因應隱私資訊管理系統驗證方案之標準改版認證作法

驗證機構認證處/黃詠婕

隱私資訊管理系統驗證機構，依據國際標準 ISO/IEC 27701:2025 隱私資訊管理系統(Privacy Information Management Systems, PIMS)驗證標準，以稽核方式確認各產業組織符合 ISO/IEC 27701:2025 驗證要求。另國際標準 ISO/IEC 17021-1 及 ISO/IEC 27706:2025 之要求事項，則是主要規範驗證機構執行隱私資訊管理系統驗證作業相關的運作流程。此兩份國際標準近期已經國際標準化組織(ISO)於 2025 年 10 月公告更新版本，將有助於認證及驗證的品質，確保產業的隱私資訊管理符合國際標準的要求。為協助讀者能瞭解隱私資訊管理系統驗證方案此兩份國際標準之重要性，以下為兩份國際標準改版的重點摘要：

- **隱私資訊管理系統驗證標準改版關鍵(ISO/IEC 27701:2025)**

新版 ISO/IEC 27701 標準由原本作為資訊安全管理系統（ISMS）之延伸標準，轉型為一套獨立且完整的管理系統標準。對於尚未建置或無須導入 ISMS，但基於法規遵循、市場要求或企業重視個人資料保護而需導入 PIMS 之組織而言，新版標準有助於降低導入門檻。然而，值得注意的是，新版 ISO/IEC 27701 在控制措施中仍保留多項資訊安全相關要求，例如資訊安全政策、資訊安全組織、資產管理、存取控制、實體與環境安全、委外開發等。因此，組織於建置 PIMS 時，仍須具備適當的資訊安全管理基礎，方能有效落實個人資料保護目標。

- **驗證機構提供隱私資訊管理系統驗證稽核與驗證之要求(ISO/IEC 27706:2025)**

對於實施隱私資訊管理系統之組織，驗證機構提供第三者驗證稽核服務。ISO/IEC 27706:2025 標準為驗證機構於執行隱私資訊管理系統稽核與驗證活動時所應遵循之關鍵國際標準，該標準明確規範驗證人員應具備的能力資格、驗證活動所需之文件要求、稽核時間規劃之計算準則，以及驗證機構於執行驗證過程活動應符合之相關要求事項。目前，ISO/IEC 27706:2025 亦為各認證組織辦理隱私資訊管理系統驗證機構認證評鑑時所依循之主要驗證方案依據。。

ISO/IEC 27706：2025 全面取代原有 ISO/IEC TS 27006-2:2021，其重要變革在於條款編號已依照 ISO/IEC 17021-1 進行對齊，使隱私資訊管理系統驗證與認證活動，不再依附於資訊安全管理系統，而是成為獨立之驗證及認證標準體系。

新版 ISO/IEC 27706:2025 標準係以 ISO/IEC 17021-1 為架構基礎，並新增與 PIMS 相關規定與指引，其主要修訂重點如下；

- 條文架構調整為以 ISO/IEC 17021-1 為基礎
- 刪除原適用 ISO/IEC 27006 之相關要求
- 強化驗證文件(Certification documents)之內容要求
- 增訂驗證參與人員須具備之 PIMS 專業能力要求
- 新增附錄 A，明確規範稽核時間之計算方式，以 PII (Personally Identifiable Information)控制者、PII 處理者或兼具雙重角色進行區分

有關上述內容，請參考本會文件「隱私資訊管理系統驗證機構認證規範(ISO/IEC 27706:2025)」。

- **本會因應隱私資訊管理系統標準改版之認證作法**

鑒於 ISO/IEC 27706:2025 新版標準係以 ISO/IEC17021-1 為基礎，並強化 PIMS 相關要求為修訂重點，尤其第 7 章「驗證人員能力」、第 8 章「驗證文件」，以及附錄 A「稽核人天計算基準」之變更，將成為本會後續推動隱私資訊管理系統新版驗證方案後，進行認證評鑑時的重要關注重點。

因應 ISO/IEC 27706:2025 隱私資訊管理系統標準與資訊安全管理系統標準正式分離，本會將同步修訂相關認證規範文件，並另行公告受理新版標準之作業期程，相關資訊將於本會官網公告周知。

ISO/IEC 27706:2025 的發布，象徵全球隱私資訊管理系統認證邁向更高層次的專業性與一致性。本會所認證之驗證機構在執行隱私資訊管理系統驗證時，將全面依循新版國際標準要求，持續提升驗證技術與專業能力，為我國個人資料保護把關。此舉不僅有助於強化我國資訊安全與個資保護環境之健全發展，亦能提升驗證活動結果的可信度。正是 TAF 推動並提供本項認證服務之核心價值與重要意義。