

109 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：109 年 8 月 15 日

第 1 頁，共 11 頁

單選題 15 題，複選題 5 題，題組題 5 題（佔 100%）

C	<p>1. 某台灣公司，業務市場及銷售據點分布在臺、美兩地，在建置資安系統時，應優先考量附圖哪些法規事項？</p> <p>1. 歐盟支付服務指令第 2 版（The Second Payment Services Directive, PSD2）</p> <p>2. 臺灣-資通安全管理法</p> <p>3. 美國-CCPA（California Consumer Privacy Act）</p> <p>4. 臺灣-營業秘密法</p> <p>5. 香港-CFI（Cybersecurity Fortification Initiative）</p> <p>(A) 12345</p> <p>(B) 1234</p> <p>(C) 234</p> <p>(D) 1235</p>
D	<p>2. 關於資安工程師定期需要執行的資安維運任務，下列何者「不」正確？</p> <p>(A) 定期備份與演練</p> <p>(B) 每週防毒報告</p> <p>(C) 每半年滲透測試</p> <p>(D) 定期向會計主任報告</p>
C	<p>3. 若要設定防火牆內對外的連線，僅開放對外的服務及網頁瀏覽，下列敘述何者正確？</p> <p>(A) Allow all</p> <p>(B) Allow http port 22</p> <p>(C) Allow https port 443</p> <p>(D) Allow smtp 25</p>
D	<p>4. 某公司在每週星期日凌晨 1 點執行完整備份（Full Backup），每日凌晨 1 點執行增量備份（Incremental Backup），每日備份資料分存放於不同磁帶。若此系統在星期三的下午 2 點發生嚴重損毀（Crash），資訊人員執行資料回復，需使用多少個磁帶的資料？</p> <p>(A) 1</p> <p>(B) 2</p> <p>(C) 3</p> <p>(D) 4</p>
D	<p>5. 某公司新網頁資訊系統上線，內含客戶相關資料，經資安風險分析，有帳號暴力破解風險，再經後續的安全測試，發現帳戶登錄機制可容許一直重複嘗試登入，關於上述狀況，下列何者作法最「不」適當？</p> <p>(A) 設定帳戶在嘗試失敗多次後鎖定一段時間</p>

109 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：109 年 8 月 15 日

第 2 頁，共 11 頁

	<p>(B) 設定密碼政策，設定的密碼至少需有 12 個字元</p> <p>(C) 設定帳戶在嘗試失敗時，寄送 eMail 由郵件通知</p> <p>(D) 設定帳戶連線時，強制使用 Https 安全連線</p>
C	<p>6. 某公司為網路電信商，其多年前研發的即時通軟體非常受歡迎，然而在面對歐盟通用資料保護規則（EU General Data Protection Regulation, GDPR）時，內部評估發現其現有系統架構無法符合 GDPR 的規範，且系統修改費用驚人，管理層最後決定停止歐洲的市場業務，關於上述狀況，屬於下列何種風險處理？</p> <p>(A) 風險降低（Risk Reduction）</p> <p>(B) 風險接受（Risk Acceptance）</p> <p>(C) 風險規避（Risk Avoidance）</p> <p>(D) 風險轉移（Risk Transfer）</p>
C	<p>7. 進行網路架構設計時，下列敘述何者「不」正確？</p> <p>(A) 如果有開發系統應該要區分一個測試區</p> <p>(B) 透過 Log Server 記錄各種警訊</p> <p>(C) 採取 HA 機制需要多一台門禁系統</p> <p>(D) 需要規劃備份機制與容量規劃</p>
C	<p>8. 關於資訊安全模型（Security Models）中的強制存取控制（Mandatory Access Control, MAC），下列敘述何者「不」正確？</p> <p>(A) 依據事前定義（Pre-defined）主體（Subject）的安全等級和被存取物件（Object）機敏等級來決定是否可以存取</p> <p>(B) 安全強度較自主存取控制（Discretionary Access Control, DAC）高</p> <p>(C) 傳統的 Unix 系統使用者（Users）、群組（Groups）和讀-寫-執行（Read-Write-Execute）管控，即為 MAC 的一種實作</p> <p>(D) 安全政策（Policy）由安全政策員（Security policy administrator）集中管控</p>
A	<p>9. 下列何者可被用來確認資料的完整性（Integrity）？</p> <p>(A) SHA-512</p> <p>(B) 3DES</p> <p>(C) RC4</p> <p>(D) EC-ElGamal</p>
C	<p>10. 某公司在一次例行檢查中，資安管理人員發現一位員工正試圖使用透過手機網路連至外部網路下載軟體至其工作用筆記型電腦，此作法等於繞過公司防火牆，該員工解釋是為了安裝部門專案使用的 X 軟體，關於上述狀況，下列何種措施應優先進行？</p> <p>(A) 重新設定公司防火牆規則讓 X 軟體可以下載並安裝</p>

109 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：109 年 8 月 15 日

第 3 頁，共 11 頁

	<p>(B) 安裝網路型入侵偵測系統進行監控，提早發現類似不當行為</p> <p>(C) 執行公司資安規範，移除軟體使用</p> <p>(D) 訪談該員工，重新進行需求分析</p>
A	<p>11. 某公司在員工個人電腦登入後會強制跳出提醒訊息：「請遵守本公司資訊安全規範，避免機敏資料外洩」，此提醒屬於下列何種控制措施？</p> <p>(A) 管理的 (Administrative)、威嚇性 (Deterrent)</p> <p>(B) 管理的 (Administrative)、預防性 (Preventive)</p> <p>(C) 技術的 (Technical)、威嚇性 (Deterrent)</p> <p>(D) 技術的 (Technical)、預防性 (Preventive)</p>
B	<p>12. 如附圖所示，關於營運持續管理 (Business Continuity Management System, BCMS) 的執行項目排序，下列何者較正確？</p> <ol style="list-style-type: none">1. 建立營運持續策略 (Business Continuity Strategy, BCS)2. 撰寫緊急應變計畫 (Emergency Plan)3. 撰寫營運持續計畫 (Business Continuity Planning, BCP)4. 營運持續計畫演練 (Business Continuity Planning Exercise)5. 執行營運衝擊分析 (Business Impact Analysis, BIA) <p>(A) 1->2->3->5->4</p> <p>(B) 5->1->2->3->4</p> <p>(C) 5->2->3->1->4</p> <p>(D) 1->2->3->4->5</p>
B	<p>13. 在進行營運衝擊分析 (Business Impact Analysis, BIA) 時，下列三項評估的先後順序為何？1.產品與服務 (Products and services)、2.流程 (Processes)、3.活動 (Activities)</p> <p>(A) 3->2->1</p> <p>(B) 1->2->3</p> <p>(C) 2->1->3</p> <p>(D) 1->3->2</p>
C	<p>14. 關於縱深防禦 (Defense in Depth)，下列敘述何者「不」正確？</p> <p>(A) 縱深防禦又稱為階層式防禦 (Layered Defense) 或洋蔥式防禦 (Onion Defense)</p> <p>(B) 縱深防禦對資訊資產套用多層安全防護，若部分防護失效仍可透過其餘機制降低受駭風險</p> <p>(C) 縱深防禦僅能應用於實體控制之情境以發揮最大效益 (如：IDC 資料中心)</p> <p>(D) 透過「網路從取控制>伺服器存取控制>應用程式存取控制>資料存取控制」此四層架構，即可稱為縱深防禦之存取控制模式</p>

109 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：109 年 8 月 15 日

第 4 頁，共 11 頁

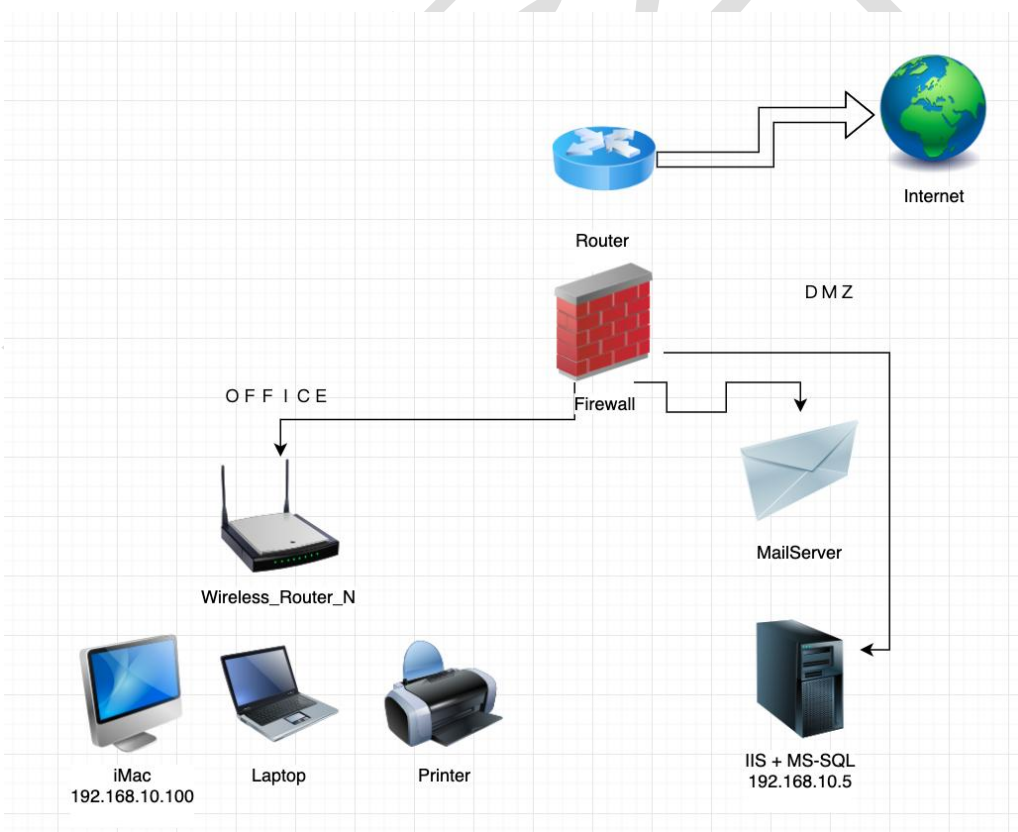
D	<p>15. 關於網站應用程式防護，下列敘述何者正確？</p> <p>(A) 為有效降低網站應用程式受駭風險，原始碼檢測不可於程式開發過程中執行，待開發完成後再一次性執行以達最大效益</p> <p>(B) 網頁應用程式防火牆（Web Application Firewall, WAF）可有效避免遭受駭客攻擊，且若啟用特徵碼定期更新機制，則受駭風險已降至最低，網站應用程式之安全性測試便可忽略</p> <p>(C) 網站應用程式所使用之元件若發現弱點，透過網頁應用程式防火牆（Web Application Firewall, WAF）套用虛擬修補（Virtual patching）能有效阻擋攻擊，則不需再對該元件進行修復</p> <p>(D) 網站應用程式應定期執行安全檢測（如：原碼檢測、弱點掃描、滲透測試），並對檢出之安全弱點進行修復，若無法修復則需實施補償性控制措施來降低安全風險</p>
A B C	<p>16. 某公司從事國際型科技大廠組裝代工業務，在合作業務上，嚴禁將未上市產品資訊外洩，包含：未上市產品間諜照、設計圖...等，相關資訊檔案讀取使用僅限制公司少數高階技術人員可以讀取，不能外洩到公司以外其他地方使用。關於上述狀況，下列風險管理敘述何者正確？（複選）</p> <p>(A) 公司與員工間簽屬相關保密協定與同意限制規範，並進行必要技術管制手段，如：手機必須放置在公司設定手機電腦保管區、嚴禁拍照裝置與私人電腦攜入公司廠區</p> <p>(B) 對公司電腦，限制外接儲存裝置的存取、電腦畫面擷取、與工具軟體使用限制，以降低公司機密資料外洩風險</p> <p>(C) 公司成立相對應資安防護措施，如：防止駭客入侵竊取、電子郵件的附件過濾、對公司內外流量封包監控</p> <p>(D) 公司不應限制禁止員工上網，這是員工午休時基本人權權利</p>
A C D	<p>17. 下列何者「不」是用來在建置資訊安全管理系統時，透過量化資安目標來協助組織瞭解是否落實所訂定之資安政策的做法？（複選）</p> <p>(A) 全面導入資安管理系統</p> <p>(B) 檔案伺服器每年中毒次數低於 2 次</p> <p>(C) 密碼設定 12 碼，文、數字與符號混合</p> <p>(D) 全面導入垃圾郵件過濾系統</p>
A C D	<p>18. 密碼學（Cryptography）除了機密性（Confidentiality）之外，還可以保護下列何者特性？（複選）</p> <p>(A) 完整性（Integrity）</p> <p>(B) 可用性（Availability）</p> <p>(C) 不可否認性（Non-Repudiation）</p>

109 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：109 年 8 月 15 日

第 5 頁，共 11 頁

	(D) 鑑別性 (Authenticity)
A B C D	<p>19. 某公司正準備規劃其識別及存取管理 (Identity and Access Management) 機制，下列何者是可選擇的存取控制類型？(複選)</p> <p>(A) 強制存取控制 (Mandatory Access Control, MAC)</p> <p>(B) 識別存取控制 (Identity-Based Access Control, IBAC)</p> <p>(C) 規則基礎存取控制 (Rule-Based Access Control, RuBAC)</p> <p>(D) 自主存取控制 (Discretionary Access Control, DAC)</p>
A C D	<p>20. 下列哪些是進行營運衝擊分析 (Business Impact Analysis, BIA) 時需考量的因素？(複選)</p> <p>(A) 財務衝擊 (Financial Impact)</p> <p>(B) 政治衝擊 (Political Impact)</p> <p>(C) 商譽衝擊 (Reputational Impact)</p> <p>(D) 法規衝擊 (Legal Impact)</p>
題組	<p>某公司的資安人員依據公司設備狀況規劃以下網路架構設計圖：</p>  <p>根據上列資訊，請回答下列問題：</p>
A B	<p>21. 題組背景描述如附圖。請問該網路架構設計中，存在下列哪些問題？(複選)</p> <p>(A) OFFICE 與 DMZ 未區分網段</p>

109 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：109 年 8 月 15 日

第 6 頁，共 11 頁

	<p>(B) 伺服器與資料庫放在同一台</p> <p>(C) 自行架設郵件伺服器安全性不足</p> <p>(D) 印表機應該使用無線分享以增加便利性</p>
A	<p>22. 題組背景描述如附圖。承上題，若要進行網路架構改善，可採取下列何種強化措施？</p> <p>(A) 伺服器與資料庫應該區分在不同網段</p> <p>(B) 增加一個 MAIL Server 做備援</p> <p>(C) 採取 HA 機制多一台印表機</p> <p>(D) Mac 電腦應該要限制上網</p>
D	<p>23. 題組背景描述如附圖。承上題，在此架構下，下列何者「不」是定期需要執行的資安維運任務？</p> <p>(A) 定期備份與演練</p> <p>(B) 每半年做一次防毒掃描</p> <p>(C) 每兩年做一次資料備份</p> <p>(D) 不需向主管機關報告</p>
B	<p>24. 題組背景描述如附圖。若要設定防火牆內對外的連線，僅開放對外的服務及網頁瀏覽，下列何者正確？</p> <p>(A) Allow all</p> <p>(B) Allow http port 80</p> <p>(C) Allow http port 1443</p> <p>(D) Deny smtp 125</p>
題組	<p>某公司為一跨國企業，公司員工約 10,000 人，所有員工皆配備一台筆記型電腦，身為資安專家的你，正在評估筆記型電腦的安全風險，並對公司高層提出建議。</p> <p>目前已搜集到以下資訊：</p> <p>每台筆記型電腦價值：30,000</p> <p>筆記型電腦遺失，價值將 100% 受損</p> <p>每年遺失數量 10 台</p> <p>同時，資安專家已完成資料防護軟體評估，以避免筆記型電腦遺失時對公司造成的損失，產品生命週期為四年，廠商報價如下：</p> <p>全硬碟加密軟體：500,000，使用期間每年維護費用：75,000</p> <p>遠端資料清除工具：100,000，使用期間每年維護費用：20,000</p> <p>根據上列資訊，請回答下列問題：</p>

109 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：109 年 8 月 15 日

第 7 頁，共 11 頁

B	25. 題組背景描述如附圖。請問你正在進行的風險分析方法為下列何者？ (A) 定性風險分析 (Qualitative Risk Analysis) (B) 定量風險分析 (Quantitative Risk Analysis) (C) 協同風險分析 (Collaborative Risk Analysis) (D) 風險分析矩陣 (Risk Analysis Matrix)
B	26. 題組背景描述如附圖。公司筆記型電腦的年度損失期望值 (Annualized Loss Expectancy) 為下列何者？ (A) 75,000 (B) 300,000 (C) 30,000 (D) 1,200,000
D	27. 題組背景描述如附圖。正在評估的資料防護軟體，每年的年度花費為下列何者？ (A) 695,000 (B) 980,000 (C) 300,000 (D) 245,000
B	28. 題組背景描述如附圖。根據分析結果，資安專家應對公司提出下列何種建議？ (A) 接受風險，購買防護軟體費用過高 (B) 導入資料防護軟體以降低風險 (C) 資料不足，需重新進行評估 (D) 接受風險，筆記型電腦遺失數量不多
題組	為因應 2019 冠狀病毒疾病疫情，中央防疫中心也提升至一級開設，對此，金管會表示，國內銀行業也積極因應，目前已有 13 家銀行採取異地辦公，A 銀行決定將資訊部門的系統管理人員及其代理人分別安排在不同的辦公地點辦公。 根據上列資訊，請回答下列問題：
C	29. 題組背景描述如附圖。請問該異地辦公的規劃與營運持續管理有下列何種關聯？ (A) 與營運持續管理無關，應屬於職業衛生安全管理 (Occupational Health and Safety Assessment Series, OHSAS) 的議題 (B) 與資料復原目標 (Recovery Point Objective, RPO) 的達成較有關 (C) 與復原目標時間 (Recovery Time Objective, RTO) 的達成較有關 (D) 屬於政治因應，配合主管機關要求

109 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：109 年 8 月 15 日

第 8 頁，共 11 頁

A 或 B	<p>30. 題組背景描述如附圖。請問 A 銀行資訊部門關鍵成員異地辦公的相關程序、作法與規定，應納入下列何種程序文件中較為合適？</p> <p>(A) 事故管理計畫 (Incident Management Plan)</p> <p>(B) 營運持續計畫 (Business Continuity Plan)</p> <p>(C) 營運復原計畫 (Business Resumption Plan)</p> <p>(D) 災害復原計畫 (Disaster Recovery Plan)</p>
A	<p>31. 題組背景描述如附圖。關於 A 銀行異地辦公地點的考量及選擇，下列敘述何者較「不」正確？</p> <p>(A) 應與系統異地備援的設置位置一致</p> <p>(B) 如系統發生異地中斷，系統管理員可由遠端連線操控，應可考量採居家辦公</p> <p>(C) 可依營運衝擊分析後的流程或服務的重要性來決定哪些角色需要異地辦公</p> <p>(D) 隨著資訊科技的進步，異地辦公的選擇應著重在工作的執行，而不是辦公室地點的選擇</p>
B	<p>32. 題組背景描述如附圖。除了異地辦公地點的選擇外，下列何項亦可增加疫情發生時的營運持續能力？</p> <p>(A) 接班人計畫</p> <p>(B) 代理人計畫</p> <p>(C) 工作輪休計畫</p> <p>(D) 員工進修計畫</p>
題 組	<p>近來有愈來愈多公司更積極擁抱新興科技，期望透過更大量的科技應用，提升公司整體營運能力，也希望從中找到新的商機，強化公司競爭力。A 公司為著名電商公司，同時十分注重資訊安全，去年已完成全公司 ISO/IEC 27001 導入與驗證，今年為強化公司競爭力，決議將公司主要電商網站由 IDC 機房移入雲端，同時相關辦公自動化服務 (Office Automation, OA) 也積極使用雲端 Solution。</p> <p>根據上列資訊，請回答下列問題：</p>
C	<p>33. 題組背景描述如附圖。就 ISO/IEC 27001 而言，若考量公司重要服務 (電商網站) 由地端移入雲端一事，下列敘述何者較適當？</p> <p>(A) 由於是將電商網站由 IDC 機房移入雲端，整體系統功能未進行調整，所以無須針對此一作業進行風險評估</p> <p>(B) 由於是將電商網站由 IDC 機房移入雲端，與 ISO 先前的驗證情況大不相同，所以應於工作結束後立即進行 ISO/IEC 27001 重新驗證</p>

109 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：109 年 8 月 15 日

第 9 頁，共 11 頁

	<p>(C) 電商網站由 IDC 機房移入雲端，屬重大服務調整，所以應針對此一作業進行風險評估</p> <p>(D) 由於是將電商網站由 IDC 機房移入雲端，雲端平台的安全性高，所以無需重新評估該網站的資安防護機制</p>
D	<p>34. 題組背景描述如附圖。因應資通系統使用雲服務，資通系統開始面臨新的風險，請問下列何種風險與資通系統在雲端環境的關聯度最高？</p> <p>(A) Account hijacking</p> <p>(B) Insecure interfaces and APIs</p> <p>(C) Data breaches</p> <p>(D) Limited cloud usage visibility</p>
D	<p>35. 題組背景描述如附圖。A 公司某日收到上個月雲端平台的帳號，發現帳單費用爆增，經過清查後發現雲端平台存有不知名的挖礦程式正在執行，導致雲端使用費大增，請問下列何者最「不」可能是遭駭客植入挖礦程式的原因？</p> <p>(A) 資通系統的識別及存取管理（Identity and Access Management, IAM）相關帳密或存取金鑰外洩</p> <p>(B) 主機作業系統或資通系統具遠端程式碼執行（Remote Code Execution, RCE）漏洞</p> <p>(C) 雲端所使用的系統映像檔受感染，系統維護人員下載並執行不明來源的映像檔（Docker Image）</p> <p>(D) 雲端之電商網站具有安全的弱點，遭駭客利用進行 Billion Laugh Attack 所導致</p>
A C D	<p>36. 題組背景描述如附圖。電商平台移至雲端後，相關系統維運作業也因應調整，請問下列敘述何者具有潛在資安合規風險？（複選）</p> <p>(A) 因應雲端作業環境與加強效率，程式開發人員將同時具有雲端平台的操作權限，程式開發完成後可直接進程式更新作業，縮短作業時間</p> <p>(B) 為確保資料的雲端安全性，資料庫管理人員要求資料在寫入資料庫前，針對機敏資料欄位，需對資料本身加密後才可存入資料庫</p> <p>(C) 為一致化管理作為，針對在雲端上的資通系統，皆未強制要求租用或安裝額外的資安防護機制，以減低成本並簡化維運作業</p> <p>(D) 由於雲端的高可用性，針對在雲端上的資通系統，不需再修訂業務持續計畫</p>
題組	<p>ABC 公司導入 ISO/IEC 27001 資訊安全管理系統，並透過第三方稽核單位執行部分單位驗證。</p>

109 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：109 年 8 月 15 日

第 10 頁，共 11 頁

內部公告且遵循之資安事件（故）通報與處理規範如下：					
	等級	定義	更新時效	處理時效	通報層級
	1	內部系統功能異常	24 小時	72 小時	單位主管
	2	內部系統無法使用或受駭	12 小時	48 小時	部門主管
	3	外部服務功能異常	8 小時	36 小時	事業體主管
	4	外部服務無法使用或受駭	4 小時	24 小時	總經理
D	37. 題組背景描述如附圖。ABC 公司網管人員於定期審查內部網域伺服器日誌時發現疑似未經授權存取，下列敘述何者正確？ (A) 尚未確認對內部系統造成影響，不需要進行資安通報 (B) 尚未確認為駭客所為，不需要進行資安通報 (C) 待確認為駭客所為且影響內部系統後，再進行通報 (D) 雖未確認駭客所為或影響內部系統，仍應儘速通報				
C	38. 題組背景描述如附圖。ABC 公司其內部專責資安團隊對日誌進行關聯分析後，已有跡證顯示部分內部伺服器遭受駭客接管且取得系統管理者權限，下列敘述何者「最」正確？ (A) 此受駭情況可能影響商譽，應由資安長裁示後續處置 (B) 已轉交專責資安團隊處理，不需要進行資安通報程序 (C) 此為內部系統受駭，進行通報並 48 小時處理完成即可 (D) 此受駭狀況非同小可，應於當日處理完成並每小時回報部門主管，待處理完成後再通知總經理				
B	39. 題組背景描述如附圖。ABC 公司已於規範之時間內進行資料採證、分析、弱點修正與資料還原後，目前服務已恢復正常運作，下列敘述何者正確？ (A) 服務恢復後應立即針對此事故執行風險評鑑，擬定資訊安全風險處理計畫並執行之 (B) 應對事故進行分析並了解可能成因，應用此知識來降低發生機率，或類似事件再發生所造成之影響 (C) 服務雖已恢復但無法確保未來不再受駭，應立即召開管理審查會議，討論與爭取改善措施所需資源 (D) 縱使服務恢復，但仍導致資訊安全關鍵績效指標無法達成，需立調整關鍵績效指標項目以確保合規性				
C	40. 題組背景描述如附圖。若未來 ABC 公司新的核心系統屬於「資通安全管理法」所定義之特定非公務機關，其未涉及關鍵基礎設施維運之核心資通系統遭輕微竄改，下列敘述何者正確？ (A) 為第一級資通安全事件，應於知悉事件後 72 小時內完成損害控制，並於指定時間內送交改善報告				

109 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：109 年 8 月 15 日

第 11 頁，共 11 頁

	<p>(B) 為第二級資通安全事件，應於知悉事件後 48 小時內完成復原作業，並於指定時間內送交改善報告</p> <p>(C) 為第三級資通安全事件，應於知悉事件後 36 小時內完成損害控制或復原作業，並於指定時間內送交改善報告</p> <p>(D) 為第四級資通安全事件，應於知悉事件後 24 小時內完成損害控制或復原作業，並於指定時間內送交改善報告</p>
--	--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------