111 年度中級資訊安全工程師能力鑑定試題

科目 1：資訊安全規劃實務
考試日期：111 年 8 月 13 日

單選題 15 題，複選題 5 題，題組題 5 題（佔 100%）

C	1. 在 ISO27000 系列標準中，下列何者為建置資訊安全管理系統的實作指引(Information security management systems — Guidance)？ (A) ISO/IEC 27001 (B) ISO/IEC 27002 (C) ISO/IEC 27003 (D) ISO/IEC 27004
A	2.「M 公司的資訊系統，每週均有進行系統與資料備份，且有異地備份，而近期公司增加了新多重加密機制，讓資料安全可以進一步確保。然近期進行系統之復原測試時，發現復原作業時間共需要 6 小時，與公司的規定 4 小時，明顯不符。」關於上述案例中，「不」符合下列何者要求？ (A) 復原時間目標（Recovery Time Objective, RTO） (B) 復原點目標（Recovery Point Objective, RPO） (C) 平均復原時間（Mean Time to Recovery, MTTR） (D) 平均失效時間（Mean Time to Failure, MTTF）
D	3. 下列選項何者作為金鑰分配（Key Distribution）的安全性較佳？ (A) 3DES (B) MD5 (C) Blowfish (D) ECC
C	4. 下列何者「不」屬於主動式攻擊（Active Attack）？ (A) DDoS Attack（分散式阻斷服務攻擊） (B) Buffer Overflow（緩衝區溢位） (C) Typosquatting Attack（誤植域名攻擊） (D) Brute Force（暴力破解）
D	5. 下列何項安全實作原則是為了預防僅因個人行為而造成可能的舞弊情形發生？ (A) 強制休假（Mandatory vacation） (B) 僅知原則（Need to know basis） (C) 最小權限（Least privilege） (D) 職責分離（Separation of duties）
C	6. 機房區域屬於防範基本設備操作直接存取的重要防護區域，下列敘述何者「不」正確？ (A) 限制具拍照或錄影功能之裝置攜帶進入機房 (B) 外包商只能在工作檯使用電腦遠距操作主機，相關隨身碟（USB Disk）資料匯入，需要經過掃毒後由機房管理人員協助使用

	(C) 只有資訊人員可以自由進出機房，不用填寫出入登記表 (D) 機房 Level 5 硬體安全模組（Hardware Security Module, HSM）設備需要另外實體隔離保護
C	7.「商業公司使用防毒和反垃圾郵件機制，以保護公司的電子郵件系統。」請問上述屬於下列何種風險處理對策？ (A) 風險避免（Risk avoidance） (B) 風險保留（Risk retention） (C) 風險修改（Risk modification） (D) 風險分擔（Risk sharing）
A	8. 下列何者為使用自動化風險分析工具主要的原因？ (A) 可將大量資訊收容於工具中 (B) 在審查期間收集的大部分數據不能重新用於後續分析 (C) 自動化方法對於風險分析訓練和知識的需要最少 (D) 大多數軟體工具有易於使用且不需要任何訓練的使用者操作界面
A	9. 某中小企業資訊部門之業務執掌包含程式開發、程式上線、應用程式管理以及資料庫管理等，該公司因故必須縮減資訊部門人力，若您是該企業之資訊部門主管，下列何種處理較無法降低資安風險的發生？ (A) 將部分資安工作移轉至其他業務單位 (B) 增加業務活動之監視紀錄 (C) 增加資安稽核頻率 (D) 導入自動化資料庫稽核管理工具
B	10. 下列何者「不」是提升服務可用性（Availability）的有效策略？ (A) 導入內容遞送網路（Content Delivery Network, CDN）服務 (B) 建置應用程式防火牆 (C) 設計自動擴展機制 (D) 規劃伺服器負載平衡架構
B	11. 依據我國《資通安全管理法施行細則》條文中規定，下列何者「不」是資通安全維護計畫應（或強制要求）包括的事項？ (A) 核心業務及其重要性 (B) 資通安全稽核組織 (C) 資通安全政策及目標 (D) 專責人力及經費之配置
B	12. 資訊單位導入新企業資源規劃系統（ERP System）進行系統安全評估時，應評估下列哪些項目？1.系統安全性評估、2.容量管制評估、3.實體環境安全、4.使用者功能性需求評估 (A) 13

	(B) 123 (C) 134 (D) 1234
B	13. AAA 公司網站常受駭客入侵，網站風險問題一直居高不下，關於降低網站風險問題處理實務，下列做法何者較為正確？ (A) 連線至後台管理系統的帳號密碼不需要區隔讀取與寫入刪除資料庫權限區隔 (B) 公司網站應定期進行網站黑箱檢測以及系統弱點掃描，對程式碼應進行 Code Review (C) 工程師在系統上直接更新新版程式，可先將舊版程式改名成 bak 作為歷史留存在官網系統中，以便日後改錯後有原始程式碼做修正使用 (D) 網站已經建立網站應用程式防火牆（Web Application Firewall, WAF）系統，其主機作業系統則不需要再升級更新
B	14. 關於風險管理步驟由先至後，下列排序何者正確？（1）全景建立、（2）風險處理、（3）風險識別、（4）監控風險處理、（5）風險評估 (A)（1）（2）（3）（4）（5） (B)（1）（3）（5）（2）（4） (C)（1）（5）（3）（2）（4） (D)（3）（5）（2）（1）（4）
D	15.「某網站伺服器經常有大量的使用者來進行異動，且常會定義不同的使用者身份，例如會員、非會員或系統管理者。」關於網站存取控制模型之選擇，下列何者管理效率較高？ (A) 存取控制清單（Access Control List） (B) 強制存取控制（Mandatory Access Control） (C) 自主性存取控制（Discretionary Access Control） (D) 以角色為基礎的存取控制（Role Based Access Control）
A B D	16. ISO/IEC 27001 中所採用的風險評鑑（Risk Assessment）主要包含下列哪些步驟？（複選） (A) 風險評估（Risk Evaluation） (B) 風險分析（Risk Analysis） (C) 風險分類（Risk Classification） (D) 風險識別（Risk Identification）
A B C	17. 關於系統存取控制管理規劃與執行，下列哪些項目適當可行？（複選） (A) 公司企業資源規劃系統（ERP System）的權限申請，依照不同部門業務面向，須先經由負責部門主管審核。（例如：採購類權限

	申請須經採購主管審核） (B) 公司依照各個基本職能於預先規劃其企業資源規劃系統系統使用權限，新進人員待用人部門主管確認後，通知權限管理人賦予其預設之權限，無須額外填單申請 (C) 公司所有系統原預設每半年進行權限檢核，本次風險評估後，其中某個系統因其重要性降低，經權責主管核准後，變更為每年進行權限檢核 (D) 公司規定委外廠商於外部連入公司內部網路，須申請以虛擬專用網路（virtual private network, VPN）方式為之，申請者使用完畢後，不需告知管理單位關閉其權限
A B D	18. 網路安全框架（Cybersecurity Framework, CSF）為美國國家標準暨技術研究院（National Institute of Standards and Technology, NIST）彙整後所提出，作為整體網路安全架構之規劃藍圖參考，請問該 CSF 之組成元素包含下列哪些項目？（複選） (A) 框架核心（Framework Core） (B) 框架設定檔（Framework Profile） (C) 實施程序（Framework Procedure） (D) 實施層級（Implementation Tiers）
A B C D	19. 關於資訊安全管理系統在決定驗證範圍時，須包含下列哪些考量議題？（複選） (A) 組織內部與外部的議題 (B) 主管機關的要求 (C) 適用法令與法規的要求 (D) 組織與其他組織履行活動間的介面及相依性
A B D	20.「某政府一級單位官網，交付政府維運機房代管，要求服務層級協議（Service Level Agreement, SLA）99.999%服務水平，監測發現該政府官網，固定在每週日，半夜 12:00 會自動停止服務 30 分鐘。該事件已經持續半年才被發現，在風險問題排除過程中：（1）IIS Web Server 都服務正常、（2）MS-SQL 資料庫服務也正常、（3）防火牆也未變動其政策、（4）檢查相關排程有每月一次定期備份檔案到 D 磁碟某目錄、（5）在檔案異動上發現有多了一個 Lcx.exe 惡意程序放在 Web Root 目錄。」下列哪些選項屬於合適的風險處置措施？（複選） (A) 問題經半年才被發現，表示目前缺乏有效監管網站存活狀態，可利用工具建立監控機制，監控 Web Server、URL 連結、資料庫 1433 通訊，就可以知道系統服務層級協議狀態與降低中斷服務的風險 (B) 在 Web root 目錄出現 Lcx.exe，確定屬被駭客入侵的資安事件，

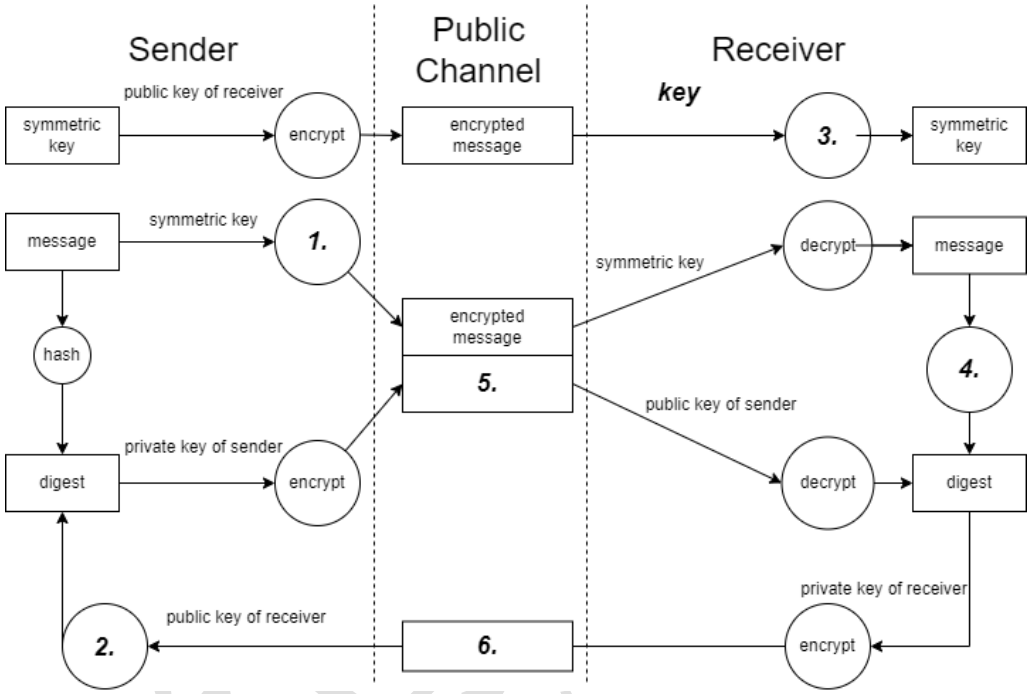
	必須先通知部會主管後，緊急補救風險處理 (C) 以 99.999%服務層級協議來看，本次事件長達半年，以一年 365 天計算仍符合 99.999%服務層級協議 (D) 必須依規定進行通報，例如：「國家資通安全通報應變網站」進行通報
A	21.【題組 1】若發現外部供應商偷偷攜帶隨身碟（USB Disk）進入公司使用，竊取公司內部資料並造成病毒蔓延，下列風險處理措施何者最「不」正確？ (A) 確實登記外部供應商隨身碟型號後歸還 (B) 確認隨身碟所使用之公司內部電腦，應進行病毒檢查 (C) 確認隨身碟所使用之公司內部電腦，相關檔案操作記錄，確認公司機密資料是否被存入隨身碟 (D) 依據資安管理辦法及與外部供應商簽署同意進入公司資安規定，對外部供應商進行開罰
C	22.【題組 1】若外部供應商攜入電腦，卻無法透過自帶智慧手機上網，且有使用網際網路需求，身為資安人員，需要對網路架構進行安全規劃，下列敘述何者正確？ (A) 讓外部供應商直接使用公司員工座位區的有線網路上網 (B) 讓外部供應商直接使用公司內部無線網路上網 (C) 外部供應商電腦使用的網路應與公司內部網路完全隔開 (D) 有線網路必須以零信任原則嚴格限制非公司電腦可以接取使用
A	23.【題組 1】外部供應商與供應鏈進到公司，進行系統建置與維護，常常需要使用自行攜帶的設備與軟硬體裝置，你身為該公司的資安管理人員，依據 ISO27001 制度的外部供應商管理，下列敘述何者「不」正確？ (A) 外部供應商與供應鏈皆是長期合作，本是信賴夥伴關係，不需要特別檢查處置 (B) 進入公司前須檢查該外部供應商人員所使用的電腦，是否安裝防毒軟體且更新到最新版，並進行掃毒檢查 (C) 攜入的儲存裝置，例如：隨身碟須經過掃毒分析與內容檢查 (D) 必須了解所攜入的物品使用目的及必要性
A B C D	24.【題組 1】許多大型敏感的產業，嚴格限制外部供應商與供應鏈攜帶智慧型手機進入公司，下列嚴格限制的理由哪些正確？（複選） (A) 智慧型手機通常會有攝影鏡頭，擔心機密資料被拍照外洩 (B) 智慧型手機具有藍牙功能，亦可用來傳輸資料 (C) 智慧型手機可利用充電線，變成儲存裝置，用來竊取資料 (D) 通常企業對於長期外部供應商，會要求使用只有電話功能，無其

<table>
<tr><td></td><td>他功能的手機</td></tr>
<tr><td></td><td>【題組 2】
迪菲-赫爾曼密鑰交換（Diffie-Hellman Key Exchange, D-H）是一種金鑰交換方法，其能夠讓通訊雙方在公開通道上建立金鑰，並且使用該金鑰在後續的通訊中作為共同金鑰來加密訊息內容。若小美和小明想要使用這個演算法來建立一個共同金鑰以利後續的訊息交換，則他們所使用的計算過程及參數如下所示：
$(g^a \bmod p)^b \bmod p = (g^b \bmod p)^a \bmod p$
・g：根數（base）
・p：任意質數
・a、b：分別為通訊兩端所各自選定的私鑰（秘密正整數值）
・mod：取餘數（modulus）
根據此式，小美和小明可以先各自選定私鑰 a 和 b，並搭配公開資訊 g 與 p 來計算得到共同金鑰 K。假設小美為金鑰交換的發起端，則金鑰建立流程如下所示：
<table>
<tr><th>步驟</th><th>小美</th><th>公開通道</th><th>小明</th></tr>
<tr><td>1.</td><td>選定 a
計算 $A = g^a \bmod p$</td><td></td><td></td></tr>
<tr><td>2.</td><td></td><td>傳送 A, g, p 給小明</td><td></td></tr>
<tr><td>3.</td><td></td><td></td><td>選定 b
計算 $B = g^b \bmod p$
計算 $K = A^b \bmod p$</td></tr>
<tr><td>4.</td><td></td><td>傳送 B, g, p 給小美</td><td></td></tr>
<tr><td>5.</td><td>計算 $K = B^a \bmod p$</td><td></td><td></td></tr>
</table>
在步驟 5.以後，雙方皆得到一個相同的金鑰 K 可作為後續訊息交換使用。</td></tr>
<tr><td>C</td><td>25.【題組 2 背景描述如附圖】假設小美和小明協議使用 g=5 和 p=11，並且小美選定其私鑰為 a=3，小明選定其私鑰 b=4。請問經過雙方計算所得到的共同金鑰 K 值為何？
(A) K=1
(B) K=2
(C) K=3
(D) K=4</td></tr>
<tr><td>C</td><td>26.【題組 2 背景描述如附圖】此時若有第三人小華獲知了雙方於公開通道中的通訊內容，在私鑰沒有外洩並且通訊內容未遭受攻擊與竄改的情況下，關於三人可獲取的資訊，下列何者正確？</td></tr>
</table>

	(A) g 和 p：小美知道，小明知道，小華不知道 (B) a：小美知道，小明知道，小華不知道 (C) b：小美不知道，小明知道，小華不知道 (D) K：小美知道，小明不知道，小華知道
D	27.【題組 2 背景描述如附圖】若小華想要得知共同金鑰 K，請問他可以透過下列何種攻擊方式得知？ (A) 跨網站指令碼攻擊（Cross Site Scripting Attack, XSS） (B) 分散式阻斷服務攻擊（Distributed Denial of Service Attack, DDoS） (C) SQL 注入攻擊（SQL Injection） (D) 中間人攻擊（Man-in-the-Middle Attack, MitM）
B C D	28.【題組 2 背景描述如附圖】小美和小明「無法」使用哪些方式來防止此類型的攻擊？（複選） (A) 在交換訊息前必須先驗證對方身分 (B) 公開雙方的私鑰（a 和 b） (C) 改採用 RSA 加密演算法 (D) 使用端點偵測及回應系統（Endpoint Detection & Response, EDR）
	【題組 3】常青公司主要的營運系統建置於北部的舊有廠房內，包含 2 百萬元的伺服器主機、儲存媒體、網路設備及先前採購的 8 百萬元可重覆安裝資訊系統軟體，提供公司辦公室、原廠房以及合作的供應商相關營運作業管理，因原有廠區周邊環境設施不夠完善，最近 5 年因為颱風與豪雨，已經造成 3 次系統運作中斷和 1 次淹水損壞所有資訊系統設備；公司於南科建置的新廠將在年底落成，總經理要求資訊部門主管開始著手規劃未來長期業務持續管理（Business Continuity Management, BCM），並且評估未來如果再發生障礙時，復原時間目標（Recovery Time Objective, RTO）不大於四小時的可行方案。
B	29.【題組 3 背景描述如附圖】業務持續管理的一大重點是業務衝擊分析（Business Impact Analysis, BIA），請問下列何者「並非」業務衝擊分析後能達成的目標？ (A) 計算失能可能造成的衝擊和損失，評估可能的損失幫助爭取改進預算 (B) 分析出外部攻擊威脅與內部系統弱點，以供研擬後續的防護機制 (C) 記錄下使用那些流程/活動，對組織產生衝擊，以及如何快速恢復 (D) 採用風險分擔（Risk sharing）時，讓公司知道需要買什麼保險與額度才能感到安全

D	30.【題組 3 背景描述如附圖】針對近年來的系統服務障礙記錄，原廠房資訊系統的預期年度損失（Annual Loss Expectancy, ALE）為多少？ (A) $10,000,000 (B) $2,500,000 (C) $1,600,000 (D) $400,000
D	31.【題組 3 背景描述如附圖】為了符合公司持續營業的需求，在本次業務持續管理中將考量增建異地備援的需求，以解決先經歷長時間營運中斷的窘境，針對評估小組提出的以下方案，請問在不考量建置成本的情況下，下列何者為最佳選擇？ (A) 在新廠房規劃建置冷備援（cold sites）方案 (B) 租用網路數據中心空間規劃建置暖備援（warm sites）方案 (C) 在新廠房規劃建置熱備援（hot sites）方案 (D) 租用網路數據中心空間規劃建置全備援（mirrored sites）方案
B C D	32.【題組 3 背景描述如附圖】總經理要求增加評估雲端服務的備援方案，在目前運作順暢的作業流程下，將優先以使用既有穩定軟體系統為前題下，除了與原軟體廠商連繫確認其軟體系統支援主機虛擬化、可移植性與配合事項之外，參考 CNS19086 系列、CNS27018 以及 CNS27002 的相關安全規範，相較於一般先建異地備援方案，選用雲服務商（Cloud Service Provider, CSP）的雲端服務之時，必須考量下列哪些安全要素？（複選） (A) 評估何種雲服務商提供的軟體即服務（Software as a Service, SaaS）是最符合公司本案相關服務運作需求與效益 (B) 評估雲服務商支援的服務等級目標（Service-Level Objective, SLO）、復原時間目標（Recovery Time Objective, RTO）與復原點目標（Recovery Point Objective, RPO）符合公司災難復原計劃與否 (C) 確認雲服務商所提供之安全過程及控制措施可以符合實體與環境安全的要求 (D) 確認雲服務商涵蓋所有建置服務的網路及通訊通道安全，並且可預防未經受權之雲端服務客戶（Cloud Service Customer, CSC）間通訊技術方法
	【題組 4】A 企業為台灣 50 大之企業之一，且為股票上市企業，實收資本額達新台幣 150 億元，主要營業項目為電商相關，該公司最近發現客服中心收到多筆客訴，內容主要都為消費者在公司電商網站購物後，就接到詐騙電話，電話中明確指出受駭者的消費明細，並誆稱要辦理退費，導引消費者去 ATM 操作，導致受駭者金錢損失。

A	33.【題組 4 背景描述如附圖】A 企業的資訊人員收到客服中心反應後，分析已知受詐騙的消費者，研判駭客可能是利用偷來的消費者資訊或密碼試圖登入網路服務的一種攻擊，下列攻擊手法何者正確？ (A) 密碼撞庫攻擊 (B) 暴力密碼破解 (C) 加密密文破解 (D) 服務阻斷攻擊
D	34.【題組 4 背景描述如附圖】針對駭客可能是利用偷來的消費者資訊或密碼試圖登入網路服務的這一種攻擊，下列何者防護措施「無法」有效防範此攻擊？ (A) 利用手機簡訊進行二次驗證 (B) 在使用者設定密碼時，檢核是否與個人資訊有關 (C) 在使用者輸入密碼時，須綁定設備或裝置，當有新裝置登入時，系統會寄發簡訊通知，要求二次驗證 (D) 系統在儲存使用者密碼時，會使用加密方式儲存
C	35.【題組 4 背景描述如附圖】由於該電商系統係該公司委外開發及維運，因應此一風險，進行了以下五種措施，下列哪些措施屬於風險分擔（Risk Sharing）？（甲）新增使用者登入簡訊驗證功能。（乙）在公司官網公告此一資安情況並請使用者注意，以及公布專線客服電話協助消費者處理。（丙）與保險公司投保資安保險，以減少公司損失。（丁）請委外廠商進行系統健檢，結果發現該系統有二項嚴重漏洞未修補，該漏洞亦有可能造成系統密碼被竊，要求廠商立即修補完成。（戊）調整與委外廠商的合約內容，新增若因系統設計維運不當，造成甲方（A 企業）的損失時，該損失皆須由委外廠商全額負擔。 (A) 甲、丙、戊 (B) 乙、丁 (C) 丙、戊 (D) 丙、丁
A C	36.【題組 4 背景描述如附圖】A 企業在此一事件發生後，未發佈任何公開聲明，僅維持與受駭之消費者進行後續糾紛處理，但受駭消費者透訴媒體，以致眾媒體已大幅報導、相關檢警調單位亦已主動介入偵辦，另由於未有專屬之資安部門與人員編制，A 企業計畫於民國 112 年 1 月 1 日、成立專門之資安單位，編制 4 人，最高資安主管為協理，直接向資訊副總經理負責。綜上所述，請問該公司可能違反下列哪些法令法規的要求？（複選） (A) 公開發行公司建立內部控制制度處理準則

	(B) 資通安全管理法 (C) 臺灣證券交易所股份有限公司對有價證券上市公司重大訊息之查證暨公開處理程序 (D) 公司法
	【題組 5】下圖為密碼學中常見的一種加密系統，請根據圖中資訊回答下列問題： 
C	37. 【題組 5 背景描述如附圖】請問圖中所使用的架構是何種加密系統？ (A) 對稱式加密（Symmetric Encryption） (B) 非對稱式加密（Asymmetric Encryption） (C) 混合式加密（Hybrid Encryption） (D) 雜湊演算法（Hash Algorithm）
D	38. 【題組 5 背景描述如附圖】關於附圖中所標示的數字 1.~6.之執行順序，下列排序何者最為合理？ (A) 2.→1.→5.→3.→4.→6. (B) 3.→5.→6.→4.→1.→2. (C) 6.→1.→4.→3.→5.→2. (D) 3.→1.→5.→4.→6.→2.
D	39. 【題組 5 背景描述如附圖】在步驟 3.之中，接收者應使用何種 Key 來進行解密以獲得共享金鑰（symmetric key）？ (A) 傳送者的公開金鑰（public key of sender） (B) 傳送者的私密金鑰（private key of sender） (C) 接收者的公開金鑰（public key of receiver）

	(D) 接收者的私密金鑰（private key of receiver）
A B D	40.【題組 5 背景描述如附圖】請問下列關於此種加密系統的敘述，哪些正確？（複選） (A) 使用對稱金鑰（symmetric key）對訊息（message）進行加解密 (B) 將對稱金鑰（symmetric key）以接收者的公開金鑰加密後再進行傳送 (C) 使用私密金鑰將訊息（message）進行加解密 (D) 此種加密方式可應用於傳輸層安全協議（Transport Layer Security, TLS）和安全殼協議（Secure Shell, SSH）