《資訊管理與資通安全概要》

一、請說明何謂零信任安全模型（Zero Trust Security Model）？並請條列說明該模型的5項基本原則。（25分）

試題評析	基本的觀念題，只須要詳述概念並盡可能用相關案例說明即可。

答：

(一)零信任安全模型是一種資訊安全的理念和框架，其核心概念是不信任內部和外部網路的任何資源、用戶或設備。這種模型假設內部網路同樣可能受到威脅，因此在存取、驗證和授權方面實行高度的安全措施。

(二)零信任安全模型的五項基本原則包括：

原則	概念	範例
最小權限原則	給予用戶和設備最低程度的權限，只允許他們完成必要的工作，這可以減少可能造成的風險。	金融機構的財務部門只能在工作時間內存取特定的財務資料庫。即使擁有該部門的賬戶，他們也無法在非工作時間或存取其他不相關的系統。
假設遭駭原則	模型不信任內部或外部的任何資源或用戶，無論其所在位置或身份，都會受到最高程度的懷疑。	雲端服務供應商在接收到來自新用戶的資料時，會先將這些資料視為有可能遭受攻擊的對象，並對其進行深度的安全審查，確保其資訊的完整性與可用性。
網路微隔離	將網路資源細分為小的微觀部分，每個部分都有自己的安全性控制，並且彼此隔離，即使一部分受到攻擊，也不會影響整體網路的安全。	醫療機構可能會將病患資訊與財務資料存放在不同的網路區域，以防止敏感資訊泄露。
持續驗證	對訪問者進行不斷的身份驗證和授權，確保他們在線上活動期間的身份和行為都是合法和受信任的。	當用戶嘗試登入企業VPN時，除了密碼之外，系統還要求提供額外的驗證方式，如簡訊驗證碼或生物識別認證。
安全設備監控	時時監控和分析資源、用戶和設備的行為，以檢測和應對可能的威脅和風險。	偵測到異常登入嘗試或非法存取資源時，系統會自動禁止相應的用戶帳戶或IP地址。

這些原則組成了零信任安全模型的基礎，並且幫助組織建立起更強大的安全防禦和管理機制，以應對當前複雜的資訊安全環境。

二、請說明身分驗證（Authentication）和授權（Authorization）的區別，並各提供身分驗證和授權的兩個實際例子。（25分）

試題評析	基本的概念題，除了要照題目說明並給例子外，找到兩者的關聯並加以描述是此題的答分關鍵。
考點命中	《高點・高上資訊管理講義》第三回，蕭維文編撰，頁94、106。

答：

身分驗證（Authentication）和授權（Authorization）是資訊安全中不同但互相關聯的概念：

(一)身分驗證（Authentication）：身分驗證是確認使用者是否是他們聲稱的那個人。它通常用於確定一個人是誰，並要求使用者提供識別自己身份的證據，例如：密碼、生物特徵（指紋或面部識別）或硬體憑證。身分驗證通過後，系統知道使用者是合法的並且可以允許他們訪問資源。

實際例子：

1.使用帳號和密碼登入到電子郵件帳戶。
2.通過指紋或面部辨識解鎖手機。

(二)授權（Authorization）：授權是確定已驗證的用戶能夠存取哪些資源或執行哪些操作。它確保使用者僅能存取他們有權限的資源，不會超越其許可範圍。授權通常基於用戶身份和其擁有的角色或權限。
實際例子：
1.在網站後台管理系統中，管理員具有編輯和刪除內容的權限，而普通用戶只能閱讀。
2.某個應用程式中，某些功能只開放給特定等級的用戶，例如：高級會員才能享有的特權功能。

總括而言，身分驗證是確定身份，而授權則是在身份確認後確定所擁有的權限和可執行的操作。身分驗證後，系統須要授予用戶特定的權限以便安全地存取資源。

三、請說明雲端運算（Cloud Computing）對資訊管理的影響，以及在雲端環境中如何確保數據的安全和法令遵循。（25分）

試題評析	雲端運算在前幾年非常重要，近幾年已經被區塊鏈、人工智慧慢慢取代。在這邊出現雲端運算的考題無非是要考驗同學對於資訊管理的學習是否全面。在答題上，要盡可能和時事結合才能夠在分數上脫穎而出。
考點命中	《高點・高上資訊管理講義》第二回，蕭維文編撰，頁82-92。

答：

(一)雲端運算對資訊管理帶來了多方面的影響，如：
1.可擴展性和彈性：雲端運算讓企業能夠更靈活地擴展資源，根據需求增減計算和儲存空間，避免固定的硬體設置成本。
2.成本效益：企業可以透過使用雲端服務按需支付，避免大規模的初始投資。這使得中小型企業也能夠使用和獲益於高級的資訊管理解決方案。
3.全球性存取：雲端提供全球性的存取，無論用戶所在的位置，都能夠存取和使用資源，提供了全球化的服務。

(二)然而，在雲端環境中確保數據的安全和法令遵循是至關重要的：
1.加密和存取控制：對於重要的數據，必須使用適當的加密技術保護數據的機密性。同時，實施嚴格的存取控制，確保只有授權的用戶才能存取數據。
2.遵循合規性：對於處理個人敏感資訊（如：歐盟的 GDPR 或美國的 HIPAA 等）的組織，必須確保數據處理符合相應的法規和標準。
3.定期備份：建立有效的備份和災難恢復計劃，以應對數據遺失或損壞的情況。
4.監控和審計：實施持續監控和審計機制，以追蹤數據的使用情況和檢測異常活動。
5.供應商的評估：選擇信譽良好的雲端服務供應商，查看他們的安全措施和遵循的合規性。

綜合來說，雲端運算對資訊管理帶來了許多好處，但同時也須要企業重視和投入資源來確保數據的安全性和合規性，以防止潛在的風險和安全問題。

四、請說明數據治理（Data Governance）的概念，並論述其在組織中的重要性和好處。（25 分）

試題評析	基本的概念題，列點與連結實際案例為此題重點。
考點命中	《高點・高上資訊管理講義》第一回，蕭維文編撰，頁5。

答：

(一)數據治理是指管理和控制組織內的數據資產，以確保數據的合法性、可靠性、安全性和可用性的一套制度和流程。它涉及制定策略、標準和流程，以確保數據的正確性、一致性和合規性。

(二)在組織中，數據治理至關重要，其重要性和好處：
1.確保數據品質：數據治理有助於確保數據的準確性、完整性和一致性。這意味著使用者可以信任和依

賴數據進行決策和業務操作。

2.符合法規和合規性：許多行業都有特定的法規和標準（例如： GDPR、HIPAA 等），要求對數據進行保護和管理。數據治理幫助組織確保數據處理符合相應的法律法規和合規性要求。

3.降低風險：通過有效的數據管理和安全措施，數據治理有助於降低數據洩露、遺失或損壞的風險。

4.提高決策質量：良好的數據治理確保了數據的準確性和可靠性，這有助於組織內的決策制定和業務營運。

5.節省成本：透過有效管理數據資產和流程，避免了數據的浪費和低效使用。

6.促進數據共享：數據治理確保數據的標準化和清晰的定義，有助於各部門之間的數據共享和協作。

總體來說，數據治理不僅提高了數據資產的價值，而且有助於組織內部的運營效率和合規性。它是一個綜合性的流程和框架，幫助組織更好地管理、控制和利用其數據資源。