACL） (C) 規則基準存取控制（Rule-based Access Control） (D) 身分識別（Identification）
D	76. 當遇到需設定密碼識別的情況時，下列何種做法可使密碼較不容易被破解？ (A) 使用純數字 (B) 英文名字加生日 (C) 身分證字號 (D) 參雜大小寫數字，越雜亂無章越好
D	77. 下列何種生物辨識方式之交叉錯誤率（Crossover Error Rate, CER）最低？ (A) 語音辨識 (B) 掌形辨識 (C) 手寫辨識 (D) 虹膜辨識
B	78. 關於身分認證機制，下列敘述何者不正確？ (A) 兩階段身分認證的方式可透過手機，或是專屬的安全金鑰裝置等工具執行 (B) 兩階段身分認證的目的，在於簡化認證程序

	(C) 動態密碼符記（Token）身份認證，是在使用者端常見的驗證工具 (D) 可透過 LDAP 服務，整合使用者在各種應用程式進行認證
C	79. 下列何種攻擊手法，無法達到竊取或偽冒 Windows 使用者身份的目的？ (E) PTT（Pass the Ticket） (F) PTH（Pass the Hash） (G) DDoS（Distributed Denial-of-Service Attack） (H) 密碼暴力破解（Brute-Force Attack）
A	80. 以下所列的都是身份認證所需的相關元素，其中何者遭公開或竊取時，不會影響身份認證的安全性？ (E) 憑證公鑰（Public Key） (F) 密碼（Password） (G) 通行碼（Pin Code） (H) 憑證私鑰（Private Key）
D	81. 關於身份識別與存取管理（Identity and Access Management, IAM），下列敘述何者不正確？ (E) IAM 重視驗證（Authentication）、授權（Authorization）及稽核（Auditing） (F) IAM 可透過你知（What you know）、你有（What you have）、你是（What you are） (G) 驗證安全其它條件，應思考通訊傳輸加密與驗證值加密保護 (H) 驗證後權限，應符合最大權限原則
C	82. 身分驗證中，生物特徵比對有靜態與動態的差異。請問下列何者不是動態比對？ (E) 聲音辨識 (F) 臉部辨識 (G) 指紋辨識 (H) 電子筆簽字辨識
C	83. 若員工重複使用先前用過的密碼，請問管理人員應執行下列何種政策，以防止這種情況發生？ (E) 強制密碼歷程記錄和密碼最長使用期限 (F) 密碼最短使用期限和密碼必須符合複雜度需求 (G) 強制密碼歷程記錄和密碼最短使用期限 (H) 密碼必須符合複雜度需求和強制密碼歷程記錄
C	84. 身分認證存取控制是一種限制資源存取的處理方式及程序，其目的在保護系統資源不會被非經授權者或授權者進行不當的存取。請問使用

	者身分被認證後，授予其應有的權限的程序稱為？ (E) Identification（識別） (F) Authentication（認證） (G) Authorization（授權） (H) Accountability（可歸責）
D	85. 下列何者不屬於資訊安全事件通報之情況？ (A) 破壞所預期之資訊完整性、機密性、可用性 (B) 違反個資法 (C) 存取違例 (D) 廠商例行維護
D	86. 下列何者不屬於資安事故應變與處理程序循環？ (E) 發現與分析（Detection & Analysis） (F) 控制移除與復原（Containment, Eradication & Recover） (G) 準備（Preparation） (H) 清除 Log 檔（Reset Log File）
D	87. 關於資訊安全事故，下列敘述何者不正確？ (E) 事件發生時，應填寫通報單，來判定是否為資安事故 (F) 應將資訊安全事件進行分級 (G) 每一個級別都可視為資安事故，有不同處理規範 (H) 天然災害為不可抗力，所以不用列入處理
B	88. 關於資安事件（Security Event），下列敘述何者最正確？ (E) 一定需要立即處理 (F) 需要留存紀錄 (G) 發生時需要啟動緊急應變計畫 (H) 與資安事故（Security Incident）沒有差別
A	89. 如發現駭客正試圖攻擊路由器或防火牆，尚未入侵網路系統。稱之為？ (A) 資訊安全事件 (B) 資訊安全事故 (C) 資訊安全風險 (D) 資訊安全分析
A	90. 下列何種備份方式，當需要完整還原所有檔案至前一個備分時間點之資料時，通常其還原速度最快？ (E) 完整備份（Full Backup） (F) 差異備份（Differential Backup） (G) 增量備份（Incremental Backup） (H) 選擇式備份（Selective Backup）

C	91. 下列幾種異地備援中心，何者可在發生重大災難時於最短時間內將服務回復至最低服務水準？ (E) 冷備援（Cold Site） (F) 暖備援（Warm Site） (G) 鏡備援（Mirror Site） (H) 熱備援（Hot Site）
C	92. 關於最大可容忍的中斷時間（Maximum Tolerable Period of Disruption, MTPD），下列敘述何者正確？ (E) 實際電力中斷的時間 (F) 實際停止上班的時間 (G) 關鍵營運活動最多可允許中斷的時間 (H) 關鍵資料可遺失的時間
B	93. 下列何者是主機備援最安全的做法？ (A) 將備用主機和備份資料，存放於營運主機所在的相同地點 (B) 將備用主機和備份資料，存放於營運主機所在的不同地點 (C) 將備用主機與營運主機存放在相同地點，備份資料則存放於不同地點 (D) 將備份資料與營運主機存放在相同地點，備用主機則存放於不同地點
D	94. 下列何者為訂定資料備份策略時，決定可接受之資料損失的項目？ (A) 復原時間目標（Recovery Time Objective, RTO） (B) 備份媒體的選擇 (C) 備份時間與週期 (D) 復原點目標（Recovery Point Objective, RPO）
C	95. 下列哪種行為並不違反智慧財產權？ (A) 複製有版權的軟體給他人使用 (B) 使用或張貼網路上的文章及圖畫 (C) 推薦網上購物商品資訊與朋友 (D) 下載網上電影並分享與他人
D	96. 下列何者並非個人資料保護法中，當事人對於個人資料的權利？， (A) 查詢或請求閱覽 (B) 請求補充或更正 (C) 請求刪除 (D) 請求永久保留
D	97. 下列何者非個資法第 6 條，不可隨意蒐集、處理或利用的個資？

	(E) 病歷 (F) 基因 (G) 犯罪前科 (H) 財務情況
C	98. 下列何種行為描述，將會損及稽核人員之專業與職業道德？ (A) 稽核人員以誠實、嚴謹及負責之態度執行其任務 (B) 不得使用資訊以圖個人利益 (C) 為維持與受稽核對象的良好關係，部份重大的稽核發現，可選擇性的不揭露在相關的稽核報告中 (D) 應謹慎使用及保護其在執行任務過程所獲得之資訊
C	99. 關於稽核軌跡，下列敘述何者正確？ (E) 為對紀錄與其他資訊進行獨立檢測的方法 (F) 用於找出與管理影響企業之潛在事件與風險 (G) 指事件發生的過程中留下可供稽核的文件或紀錄 (H) 提供組織一個正確的電腦稽核管理方向與趨勢
D	100. 小張擔任公司的個人資料保護作業內部稽核人員，因時間不足，他於稽核完每個部門的業務負責人後，未向該單位進行稽核結果說明，即直接前往下一受稽核單位，請問關於這樣的稽核方式，下列敘述何者最適當？ (E) 此做法正確，稽核應於預定的時間內完成為首要目標 (F) 此做法正確，稽核結果在結束會議時統一說明即可 (G) 此做法不適當，應該減少稽核項目，隔年稽核再補查，但需向受查單位說明此一狀況 (H) 此做法不適當，每次稽核結束，都應向受稽核單位說明稽核結果，並且取得受稽單位對稽核結果的共識