

## 個資上雲落實保護之實務探討

# 將個資保護責任帶上雲 落實雲端共享安全責任

個資保護有望在新的年度進入實質的監管階段，現今幾乎資訊服務都要上雲的狀況，落實個資保護的方方面面，將是雲端業者與用戶要直接面對的課題。

文／林逸塵（國立政治大學資訊管理博士）

雲端運算是透過網路，以便利及隨選所需的方式存取共享式運算資源池（例如網路、伺服器、儲存空間、應用程式與服務）的運作模式，所提供的運算資源只需最少的管理作業，就能快速配置與發佈運算資源。提供清晰且全面的雲端服務框架，用於理解雲端運算及服務模型，能為規劃者、專案經理及技術人員提供概念性指導。

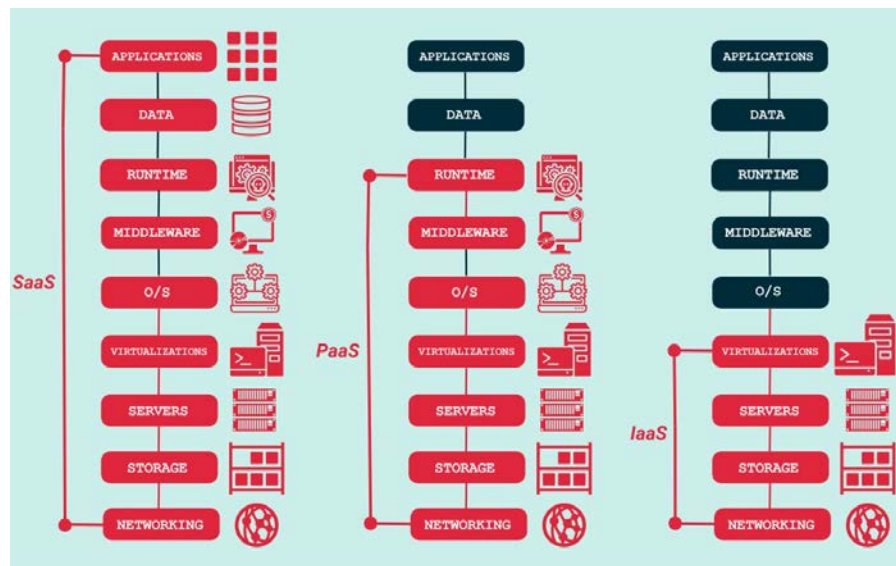
依照美國國家標準與技術研究院（NIST）所定義雲端安全標準，包含

五項基本特性：

- (1) 隨需自助服務 (On-demand Self-service)
- (2) 廣泛網路存取 (Broad Network Access)
- (3) 資源池化 (Resource Pooling)
- (4) 快速彈性 (Rapid Elasticity)
- (5) 衡量服務 (Measured Service)

三種服務模型：

- (1) 軟體即服務 (SaaS)
- (2) 平台即服務 (PaaS)
- (3) 基礎設施即服務 (IaaS)



圖一、紅色區域為 CSP 責任區；綠色區域為 CSC 責任區。

四種部署模型：

- (1) 私有雲 (Private Cloud)
- (2) 社區雲 (Community Cloud)
- (3) 公有雲 (Public Cloud)
- (4) 混合雲 (Hybrid Cloud)

無論是雲端服務供應商 (Cloud Service Provider, CSP) 或雲端服務客戶 (Cloud Service Consumers, CSC)，各角色最終仍是彼此分工建立解決方案，CSC 藉此無需在本地球端 (On-Premise) 部署，避免複雜實作與龐大人力成本負擔，而在雲端服務模型的資安責任因不同的角色責任分擔仍有所區別。（見圖一）

## 雲端服務隱私風險控制

雲端服務 (IaaS、PaaS、SaaS) 所帶來的便利性及彈性，使各領域使用雲端服務的發展迅速，PaaS 和 IaaS 主要偏向開發團隊使用，相對於 SaaS 的應用範圍則更廣泛，可能會包含終端使用者及非技術部門，其共通點都會蒐集、處利及利用大量的客戶資料。為了保護雲端上的個人資訊隱私，應聚焦雲端服務在使用模式中，所面臨的**資料安全與生命週期管理 (Data Security and Privacy Lifecycle Management)** 相關議題。

本期首先介紹**雲端共享安全責任 (Shared Security Responsibility, SSR)** 概念，可發展為雲端應用的基本安全原則、控制項目及準則，在共同的概念基礎下，CSP 與 CSC 得以安全地導入、評估及管理雲端服務，以控制隱私風險，清楚劃分責任歸屬。

## 雲端共享安全責任 (SSR)

雲端服務的跨區域性與特定國家或法規有所關聯，個人資料保護須透過了解雲服務情境下的控制措施的歸屬責任，以促進產業或領域的參考作法。在符合主要隱私法規的共同要素及要求下，組織決定採用雲端服務的首要考量，在於雲端控制措施要能兼顧可執行性。

當資料由 CSC 蒐集、建立到銷毀的過程，須涵蓋完整的資料生命週期，例如從執行資料分類、盤點、保存與銷毀程序，經由識別其風險層級進行控制，此舉將有助於 CSP 與 CSC 共同保護隱私相關資料，更能確保資料在生命週期中有效安全管理。

雲端共享安全責任 (SSR) 實現**透明性與問責性**，將資料保護落實於雲端生態系。

舉例而言，CSP 負責雲端架構的安全，提供 CSC 安全的資料儲存、存取與銷毀等機制；CSC 則負責雲端中資料的安全。若套用在雲端服務使用情境下，CSC 應運用

CSP 提供資料加密與存取控管的保護功能，確保雲端服務遵守資料隱私法規，由 CSP 與 CSC 共同維護穩健、合規的雲端控制項目，達到當責性的效果。

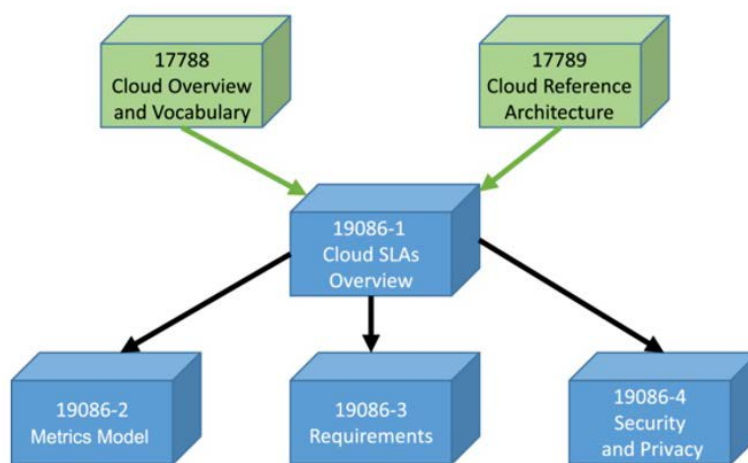
## 國際標準下的 SSR

在資訊安全的國際標準有定義雲端資安規範，例如 ISO/IEC 27001:2022 A5.23 雲端服務與資訊安全，要求建立獲取、使用、管理及退出雲端服務的流程。ISO/IEC 27017 與 ISO/IEC 27001 系列標準配合使用，為雲端服務提供者、雲端服務客戶提供了加強控制。

與許多其他技術相關標準不同，ISO/IEC 27017 標準闡明了雙方在雲端服務中，客戶和服務提供者各自需要負起的安全責任。而 ISO/IEC 27018 則是針對公共雲端服務中保護**個人可識別資訊 (Personally Identifiable Information, PII)** 提供指引，特別適用於 CSP 擔任 PII 資料處理者的情境，將標準建構在 ISO/IEC 27002 之上，提供專為雲端環境設計的控制措施與原則，確保雲端服務提供者能以負責、透明且安全的方式處理 PII。

ISO/IEC 19086 建立雲服務服務等級協議 (Service Level Agreement, SLA) 的共同概念。(見圖二)

為促進雲端運算生態系中有效且全面的安全與隱私風險管理。無論組織的類型是 CSP 或 CSC，會因為不同的企業規模 (大型企業或小公司) 採取不同



圖二、ISO 19086-1: 2016 建立雲服務 SLA 的共同概念。

的雲端部署模式 (IaaS、PaaS、SaaS)，建立雲端共享安全責任 (SSR) 可用於劃分、實施及強制執行安全需求並監控其落實情形。協助公司將其內部的組織、營運與法規轉化為一套標準，形成與個資保護相關的資安政策、程序與技術控制目標。

根據內部風險評鑑，組織首先要辨識出需要保護與業務流程相關資訊的機密性、完整性與可用性。而這些資料集 (Data Sets) 通常具有不同的敏感性與關鍵性，尤其是資訊儲存在雲端資料庫，透過不同的雲端應用程式負責處理，及分別由 CSP 或 CSC 共同執行安全管理的責任。

組織可以利用 SSR 來識別具體的政策、程序及技術需求，並界定責任區納入組織安全計畫的控制目標，透過控制目標來強制執行，達成內部使用者、業務夥伴及雲端業者等利害關係人的相關要求，以及監控內部政策與外部合規性要求的遵循情形。

至此，CSP 與 CSC 透過符合全球隱私原則強化彼此信任，並釐清雲端服務供應商與客戶間的角色責任，使雲端服務供應商滿足監管與契約義務，促進 PII 處理的透明度、可稽核性與責任制，進一步導入隱私設計 (Privacy-by-Design, PbD) 在雲端服務開發中的應用。

### 資料安全與生命週期管理

資料安全與生命週期管理是 CSP 與 CSC 對於客戶隱私與資料安全的承諾，落實管理措施並非針對特定產業或部門，亦不專屬於某一特定國家或法規。然而，這些控制措施要考量主要隱私法規的共同要素與要求，對於雲端服務而言，通常要適用於全球各地的組織，並預期作為可執行的行動基準，CSP 與 CSC 要特別瞭解資料流的地域性規範，例如在某些特定國家、地點或部門營運的組織，可能必須實施當地所規定或補充的資料保護控制要求。

完整的資料生命週期包含從資料建立到銷毀的過程，依資料類型、資料分類、盤點清查、保留及處置程序，應對齊所適用之法律、法規、標準及風險等級進行適當處置，使 CSP 與 CSC 當責保護其擁有資料，以遵守個人資料保護相關法規。

在 SSR 分責治理框架下，大致上 CSP 負責雲端

環境安全 (Security of the Cloud)，提供 CSC 安全的資料儲存、存取與處置機制。另一方面，CSC 則負責保護其在雲端上儲存或處理的資料 (Security in the Cloud)，進行資料分類、資料安全的規劃，並利用 CSP 提供的資料保護、加密設定功能，以及透過指定存取權限的不同等級，提升雲端資料的整體安全與隱私，這種 SSR 責任共同承擔的模式，可促成 CSP 與 CSC 共識經營強健符規的雲端基礎環境，並且對於雙方在責任的歸屬產生實質的效益。(見表一)

### 資料安全與控制目標

雲端共享安全責任在三種主要雲端服務模式 (IaaS、PaaS、SaaS) 會有所區分，主要依當責性而指派為實作特定控制措施，使不同的責任分區在 CSP 與 CSC 間進行分配，有些控制是明顯屬於 IaaS 提供者的職責範圍 (例如雲端資料中心的安全控制、實體安全、基礎設施安全)，而某些控制則適用於所有服務模式 (例如身分與存取管理)。

這些控制項目著重於多個面向，包括實體、網路、運算、儲存、應用與資料等，此外更有助於各種法律與監管框架中，依照現有的安全規範進行對應，以便於決定採用雲端服務的政府機關、企業組織進行評估，哪些能力符合適用的法規與最佳實務作法。

再者，這些控制措施與組織業務活動具有高度相關性，並且與雲端服務的營運職能高度相關，理想的實施上所涵蓋的職能包括：資訊安全 (Cybersecurity)、內部稽核 (Internal Audit)、架構師 (Architecture Team)、軟體開發 (Software Development Team)、營運 (Operations)、法務 (Legal/Privacy)、風控治理 (Governance/Risk/Control)、供應商管理 (Supply Chain Management) 及人力資源 (Human Resources)。

雲端服務用戶可使用控制目標及項目來執行下面的操作：

- (1) 將組織、營運與法律需求對應至控制目標、
- (2) 建立雲端營運的風險管理計畫、
- (3) 建立第三方風險管理計畫、
- (4) 建立內部與外部的雲端稽核計畫。

共享安全責任	說明
控制者 CSP擁有	<ul style="list-style-type: none"> <li>• 控制的所有權與實作責任屬於 CSP。</li> <li>• CSP 對控制目標的實作負有全部責任與問責。</li> <li>• CSC 對控制目標的實作不負責任。</li> </ul>
控制者 CSC擁有	<ul style="list-style-type: none"> <li>• 控制的所有權與實作責任屬於 CSC。</li> <li>• CSC 對控制目標的實作負有全部責任與問責。</li> <li>• CSP 對控制目標的實作不負責任。</li> </ul>
控制者 CSP、CSC共享 (獨立型)	<ul style="list-style-type: none"> <li>• 控制的所有權與實作責任由 CSP 與 CSC 共同承擔 (雙方皆應實作)，但雙方之間沒有實作的相依關係。</li> <li>• CSP 與 CSC 共同分擔控制目標的實作責任與問責。</li> </ul> 例如： <ul style="list-style-type: none"> <li>• 由 CSC 進行的獨立稽核不會影響 CSP，反之亦然。</li> <li>• CSP 與 CSC 都必須進行訓練演練，但需彼此獨立進行。</li> </ul>
控制者 CSP、CSC共享 (相依型)	<ul style="list-style-type: none"> <li>• 控制的所有權與實作責任由 CSP 與 CSC 共同承擔，且兩者之間存在實作的相依關係 (其中一方必須為另一方提供支援以落實該控制應日)。</li> <li>• CSP 與 CSC 共同分擔控制目標的實作責任與問責。</li> </ul> 例如： <ul style="list-style-type: none"> <li>• 應允許變更其靜態資料儲存的地理位置，以便 CSC 將其資料移動到所需的地理位置。CSC 也應選擇其期望的位置，以便 CSP 協助進行移動。</li> <li>• CSP 提供身分與存取管理工具和功能予 CSC，但 CSC 需要適當地配置存取權限。</li> </ul>

表一，CSP 與 CSC 共享安全責任類型。

組織建立雲端風險管理計畫時，要設定控制項目來衡量、評估並監控，將 CSP 相關的風險納入有下列的好處：

- 用戶易於了解其自身安全需求與 CSP 具備安全能力之間的差距，用戶使用控制項目來識別風險轉嫁後的補償性控制。
- 建立第三方風險管理計畫時，資料安全的控制目標使用戶在整體服務生命週期中評估雲端服務，明確雲端模式的責任歸屬。
- 在採購雲端服務前進行評估，比較不同 CSP 的服務提供及控制差異，使服務監控與內部需求達一致性。

雲端服務的供應商透過控制目標，提供給 CSP 應遵循的內部安全計畫，以建立特定或經業界驗證的最佳實務。包含：

(1) 建立成熟且業界公認的最佳實務為基礎的內部安全計畫。

- (2) 促進與商業夥伴及客戶之間的溝通與互通性。
- (3) 展現對安全的承諾並透明地揭露安全態勢。
- (4) 透過控制目標與其他國家及產業框架中的控制項間建立對應 (例如 ISO 組織、NIST CSF、PCI DSS 標準等)，以簡化合規性。
- (5) 減少回應客戶評估所需時間與成本。
- (6) 藉由計畫執行向監管機構展示對資料安全性承諾。
- (7) 制定雲端內部與外部稽核計畫。



作者林逸塵任職於個人資料保護委員會籌備處隱私科技組組長，具有多年資訊安全及資訊管理相關經歷，專業領域在個人資料安全維護、資通安全、人工智慧、系統設計科學、資訊策略及新興技術應用，並曾發表多篇相關領域主題的文章及學術期刊。