IPAS資安工程師認證題庫\_資訊安全管理概論

|  |  |  |
| --- | --- | --- |
| 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 |
| B | 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 |
| D | 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 |
| D | 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 |
| C | 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 |
| C | 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 |
| B | 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 |
| C | 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 |
| A | 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 |
| B | 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 |
| 無答案 | 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?  (A) 確保被使用的為正確資料,未遭人竄改  (B) 確保網路通訊中的參與者,不會拒絕承認他們的行為  (C) 確保資訊服務隨時可被取用  (D) 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?  (A) 機密性  (B) 完整性  (C) 可用性  (D) 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?  (A) 可用性  (B) 機密性  (C) 完整性  (D) 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?  (A) 計畫(Plan)  (B) 執行(Do)  (C) 檢查(Check)  (D) 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?  (A) 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  (B) 資訊資產攜出,必須經過適當的授權與核可  (C) 印有機敏性資料的文件,集中到大樓回收箱即可  (D) 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?  (A) 保護組織資訊資產的安全  (B) 確保資訊系統能夠穩定的運作  (C)降低企業的營運和人員成本  (D)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?  (A) 計畫(Plan):依照組織政策,建立必要的資安目標  (B) 執行(Do):實施此計畫的過程  (C) 檢查(Check):針對資安目標,確認監督及量測過程,並報告及  結果  (D) 行動(Act):單位執行內部稽核 |
| D | 59. | 關於資訊資產控管原則,下列敘述何者正確?  (A) 關鍵系統設備不需建立備援機制  (B) 網路設備不用建立備用系統  (C) 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  (D) 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?  (A) 網路設備  (B) 電力  (C) 請假單  (D) 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?  (A) 擁有者(Owner)  (B) 保管員(Custodian)  (C) 資訊安全經理(Information Security Manager)  (D) 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?  (A) 資產的採購者  (B) 資產的盤點者  (C) 對資產的使用負有管理責任者  (D) 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?  (A) 資訊資產包含組織內與資訊活動相關的任何人事物  (B) 資訊資產的擁有者對該資產具有實質的財產權  (C) 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  (D) 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?  (A) 風險接受  (B) 風險降低  (C) 風險移轉  (D) 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?  (A) 取決於其中「最長」的那塊木板  (B) 取決於全部木板長度的「平均值」  (C) 取決於其中「最短」的那塊木板  (D) 以上皆非 |
| A | 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 |
| D | 70. | 關於風險管理,下列敘述何者不正確?  (A) 管理組織風險,避免風險擴大  (B) 協助組織隱藏風險,避免驗證失效  (C) 協調實作控制風險,降低風險  (D) 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?  (A) 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  (B) 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  (C) 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  (D) 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) |
| D | 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?  (A) PTT(Pass the Ticket)  (B) PTH(Pass the Hash)  (C) DDoS(Distributed Denial-of-Service Attack)  (D) 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?  (A) 憑證公鑰(Public Key)  (B) 密碼(Password)  (C) 通行碼(Pin Code)  (D) 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?  (A) IAM 重視驗證(Authentication)、授權(Authorization)及稽核  (Auditing)  (B) IAM 可透過你知(What you know)、你有(What you have)、你是(What you are)  (C) 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  (D) 驗證後權限,應符合最大權限原則 |
| D | 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?  (A) 聲音辨識  (B) 臉部辨識  (C) 指紋辨識  (D) 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?  (A) 強制密碼歷程記錄和密碼最長使用期限  (B) 密碼最短使用期限和密碼必須符合複雜度需求  (C) 強制密碼歷程記錄和密碼最短使用期限  (D) 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?  (A) Identification(識別)  (B) Authentication(認證)  (C) Authorization(授權)  (D) 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?  (A) 發現與分析(Detection & Analysis)  (B) 控制移除與復原(Containment, Eradication & Recover)  (C) 準備(Preparation)  (D) 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?  (A) 事件發生時,應填寫通報單,來判定是否為資安事故  (B) 應將資訊安全事件進行分級  (C) 每一個級別都可視為資安事故,有不同處理規範  (D) 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?  (A) 一定需要立即處理  (B) 需要留存紀錄  (C) 發生時需要啟動緊急應變計畫  (D) 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 |
| C | 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?  (A) 完整備份(Full Backup)  (B) 差異備份(Differential Backup)  (C) 增量備份(Incremental Backup)  (D) 選擇式備份(Selective Backup) |
| D | 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?  (A) 冷備援(Cold Site)  (B) 暖備援(Warm Site)  (C) 鏡備援(Mirror Site)  (D) 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?  (A) 實際電力中斷的時間  (B) 實際停止上班的時間  (C) 關鍵營運活動最多可允許中斷的時間  (D) 關鍵資料可遺失的時間 |
| D | 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 |
| 都不可 | 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?  (A) 病歷  (B) 基因  (C) 犯罪前科  (D) 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 |
| B | 99 | 關於稽核軌跡,下列敘述何者正確?  (A) 為對紀錄與其他資訊進行獨立檢測的方法  (B) 用於找出與管理影響企業之潛在事件與風險  (C) 指事件發生的過程中留下可供稽核的文件或紀錄  (D) 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?  (A) 此做法正確,稽核應於預定的時間內完成為首要目標  (B) 此做法正確,稽核結果在結束會議時統一說明即可  (C) 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  (D) 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 |
| A | 101. | 下列哪一種攻擊手法,主要目的是在破壞「機密性」?  (1) 社交工程  (2) 搜尋引擎攻擊(Google-Hacking)  (3) 拒絕服務(Denial-of-Services)  (4) 駭客侵入銀行資料庫竄改存款金額  (A) (1), (2)  (B) (3), (4)  (C) (2), (3), (4)  (D) (1), (2), (4) |
| A | 102. | 請問「無論是資源、通訊、資料或是資訊等,只能讓經授權的使用者使用」所代表的意義是下列何者?  (A) 機密性  (B) 完整性  (C) 可用性  (D) 可讀性 |
| B | 103. | 建立資訊系統資料備份機制,與下列何者關聯性最高?  (A) 可歸責性  (B) 可用性  (C) 完整性  (D) 機密性 |
| C | 104. | 請問系統安全程序、設計、裝置、或內部控制裡的一個瑕疵或缺點,若被運用,會破壞安全性或違背系統安全政策,此為 NIST SP800-30對下列敘述何者的定義?  (A) 威脅  (B) 弱點  (C) 風險  (D) 衝擊 |
| D | 105. | 關於文件管制措施,下列敘述何者正確?  (A) 所有制定的 SOP 皆須書面發行  (B) 制定的各項管理制度、程序,不宜以電子檔案公佈  (C) 所制訂管理辦法及作業程序需要被遵守,因此所有人皆可閱讀所有文件  (D) 文件管制宜訂定標準作業程序,以利組織成員遵循 |
| D | 106. | 關於資訊安全政策的審查,下列敘述何者不正確?  (A) 資訊安全政策應定期審查  (B) 相關法令有重大變更時,應進行審查  (C) 公司主要營業項目有重大改變時,應進行審查  (D) 資訊安全政策之審查由資訊主管單獨進行即可 |
| B | 107. | 在資訊安全管理系統(Information Security Management System, ISMS)的維運過程中,「文件化資訊」是必要的要求,下列何者不是所有文件化資訊需確保的事項?  (A) 制訂需要有可識別的方式,例如:標示文件的標題和日期  (B) 發行需要由文件管理人員審查之後,即可對外公佈發行  (C) 在需要時得提供給相關人員  (D) 需要受到適切的保護,以避免不當使用和外洩 |
| C | 108. | 資訊安全政策是資訊安全管理系統中的最高指導原則,有不可缺少的重要性,下列敘述何者正確?  (A) 滿足相關的要求事項的承諾後,無需持續改善  (B) 在四階管理文件中屬於第二階管理程序文件  (C) 建立的資訊安全政策必須符合組織的目的及資安目標  (D) 屬於內部或機密文件,不可對外公告 |
| C | 109. | 資訊資產群組化的好處是簡化並縮短資訊資產之風險評鑑時間,減少威脅、弱點的重複判斷。下列何者資訊資產比較不適合群組化為同一類型?  (A)機房內的所有主機  (B) 同部門的工作電腦  (C) 識別門禁卡  (D)系統開發規格書 |
| A | 110. | 進行資產分類為下列哪一種安全控管類型?  (A)預防性控制(Preventive)  (B) 檢測性控制(Detective)  (C) 指令性控制(Directive)  (D)糾正性控制(Corrective) |
| D | 111. | 資訊資產價值需考量資訊資產的機密性、可用性及完整性,下列何種情況是應該考量提高可用性?  (A) 公司官網遭竄改  (B) 未授權存取人事資料  (C) 電腦安裝免費軟體  (D) ERP 系統當機 |
| A | 112. | 關於資訊資產,下列敘述何者不正確?  (A) 資訊資產安全等級之影響評估構面通常至少會包含機密性、完整性等  (B) 資訊資產重要性等級一旦區分完成,之後不需要再重新檢視或變更  (C) 資產分類分級作業通常是為了之後進行風險管控作業所需  (D) 資產標示並不僅限於硬體資產 |
| C | 113. | 關於資產分類分級,下列敘述何者正確?  (A) 資產評估不需考量資產之完整性、可用性、機密性  (B) 資產分類分級不需考慮產業別差異  (C) 資產分類分級可以做為風險評估重要的依據  (D) CCTV 系統歸在人資行管部門管控,可不列入分類與評估建議 |
| B | 114. | 關於雲端服務資產識別議題,下列敘述何者有待商榷?  (A) 租賃雲端服務系統,未列會計科目資產,所以不列入資訊資產盤點項目  (B) 雲端服務資料屬於企業組織之資產  (C) 雲端服務系統,仍屬於資產識別需考量之範圍  (D) 法規的適用上,在雲端資訊資產處理方式,各國無一致標準,需審慎使用 |
| C | 115. | 在進行資產盤點和建立資產清冊時,下列何者不是必要做法?  (A) 資產清冊需要識別與資訊及資訊處理設施有關的資產  (B) 資產清冊需要標示資產購置時的成本和費用  (C) 對已識別的資訊資產,需要指派資產的擁有者  (D) 資產清冊應予文件化 |
| A | 116. | 風險不可能不存在,面對風險有哪四種處置的方法?  (A) 接受、降低、移轉、避免  (B) 規劃、評估、排序、避免  (C) 面對、處理、解決、接受  (D) 評估、分析、處理、降低 |
| B | 117. | 假設災難一定會發生(不論機率再低),當災難發生時,為了確保組織在災難發生時有可遵循的作業程序,以降低損失,所以必須要制定哪一種文件?  (A) 風險管理計畫  (B) 緊急應變計畫  (C) 適用性聲明  (D) 內部稽核計畫 |
| A | 118. | 為能達成 ERP 系統不中斷的使用要求,資訊單位決定建立 ERP 備援系統,請問這是風險處理哪一種行為?  (A) 風險規避(Avoid)  (B) 風險轉嫁(Transfer)  (C) 風險降低(Reduce)  (D) 風險接受(Accept) |
| C | 119. | 關於風險降低,下列敘述何者不正確?  (A)其方式包括稽查及遵守計畫  (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 |
| C | 120. | 關於風險處理,下列敘述何者正確?  (A) 只要進行風險處理,就可以消弭所有的風險因子  (B) 風險處理,不需要考慮成本或法規要求  (C) 風險處理後,可能產生新的風險項目或是殘餘風險  (D) 風險處理僅能選擇暫時接受風險,別無他法 |
| B | 121. | 關於網路及系統存取管理,下列敘述何者不正確?  (A) 系統主機應考量保護機制,如設定在一段時間未操作時即會自動登出的機制  (B) 若因人為因素誤植帳號及密碼,無需保存紀錄檔  (C) 連線的來源位址與目的位址應建立路由(Routing)控管  (D) 管理者應依照使用者身份,控制系統應用程式的存取 |
| D | 122. | 關於特權管理,下列敘述何者最為正確?  (A) 登入主機應該使用 Administrator or Root 帳號,以利管理相關權限設定  (B) 資料庫管理員除了備份資料外,還需要讀取資料以利調校資料庫效能  (C) 基於代理人機制,系統管理員除了網路管理帳號外也需本機管理帳號  (D) 應該定期審查特權帳號,若有人員離職也須立即審查相關系統帳號 |
| D | 123. | 為了防止非授權的存取,企業應根據存取控管政策對使用者(包括內、外部使用者)存取權限進行管理。下列何者較無關於管理存取權限?  (A) 定期變更密碼  (B) 定期審查使用者存取權限  (C) 保留存取紀錄  (D) 資料備份 |
| C | 124. | 您是資訊業務承辦人員,當您有特殊業務需求進行存取敏感性資料時,需要獲得存取許可,即使您有資料存取權限,還需要提出資料存取的理由。上述說明主要為?  (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) |
| D | 125. | 關於權限管理,下列敘述何項較不適?  (A) 採購人員擁有採購系統新增、編修、存檔的權限,但無刪除權限  (B) 總經理只擁有採購系統所有模組的查詢權限  (C) 總經理將採購系統最高管理者的帳號密碼,存放於保險箱未使用,另外使用其他帳號登入系統  (D) 資訊主管的系統帳號已是採購系統管理者,因此無須監控其系統操作行為 |
| A | 126. | 常見的密碼驗證攻擊中,以下何種方法「不是」透過反覆嘗試密碼的方式破解密碼?  (A) 雜湊注入(Pass-the-Hash)  (B) 暴力攻擊(Exhaustive Search Attack)  (C) 字典攻擊(Dictionary Attack)  (D) 猜測攻擊(Guessing Attack) |
| A | 127. | 使用者在選定密碼時需注意避免太容易被攻擊者破解,請比較下面四組密碼,指出何組密碼較不容易遭到攻擊者破解?  (A) qwA$c&1!e  (B) password  (C) 12345678  (D) abcd0229 |
| C | 128. | 我們常使用密碼來做為認證身份的主要方式,關於密碼強度,下列敘述何者不正確?  (A) 符合密碼複雜性原則可增強密碼強度  (B) 對於複雜程度相同的密碼而言,長度較長的密碼安全度較短密碼為高  (C) 密碼複雜性原則不包含數字  (D) 密碼複雜性原則不包含圖片 |
| C | 129. | 為強化身份認證機制,我們常會使用雙因素認證機制,請問下列何種組合並不屬於雙因素認證的定義?  (A) 密碼(Password) + RFID 感應卡(如悠遊卡)  (B) RFID 感應卡 + 自然人憑證 IC 卡  (C) 自然人憑證 IC 卡 + 指紋  (D) 指紋 + 密碼 |
| A | 130. | 下列何者非單一登入(Single Sign-On, SSO)的優點?  (A)集中權限控管  (B) 降低不同的帳號密碼組合的困擾  (C) 減少重新輸入密碼的程序  (D)簡訊認證 |
| A | 131. | 關於 Kerberos,下列敘述何者不正確?  (A) 針對個人通信安全,可進行身份認證  (B) 是一種非對稱金鑰管理機制來進行金鑰管理的系統  (C) 可採複合 Kerberos 伺服器和缺陷認證機制來補救  (D) 具備加密機制,可保護資料完整性 |
| C | 132. | 關於設計網際網路服務使用者身分驗證機制的考量因素,下列何者不正確?  (A) What you know?使用者所記住的身分內容,如:個人識別名稱及對應的密碼  (B) What you have?使用者所擁有之認證裝置,如:金融卡、智慧卡  (C) Who you are?使用者所扮演的角色:如:學代、班聯會主席?  (D) What you are?使用者擁有之特徵,如:指紋、虹膜 |
| D | 133. | 請問在系統服務裡,關於身分驗證,下列敘述何者正確?  (A) 只要通過身分驗證,就可以暢行無阻。  (B) 身分驗證後,即是擁有最高權限。  (C) 身分驗證後,所有的使用行為都是適合理的,不需要軌跡。  (D) 依照最小權限原則,劃分給予適當的權限控管。 |
| C | 134. | 中華民國目前使用自然人憑證,做為民眾於網路應用時之合法身份識別依據。關於自然人憑證,下列敘述何者不正確?  (A)自然人憑證是基於 PKI(Public Key Infrastructure)架構下之應用  (B) 自然人憑證在網路上使用時,其代表申請人之身分識別上具有法律效力  (C) 自然人憑證申請一次永久有效,無需換發  (D)自然人憑證於網路上的相關應用具有不可否認性 |
| C | 135. | 關於營運持續管理處理策略之選擇,下列敘述何者不正確?  (A) 轉移風險(Transfer)  (B) 避免風險(Avoid)  (C) 調整風險(Adjust)  (D) 接受風險(Accept) |
| A | 136. | 依據「行政院國家資通安全會報通報及應變作業流程」,判定事故影響等級時,應評估資安事故造成之機密性、完整性以及可用性衝擊,下列何者非 4 級事件?  (A) 國家機密資料遭洩漏  (B) 關鍵資訊基礎設施系統或資料遭嚴重竄改  (C) 關鍵資訊基礎設施運作遭影響或系統停頓,無法於可容忍中斷時間內回復正常運作  (D) 機關業務系統或資料遭嚴重竄改 |
| B | 137. | 將不同的設備或不同時間的日誌進行比對,強化判斷是否為真正資安事件之動作,稱之為?  (A) 根因分析(Root Cause Analysis)  (B) 關聯分析(Correlation)  (C) 暫時解決方案(Workaround)  (D) 升級(Escalation) |
| D | 138. | 請問下列何者可以確定為資安事故(Security Incident)?  (A) 防毒軟體成功地更新了病毒碼  (B) 監控系統出現「硬碟使用量超過 80%」的訊息  (C) 執行 google 蒐尋,發現結果出現有公司機密文件  (D) 設備廠商進入機房維修 |
| B | 139. | 企業委託信賴的第三方團隊,對企業網路目標範圍進行安全性評估,找出存在的弱點或錯誤安全設定問題;並藉此瞭解員工對各種攻擊異常事件的反應。該進行哪種測試?  (A) 原始碼測試( Source Code Review)  (B) 壓力測試(Stress Testing)  (C) 迴歸測試(Regression Testing)  (D) 滲透測試( Penetration Test) |
| D | 140. | 您是資安專家,希望能估計營運可承受之最長中斷時間(Maximum Tolerable Period of Disruption),而您最有可能從下列何者取得?  (A) 平衡計分卡(Balanced Score Card)  (B) 風險估算(Risk Evaluation)  (C) 恢復點目標(Recovery Point Objective)  (D) 營運衝擊分析(Business Impact Analysis) |
| A | 141. | 公司或組織願意提供資源建立 Hot Site 即時備援系統,下列何者是較不可能的原因?  (A) 營業項目有法規的要求  (B) 為了符合所訂定的資訊安全目標  (C) 與客戶訂定的合約條款要求  (D) 客戶在公司提供的服務資源上,建立重要機密的管理系統 |
| D | 142. | 針對相同資料,請問下列三種備份方式,依其執行備份所需的時間,由大到小排列為下列何者?甲:完整備份(Full Backup) 乙:增量備份 (Incremental Backup) 丙:差異備份 (Differential Backup)?  (A) 甲>乙=丙  (B) 甲<丙<乙  (C) 甲=乙>丙  (D) 甲>丙>乙 |
| C | 143. | 關於復原的目標時間(Recovery Time Objective),下列敘述何者正確?  (A) 實際系統復原的時間  (B) 系統無法復原的時間  (C) 發生災難後,預計完成系統復原的時間  (D) 發生災難後,預計系統可能中斷的時間 |
| B | 144. | 下列何者非現代常用的備份媒體?  (A) 磁片  (B) 磁帶  (C) 光碟  (D) 外接硬碟 |
| A | 145. | 智慧財產權(Intellectual Property Rights)是指由人類思想、智慧、創作而產生具有財產價值的產物。下列何者不屬於智慧財產權?  (A) 肖像權  (B) 專利權  (C) 著作權  (D) 營業秘密法 |
| C | 146. | 商標註冊後,商標註冊人享有商標專用權,圖形為 『® 』,表示某個商標經過註冊,並受法律之保護。關於商標與專利,下列敘述何者不正確?  (A) 專利需要具有發明、新型及新式樣等  (B) 商標是一個圖樣,或文字,或符號,或顏色,或聲音  (C) 德國愛迪達公司控告美國威名百貨銷售的佩雷斯運動鞋有三條線,是非法使用其『愛迪達』專利權  (D) 專利權是對發明授予的權利,對專利權人之發明予以保護,保護權利在一段期間內有效,一般期限為 20 年 |
| c | 147. | 下列何者不是展現保護智慧財產權的良好做法?  (A) 建立銷毀軟體或是轉讓給他人的政策  (B) 允許暫時超過軟體授權內的使用人數上限  (C) 將合法授權的軟體光碟複製一份作為備用  (D) 妥善保存軟體光碟的授權書和啓用碼 |
| B | 148. | 根據我國內部稽核協會所訂定之「內部稽核與職業道德規範」,認為內部稽核人員應遵守四大原則,下列何者未包含在其中?  (A) 誠正  (B) 節省  (C) 客觀  (D) 保密 |
| B | 149 | 下列稽核的程序活動中,何者較為優先?  (A) 評估內部控制之有效性  (B) 規劃稽核目標及範圍  (C) 營運活動的觀察  (D) 準備稽核報告 |
| A | 150 | 下列何種權利必須到經濟部智慧財產局申請,才可享有?  (a)專利權(b)商標權(c)著作權  (A) (a)(b)  (B) (a)(c)  (C) (b)(c)  (D) (a)(b)(c) |