ITE 資訊專業人員鑑定

資訊安全類-資訊與網路安全管理概論試題

試卷編號：ISN-109

【注意事項】

一、本測驗為單面印刷試題，共計 13 頁。第 2 至 13 頁為 40 道學科試題，每題 2.5 分，測驗時間 90 分鐘。

二、執行「ITE 測驗系統-Client 端程式」，請依指示輸入：

1. 身份證號碼，如 A123456789 後按下『登錄』。
2. 開始測驗畫面，聽候監考老師口令開始測驗。

三、有問題請舉手發問，切勿私下交談。

學科 100% （為單複選題，每題 2 分，共 100 分）

001. 將公司資訊技術服務化是資訊技術服務管理(ITSM)的基礎理念，下面何者不是資訊技術服務管理的特色？

(A)將公司內、外部各單位視為資訊部門的「客戶」，並與客戶簽定服務水準約定

(B)除技術外，更要從人員、流程與組織進行管理

(C)強調完整服務(End-to-end service)

(D)強調資料的保護與提供

Ans：D

002. 現在資訊基礎架構的部署常採用虛擬機器(virtual machine)架構，以下何者不是採用虛擬機器架構下的好處？

(A)平台互通(platform independent)

(B)提昇應用程式安全性

(C)更具彈性的運算及儲存資源的調配

(D)資料不易受損

Ans：D

003. 面對組織內日益龐大且複雜的資訊資源，組態管理(configuration management)變得越來越重要，下面哪一個程序不是組態管理主要可支援項目？

(A)異常事件管理程序(incident management)

(B)變更管理程序(change management)

(C)上線管理程序(release management)

(D)財務管理程序(financial management)

Ans：D

004. 資料超市(data mart)的設計通常包含以下哪些性質？**(複選)**

(A)包含特定主題資料

(B)常為資料倉儲的部分資料的快照

(C)常用在日常作業系統資料交換之用

(D)常存有即時交易資料

Ans：AB

005. 在網站系統開發後期為避免上線程式存在資安漏洞，常使用源碼檢測(code review)工具，來協助評估所開發之程式是否存在資安漏洞，此類工具無法偵測以下何項漏洞？

(A)資料隱碼攻擊(SQL injection)

(B)使用已知弱點元件(Using Components with Known Vulnerabilities)

(C)不安全的反序列化漏洞（Insecure Deserialization）

(D)零時差攻擊(Zero day attack)

Ans：D

006. 在一般狀況下，以下哪些是正確的開發環境安全控管？**(複選)**

(A)為使開發可以和真實環境相符，可以讓開發環境使用與真實環境相通的網段

(B)為使開發人員可以清楚理解真實的問題狀況，可將真實資料匯入開發環境，開發完畢後刪除

(C)開發環境也必須有正式權限管理

(D)開發環境所使用的資料庫必須與正式環境有區隔

Ans：CD

007. 當系統管理人員收到原廠作業系統之安全漏洞修補程式(patch)時，應該如何處理？
(A)立即更新，以避免該安全漏洞受外部駭客利用
(B)立即下載歸檔，待發生相關安全風險時可立即安裝
(C)使用弱點掃瞄軟體掃瞄，驗證系統有該風險後安裝
(D)進行測試，確認該修補不會影響應用程式正常運作後，方儘速排程更新

Ans：D

008. 容量管理(capacity management)的目標為何？
(A)將所有資源利用最大化，確保每一項資訊資源都被充份利用
(B)將資訊資源做最佳運用，並保有適當的擴充彈性
(C)盡可能爭取大量資訊資源，以確保未來擴充無虞
(D)主要為協調各權責單位衝突，合理分配資訊資源

Ans：B

009. OSI 模型各層的名稱與描述，下列何者錯誤？
(A)網路層(Network)：基本功能為提供網路連結並將封包由來源送到目的地
(B)傳輸層(Transport)：TCP 及 UDP 均屬於傳輸層的協定
(C)實體層(Physical)：描述了實際採用的網路拓樸
(D)應用層(Application)：翻譯、加密及壓縮資料

Ans：D

010. 下列哪一個網路設備最容易被攔截及監聽？
(A)集線器(hub)
(B)交換器(switch)
(C)路由器(router)
(D)防火牆(firewall)

Ans：A

011. 以下網路拓樸及其缺點的配哪些敘述正確？**(複選)**
(A)樹狀(tree)：交換器故障會影響下面所有原件
(B)環狀(ring)：任何組件故障，網路就無法運作
(C)網格狀(Mesh)：匯流排故障，整個網路無法運作
(D)輻射狀(star)：成本高且較難以管理

Ans：AB

012. 為落實資料保護保護，公司希望可以在網路層級可以對內部員工對外傳輸的資料進行掃描及過濾，下列哪一類防火牆可以符合公司的需求？
(A)封包過濾防火牆(packet filter firewalls)
(B)狀態檢查防火牆(stateful inspection firewalls)
(C)應用代理閘道防火牆(application-proxy gateway firewalls)
(D)個人防火牆(personal firewall)

Ans：C

013. 下列哪些技術主要不是用來加密傳輸資料？**(複選)**
(A)數位簽章
(B)雜湊涵數(hash function)
(C)AES
(D)SSL

Ans：AB

014. 有關實體安全的控管，以下哪些敘述是錯誤的？**(複選)**
(A)機房門禁可以使用門禁卡或密碼，就是所謂的雙重認證
(B)機房如發生火災可使用乾粉式滅火器或氣體式滅火器
(C)為避免機房遭受水災威脅，可以將機房設在頂樓
(D)除機房不建議設於地下室或低樓層外，電力供應設備及發電機也不建議設於地下室或低樓層

Ans：AC

015. 身分認證(authentication)常用 3 種認證要素與實際應用，以下哪一個選項正確？
(A)所知之事(something you know)：身分證字號
(B)所持之物(something you have)：指紋
(C)所具之形(something you are)：智慧卡
(D)所知之事(something you know)：同步電子代符(OTP)

Ans：A

016. 在組織遭遇重大災害時需依緊急應變計畫，啟動緊急應變措施，說明如何將資訊服務回復原本運作模式的作業是包含在計畫內的哪一個階段？
(A)通知與啟動階段(notification/activation phase)
(B)復原階段(recovery phase)
(C)重建階段(reconstitution phase)
(D)回朔階段(roll back phase)

Ans：C

017. 卡耐基美隆大學所提出的「能力成熟度模型整合」CMMI 各階段與其主要特定的匹配，下列何者為非？
(A)初始階段：無管理，無固定流程
(B)已管理階段：相似的專案，可以重覆使用以前的經驗
(C)已定義階段：建立了標準化的 SOP
(D)量化管理階段：經量化回饋機制，產生新的想法與新的技術，以最佳化流程

Ans：D

018. IC 設計公司如果服務多個具有競爭關係的客戶，為了避免經理人同時知道各家的機密資訊，常會採取以下哪一個安全模型？
(A)不干擾模型(noninterference model)
(B)Brewer & Nash 模型
(C)Clark-Wilson 模型
(D)Biba 模型

Ans：B

019. 以下哪一句話最清楚說明資訊安全風險管理的目的？

(A)消滅組織所有可能面臨資訊安全威脅

(B)瞭解組織所面臨的資安風險，並適當控管風險至組織的可接受風險程度內

(C)避免執行任何有資安風險的業務

(D)瞭解組織所面臨的資安風險，適當地分散至各部門，避免單一部門承載過大風險

Ans：B

020. 由公司對外部資訊廠商發動的稽核，稱為？

(A)第一者稽核

(B)第二者稽核

(C)第三者稽核

(D)內部稽核

Ans：B

021. 網路上的資訊交換與意見發表越來越頻繁，下面何者不是在網路上發表言論時需遵守的事項？

(A)不可在網路上隨意張貼別人的隱私

(B)不可在網路上隨意分享別人的創作

(C)可以在網路上隨意分享在網路上看到的內容

(D)可以在網路上隨意分享個人對於時事的心得感想

Ans：C

022. 資訊安全教育訓練重點宣導項目應包含以下哪些內容？**(複選)**

(A)公司相關的資訊安全政策及程序

(B)最近出現的資訊安全威脅

(C)最近出現資安詐騙案例

(D)最近上線系統的使用方法

Ans：ABC

023. 有助於提升人員資訊安全認知的 PDCA(Plan-Do-Check-Act)環循中，下列哪些屬於 C(Check)的措施？**(複選)**

(A)每年重新擬定資訊安全認知宣導計畫

(B)社交工程測試

(C)一般人員資訊安全規定落實狀況查核

(D)資訊安全作業實作練習

Ans：BC

024. 使用駭客手法侵入對手的網路及取得對手的研發資料是屬於那一類的電腦犯罪？

(A)商業間諜

(B)社交工程

(C)惡意程式

(D)內部犯罪

Ans：A

025. 小華在民營企業上班，有一天看到同事的密碼寫在桌上，便使用同事密碼登入同事的電腦，請問他是違反了何項法令？

(A)刑法

(B)民法

(C)個人資料保護法

(D)營業秘密法

Ans：A

026. 以下何種情形非「個人資料保護法」內針對非公務機關欲國際傳輸個人資料，中央目的主管機關得限制之？

(A)涉及國家重大利益

(B)國際條約或協定有特別規定

(C)接受國對於個人資料之保護未有完善之法規，致有損當事人權益之虞

(D)與接受國未有司法互助協議者

Ans：D

027. 雲端技術的應用越來越普遍，根據 CSA(雲端安全聯盟)提出使用雲端技術所面臨的資安威脅，以下何種選項不是使用雲端技術時會面臨的資安威脅？

(A)不安全的接口和應用程式編程接口(API)

(B)高級持續性威脅(APT)

(C)共享的技術漏洞

(D)硬體遭竊取

Ans：D

028. Deepfake 是指什麼資安威脅？

(A)利用人工智慧中的深度學習技術，變造影片中的動作與聲音，傳遞扭曲不實的內容

(B)偽造多個社群媒體帳號，與使用者分別互動，串聯場景，騙取帳號密碼

(C)模擬被害者，使用被害者帳號透過社群媒體對其朋友進行詐騙

(D)截取並模擬使用者的操作，登入系統竊取資料

Ans：A

029. 下列哪些措施是公司允許員工遠端工作時常採用的安全控管措施？**(複選)**

(A)行動裝署儲存媒體加密

(B)使用 VPN 與公司資源連線

(C)部署安全設置檔至行動裝置

(D)伺服器間存取認證

Ans：ABC

030. 物聯網技術日漸普及，下列何種選項不是其帶來的資訊安全風險變化？

(A)更多資料的蒐集，帶來更大的隱私疑慮

(B)虛擬與實體有更多的連結，也可能帶來更的傷害

(C)更多的設備有聯網的能力，也帶來更多的可攻擊點

(D)去中心化的儲存，使資料外洩的風險降低

Ans：D

031. 以下哪些方法是屬於強調快速開發的軟體開發方法？**(複選)**

(A)Agile Software Development

(B)Extreme Programming

(C)Scrum

(D)System Development Life Cycle

Ans：ABC

032. 下列有關系統管理行為的描述，哪一項是不適當的？

(A)使用者離職時，必須在規定時間內註銷使用者帳號

(B)隨時監視控制台，檢視是否有不明身分使用者企圖登入系統

(C)系統稽核檔（Log File）很多，有空再檢查是否有異常狀況即可

(D)定期備份資料，並確認備份資料是否放置於安全地方，以及是否加以管制

Ans：C

033. 當一台電腦透過瀏覽器造訪 Google (http://www.google.com/) 網站時，該電腦可能會引發哪些通訊協定？**(複選)**

(A)DNS

(B)ARP

(C)HTTP

(D)SMTP

Ans：ABC

034. Cyber security 已經是全球企業組織所面臨的三大關鍵威脅之一，建立有效的 Cyber security 事件回應流程將是一個重要議題。相關主要步驟包含：1. 準備（Preparation）、2. 經驗學習（Lesson Learned）、3. 復原（Restore）、4. 識別（Identification）、5. 控制（Contain）、6. 根除（Eradicate），請依事件回應流程的執行順序進行排序為何？

(A)1-2-3-4-5-6

(B)1-4-5-6-3-2

(C)1-6-4-3-2-5

(D)1-4-3-2-5-6

Ans：B

035. 請問下列哪一項不是企業組織目前面臨到的網路安全風險？

(A)勒索軟體（Ransomware）

(B)Bot 傀儡程式

(C)進階持續性滲透攻擊（Advanced Persistent Threat, APT）

(D)關鍵資料未妥善進行備份

Ans：D

036. 制訂適切的最高存取政策（Access Control Policy）可降低企業組織因內外部使用者未經授權的存取，而造成資安事件的發生，請問下列哪一種存取控制的原則是不好的？

(A)僅知原則（need-to-know）

(B)除非許可，否則一律禁止之原則

(C)除非禁止，否則一律許可之原則

(D)僅用原則（need-to-use）

Ans：C

037. Fintech 金融科技已經是全球金融產業所面臨到的趨勢及挑戰，當非金融產業開始涉及金融相關業務的提供（如: 悠遊卡、一卡通、第三方支付等），金流交易的安全將是一個關鍵議題。在企業開始提供信用卡的交易服務時，請問下列哪一個標準或要求是須要特別關注及遵循的？

(A)GDPR（歐洲隱私權法律 - 一般資料保護規定）

(B)Data Governance 資料治理

(C)Agile 敏捷式專案管理

(D)PCI DSS 支付卡產業資料安全標準

Ans：D

038. 執行資訊安全的稽核時，稽核員能否與受稽的人員進行有效的溝通及互動將會影響到該稽核能否順利圓滿及有效地完成，所以企業組織一般都會針對稽核人員的個人特質進行評估，請問下列哪一項非一個好的稽核員應具備的個人特質？

(A)心胸開闊

(B)不善於社交

(C)善於觀察

(D)果斷

Ans：B

039. 資訊倫理是在討論人們對資訊的態度以及行為，應用於電腦的使用、資訊科技、資訊系統、資訊網路的倫理規範。下列哪一項不包含在資訊倫理的四大議題（PAPA）之中？

(A)隱私權(Privacy)

(B)可用性(Availability)

(C)財產權(Property)

(D)使用權(Accessibility)

Ans：B

040. 在網路新聞或消息未有完整說明前，任意和他人一起在網路上出言不遜謾罵當事人，此舉可能構成何項網路犯罪行為？

(A)網路誹謗與公然侮辱

(B)網路煽惑他人犯罪

(C)網路詐欺

(D)網路恐嚇

Ans：A