5.1 Trust and Security in the Cloud

5.1.1 關鍵安全術語和概念 (Key security terms and concepts)

降低未經授權訪問敏感資料的風險 (reducing the risk of unauthorized access to sensitive data.)

- **特權訪問安全模型 (Privileged access security model)：** 授予特定使用者比一般使用者更廣泛的資源存取權限，例如系統管理員。需謹慎管理與監控。
- **最小特權安全原則 (Least privilege security principle)：** 僅授予使用者執行其工作職責所需的最小存取權限，降低未經授權存取的風險。
- **零信任架構安全模型 (Zero-trust architecture security model)：** 預設不信任任何使用者或裝置所有存取資源前都必須經過身份驗證和授權。

如何保護自己免受網絡威脅 (how an organization can protect itself from cyber threats)

- **預設安全 (Security by default)：** 從開發初期就將安全措施整合到系統和應用程式中。
- **安全姿態 (Security posture)：** 雲環境的整體安全狀態，評估組織防禦網路攻擊的準備程度。
- **網路彈性 (Cyber resilience)：** 組織承受和快速從網路攻擊中恢復的能力。

基本安全措施(essential security measures)

- **防火牆 (Firewall)：** 根據預定義的安全規則調節網路流量的設備，阻擋未經授權的存取。
- **加密 (Encryption)：** 將資料轉換為不可讀格式的過程，解密則是使用金鑰將其還原。保護金鑰至關重要。

5.1.2 雲安全組件 (Cloud security components)

CIA 資安鐵三角

- **機密性 (Confidentiality)：** 確保只有授權人員可以存取敏感資料，加密是重要的手段。
- **完整性 (Integrity)：** 確保資料準確且未被竄改，例如使用校驗和或數位簽章。
- **可用性 (Availability)：** 確保雲系統和服務在需要時可供使用，透過冗餘、故障轉移和災難恢復計畫來達成。

控制和合規性

- **控制 (Control)：** 為管理和減輕安全風險而實施的措施和流程，例如身份驗證、存取限制和安全意識培訓。
- **合規性 (Compliance)：** 遵守行業法規、法律要求和組織政策。

5.1.3 雲安全與傳統本地安全比較 (Cloud security versus traditional on-premises security)

項目	雲安全	本地安全
位置 (Location)	雲服務提供商的異地資料中心	組織自身的伺服器和基礎設施
責任 (Responsibility)	提供商負責基礎設施， 客戶負責資料和應用	組織負責所有部分
可擴展性 (Scalability)	高，可彈性擴展或縮減資源	較低， 擴展或縮減較耗時且成本高昂
維護和更新 (Maintenance and Updates)	提供商負責基礎設施， 客戶負責應用和資料	組織負責所有維護和更新
資本支出 (Capital Expenditure)	營運支出 (OpEx)，訂閱制	資本支出 (CapEx)， 需自行購買和維護基礎設施

總結

- **雲安全的優勢**：減少基礎設施管理、提供可擴展性和成本靈活性。
- **本地安全的優勢**：對整個基礎設施的直接控制。

5.1.4 Cybersecurity threats 網路安全威脅

1. 欺騙性社會工程 deceptive social engineering : 利用釣魚攻擊等手法，誘騙使用者洩露敏感資訊。
    - 網絡釣魚（Phishing）: 通過偽造電子郵件來收集個人信息。
    - 誘餌攻擊（Baiting）: 下載惡意附件、洩露密碼或洩露敏感資料。
    - 假冒身份（Pretexting）
2. 物理損壞 physical damage : 硬體損壞、電力中斷或自然災害等對資料造成的威脅。
3. 惡意軟件、病毒和勒索軟體(malware, viruses, and ransomware) : 透過惡意軟體干擾營運、造成損害或進行勒索。
    - malware:干擾操作、造成損害或獲取未經授權的電腦系統訪問
    - ransomware: 勒索軟體尤其危險，會劫持關鍵文件直到支付贖金。
4. 脆弱的第三方系統 (vulnerable third-party systems) : 合作的第三方系統若缺乏足夠安全措施，可能成為威脅。
5. 配置失誤 (configuration mishaps) : 資源設定或配置錯誤導致敏感資料暴露，是雲安全中最常見的威脅之一。應採用最小特權和特權存取原則。

總結： 組織應投資於專業知識，以評估、開發、實施和維護強健的資料安全計畫，以應對不斷變化的網路威脅。

5.2 Google's Trusted Infrastructure

5.2.1 資料中心 (Data Centers)

- Google 擁有超過 30 個全球資料中心，強調可靠性、安全性、效率和環境永續性。
- **零信任架構：** 採用客製化硬體和軟體（防篡改、安全啟動、硬體加密）以及嚴格的物理安全措施（存取控制、生物識別）。
- **默認安全 (Security by default)：** 從設計到實施都以安全為優先。
- **網路韌性 (Cyber resilience)：** 具備承受和從安全事件中恢復的能力。
- **效率：** 專用伺服器針對特定任務優化，降低能源消耗，使用電源使用效率 (PUE) 衡量成效。例如芬蘭哈米納資料中心使用海水冷卻。
- **可擴展性：** 可快速容納新硬體和伺服器，處理大量資料和流量。
- **客製化：** 自行管理伺服器和網路，提供獨特服務和功能。
- 長期而言，透過效率和可擴展性可大幅降低成本。

5.2.2 安全儲存 (Secure Storage)

- **加密：** 將資料轉換為不可讀格式，保護資料免受未經授權的存取、丟失或損壞。
- **資料狀態與加密：**
  - **靜止資料 (Data at rest)：** 儲存在物理設備上時加密，Google Cloud 自動加密所有靜止的客戶內容，也可使用 Cloud KMS 自行管理金鑰。
  - **傳輸中資料 (Data in transit)：** 透過網路傳輸時加密，Google Cloud 在多個網路層加密和驗證資料。
  - **使用中資料 (Data in use)：** 計算機正在處理的資料，使用內存加密技術。
- **加密演算法：** 使用高級加密標準 (AES)。

5.2.3 身分 Identity

三個 A：

- **身份驗證 (Authentication)：** 驗證用戶或系統的身份，使用密碼、令牌或生物識別等憑證。雙重驗證 (2SV/2FA/MFA) 增加額外保護。
- **授權 (Authorization)：** 驗證後決定用戶或系統在系統內被允許執行的操作，根據角色和職責分配權限。
- **審計 (Auditing/Accounting)：** 監控和追蹤用戶活動，檢測異常、安全漏洞和政策違規。

身份和訪問管理（IAM）

提供對 Google Cloud 資源的細粒度控制，管理用戶帳戶、角色、權限和審計。

5.2.4 網路安全 (Network Security)

- **零信任網路：** 使用 Google Cloud 的 BeyondCorp Enterprise 驗證每個訪問請求的用戶身份和上下文。
- **保護與本地和多雲環境的連接：** 使用 Cloud VPN 和 Cloud Interconnect 建立安全連接。
- **保護邊界：** 使用防火牆和虛擬私有雲 (VPC) 服務控制，以及共享 VPC。
- **網絡應用防火牆 (WAF)：** 使用 Google Cloud Armor 提供 DDoS 保護。
- **自動化基礎設施配置：** 使用 Terraform、Jenkins 和 Cloud Build 等工具創建不可變的基礎設施，提高安全性並快速修復問題。

當您擴展網絡以包括雲環境時，安全考慮將會有全新的維度。與具有明確邊界的傳統本地設置不同，雲帶來了新的可能性和挑戰。以下是一些策略，以確保您組織的網絡安全並確保您在 Google Cloud 中的寶貴資料和工作負載的安全。

5.2.5 Security Operations 安全營運（SecOps）

重要活動：

- **漏洞管理：** 使用 Google Cloud 的安全指揮中心 (SCC) 識別和修復安全漏洞。
- **日誌管理：** 使用 Cloud Logging 收集和分析安全日誌。
- **安全事件響應：** Google Cloud 提供專家事件響應者。
- **安全意識培訓：** 教育員工關於安全最佳實踐。

實施 SecOps 的好處：

- 降低資料洩露風險。
- 提高正常運行時間。
- 改善合規性。
- 提高員工生產力。

總結：透過以上措施，組織可以有效地保護其在 Google Cloud 中的資料和系統安全。

5.3 Google Cloud 的信任原則與合規性 (Google Cloud's Trust Principles and Compliance)

5.3.1 Google Cloud 的信任原則與透明度報告 (The Google Cloud Trust Principles and Transparency Reports)

Google Cloud 信任原則：

- 您擁有您的資料，而非 Google。
- Google 不會將客戶資料出售給第三方及用於廣告。

- 所有客戶資料預設都經過加密。
- 我們防範內部人員未經授權存取您的資料。
- 我們絕不給予任何政府實體「後門」存取權限。
- 我們的隱私實踐按照國際標準進行審計。

透明度報告與獨立審計：

- 提供透明度報告，揭示影響隱私、安全和資訊存取的政府和企業行動。
- 接受獨立第三方審計和認證，符合業界標準。
- 參與《歐盟雲端行為準則》等倡議。

5.3.2 資料落地與資料主權 (Data Residency and Data Sovereignty)

資料主權 (Data sovereignty)： 資料受其所在國家法律和法規管轄的法律概念。例如歐盟的 GDPR。

資料落地 (Data residency)： 資料儲存或處理的物理位置。一些國家或地區有法律或法規要求資料必須儲存在其境內。

Google Cloud 如何應對資料落地需求：

- 透過地區 (regions) 控制資料的物理位置，每個地區包含一個或多個資料中心。
- 提供組織政策約束 (Organization Policy constraints) 和 IAM 配置，防止資料意外儲存在錯誤的地區。
- 提供 VPC 服務控制 (VPC Service Controls)，根據定義的邊界限制網路存取。
- Google Cloud Armor 允許限制外部負載平衡器的流量位置。

5.3.3 產業與區域合規性 (Industry and Regional Compliance)

- **Google Cloud 合規資源中心：** 提供關於認證和合規標準的詳細資訊，以及區域和行業特定法規的文件。例如 HIPAA 和 PCI DSS。網址：cloud.google.com/security/compliance
- **Compliance Reports Manager：** 提供按需存取關鍵合規資源的平台，包含 ISO/IEC 證書、SOC 報告和自我評估。網址：cloud.google.com/security/compliance/compliance-reports-manager
- Google Cloud 的工程師和合規專家團隊與使用者合作，創建綜合的控制和治理框架，確保強大的合規態勢。

總結：Google Cloud 致力於提供安全可靠的雲端環境，並透過信任原則、透明度報告、資料落地和主權控制，以及符合產業和區域法規等措施，協助使用者達成合規要求。