【PIMS 個資管理系列】之一

ISO/IEC 27701 隱私保護國際標準新登場

撰文：BSI 英國標準協會
網路安全及雲端個資保護產品經理
花俊傑（Jack Hua）

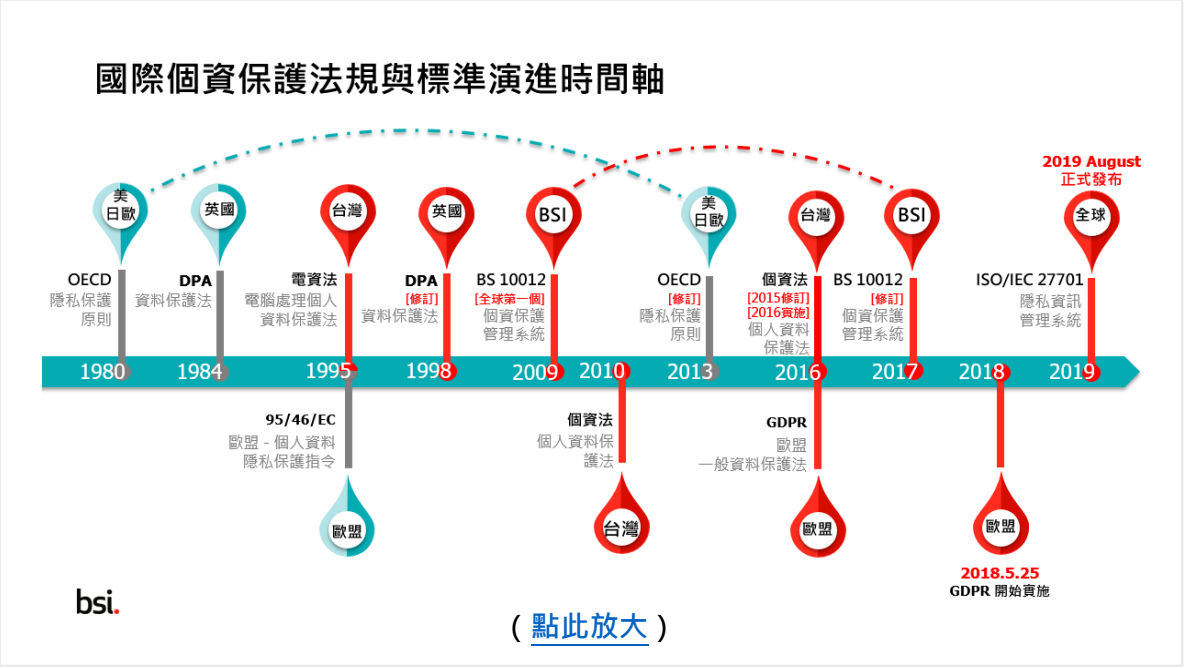
隨著全球化、數位化和服務個人化的時代來臨，包括了政府機關、民間企業及非營利組織，都不可避免地會在日常營運和業務發展過程中，處理到與個人隱私有關的資訊。同時，有鑑於個資外洩的事件層出不窮，以及國際上愈來愈多對於隱私保護和法令法規的要求，保護個人資訊安全和隱私已然成為民眾普遍的期望。

在歐洲，歐盟 GDPR 的實施即是反映了目前針對個人隱私保護的迫切需求，而透過導入和實施國際標準的好處，就在於可以幫助組織在不同法規的要求之下，展現出對於個人隱私保護的可信度和承諾。舉例來說，像是目前許多組織參考實施的 **BS 10012:2017 + A1:2018 就是英國所率先發布的個資管理標準，它為想要展現符合 GDPR 的組織所建立的個人資訊管理系統，提供了一個實務上可行的最佳方案。**

國際隱私標準的發展趨勢

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，但是在隱私保護部份，除了所需要的安全控制措施之外，還必須要因應不同法規對於個人資訊和隱私保護的要求，以及考量從 PII 控制者和 PII 處理者的不同角度來實現和滿足實務的需要，這些因素驅動了 ISO 組織開始著手編寫和隱私保護有關的標準，希望在既有的資訊安全管理系統（ISMS）之上，也能夠同時延伸補充個資管理的要求和實務指引。

如今，「**ISO/IEC 27701:2019** Security techniques - Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management - Requirements and guidelines」已在 2019 年 8 月正式發布，成為第一個兼顧隱私保護和個資安全管理的 ISO 標準。



（點此放大）

基本上，**ISO/IEC 27701 和 BS 10012 之間是屬於一種互補而非取代的關係，因為 BS 10012 本身具備了完整且符合 PDCA 的管理體系，同時也更為貼近歐盟 GDPR 對於隱私保護的要求**，包括像是 Open Data 的去識別化機制、跨境傳輸的實質要求，以及擴充被遺忘權至刪除權、自動化決策權和反對權等，都展現了一個成熟且可應用至實務的標準方案，這對於那些有責任和義務需考量遵循各國隱私法規的組織來說，驗證 BS 10012 會是最適切的選擇。

至於 **ISO/IEC 27701 和 BS 10012 之間的區別，主要是 ISO/IEC 27701 的內容結構使隱私資訊管理可以被視為現有 ISMS 要求和控制措施的擴展**，ISO/IEC 27701 的設計目標是藉由補充額外的管控要求，以便建立、實施、維護和持續改善隱私資訊管理系統（PIMS），並且特別針對 PII 控制者和 PII 處理者來提供隱私保護的框架，透過實施相關的控制措施來降低隱私資訊所面臨的風險。這也就表示，ISO/IEC 27701 適合在範圍內已實施完整 ISMS 的 PII 控制者（包括作為 PII 協同控制者）和 PII 處理者（包括使用分包商的 PII 處理者）來參考使用。

個人資訊管理的角色

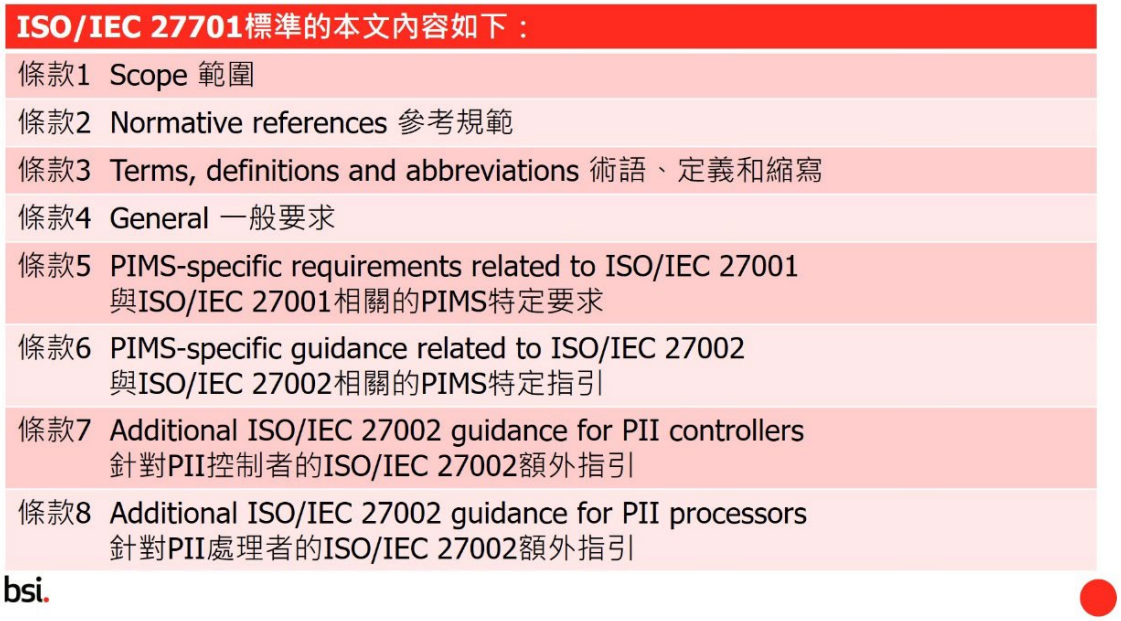
bsi.

PII控制者	PII處理者
收集個人資訊並確定處理它的目的。 可能不止一個組織可以作為PII控制者，一般稱為協同控制者，這是可能需要資料分享協議的地方。	代表並且僅根據PII控制者的指示來處理個人資訊。
ISO/IEC 27701 如何幫助PII控制者	**ISO/IEC 27701 如何幫助PII處理者**
• 提供最佳實務指引 • 增加PII控制者之間的透明度 • 提供管理PII流程的有效方法	• 提供最佳實務指引 • 向客戶保證PII得到有效管理

ISO/IEC 27701 標準的內容架構

一般而言，依照國際標準內容架構可區分為要求（Requirements）與指引（guidelines）兩大類型，ISO/IEC 27701 最特別的地方就在於同時兼顧了這兩種特色，也就是有著可以驗證的標準要求內容，同時也提供了實務上的參考指引。ISO/IEC 27701 所保護的對象就是個人隱私資訊，它參照了 ISO/IEC 27001 和 ISO/IEC 27002 的特定要求，並且為 PII 控制者和 PII 處理者提供了額外的實施指引。

ISO/IEC 27701 標準的條款 1 到條款 3，主要是說明其適用範圍、參考標準和名詞定義，無論組織的規模和大小，基本上 ISO/IEC 27701 適用於任何類型的組織。條款 4 則是針對標準的整體性說明，包括 PIMS 的要求如何對應到 ISO/IEC 27001 的條款 4~10 管理體系，以及 PIMS 的增項指引如何對應到 ISO/IEC 27002 條款 5~18 的控制措施。



而條款 5 和條款 6 的內容，則是進一步敘述在條款 4 所提到的 PIMS 所對應 ISO/IEC 27001 管理體系要求和 ISO/IEC 27002 控制措施實施指引，在內容方面，條款 5 結合了 ISO/IEC 27001 管理體系中 PDCA 的精神，條款 6 則結合了 ISO/IEC 27002 的 14 個控制領域和 114 個控制措施，並且從中額外補充強化了 32 個控制措施。

條款 7 和條款 8 則分別從 PII 控制者和 PII 處理者的角度，分別針對「蒐集和處理的條件」、「對 PII 當事人的責任」、「隱私設計和隱私預設」及「PII 分享、傳輸和揭露」等四個領域，提出了相關的要求（可參照附錄 A 和 B）和實施指引。

最後，在標準的附錄 A~F 中，還補充了 PII 控制者和 PII 處理者可參考的控制目標和控制措施，以及對應到 GDPR、ISO/IEC 29100、ISO/IEC 29151 及 ISO/IEC 27018 的條款編號，並且加上如何應用此一標準的說明，對於想要整合多項標準和需要遵循

GDPR 的組織而言，這部份是相當清楚的參考資訊。針對 ISO/IEC 27701 條款內容的進一步分析及對照，將在後續的文章中一一為讀者來解析說明。

ISO/IEC 27701 的效益和未來驗證方式

ISO/IEC 27701 的重點主要在於提供隱私保護的要求和實務指引，它並不強調要去取代任何一個標準，而是希望藉由與 BS 10012、ISO/IEC 27018、ISO/IEC 29100、ISO/IEC 29151、GDPR 或其他標準的對應互補，讓組織能夠將隱私保護落實的更加完善，並且更進一步展現組織在隱私保護的實施成果。因此，若同時導入 ISO/IEC 27701 和 BS 10012，或是加上 ISO/IEC 27018 與 ISO/IEC 29100，在隱私保護和法規遵循方面，對組織而言都可達到相輔相成的效果。

有關此標準未來的驗證方式，由於 ISO/IEC 27701 是基於 ISO/IEC 27001 標準的延伸，因此 ISO/IEC 27701 的驗證範圍就必須要在原本的 ISO/IEC 27001 範圍之內，所以組織在進行 ISO/IEC 27701 的正式驗證前，最基本的條件就是 ISO/IEC 27701 的驗證範圍必須先通過 ISO/IEC 27001 的驗證，若是不在 ISO/IEC 27001 範圍之內，就必須要再進行 ISO/IEC 27001 的擴大驗證。另外，組織在順利通過 ISO/IEC 27701 驗證之後，獲得 ISO/IEC 27701 證書的有效期限和後續的追查稽核時間，也會與原本 ISO/IEC 27001 的週期相同。

實施 ISO/IEC 27701 的效益

- 提供組織增強合規的證據
- 使利害相關人之間保持透明
- 有助於建立客戶的信任
- 提供更有效的實施協作方法
- 提供更有效的商業協議參考
- 更明確的管理角色和責任
- 與ISO/IEC 27001的高度整合

舉例來說，如果組織原先在 ISO/IEC 27001 的驗證範圍只有資訊部門，但是卻有其他的行政、業務或個資相關部門想要進行 ISO/IEC 27701 驗證，那麼就必須要採取擴大驗證方式，將資訊部門以外的單位都納入 ISO/IEC 27001 的驗證範圍才行。換句話說，對於有心想要導入和驗證 ISO/IEC 27701 的組織，應該從個資的處理流程來考量實施範圍，並且理解保護個資安全的重點不應僅僅限於特定單位，而是組織所有與個人資料蒐集、處理和利用有關的人員，都應該要先落實資訊安全的工作，這也是 ISO/IEC 27701 標準要求的精神所在。 ▶【PIMS 個資管理系列】之二待續

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