【PIMS 個資管理系列】之二

ISO/IEC 27701 隱私保護國際標準解析

——條款 5 和 6

基於資訊安全要求的延伸隱私保護

撰文：BSI 英國標準協會客戶經理
孫文良（Sunny Sun）

誠如前文所言，在資訊安全方面，ISO/IEC 27001 已是國際上公認為資訊安全管理系統的首要標準。現今組織業務運作上，大多數需依賴資訊系統的支持，才能使業務有效率的達成，進而為組織產生價值。然而，組織會先面臨到的是資訊安全的挑戰──就因為組織有價值，所以會成為外部威脅的目標。除非組織選擇不進行業務，實難以改變外來威脅且不能完全阻止事故的發生，所以，組織可以利用管理系統來降低發生機率與造成影響的程度，並於發生事故之後利用經驗學習與持續改善，使得未來不會再發生相同的問題或是將風險降至最低。

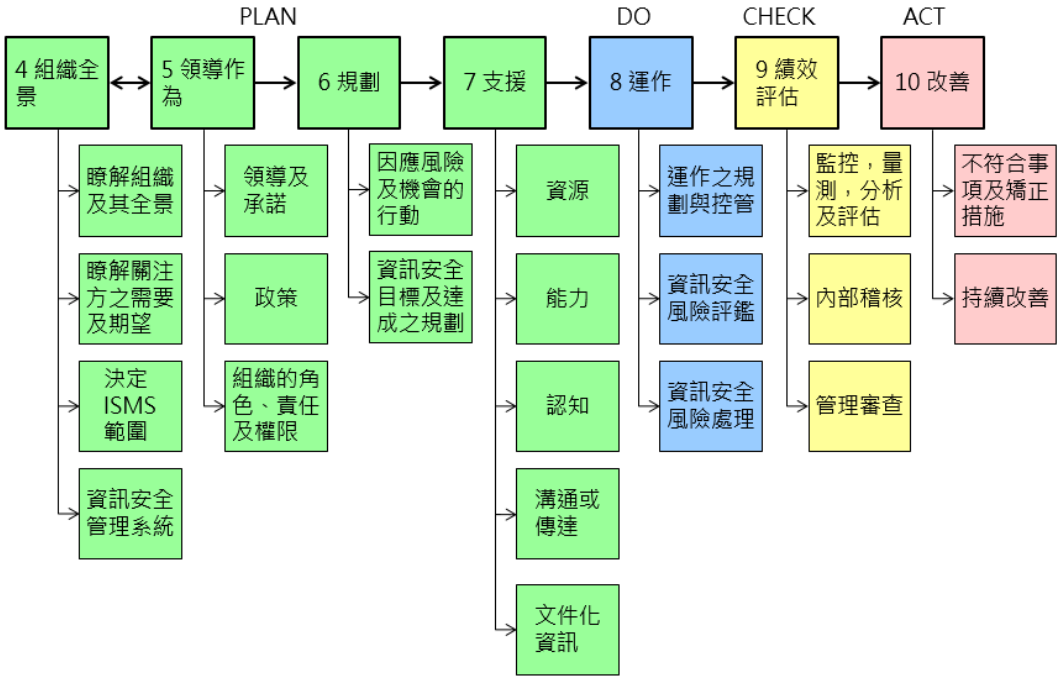
ISO/IEC 27701 遵循管理系統持續精進改善的方式，在既有的資訊安全管理系統 ISMS 之上，同時延伸補充個人資料管理的要求和實務指引。就組織風險管理的角度，業務對資訊系統存在依賴性，資訊安全管理成為組織不得不考量的重要議題，而個人資料管理就會與資訊安全無法脫鉤，即沒有妥善的資訊安全管理，就難以證明可確保個人資料的安全，這就是 ISO/IEC 27701 架構在 ISO/IEC 27001 上的目的，組織就可以在原 ISO/IEC 27001 資訊安全管理的架構上，增加對個人資料管理的遵循要求，對個人資料產生保護效果。

ISO/IEC 27001 標準的內容架構

ISO/IEC 27001 資訊安全管理系統，是依 ISO Annex SL 的高階結構設計，而管理系統導入與稽核流程是依循條款要求，是由條款 4~10 進行實作。

ISO/IEC 27001:2013 標準章節
0. Introduction 簡介
1. Scope 適用範圍
2. Normative references 引用標準
3. Terms and definitions 用語及定義
4. Context of the organization 組織全景
5. Leadership 領導作為
6. Planning 規劃
7. Support 支援
8. Operation 運作
9. Performance evaluation 績效評估
10. Improvement 改善
Annex A (normative) Reference control objectives and controls 附錄A (規定) 參考控制目標及控制措施

以另一種方式來看 ISO/IEC 27001 條款 4~10，以 PDCA 方式區分，條款 4 組織全景、條款 5 領導作為、條款 6 規劃與條款 7 支援，組織需先瞭解其全貌、評鑑風險、界定出其管理系統的範圍，高階管理層需給予必要的資源與支持，並需產出必要的文件，也就是進行所謂的計畫（Plan）階段。條款 8 著重在運作，在 Plan 階段程序有了，組織照表操課，依計劃進行（Do）。條款 9 在對運作狀況進行績效評估，組織會利用監控量測、內部稽核與管理審查的方式進行確認(Check)，做出必要性決策的產出。條款 10 就依決策的結果，進行相對的改善實踐（Action）。整個管理系統就是依此精神來做持續不斷的精進循環。



ISO/IEC 27701 條款 5 與 ISO/IEC 27001 相關的 PIMS 特定要求

ISO/IEC 27701 條款 5 內容敘述為在 ISO/IEC 27001 條款擴展對隱私保護的要求（條款 5.1~5.8.2）。因為各標準的制度面要求都依循一樣的架構，相對比較容易整合，簡單來看 ISO/IEC 27701 在 ISO/IEC 27001 增加的部份。

依 ISO/IEC 27701 標準的基本要求，將資訊安全的要求擴展到在 PII 處理時的隱私保護。原本組織在進行資訊安全管理時，僅要瞭解對影響資訊安全的內部、外部議題與利害關係人，而在 ISO/IEC 27701 組織需要先確認面對個人資料處理的是屬於何種角色（控制者、共同控制者或處理者），此部份與 BS 10012、GDPR 的要求相同。由於組織在角色上的差異，對其產生影響的內部、外部議題與利害關係人也會相異，直接反應在管理系統標準上適用的控制措施選擇就不同。在利害關係人部份則增加包含其他的 PII 控制者、PII 處理者，其中最大的差異是必需包含 PII 資料主體，此利害關係人的差異部份在 ISO/IEC 27001 資訊安全管理系統中就無特別要求。另外，在 ISO/IEC 27701 的實施範圍部份要求是必需包含 PII 的處理活動，簡單來說，如定義範圍沒有任何 PII 的處理活動，就無法實施。

ISO 27001本文條款	ISO 27701條款5要求	核心重點
N/A	5.1 一般要求	ISO 27001擴展至PII處理時的隱私保護
4.1	5.2.1 瞭解組織及其全景	1.確認PII角色(控制者、協同控制者與處理者) 2.瞭解有關影響PII達成的內外部議題
4.2	5.2.2 瞭解利害關係人之需要及期望	瞭解對PII處理的利害關係人
4.3	5.2.3 決定資訊安全管理系統之範圍	範圍必需包含PII的處理
4.4	5.2.4 資訊安全管理系統	依ISO 27001條款4至10實施並依ISO 27701條款5進行擴展
6.1.2	5.4.1.2 資訊安全風險評鑑	1.應用風險評鑑流程，識別PII處理的風險 2.風險發生之潛在影響考量需包含組織本身與PII主體
6.1.3	5.4.1.3資訊安全風險處理	1.比對確認ISO27701附錄A、附錄B，ISO 27001附錄A的控制措施 2.依組織PII角色建立適用性聲明

組織在風險評鑑部份，最重要的是要先能識別風險。ISO/IEC 27701 要求在 PIMS 範圍內，組織可以利用原來的資訊安全風險評鑑流程來進行機密性、完整性、可用性相關影響風險的確認，並增加要求要有隱私風險評鑑流程來識別與 PII 處理相關的風險。不論組織選擇的方法論為何，重點是要確保評鑑流程能讓資訊安全與 PII 保護之間被適當的管理。而識別風險之後，則要對潛在影響做分析評鑑。新的要求將識別出的風險除了原本在 ISO/IEC 27001 對組織本身潛在影響，增加要求必需對 PII 資料主體的進行考量，這呼應了對利害關係人的要求差異，例如：發生對個人資料有影響的風險時，勢必對 PII 資料主體產生某種程度上的影響。組織不能再單純以只思考對自身的潛在影響，

這點是在原來 ISO/IEC 27001 沒有要求到的點，在 ISO/IEC27701 與 BS10002 的要求是有一致性的。

風險評鑑後的風險處理，ISO/IEC 27701 要求需與 ISO/IEC 27701 的附錄 A、附錄 B 及 ISO/IEC 27001 的附錄 A 的控制措施進行比較，確認沒有遺漏掉任何必要的控制措施。在 ISO/IEC 27001 資訊安全控制措施要求依序為 A.5 資訊安全政策、A.6 資訊安全之組織、A.7 人力資源安全、A.8 資產管理、A.9 存取控制、A.10 密碼學、A.11 實體及環境安全、A.12 運作安全、A.13 通訊安全、A.14 系統獲取、開發及維護、A.15 供應者關係、A.16 資訊安全事故管理、A.17 營持續管理之資訊安全層面，最後到 A.18 遵循性。而 ISO/IEC 27701 的附錄 A 與附錄 B，就是對 PII 控制者與 PII 處理者的控制措施要求（在後續文章會介紹），差異點在選擇 ISO/IEC 27001 附錄 A 控制措施時，除原資訊安全風險外必需要再包含考量對 PII 處理與 PII 資料主體的相關風險。

組織必需依 ISO/IEC 27701 附錄 A、附錄 B 與 ISO/IEC 27001 附錄 A 中選擇出控制措施，與 ISO/IEC 27001 一樣建立適用性聲明，與 ISO/IEC 27001 不同之處在於必需包含組織依處理 PII 的角色對決定排除控制項目的理由。由此可知，依據組織角色確定的不同，適用性聲明對控制措施的選擇就相對不同。整體而言 ISO/IEC 27701 是對管理系統 PDCA 的 Plan 部份增加了對隱私保護新的要求，讓組織先行建立在個人資料管理的保護的控制程序。因為是管理系統本文的要求，組織在導入時，就一定必需參照條款 5 要求進行組織程序的調整。

ISO/IEC 27002 實作指引的內容架構

ISO/IEC 27002（資訊安全控制措施之作業規範）就是 ISO/IEC 27001 附錄 A 控制措施的實作指引，依條款 5 要求，組織必需要將 ISO/IEC 27001 附錄 A，14 個控制領域和 114 個控制措施經由風險評鑑做適用性聲明建立，而在控制措施實施就必然要考量到 ISO/IEC 27002 針對安全控制措施的實作指引。ISO/IEC 27002 章節部份，因 ISO/IEC 27001 附錄 A 的控制措施是由 A.5 開始，而 ISO/IEC 27002 是對齊 ISO/IEC 27001，主要是由章節 5 開始到章節 18（例如：ISO/IEC 27001 附錄的 A.5.1 對應到 ISO/IEC 27002 就是章節 5.1）。

ISO 27001 附錄 A、ISO 27002 與 ISO 27701 條款 6 之對應關係

ISO 27001(附錄A)	ISO 27002	ISO 27701
A.5 資訊安全政策	5	6.2
A.6 資訊安全之組織	6	6.3
A.7 人力資源安全	7	6.4
A.8 資產管理	8	6.5
A.9 存取控制	9	6.6
A.10 密碼學	10	6.7
A.11 實體及環境安全	11	6.8
A.12 運作安全	12	6.9
A.13 通訊安全	13	6.10
A.14 系統獲取、開發及維護	14	6.11
A.15 供應者關係	15	6.12
A.16 資訊安全事故管理	16	6.13
A.17 營運持續管理之資訊安全層面	17	6.14
A.18 遵循性	18	6.15

ISO/IEC 27701 條款 6 與 ISO/IEC 27002 相關的 PIMS 特定指引

ISO/IEC 27701 條款 6 的內容，是依 ISO/IEC 27002 的實作指引進行擴展到對隱私的保護（條款 6.1~6.15.2.3），組織角色因條款 5 有提到需要區分為（PII 控制者、共同控制者及 PII 處理者），而在條款 6 如果沒有特別說明，敘述的內容就同時適用於 PII 控制者和 PII 處理者。下面舉例對 ISO/IEC 27701 條款 6 有擴展部份與 ISO/IEC 27002 控制項目實作指引（尚有其他資訊供導入時參照）來說明。

- **條款 6.2：**資訊安全政策。組織的最高管理階層展現出對資訊安全的實際支持及指引資安實施的方向。ISO/IEC 27701 中，除原有的資訊安全政策外，要另外制定遵守 PII 法律規範、組織間簽定合約的責任聲明。這個聲明也就是最常見到的組織隱私權聲明或隱私權政策，組織宜先達到合規要求。

- **條款 6.3：**資訊安全之組織。組織在推動資安，內部會對相關的推行小組架構、權責等進行明確的定義。ISO/IEC 27701 在內部組織上，增加了宜要指定 PII 的聯絡人與負責制定、實施、維護和監督組織治理與隱私計劃的人，除協助客戶處理 PII 的事務，並確保 PII 適用法律法規的遵循。而在行動裝置政策上，宜確保使用不會導致 PII 損害發生，這個部份與資訊安全的要求相差不大，但重點在 PII 保護。

- **條款 6.4：**人力資源安全。組織宜從不同的人力資源角度進行安全管理，在聘用前、聘用中及聘用後加強認知、宣導及訓練。ISO/IEC 27701 增加了在人員的認知上組織宜有控制措施在於對違反相關隱私時的後果（懲罰）與對 PII 資料主體的影響，即呼應在風險評鑑時要求必需對 PII 資料主體的影響確認。

由上述舉例 ISO/IEC 27701 在條款 6 增加的部份可以知道，對 PII 保護是重點，所以額外增加在 PII 資料主體的影響考量、政策程序、適用的法律法規識別、人員認知訓練、運作備份與日誌記錄的留存、存取控制與加密措施、通報責任與從設計著手保護隱私...等的實作指引。而組織在實施 ISO/IEC 27701，依據條款 5 必需要將 ISO/IEC 27001 附錄 A 的控制項經由風險評鑑做適用性聲明建立，而控制措施實施就要考量到 ISO/IEC 27002 14 個控制領域和 114 個控制措施所有安全控制措施的實作指引，此部份依據 ISO/IEC 27001 在 PII 處理安全上的要求與 ISO/IEC 27002 實作指引的 ISO/IEC 27701 就顯得相當細化，相對在 BS10012 對 PII 處理安全議題僅在條款 8.2.11.1~8.2.11.11 的要求差異相當大，所以組織在導入時需特別考量此點。▶【PIMS 個資管理系列】之三待續

BSI英國標準協會
T: +886 2 2656 0333 ｜ E: infotaiwan@bsigroup.com ｜ www.bsigroup.tw