資料治理的數據風險管理與推動建議

葉耿志　勤業眾信風險管理諮詢股份有限公司副總經理

摘要

近年來，各級政府機關（構）開始推動資料之應用與治理，資料治理顯然已成為相當重要之角色。組織於開始進行資料治理之初，應重新檢視各類資料於該組織中所存在的價值，進而藉由價值之產生，制定符合組織文化之資料治理框架，鏈結組織業務特性之策略內容，最後再透過資料保護之推動方法，達成組織資料治理之目的。

關鍵字：資料治理價值、資料治理架構、資料治理推動建議、資料保護方法論

壹、資料治理之組織價值

勤業眾信認為，在資料治理方面，組織用於管理所有資料的內部治理程序，應採用一致性的應用標準，以及更廣泛程度地利用資料資產來為業務衍生更多價值。茲針對為組織帶來之價值說明如下：

一、保護使用者資料

資料治理流程（例如資料探索、分類、保留和處置，以及存取管理）有助於追蹤和管理使用者資料，進而降低資料遺失和未經授權的存取風險，並遵循個人資料保護法規和使用者存取要求。

二、保護組織資料

隨著電子化政府的飛速發展，知識財產權和其他組織資料變得越來越有價值。組織資料治理將有助於追蹤、管理和保護組織資料，從而減少違反法規或意外洩露。

三、提昇使用者體驗

數位政府資訊服務使用者越來越希望獲得無縫的客戶體驗，並且與潛在資訊服務使用者的接觸點將繼續增加，進而幫助簡化客戶體驗並維護寶貴的關係。

四、驅動組織決策制定

了解可用的資料資產，提高資料可靠性與可存取性，以及了解如何匯總和利用資料資產幫助政府部門推動創新的應用體驗並探索數據趨勢，以支持執行決策。

貳、資料治理框架

基於組織資料治理所帶來之價值，資料治理推動過程中，將面臨組織、流程、技術、人員等各式風險，為有效降低其對組織帶來之影響，勤業眾信建議組織應建立符合其組織特性之資料治理框架，將有助於增強資料完整性，可用性和安全性，並支持組織業務決策，降低推動。

一、治理層級

提供組織整體策略指導和資金，以確認資料治理政策、流程、標準和架構的實施範圍和資源；組織應針對本身組織模式，設定合適的角色權責分工，並依組織模式決定是否設置專責人員，負責推動組織資料治理事宜，協助訂定整體運作流程與程序、推動政策與標準，以及如何衡量資料治理推動之績效模式。

二、策略鏈結

基於組織業務需求，啟用或調整組織資料治理功能之要求。以行政院為例，交通部、內政部、衛生福利部等，各單位因負責業務不盡相同，所擁有的資料內容大相逕庭，因此各單位推動資料治理，應考慮如何與其組織主要業務策略進行鏈結，針對各業務需求進行資料治理方向、資料功能、資料內容等各項工作之調整，以符合其業務推動方向，達成策略目標進而實現該單位組織之價值。

圖 1　組織資料治理架構圖

資料來源：作者提供

三、資料治理

資料治理元素之相關政策與標準，將支持資料品質、完整性、可用性與安全性。由於各單位資料累積已久，各式資訊系統與紙本資料類型繁多，在推動資料治理的過程中，組織應先訂定各資料元素之政策與標準，包含資料政策、生命週期、資料標準（如資料格式、資料型態）、資料安全管理等，再針對過往資料進行調整，未來新資料產生亦需遵循上述政策與標準之要求。

四、資料治理能力

資料治理的核心服務能力，針對組織資料治理推動方向，決定其產出之內容與品質。組織必須針對資料政策與標準，進行組織之主資料界定與資料品質之有效管理，並養成組織資料治理之能力，保護組織資料安全。

五、資訊基礎架構服務

針對資料治理服務之交付與品質，建立其底層資訊基礎架構。此部分為資訊基礎架構之基本功，透過組織資料生命週期之制定，定義資料獲取、使用、整合、聚集、儲存、分析等各項活動，進而提供滿足該活動之資訊基礎架構，以便組織推動資料治理時，提供符合業務需求之資料資訊服務。

六、人員

建立資料治理能力、技能和可持續推動資料治理所需的人員和變更管理。組織在推動資料治理過程，人員乃是非常重要的一項因素，因此透過每年定期宣導，亦或是內外部教育訓練，說明資料治理於組織之重要性，進而形塑組織資料治理文化，養成人員資料治理能力與行為，並可透過知識管理機制之建立，方便人員分享資料治理之知識與經驗，將更有助於組織資料治理事務之推動。

參、資料治理之資料保護推動建議

組織為了提昇資料本身與衍生之價值，除了針對資料治理制定符合自行需求之資料治理架構外，亦應注意資料治理所帶來之風險議題。因此，該如何於進行資料治理過程中，推動資料保護之風險議題亦應特別留意。例如近年來網路攻擊事件增加、組織因管理措蒐不足造成資料外洩、隱私法規日益嚴格等各項因素，皆顯示出資料保護不當為組織帶來之風險。因此，如何在資料治理推動過程中，兼顧資料保護之議題，進而降低衍生之風險，勤業眾信建議可以採用資料保護方法論，讓組織可以更易於了解他們蒐集、儲存、處理和共享的個人和組織機密資訊。

組織可依據下列初步評估與五大階段之步驟作法，規劃與實施合適之解決方案，提昇當前資料保護的成熟度，以及降低資料未完善管理之風險。茲針對資料保護之推動，說明五大階段之重點內容如下：

一、資料保護之規劃

（一）目的

組織需要建立專案計畫，並蒐集內外部需求，建立該專案計畫所需之資料，具體包括如下：

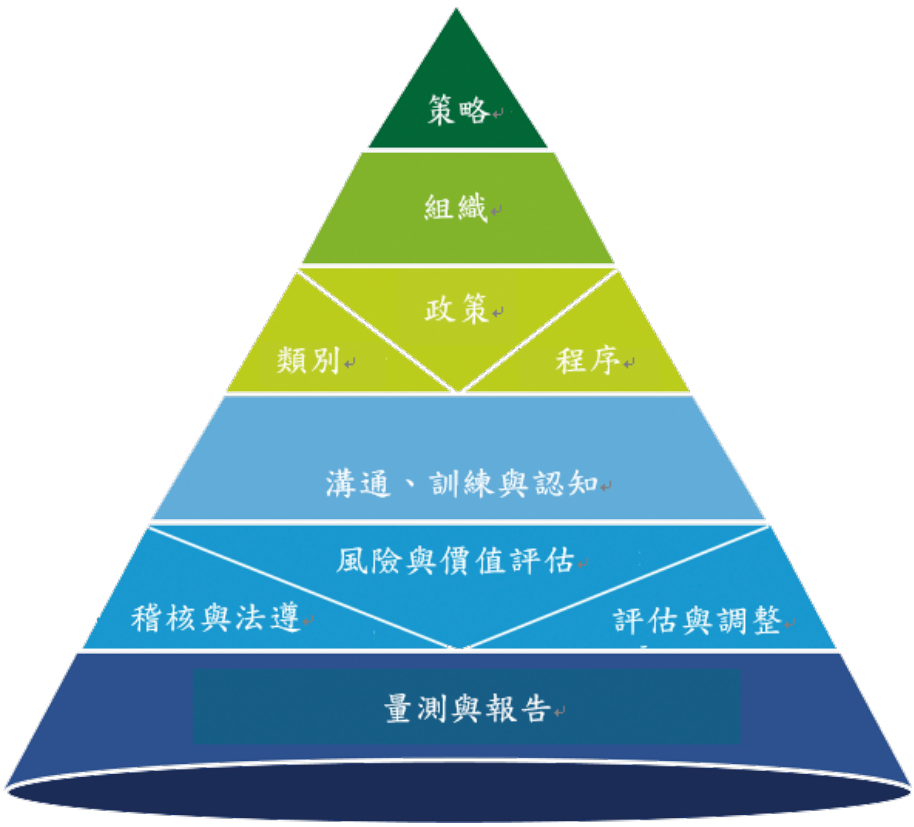

圖 2　組織資料保護方法論

資料來源：作者提供

1. 了解組織業務目標，利益相關者的優先事項和觀點，例如各中央部會業務推動方向、各地方政府施政方針。

2. 帶領利益相關者達成共識和資料保護願景，組織可針對利益相關者訂定合適資料保護方向，並可列入組織資料保護政策之內容。

3. 與利益相關者建立並維護有關資料保護目標的協議，以公部門而言，建議可以作為以政策宣告與官網公告方式，說明其資料保護之機制與方式。

（二）主要工作

1. 建立一個高階專案計畫，用以管理與該專案相關的活動和預期交付成果。

2. 確定業務和技術主題專家人選，以便專案執行過程中參加訪談與研討會。

3. 蒐集組織現有相關文件，如政策、程序、參考指引等。

4. 建立預計舉辦之訪談與研討會時間表。

5. 安排並舉行專案啟動會議。

二、資料保護需求分析

（一）目的

根據對組織資料保護要求，進行識別和分析，基於適用法律、法規、國際標準、合約義務和國家政策等，建立資料保護與控制框架。如國家發展委員會是否訂定相關資料治理之政策、個人資料保護法等。

（二）主要工作

1. 與國家政策顧問和其他主題專家合作，確定法律、法規、國際標準和合約資料保護要求來源，以將其納入資料保護框架。

2. 組織可以在資料需求和控制活動中，針對治理、業務流程和功能／技術類別等面向進行分類。

3. 可依照資料類別和子類別，並引用需求來源，藉以辨識關鍵的外部需求，定義出資料保護和控制框架的通用需求內容。

三、資訊基礎環境分析

（一）目的

組織應透過研討會、訪談、文件審查、問卷，以及對自身環境（例如，資料類型、業務功能、業務流程、資訊系統、人員等）的熟悉程度，找出與先前建立的資料保護要求和控制框架間的具體差異。

（二）主要工作

1. 識別資料元素、業務單位、業務功能、業務流程和資訊系統，並確定其優先等級。

2. 執行業務流程和資訊系統資料流分析。

3. 依據資料保護要求和控制框架執行業務流程和資訊系統差異分析。

4. 依據資料保護要求和控制框架進行治理差異分析（例如角色和職責、政策和程序、培訓和意識、監控和報告等）。

5. 依據資料保護要求和控制框架進行資訊技術資料保護差異分析（例如，資訊安全控制、存取控制、加密、安全事件監控、漏洞管理等）。

四、資料保護之策略與建議

（一）目的

組織應針對資料保護環境分析過程中發現的差異，制定資料保護策略並擬定改善建議。

（二）主要工作

1. 組織應將資訊基礎環境分析結果，分類至潛在改善項目中。

2. 組織應依據先前制定之標準，對改善項目進行優先順序排序。

3. 組織應針對每個確定的改善項目建立一份報告，並記錄以下內容：

   - 目標
   - 範圍
   - 降低風險
   - 估算預計完成時間

- 依賴關係和限制
- 所需技能與預算成本
- 重要注意事項

五、資料保護解決方案建置

（一）目的

組織應開始實施資料保護策略和建議，進行相關程序開發的活動和預期可交付的成果。

（二）主要工作

1. 制度架構

- 資料保護組織架構：記錄資料保護角色和職責，以及相關流程。
- 隱私聲明：向使用者或個人提供有關資訊蒐集、處理、利用之活動通知。
- 資料保護政策（例如，隱私政策、資料分類政策等）：概述有關尊重個人隱私和保護其個人資訊的組織政策。

2. 制定流程和程序

- 隱私流程（例如，同意處理、存取請求處理、客訴處理、事件通報等）：允許使用者個人行使選擇權、獲取並更正其個人資訊、提交隱私投訴並通報隱私事件的流程。
- 資料保護培訓和意識：培訓和意識計畫，基於內外部教育訓練的培訓、訊息交流等，以提高組織全員對隱私責任的意識。
- 監視和報告：制定資料保護指標，用於監控隱私保護運作情形。
- 第三方資料保護風險管理流程：監控第三方個人資訊共享風險的流程機制（例如，風險評估、合約條款、定期與不定期查核等）。

3. 實施流程

- 跨境轉移機制（例如，資料保護安全港、合約範本、公司政策等）：合法地將個人資訊轉移出某些國家（例如，歐盟）的機制。
- 監管註冊（例如，歐盟數據保護局）：向國際間監管機構註冊資料處理活動。

肆、結論

綜合上述說明，勤業眾信建議基於資料治理的數據風險，可依上述各階段進行推動。首先，組織可搭配近年來電子化政府之推動，定義資料治理對於組織本身所衍生之價值，例如提昇國民於資料應用之體驗感受，並可讓組織依相關資料分析結果決策未來國家各領域之政策方向。當資料越來越活用，持續產生其資料價值後，組織可開始思考定義資料治理框架，並依照前述資料保護推動建議，逐步建立符合自身需求與文化特性之框架內容，以完善組織資料治理機制。