ISO 27701 新版將面世

PIMS 標準出新版 個資保護國內外升級

就在國內個資保護委員會將成立之際，有關 PIMS 的國際標準 ISO 27701 第二版也將公告，個資保護措施與法規將逐步落實，值得重視。

文／梁日誠

隱私資訊管理系統（Privacy Information Management System；PIMS）的國際標準 ISO 27701 初版 [ED.1] 於 2019 年公告，**最新版（第二版，簡稱 ISO 27701 [ED.2]）**已經進展到最終版國際標準草案（FDIS，2024-12-19）階段，可望於 **2025 年第一季或第二季間公告**，此時正值我國個人資料保護法規持續修法（個人資料保護委員會籌備處於2024-12-20預告修正「個人資料保護法」部分條文）、個人資料保護獨立監督機制積極建立之際（憲法法庭111年憲判字第13號判決要求於114年8月前成立我國個人資料保護獨立監督機制），如同 ISO 27001 之於資通安全管理法，ISO 27701 可望成為各適用於個人資料保護法的組織的合規與良善管理的展現機制。

此外，為完善個資保護，伴隨著 ISO 27701 [ED.2] 同時發展的，亦有 ISO 27706 - PIMS 驗證機構認證規範（發展中，簡稱 ISO 27706 [UD]），將取代目前的 ISO 27006-2（對應於現有的ISO 27701 [ED.1]），目前位於最終版國際標準草案（FDIS，2024-11-07）階段，將間接影響 PIMS 的驗證客戶，預計的公告時程與 ISO 27701 [ED.2] 相近，也將使 PIMS 的國際認證（Accreditation）與驗證（Certification）機制趨於同步，朝著納入國際認證論壇（IAF）多邊相互承認協議（Multilateral Recognition Arrangement；MLA）範疇的可能性更進一步。相較於現有的 ISO 27701 [ED.1]，新版 ISO 27701 [ED.2] 於數個章節進行了變更，說明如下。

適用管理系統標準

ISO 27701 [ED.2] 異於現有的ISO 27701 [ED.1]（ISO 27701 [ED.1] 以 ISO 27001 與 ISO 27002 於隱私資訊管理領域延伸的方式），**改採用管理系統標準（Management System Standard；MSS）來形成 PIMS**，包含了要求（Requirements）與指引（Guidelines）兩部分，一則與其他 ISO 管理系統標準，如：ISMS-ISO 27001、BCMS-ISO 22301、AIMS-ISO 42001 等，以 MSS 相校準，同時也提高與其他 ISO 管理系統整合而成 IMS（Integrated Management System）的機會。

其次，ISO 27701 [ED.2] 也使得 PIMS 如同其他管理系統，具備單獨進行驗證並取得驗證證書的特性，可以但不強制（若依現有的 ISO 27006-2 要求，為強制性）與 ISMS 整合（意指，驗證組織同時滿足 ISO 27001 與 ISO 27701 規定），使得 PIMS 的範圍界定（不論是 PII 控制者及／或處理者）更具彈性，在資通安全與隱私保護的權責界定（如：資安長、個人資料保護長的任命與權責）與資源安排上，提供組織較多元的選項。再者，ISO

ISO 27701 [ED.2] Table A.3 Control	Control Title 控制措施名稱	ISO 27001:2022 Table A.1 Control
A.3.3	Policies for information security 資訊安全政策	A.5.1
A.3.4	Information security roles and responsibilities 資訊安全之角色及責任	A.5.2
A.3.5	Classification of information 資訊之分類分級	A.5.12
A.3.6	Labelling of information 資訊之標示	A.5.13
A.3.7	Information transfer 資訊傳送	A.5.14
A.3.8	Identity management 身分管理	A.5.16
A.3.9	Access rights 存取權限	A.5.18
A.3.10	Addressing information security within supplier agreements 於供應者協議中闡明資訊安全	A.5.20
A.3.11	Information security incident management planning and preparation 於供應者協議中闡明資訊安全	A.5.24
A.3.12	Response to information security incidents 資訊安全事故之回應	A.5.26
A.3.13	Legal, statutory, regulatory, and contractual requirements 法律、法令、法規及契約要求事項	A.5.31
A.3.14	Protection of records 紀錄之保護	A.5.33
A.3.15	Independent review of informationsecurity 資訊安全之獨立審查	A.5.35
A.3.16	Compliance with policies, rules, and standards for information security資訊安全政策、規則及標準之遵循性	A.5.36
A.3.17	Information security awareness, education and training 資訊安全認知及教育訓練	A.6.3
A.3.18	Confidentiality or non-disclosure agreements 機密性或保密協議	A.6.6
A.3.19	Clear desk and clear screen 桌面淨空及螢幕淨空	A.7.7
A.3.20	Storage media 儲存媒體	A.7.10
A.3.21	Secure disposal or re-use of equipment 設備汰除或重新使用之保全	A.7.14
A.3.22	User endpoint devices 使用者端點裝置	A.8.1
A.3.23	Secure authentication 安全鑑別	A.8.5
A.3.24	Information backup 資訊備份	A.8.13
A.3.25	Logging 存錄	A.8.15
A.3.26	Use of cryptography 密碼技術之使用	A.8.24
A.3.27	Secure development life cycle 安全開發生命週期	A.8.25
A.3.28	Application security requirements 應用系統安全要求事項	A.8.26
A.3.29	Secure system architecture and engineering principles 安全系統架構及工程原則	A.8.27
A.3.30	Outsourced development 委外開發	A.8.30
A.3.31	Test information 測試資訊	A.8.33

◤ <表A>

27701 [ED.2] 也如同其他管理系統，納入了氣候變遷（Climate Change）的相關要求。

在隱私風險評鑑（Privacy Risk Assessment）章節中，ISO 27701 [ED.2] 指出了 ISO 27557（Application of ISO 31000:2018 for organizational privacy risk management） 做為組織的隱私風險管理的參考標準。

在隱私風險處理（Privacy Risk Treatment）章節中，ISO 27701[ED.2] 要求組織應文件化實作的資訊安全方案，此方案所包含的資訊安全控制措施至少須包含資訊安全風險管理、資訊安全政策、資訊安全組織、人力資源安全、資產管理、存取控制、運作安全、網路安全管理、開發安全、供應者管理、事故管理、資訊安全持續、資訊安全審查、密碼技術、實體及環境安全等，ISO 27001 與 ISO 27002 可以是資訊安全方案依據的標準。

控制措施納入資訊安全

ISO 27701[ED.2] 於附錄 A 保留（編號重新調整）了適用於 PII 控制者（Table A.1）與 PII 處理者（Table A.2）的控制措施，並新納入適用於PII 控制者與 PII 處理者的資訊安全控制措施（Table A.3），以供隱私風險處理作業之需。

ISO 27701 [ED.2] 的附錄 B 則提供對應於附錄 A 的各控制措施的實作指引。ISO 27701[ED.2] 於附錄 F 提供了 Table A.3 的控制措施與 ISO 27701 [ED.1]（2019年版）的資訊安全控制措施的交互對應（於 Table F.1 與 Table F.2 中）關係，惟 ISO 27701 [ED.1] 的資訊安全控制措施的分類建立於 ISO 27001、ISO 27002 的 2013 年版（已被2022年版取代）標準之上。

有關 ISO 27701 [ED.2] Table A.3 的控制措施（源自於 ISO 27701 [ED.2] 的 DIS 標準草案）與 ISO 27001的2022年版的控制措施（Table A.1），例舉對應關係如 **<表A>**，可做為 PIMS 與 ISMS 間整合或分立（意指整合程度不高，惟仍可能具有不同程度的交互關係）的評估參考。至於，ISO 27701 [ED.2] 於附錄中，亦一併更新了與 ISO 29100、ISO 27018、ISO 29151、EU GDPR 等的對應關係。

新規範協助完善建立 PIMS 組織

在目前的 ISO 27006-2 中規定，ISO 27701（意指 ISO 27701[ED.1]）驗證文件應載明係依據 ISO 27001 驗證，且組織符合 ISO 27701 規定，也因此，組織在建立與驗證 PIMS 時，都需要面對現有或需要新建的 ISMS 的範圍的議題，包含了如組織架構、角色、職責、資源、能力、法遵、治理等面向的考量。可以預見的，ISO 27701 [ED.2] 與 ISO 27706 [UD] 所帶來的改變，將影響組織採用 PIMS 的意願。

在 ISO 27701 [ED.2] 的改版與 ISO 27706 [UD] 的新建過程中，均考量到國際間對 PIMS 的更新需求，對於已建立或將新建立 PIMS 的組織，提供了較多的整合（並未有上述強制性要求）或分立的選擇，組織可依各自的隱私／個資保護與資訊安全的狀況與時程，進行評估以選擇 ISO 27701 [ED.1] 或 ISO 27701 [ED.2] 建立或驗證 PIMS。

同樣的，PIMS 驗證機構也須評估以 ISO 27006-2 或 ISO 27706 [UD]（意指公告後）來取得或先後取得認證資格，進而提供 PIMS 驗證客戶 ISO 27701（ED.1或ED.2）第三方驗證服務，惟須考量取得認證資格的過程需要一定的時間。組織在選擇建立同仁 PIMS 能力時也宜將 ISO 27701 [ED.2] 的公告發行時程列入考慮，使得 PIMS 的能力培養與附加的資通安全專業證照的價值較為理想，個資法主管機關所訂定個資長及個人資料保護稽核人員的職能條件、訓練或隱私／個資保護相關證照等資訊，也是組織培養同仁能力的優先考量方向。

作者: 梁日誠 (Lead CCA^I CCP^I PII CISSPI CISSOI CPTEI CCSOI CDREI CCISOI ISMI ISAI AIMPI FIAAISI FHCA-EU AI ActI CAIEI CAIPCI CDEI CDAI DSFMI FHCA-GDPRI IDPPI ICEPI GRCAI GPM-bI IMPCI, ^ Pending)，現為加拿大SCC／MC ISO／IEC JTC1／SC42、SC27、ISO／TC22／SC32、IEC／TC65 技術組成員，ISO 42001／ISO 27001／ISO 27701／ISO 22301／ISO 20000-1／IEC 62443-2-1 稽核師及講師，TCIC 環奧國際驗證公司全球營運總經理。