ITE 資訊專業人員鑑定

資訊安全類-資訊與網路安全概論試題

試卷編號：ISN-110

【注意事項】

一、本測驗為單面印刷試題，共計 14 頁。第 2 至 14 頁為四十道學科試題，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 2.5 分，共 100 分）

001. 現今大多數網站採用 HTTPS 服務，請問 HTTPS 的預設連接埠口是下列哪一個？

(A)80

(B)443

(C)1433

(D)445

Ans：B

002. 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

003. IT 與 OT 網路逐步在融合中，OT 的資安威脅隨之上升，企業面臨更多的挑戰，也急需更合適的切入點與因應方案，下列哪些是可考量的議題？1.建立資產清單以提高資產掌握程度。2.建置完善的隔離與權限分級機制。3.識別系統重要性與脆弱性以進行風險評估。4.管控或規範供應鏈人員，提高人員資安意識。5.建立 OT-SOC 機制。

(A)1-2-5

(B)1-3-4

(C)1-2-4-5

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

Ans：D

004. 電腦犯罪事件層出不窮，當企業不幸遭受駭客入侵事件時，ISO/IEC 27001 條文中的哪項可協助企業追蹤外洩的資料、範圍、駭客的位置及保存證據？

(A)A.12.2.1 防範惡意軟體之控制措施

(B)A.12.4.1 事件存錄

(C)A.12.6.1 技術脆弱性管理

(D)A.12.7.1 資訊系統稽核控制措施

Ans：B

005. ISO 標準的優點之一為採用 ISO/IEC Directives、Part 1, Consolidated ISO Supplement 之附錄 SL 所定義之高階結構，擁有相同的結構、相同的節次標題、相同的內容，共通的用語及核心定義，因此可與其他已採用該附錄之標準維持相容性，請問下列哪些標準採用了此架構？**(複選)**

(A)GDPR: General Data Protection Regulation（歐洲隱私權法律 - 一般資料保護規定）

(B)ISO/IEC 27003: Information security management system implementation guidance

(C)ISO/IEC 27004: Information security management – Measurement

(D)ISO/IEC 27005: Information security risk management

Ans：BCD

006. 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

007. 基於資安需求，對資訊系統建立權限配置與存取控管機制，以防止未經授權的存取，下列何者非登入作業系統所採用的網路身分驗證服務？

(A)IMAP（Internet Message Access Protocol）

(B)Windows AD（Active Directory）

(C)LDAP（Lightweight Directory Access Protocol）

(D)NIS（Network Information Service）

Ans：A

008. 下列哪些是屬於國內危機處理暨協調中心（Computer Emergency Response Team）組織？**(複選)**

(A)TWNCERT

(B)EC-CERT

(C)NCC-CERT

(D)TWCSIRT

Ans：ABCD

009. PING 指令常被用於檢測網路狀態，下列有關 PING 指令的敘述，何者有誤？

(A)PING 是向目標主機傳出一個 UDP 的請求封包

(B)有些網路設備機於資安考量，會設定為不理會 PING 指令

(C)PING 指令常用於檢查網路連線狀態

(D)PING 指令可以於一般 Windows 電腦上使用

Ans：A

010. 以下哪些是安全電子郵件系統？**(複選)**

(A)Pretty Good Privacy

(B)Privacy Enhanced E-Mail

(C)Secure Multipurpose Internet Mail Extensions

(D)Secure Socket Layer

Ans：ABC

011. 為確保資料於網路傳輸時具有安全性，有關網路傳輸層通訊加密協定，宜採用哪些加密協定？**(複選)**

(A)SSL V2.0

(B)SSL V3.0

(C)TSL V1.1

(D)TSL V1.2

Ans：CD

012. 系統的嚴重漏洞要及時修補，若在網路上閱讀到新發現的系統嚴重漏洞文章，主管要求立即更新所有的系統，廠商也因應釋出漏洞的修正檔，請問應採取下列何項做法較適當？

(A)立即將所有系統套用修正檔

(B)更新防毒軟體即可，不用另行套用修正檔

(C)先測試修正檔於系統上是否有相容性等問題，無誤後再進行修正

(D)先執行系統弱點掃描後套用修正檔

Ans：C

013. 近年因應物聯網技術應用的興起，世界各國紛紛針對物聯網（IoT）應用制定並公布相關法規，下列何者非屬 IoT 設備？

(A)補摺機

(B)乾洗手機

(C)印表機

(D)Wi-Fi AP

Ans：B

014. 為確保資訊安全管理系統有效性，企業應定期執行內部稽核自我檢視，但每次執行內部稽核前都須事前擬定相關稽核計畫，請問哪些是企業進行稽核前，稽核計畫應考量到的項目？**(複選)**

(A)之前稽核的結果

(B)稽核的範圍

(C)合適的稽核人員

(D)稽核結果後續該如何追蹤

Ans：ABC

015. 當發生資安事件時，有完整資料備份能幫助企業組織降低回復時間與成本，是營運持續不可或缺的重要環節，為達到有效的備份，可遵照備份「三二一原則」執行，下列關於備份「三二一原則」之敘述何者有誤？

(A)建立三份副本

(B)使用兩種不同存放媒體

(C)至少一份副本且由不同人員執行備份

(D)一份副本異地存放

Ans：C

016. 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

017. 下列何者網路設備主要功能在於負責不同網路間封包的傳遞？

(A)IP 分享器

(B)路由器

(C)防火牆

(D)交換器

Ans：B

018. OWASP（Open Web Application Security Project）蒐集各種網頁安全漏洞，並彙整出十大資安問題項目（OWASP Top Ten），其中注入攻擊（Injection）為第一名，常見的為 SQL Injection，主要是在輸入字串中夾帶 SQL 指令，若系統未設計有妥善的檢查機制，進而造成系統被攻擊。請問以下何者為防禦方式？

(A)加入圖形驗證碼

(B)建立黑名單過濾

(C)使用 Prepare Statement 建立參數化查詢

(D)使用 Https

Ans：C

019. 藍牙裝置使用者可以透過哪些措施來保護自己的隱私？**(複選)**

(A)將裝置設為隱藏模式

(B)不要和不認得的裝置配對，但是可以接收其傳送的內容

(C)使用八個字元以上且字母和數字混合的 PIN 碼

(D)利用軟體修補程式來防止安全問題

Ans：ACD

020. 下列對 Single Sign-on 的解釋，何者正確？

(A)使用者在所有系統都設定同樣的一組帳號密碼以方便登入

(B)只需要單一的登入動作，就可以取得對於多個系統的存取權限

(C)使用者只需要在一台系統中設定帳號密碼，其他台系統都不需要設定帳號密碼

(D)使用者對任一個系統只需要成功登入一次，以後就不需要再登入即可使用此系統

Ans：B

021. 檢視多數資訊安全事件，可以發現大多數事件的發現並非缺乏設備、技術，而是人員認知不足所導致，因此企業會定期或不定期舉辦企業內部認知教育訓練藉此提升員工的資訊安全認知，請問下列哪些人員不在組織應規劃須參加認知教育訓練的範圍？

(A)基層員工

(B)主管

(C)委外廠商

(D)主管機關

Ans：D

022. 近期新型冠狀病毒肺炎肆虐，導致部份企業營運中斷帶來極大損失，為避免天災、人禍對企業造成損失，企業平時就應該考量如何做到營運持續管理，下列哪些為企業應做到的內容？**(複選)**

(A)訂定營運持續運作相關程序

(B)統一由主管指示後才進行動作

(C)定期執行營運持續演練確認員工

(D)針對重要設備建立備援機制

Ans：ACD

023. 通訊網路安全管理目的是在確保對網路及其支援之資訊處理設施中資訊之保護。下列何者不利於通訊網路安全？

(A)定期檢視網路設備之帳號權限

(B)切勿刪除原有的防火牆政策

(C)定期備份網路設備之重要設定檔

(D)架構異動或設備增減時應即時更新網路架構圖

Ans：B

024. Deepfake 是以 AI 技術合成影像與模擬聲音來偽冒身分，例如同事或主管，取得信任後進而取得授權或進行詐騙以達成其攻擊目的，這是屬於何種駭客攻擊手法？

(A)中間人攻擊

(B)阻斷服務攻擊

(C)社交工程

(D)連線劫持

Ans：C

025. 安裝並使用正版軟體可避免惡意軟體帶來的安全威脅，盜版軟體除了會導致侵權問題外，也會提高資安風險，下列何者非使用盜版軟體可能帶來的資安風險？

(A)電腦病毒

(B)孤兒軟體

(C)社交工程攻擊

(D)無法獲得原版軟體所能獲得的軟體升級資格

Ans：C

026. 目前您正在製作資訊安全認知教育訓練的簡報，請問下列哪項不需放入此份簡報中？

(A)資訊安全政策

(B)各部門執掌

(C)員工對於資訊安全管理系統有效性之貢獻，包括改善之資訊安全績效的益處

(D)未遵循資訊安全管理系統要求事項之可能後果

Ans：B

027. 下列何者為常見的網路服務安全管理機制？**(複選)**

(A)管控登入管理介面之帳號

(B)使用具複雜度（如:八個字元以上且字母、數字、特殊符號混合）密碼

(C)套用原廠提供的修補程式來防止安全問題

(D)將網路設備放置於設置門禁之管制室

Ans：ABCD

028. 面對複雜多變的商務需求與 IT 架構，為有效控制、維護與改善所提供之服務的可靠性，各企業組織逐漸著手導入組態管理資料庫（Configuration Management Database；簡稱 CMDB），下列何者非組態管理資料庫能帶來的好處？

(A)提供組態的正確資訊及其文件說明以支援所有其它的「服務管理」程序

(B)為「事件管理」、「問題管理」、「變更管理」與「版本發佈管理」提供紮實基礎

(C)將組態記錄與基礎架構相比較並修正例外

(D)確保組態設定檔不被非法入侵或竄改

Ans：D

029. 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

030. 以下針對零時差攻擊（Zero Day Attack）的描述何者正確？

(A)當系統被發現具有風險性弱點後，立即進行的惡意攻擊行為

(B)當系統被惡意攻擊後，系統立即失效無法使用

(C)惡意攻擊系統的時間不超過 1 天

(D)當系統被發現具有風險性弱點後，在修正程式發佈之前或是使用者更新前，所進行的惡意攻擊行為

Ans：D

031. 下列電腦中的儲存單元何者存取速度最快？

(A)記憶體

(B)快取

(C)硬碟

(D)快閃記憶體

Ans：B

032. 為避免因系統容量不足，導致系統服務中斷，需監看系統運作情形，以預先掌握系統情況，並能預先評估是否需擴充資源，以規劃系統的配置，以下哪些為容量監控標的？**(複選)**

(A)CPU

(B)記憶體

(C)硬碟空間

(D)Patch

Ans：ABC

033. 有關管理資訊系統時應注意之資訊安全控管點，下列何項措施較為適當？

(A)安裝的軟體應以安裝最新版本為原則，以避免安全性漏洞

(B)應盡量避免任意升級作業系統更新，以免造成系統不穩

(C)給予所有使用者帳號最高權限，避免執行作業時權限不足之問題

(D)應允許安裝 2P（Peer-to-peer）軟體，以避免需連外網下載檔案

Ans：A

034. 依據 BSI 統計，目前全球有 132 個國家有隱私保護法案，企業若希望和資安流程做整合，在既有的 ISO 27001 標準下，參考 ISO 27701 是一個可行的方案，請問 ISO 27701 特色為何？**(複選)**

(A)定義了隱私管理流程，並提供在持續發展的基礎上保護個人識別資訊的實務指南

(B)同時整合 ISO27701、ISO27702、ISO29110 之實務作法

(C)著重在資訊安全的控制措施

(D)於 2019 年公布，為目前相關標準中最新的版本

Ans：ABD

035. 安全性測試用以驗證應用程式並識別潛在的安全性缺陷，一般會採用哪些檢測技術？**(複選)**

(A)滲透測試

(B)弱點掃描

(C)源碼檢測

(D)單元測試

Ans：AC

036. 於民國 107 年公布之資通安全管理法與其施行細則說明公務機關與非公務機關應每年向上級或監督機關提出資通安全維護計畫，其內容不包括下列哪項？

(A)企業財務報告

(B)專責人力及經費之配置

(C)資通訊系統之盤點，並標示核心資訊系統及相關資產

(D)資通安全事件通報、應變及演練相關機制

Ans：A

037. 近年來供應鏈攻擊事件趨於多元，供應鏈攻擊所牽涉的層面，以上游來看，駭客能針對 DNS、PKI、雲端服務供應商、VPN 服務供應商、網路服務供應商，以及合作夥伴。下列何者非供應鏈攻擊的類型？

(A)遭竊的程式碼簽署憑證

(B)已遭破解的特定程式碼安裝到硬體或韌體的元件

(C)預先安裝的惡意程式碼上的裝置

(D)更新受認可的 SSL 和憑證

Ans：D

038. 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

039. 您是一位企業系統委外開發商，目前正在協助某企業建置新系統，請問在開發過程中您應做到何種行為才符合資訊倫理？

(A)為方便後續維護作業需要，偷偷在系統裡留下後門

(B)為避免忘記密碼影響開發進度，開發團隊共用帳號密碼

(C)遵守保密切結，不將客戶提供之資料洩漏

(D)發現客戶的資料庫保護不夠，偷偷抓取資料在外面販售

Ans：C

040. 2019 年 11 月 5 日，趨勢科技於部落格坦承發現有員工竊取客服資料庫的內容，販賣給不知名的犯罪組織牟利，影響近 12 萬名用戶。之後趨勢科技也採取了因應措施，包含立即中止未經許可的帳號存取行為，並解雇該員工，同時配合執法單位持續調查。請問下列的處理方法哪一項可提升員工的資訊倫理認知？

(A)進行帳號盤查，清除不須使用的帳號

(B)監控重要的系統、資料庫，如有異常立即中止異常連線

(C)舉辦教育訓練，內容可包含業界的類似事件及處置、員工應做或不應做之行為，以及犯罪後之刑責，並於訓練進行測驗

(D)針對機敏資料設定不同帳號權限可查閱全部或部分內容

Ans：C