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：ISN108

學科 **100%** （為單複選題，每題 **2.5** 分，共 **100** 分）

1. 某公司之異地備援方案為當發生重大災害時可在 3~6 小時內回復系統服務，其採用之異地備援方案應為以下何種？
   （A）全備援（mirrored sites）
   （B）熱備援（hot sites）
   （C）暖備援（warm sites）
   （D）冷備援（cold sites）

Ans：B

2. 十進位與十六進位的轉換，是計算機概論的基礎，更是駭客攻防不可或缺的能力。某生在進行程式存檔的修改，發現底下紅框的數字（十六進位）與該程式的某個設定值（十進位）有關，如附圖說明，請問該生要如何修改紅框的內容才能得到最大的設定值？（請參閱附圖作答）

   （A）7F FF
   （B）FF 7F
   （C）80 00
   （D）00 80

   1. 如果將紅框內的數值改為「00 10」，該設定值會變成 4096
   2. 如果將紅框內的數值改為「10 00」，該設定值會變成 16，
   3. 如果將紅框內的數值改為「FF FF」，該設定值會變成 -1。

```
000002e0h: 09 00 00 00 00 C0 3E 01 00 02 00 00 00 CE 31 01 ; .....?......?.
000002f0h: 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 C0 ; ............@..?
00000300h: 2E 72 73 72 63 00 00 00 58 27 01 00 00 D0 3E 01 ; .rsrc...X'...?.
00000310h: 00 28 01 00 00 D0 31 01 00 00 00 00 00 00 00 00 ; .(...?.........
00000320h: 00 00 00 00 40 00 00 40 00 00 00 00 00 00 00 00 ; ....@..@........
00000330h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ; ................
00000340h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ; ................
```

Ans：B

3.	關於資料倉儲（data warehouse）的敘述，下列哪些正確？**【複選】** （A）支援資料探勘（data mining）的應用 （B）包含特定主題的資料市集（data mart） （C）作為即時線上交易處理（on-line transaction processing）的資料庫 （D）可支援線上分析處理（on-line analytical processing）
Ans：ABD	
4.	作業系統常使用硬碟做為主記憶體的延伸，稱為虛擬記憶體（virtual memory），這種方式會造成以下哪種風險？ （A）非正常中斷時會導致資料存於硬碟之上，易遭有心人士竊取 （B）多人共用時易發生資料衝突的狀況 （C）無法加密 （D）無法掃毒
Ans：A	
5.	強化資訊部門軟體開發的安全流程（Secure SDLC）已是一個趨勢，許多企業組織目前正在加強相關的流程優化。請問針對資訊系統可能面臨的安全及隱私風險，應在下列哪一個階段鑑別？ （A）安全軟體實作（Implementation） （B）安全軟體需求（Requirement） （C）安全軟體測試（Testing） （D）安全軟體設計（Design）
Ans：B	
6.	基於目前全球諸多資安事件的發生多與系統被未經授權存取有關，強化使用者身分認證已是一個關鍵議題，請問下列哪些為強化使用者身分認證常採用的控制措施？**【複選】** （A）帳戶鎖定機制的啟用（Account lockout） （B）密碼政策的啟用（密碼大小寫、長度、更換頻率等） （C）圖形驗證碼（Captcha） （D）密碼暴力破解法
Ans：ABC	

7.	由於企業組織所使用的資訊服務愈趨複雜及多樣化，資訊服務或是系統開發的委外已經是不可避免之趨勢。如果系統或服務上線後發現系統欠缺所須的安全控管機制，請問從委外開發或維運管理的生命周期中，下列哪一個階段可能是最大的問題？ （A）委外專案的合約簽署流程 （B）委外專案的日常監督管理流程 （C）委外專案的合約中止或異動流程 （D）委外專案於規畫階段應執行的功能及安全評估流程
Ans：D	
8.	基於企業組織對外提供的資訊服務（尤其是 customer facing 的服務）可能須具有高可用性的特性（high availability）。當資訊服務發生非預期中斷時，營運持續計畫或是服務持續計畫的制定及演練將會是能否及時恢復運作的關鍵成功要素，因此，請問下列哪一種演練的頻繁度應該會較高？ （A）相關復原流程的書面審查演練 （B）系統或服務元件的復原演練 （C）單一資訊系統或服務的復原演練 （D）異動備援中心啟動的演練
Ans：A	
9.	下列哪個不是 TCP/IP 連線劫持（session hijacking）攻擊成功的必要前提？ （A）與受害主機位於同一網段 （B）取得要劫持連線的 TCP 序號（sequence number） （C）偽裝成受害主機，發送特定 TCP 序號的封包 （D）入侵受害主機並奪取執行權限
Ans：D	

10.	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。 （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	
11.	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	
12.	為有效因應網路安全，企業組織多會採取多層次防禦縱深以提高攻擊難度，請問企業組織可以導入下列哪些技術以強化控管的強度？**【複選】** （A）入侵偵測或防禦系統（IPS） （B）防火牆和閘道防毒 （C）高可用性（HA - High Availability） 技術 （D）網頁安全閘道
Ans：ABD	
13.	雲端及虛擬化服務的安全一直是企業組織在使用時所關注的議題，尤其是雲端服務提供者（CSP）提供的服務涉及到個人資料及隱私時（如 SaaS 相關服務），CSP 如果要展現其服務在資安及隱私的保護是與國際接軌，可考慮遵循下列哪一個標準的要求？ （A）ISO/IEC 27032: Guidelines for cybersecurity （B）ISO/IEC 27034: Application security （C）ISO/IEC 27018: Protection of personally identifiable information（PII） in public clouds （D）ISO/IEC 27036: Information security for supplier relationships
Ans：C	

14.	勒索軟體為近年來全球常見的網路攻擊手法，請問下列哪一項不是勒索軟體的主要傳播途徑？ （A）網路釣魚郵件 （B）使用者擁有本機管理者帳號 （C）網路惡意廣告 （D）網頁掛馬
Ans：B	
15.	BYOD（Bring Your Own Device）已是企業組織必須面對的風險及挑戰，在安全性及便利性間取得一個平衡點並不容易達成，請問下列哪一項不是企業組織必須要考量的控管？ （A）BYOD 及行動設備管理政策的訂定 （B）BYOD 裝置在私用及營運使用的區隔控管 （C）BYOD 的設備保固及維修管理 （D）BYOD 裝置遭竊或遺失時的處理
Ans：C	
16.	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	
17.	啟動系統的稽核日誌並進行必要監控及審查，可有效的協助企業組織發現潛在的議題或風險，請問下列哪個項目不是「啟動系統稽核日誌」議題須最優先考慮的？ （A）導入 NOC（網路維運監控中心）機制 （B）時鐘同步以確保稽核日誌時間的正確性 （C）稽核日誌的完整性保護（證據效力的考量） （D）定義需啟動及審查的稽核日誌類型
Ans：A	

18. 某資訊部門最近針對關鍵系統進行了功能變更，但是該程式變更上線之後卻發生多項 bug 並導致業務部門無法處理作業。資訊部門立即啟動了應變計畫將相關的服務復原（程式退版），數小時後也再次修改程式並再次進行程式上線且順利完成變更。資訊部門主管認為這僅是偶發事件，不須要再浪費資源進行後續調查，未來僅須相關同仁注意事項即可。請問實際上資訊部門應針對此事件於後續進行哪一項活動，以避免未來再次發生雷同的事件？

（A）系統及服務相關的容量管理規劃

（B）變更管理流程的再檢討

（C）進行事件的調查及根因分析

（D）Outage 的應變處理流程

Ans：C

19. 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

20. 關於 SYN 洪水攻擊（flood attack），下列描述何者正確？

（A）此攻擊針對 UDP 協定

（B）直接損害是導致被攻擊主機的檔案外洩

（C）屬於服務阻斷 （denial of service） 攻擊的一種

（D）攻擊者必須持續發出 SYN/ACK 封包

Ans：C

21.	物聯網（Internet of Things, IoT）的發展將會對我們的日常生活及工作造成關鍵性的改變(包含智慧家庭、工業 4.0、智慧交通、智慧金融…等），您認為下列與 IoT 服務有關的元件有那些可能須要強化安全控管以降低 cyber attack 成功的機會？ 1. the device、 2. the cloud infrastructure、3. the network。 （A）1-2 （B）1-3 （C）1-2-3 （D）2-3
Ans：C	
22.	下列關於跨站腳本攻擊（Cross-site Scripting）的描述，哪些正確？**【複選】** （A）惡意腳本可能來自於使用者端的網址列 URL （B）惡意腳本可能來自於伺服器端的資料庫 （C）惡意腳本可能來自於使用者端瀏覽器的 DOM（Document Object Model） （D）惡意腳本可能來自於檔案輸入，即使是純文字檔（.txt）
Ans：ABCD	
23.	以下哪些功能可以利用數位簽章憑證達到？**【複選】** （A）加密資料 （B）確保資料完整性 （C）不可否認 （D）確認對方身份
Ans：ABCD	
24.	關於 VPN 虛擬私有網路（Virtual Private Network），下列哪些是客戶端設備 VPN 常見的協定之一？**【複選】** （A）L2TP 協定 （B）PPTP 協定 （C）IPSec 協定 （D）MPLS 技術
Ans：ABC	
25.	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	
26.	ISO/IEC 27001（資訊安全管理系統）、BS 10012（個人資訊管理系統）等風險類的國際管理系統標準都要求企業組織必須執行風險評鑑，以鑑別企業組織所面臨的風險並投入適當資源進行處理。請問下列哪一個標準針對風險評鑑及風險處理有明確的指引及介紹？ （A）ISO/IEC 27021: Competence requirements for ISMS professionals （B）ISO/IEC 21878: Design & implement of virtualized servers （C）ISO/IEC 29134: Guidelines for privacy impact assessment （D）ISO 31000: Risk management - Guidelines
Ans：D	
27.	有效的實施風險評鑑並進行必要的風險處理，將可協助企業組織有效的因應所面臨的風險。企業組織常因資源、技術或是其他考量將內部某些資訊業務委外給廠商，請問這種做法是風險處理中的哪一種選項？ （A）避免風險（Avoid Risk） （B）轉移風險（Transfer Risk） （C）接受或增加風險以追求機會 （Taking or increasing the risk in order to pursue an opportunity） （D）降低風險（Reduce Risk）
Ans：B	
28.	策略面、管理面、技術面及認知面的強化將可協助企業組織有效的強化資安的推動及提升成效。行政院國家資通安全會報也陸續訂定相關的管理規範，以協助政府機關提升資訊安全能量及成熟度。請問在防護縱深、監控管理、安全性檢測進行強化是屬於哪一個面向？ （A）政策面 （B）技術面 （C）認知面 （D）管理面
Ans：B	

29. ISO/IEC 27001 附錄 A 中有定義 14 個安全控制章節讓企業組織遵循及導入，請問下列哪些選項與實體與環境安全章節的要求有關？**【複選】**

（A）設備維護（Equipment maintenance）

（B）存取權限之移除或調整（Removal or adjustment of access rights）

（C）網路之區隔（Segregation in networks）

（D）設備汰除或再使用之保全（Secure disposal or reuse of equipment）

Ans：AD

30. 行動支付已經是未來的趨勢，請問企業如何果要提供行動支付的服務，那些議題是必須被考慮及進行控管？ 1. 行動支付平台開發的安全、2. 交易資料的保護、3. 交易平台的維運安全、4. 服務的可用性、5. 法規的遵循

（A）1-2-3-4

（B）2-3-4-5

（C）1-3-4-5

（D）1-2-3-4-5

Ans：D

31. 某個企業的 RD 部門發現目前針對客戶提供的研發資料未有充足的安全防護措施，並可能違反客戶合約要求甚至造成訂單被取消，因此將此列為高風險並優先進行風險處理。目前因為資源限制，所以 RD 部門決定先行採取幾項措施；包含重新跟 RD 同仁簽屬保密協議、強化 RD 部門的門禁控管及加強 RD 人員的教育訓練及宣導。請問上述控制措施，從風險處理的精神是可降低客戶研發資料外洩風險的可能性（likelihood）或是外洩後的衝擊（impact）？

（A）可同時降低可能性及衝擊值

（B）僅能降低衝擊值

（C）僅能降低可能性值

（D）無法降低可能性及衝擊值

Ans：C

32.	資訊安全的核心精神是保護企業組織中重要“資訊”的 CIA（機密性、完整性及可用性）。請問一個企業組織如要有效推動資訊安全，其導入範圍應該以下列哪一種為佳？ （A）導入範圍僅為企業組織的核心資訊系統 （B）導入範圍僅為企業組織資訊部門 （C）導入範圍僅為企業組織的關鍵業務部門 （D）導入範圍為全企業組織（但可分階段導入）
Ans：D	
33.	在所有的國際管理系統標準中都會要求導入的企業組織必須實施內部稽核，以確認相關管理制度的遵循性及有效性。請問內部稽核的頻率何者有誤？ （A）可考慮每季執行一次 （B）可考慮每半年執行一次 （C）可考慮每年執行一次 （D）可依實際須要再執行 （可超過一年再執行）
Ans：D	
34.	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，請問下列哪一項不是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	
35.	您現在正在準備稽核系統發開部門，但是因為時間的限制，只能進行重點活動的確認。請問下列哪些安控章節可能是您確認的重點(請挑選 3 個最重要的安控章節）？1. 資訊安全政策、2. 人力資源安全、3. 密碼學、4. 系統獲取、開發維護、5. 作業安全、6. 供應者管理。 （A）1-2-3 （B）2-3-4 （C）4-5-6 （D）3-4-6
Ans：C	

36. 有效的提升企業組織人員的認知將可有效的降低資安事件的發生，因此許多企業及政府機關均會於每年定時不定時進行資安宣導，並透過必要的社交工程演練或其他方式來測試人員的認知程度。請問下列哪些可能是常見的社交工程攻擊方式？**【複選】**

（A）利用電話佯裝 IT 人員，騙取使用者帳號及密碼

（B）利用電子郵件誘騙使用者登入偽裝之網站以騙取帳號及密碼

（C）利用電子郵件誘騙使用者開啟附件檔案或圖片，並植入惡意程式、暗中收集敏感資料

（D）利用即時通訊軟體如 Line，假冒親友來訊，誘騙點選來訊中之連結後中毒

Ans：ABCD

37. 您最近閱讀報章發現某個金融單位在運送客戶紙本申請資料到倉庫存放的過程中，物流業者不小心將運送的紙本資料散落在快速道路上。您發現您的公司可能也會有雷同的問題發生，也擔心違反個人資料保護相關要求，請問這個議題是屬於個人資料保護生命周期的哪一個環節？

（A）蒐集

（B）處理

（C）利用

（D）蒐集、處理及利用都有涵蓋

Ans：B

38. 關鍵基礎設施保護（Critical Infrastructure Protection, CIP）及關鍵資訊基礎設施保護（Critical Information Infrastructure Protection, CIIP）是全球各國關注的議題，我國的關鍵基礎設施保護有八大領域，請問下列哪一個領域不是八大領域之一？

（A）電商產業

（B）銀行與金融

（C）通訊傳播

（D）能源

Ans：A

39.	保護隱私已經是全球各國關注議題，如果企業組織所提供的業務或是資訊服務涉及到客戶的個人或隱私資料，如何有效的保護將是一個挑戰。從設計著手保護隱私（Privacy by design）已是一個關鍵課題，請問下列哪些活動應該被考慮？**【複選】** （A）預設最小化（minimized by default） （B）盡可能地使用“已去識別化”的資訊（de-identified information） （C）相關功能及處理的透明化考量 （D）確保鑑別出的隱私控制措施已被適當實施
Ans：ABCD	
40.	基於全球數位化及全球化的趨勢，許多企業皆已面臨到異業的高度競爭，time to market 或是 first to market 已經企業不可避免的挑戰。對企業來說，能否有效地推動資安治理將是影響到是企業能否永續的關鍵之一。請問下列哪些標準是全球資安治理的主要依循參考？ 1. 資訊安全管理系統（ISMS）、2. 個人資料管理系統(PIMS)、3. 資訊服務管理系統(SMS)、4. 營運持續管理系統（BCMS）。 （A）1-2 （B）1-2-3-4 （C）2-3 （D）1-2-4
Ans：B	