《資通安全》

一、資訊安全管理中緊急應變計畫是重要項目，緊急應變計畫中包含「訂定復原策略」，請說明「復原策略」的目的。復原策略內容包含資料備份與主機房異地備援，請說明「資料備份」的重要性。主機房異地備援分冷備援站（cold sites）、暖備援站（warm sites）、熱備援站（hot sites）、全備援站（mirrored sites），請條列逐一說明，內容需包含這四種備援站的成本與復原速度的比較。（24 分）

命題意旨	本題考取資料備份重要性與類型，屬於綜合分析題型。
答題關鍵	本題關鍵在於資料備份種類、成本高低與復原速度等分析比較，屬於綜合型應用題類。

【擬答】

(一) 資料備份的重要性：

由於資訊科技發展迅速，人們生活透過網路，進行商務活動、娛樂和他人互動溝通等等，然而若是遇到天災(電力中斷)、設備遺失和故障、病毒感染等，可能對原有生活和工作產生巨大影響。因此透過備份資料可以減少資料損失或是中斷程度，盡速恢復原有系統，使設備呈現原先可使用狀態，減少因意外造成的工作效率低落與生活品質的下降。

(二) 四種備援機制比較:

	冷備援站	暖備援站	熱備援站	全備援站
說明	沒有提供任何軟硬體服務,只有基本環境的場地、電力、機櫃等等。事件發生，IT人員帶著復原檔案和備份資料到備援機房架設系統,需要花費大量時間和精力。	發生事件時，必需啟動BCP(Business Continuity Planning)搭配資源災害應變，派遣IT人員介入恢復系統，而備用系統已安裝部分硬體設備或軟體。	擁有完整的基礎設施，如網路、電力等等，且擁有和主站點相同的硬體軟體的工作環境。一旦事件發生，可以迅速啟用，資料損失少。平時作為災害演練時的切換測試，熱備援站一直是準備好的狀態。	全備援網站提供相同資料可同時存取，平均負載流量，提供可靠性，並加快存取速度與效率，此外也達到重複資料儲存。假設事件發生，主站無法存取時，還有備用站點可以存取；鏡像資料會定期存取主站，以更新資料，可能存在更新時間差，資料有缺少情況。
成本	最便宜	次之	位於四者中的第三	成本最高
復原	復原速度最慢	速度位於四者中的第三	次之	復原速度最快

二、洛克希德馬丁公司發表網路攻擊鏈（Cyber Kill Chain）白皮書，透過軍事行動上常見的攻擊鏈來分析網路安全威脅，被視為解析駭客攻擊方法重要參考，其把駭客攻擊拆解成如後七個步驟：偵查（Reconnaissance）、武裝（Weaponization）、遞送（Delivery）、開採（Exploitation）、安裝（Installation）、發令&控制（Command & Control）和行動（Actions on Objectives）。請針對駭客此七個攻擊步驟逐一提出受害者可以降低攻擊風險或威脅的作為或行動。（28分）

命題意旨	本題題旨主要測驗考生對於國際工控系統資安的防護是否了解。
答題關鍵	駭客攻擊步驟有許多，ISMS只是基本要求，隨著5G網路、物聯網、AI運算的蓬勃發展，因此許多工業應用的資安防護因應而生。題目是時事題，屬於較難且靈活應用題型。

【擬答】

攻擊步驟：
1.偵查階段
防範：使用網路管制與防火牆，禁止高風險網站連線與管制可以存取的網路協定。
2.武裝階段
防範：
(1)若程式或資料庫已知漏洞，若是有重大更新必須更新至最新版本。
(2)使用正版與原廠仍支援更新的作業系統。
3.傳遞階段
防範：資安政策建立跟定期演練，訓練與養成員工不亂點來路不明信件與副檔。
4.開採階段
防範：可以透過防毒軟體與即時防禦系統，阻擋不小心逃過防火牆的惡意程式。
5.安裝階段
防範：此階段已經被滲入，因此有賴於 SOC 監控中的日誌比對、對外連線與流量異常和入侵偵測系統的發現。
6.發令&控制階段與 7.行動階段
防範基本上此階段入侵者已能發動攻擊並執行命令，導致系統設備受到影響，因此要盡快將未感染區域網路隔離，避免持續感染，同時，對外連線阻斷，避免資料外流和傷害擴大；此外，平時不同區域網路應有多道防火牆隔離和權限分離控管，將傷害局限於部分區域而非全部場所。

三、2021年OWASP公布新版網站安全十大安全威脅（OWASP TOP 10 2021），其中前四名分別為：權限控制失效（Broken Access Control）、加密機制失效（Cryptographic Failures）、注入式攻擊（Injection）、不安全設計（Insecure Design）。請說明針對此四項威脅各自的預防措施。（24分）

命題意旨	時事題，考的主旨於OWSAP 2021年的新版本TOP10網站應用程式風險。
答題關鍵	解題應說明OWSAP威脅的變化，若有與2017年版本不同之處，則應說明與解釋變遷的內容與合併理由，各類項目攻擊排名隨著網路變遷，亦有高升下降之分。

【擬答】
(一)權限控制失效(Broken Access Control):
1.威脅：攻擊者利用 Web 的檔案讀取功能，不需透過身分認證，瀏覽需具權限目錄，任意存取系統的機敏檔案或資料，或是進行修改與刪除，更甚者可以進行權限修改與後門建立，簡單來說就是繞道認證頁面而行。
2.防範：
(1)避免暴露與瀏覽根系統目錄資訊。
(2)用於 URL 的輸入的字串需過慮。
(3)重要機敏資料閱讀或是修改，檢查其憑證或是連線會期是否有效。
(二)加密機制失效（Cryptographic Failures）:
1.威脅：2021 年將敏感資料暴露整合加密機制的問題，除了原有資料備份或是傳送未保護外，由於加密機制的不完善或是密碼易被破解，導致機敏資料被攻擊者瀏覽或保存下來。
2.防範：
(1)使用加密連線傳送資料，如 SSL 防護。
(2)傳送機敏的資料的演算法需夠強韌，如 AES-256、PKI 憑證加密。
(三)注入攻擊（Injection）:
1.攻擊：OSWAP:CWEs included are CWE-79: Cross-site Scripting, CWE-89: SQL Injection，把之前獨立的 XSS 跨站腳本整合至注入攻擊。
2.防範：
(1)過濾傳入參數字串的檢查，避免跳過密碼檢查。
(2)禁止回傳系統錯誤訊息。
(3)限制應用程式直接存取資料庫。
(四)不安全設計（Insecure Design）:
1.攻擊：定義了應用程式設計缺陷相關的風險，缺乏不安全設計是指沒有控制措施，商業邏輯也未正常應做出相對應的判斷，導致一般合法使用者無法使用或權益受損。

2.防範：
(1)撰寫單元、整合自動化測試，關鍵流程(存取控制、權限認證、商業邏輯)應驗證可能威脅的測試，如 DDoS、滲透威脅、繞道攻擊、重複消費等。
(2)使用已完成或是經過驗證的元件庫或是安全模組。
(3)採取與建立安全的系統開發週期。

四、ISO27001是廣為國內公務機關或私人企業所遵循資訊安全應用與稽核的國際標準。ISO27001推行以PDCA循環持續地推動ISMS活動落實控制措施。請說明何謂PDCA循環並繪製一圖簡述此循環推動ISMS。ISO27001將組織文件分成四個階層，亦即所謂四階文件，請說明四階文件各階的特質。(24分)

命題意旨	本題在考取ISO27001定義與如何透過PDCA循環落實。
答題關鍵	說明ISO27001主要精神與項目，PDCA是如何推動改善的持續進行。題目要求的IOS 27001四階段文件是關鍵所在，對於班內學生屬於基本型題目，掌握度相當高。

【擬答】
(一)PDCA 循環示意圖:

(圖片引用:行政院資通安全處)

1.Plan(規劃階段)：
建立未來願景、政策、目標與程序，確認服務項目與內容，制定擬定建置團隊與計畫。
2.Do(執行階段)：
系統實作並部署至實體環境，訂定與實作相關規範與作業程序以利日後系統進行維護。
3.Check(檢查階段) ：
根據預期目標，落實業務之檢視衡量、測試演練計畫與評鑑作業，以執行相關作業項目與程序。
4.Act(改善階段)：
依據管理審查管理機制，訂定預期目標改善計畫，落實追蹤並定期督導考核。
(二)ISMS 文件在公務體系通常稱為資訊安全文件。
1.第一階文件→政策性：
說明本部 ISMS 之目標、方向及執行原則。
2.第二階文件→規範性：
針對本部 ISMS 所需訂定之行政規則。規範性文件名稱可命名為規範、要點、注意事項等。
3.第三階文件→程序性：
針對規範性文件中之規定，敘述相關作業之辦理程序。
4.第四階文件→空白表單、紀錄及其他：
(1)空白表單：本部 ISMS 作業所需使用之空白表單。
(2)紀錄：本部 ISMS 作業已填寫資料之表單。
(3)其他：本部 ISMS 作業所產生之文件、報告、計畫及相關參考資料。