資訊安全及個資管理不可偏廢

個資管理系統國際標準 ISO 27701正式公告

許多人已經開始意識到資訊安全的重要性，卻不知道個資管理另有專業的規範要求。隨著個資管理系統國際標準 ISO 27701 正式公告，個資管理也將進入全新的視野。

採訪／施鑫澤 文／楊迺仁

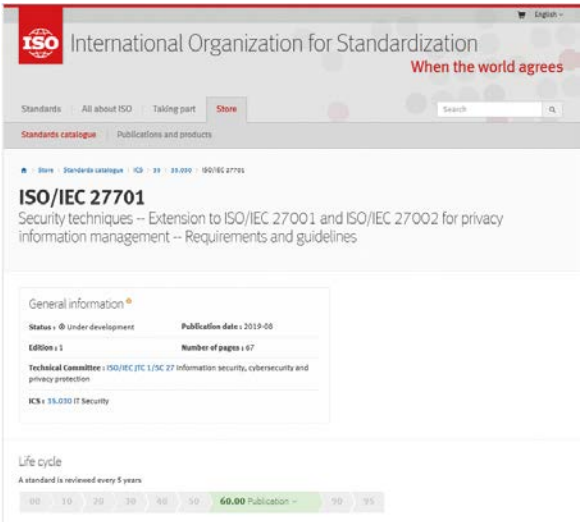
對於個資保護的重視，促成國內外近兩年相繼公告或實施各個重要的資安與個資法規，如台灣的個人資料保護法、資通安全管理法、歐盟的General Data Protection Regulation（GDPR）等，但這些法規彼此因為缺乏一致性的對照機制，企業想要做出合規展現時，可能會有顧此失彼的困擾，而且對早已投入各種資安標準驗證如ISO/CNS 27001的組織而言，若要不斷的因應層出不窮的外國標準如美國ANSI、英國BS等，也會有重複投資的疑慮。

所幸前述問題都將因為8月6日公告的全方位個資管理系統國際標準ISO 27001，而可望迎刃而解。因為ISO 27701為ISO 27001與ISO 27002於個資管理的延伸標準，包括可供驗證的ISO 27001各項要求及提供實作指引的ISO 27002，且附加或微調個資管理的要求與實作指引，不僅整合資訊安全管理系統（ISMS）與個資管理系統（PIMS），也提供國際間所有不同型態與規模的機構，可用於驗證的PIMS國際標準，象徵著資訊安全、隱私與個資保護，在國際間的法律與法規的合規展現，將有一致性的對照機制。

ISO 27701可望成為GDPR驗證機制主要選項

加拿大TCIC環奧國際驗證公司全球營運總經理梁日誠（Daniel）指出，ISO 27701在發展階段時期稱之為ISO 27552，它是基於ISO 27001及27002兩標準之延伸擴充，對於個資管理系統(PIMS)的要求準則。之所以需要ISO 27701，是因為如果只用資訊安全管理的角度來看個資管理，可能會有客觀的不足。

梁日誠強調，完整的資通安全，應該要包含兩個部分，一個是IT安全，另一個是OT安全。IT的部分又可以分成兩個範疇，一個是一般資訊(information)，另一個則是隱私資訊或個人可識別化資訊(personally identifiable information)，也就是個資。要保護個資，需要注意11個隱私原則，資訊安



ISO組織再2019年8月6日公告的全方位個資管理系統國際標準ISO 27701。

全只是其中之一，這11個隱私原則如果只做資訊安全，就會有很明顯的不足。ISO 27701對於台灣為數不少已導入並通過ISO 27001驗證的機構而言，可以很容易地用ISO 27001的標準去延伸，把資訊安全及個資保護一併整合起來，做完整的展現。

梁日誠指出，ISO 27701在發展初期，是由法國的資料保護權責機構經由代表法國出席ISO組織的國家機構(National Body)所提出，因為那時歐盟的GDPR監管組織EDPB（在2018年5月之前叫做Article 29 Working Party）主席即來自於法國，所以法國承擔了很多個資保護國際標準制定工作。後來EDPB每一次在不同階段的標準發展中，都有提出意見，其貢獻最多的部分之一，就是在附錄中有一個ISO27701和GDPR的對應表。

所以不管是業界或國際標準界，都認為ISO 27701很有機會成為GDPR驗證機制的其中一個基礎或選項。因為ISO 27701是EDPB唯一參與制定，又經過ISO合議原則最後公布的PIMS國際標準。梁日誠指出，由於之後的GDPR驗證機制，除了要透過EDPB核准，期間還要彙整所有歐盟會員國的意見，但因為在ISO 27701制定階段，就已經彙整過一次，所以應該是最容易達到合議原則，可望成為泛歐的GDPR驗證標準。

雖然目前還沒有直接針對GDPR法律的被認可驗證機制，但梁日誠認為，企業還是可以先準備，雖然正式的驗證機制出爐後，某些條文可能要求驗證的更深入，但現在的GDPR詮釋文件其實已經規定的很詳細，所以企業只要實作ISO 27701，同時參考GDPR對應條款詮釋文件，將詮釋文件的精神放在ISO 27701的管理制度中，在合規展現方面應該就不會構成太大的問題，而且也比較有系統性。

梁日誠指出，當政府單位下決定要蒐集個資時，它的角色就是個資控制者，除了自身執行ISO 27701有關個資控制者的相關規範外，並可用ISO 27701有關個資處理者的相關規範，作為委外廠商能否符合要求的條件，不但有依據，而且還是國際標準的要求。政府單位都必須依資安法來選任及監督受託者，選任監督時，針對個資如果有任何委外事項，就可有監督的依據。

加拿大TCIC環奧國際驗證公司全球營運總經理梁日誠（Daniel）。

參考ISO 27701做好數位證據保存

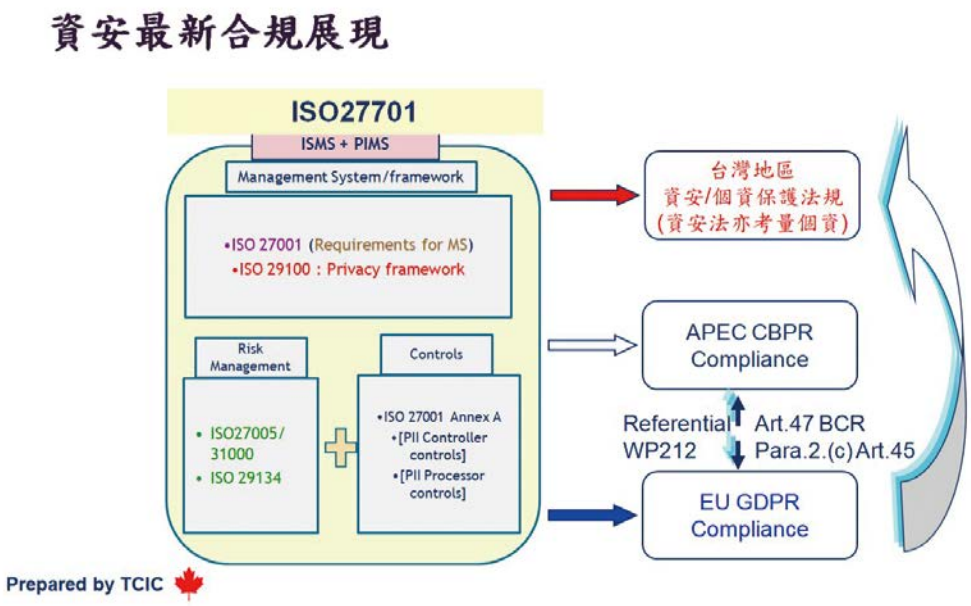
梁日誠指出，GDPR的特性，就是在談個資保護時，裡面有安全方面的處理要求，ISO 27701剛好又是兼顧兩者，而不是個資保護及安全處理分開，經由這樣的管理制度運行，相關的證據就比較容易保存出來，如果再配合第三方的稽核機制，它的可信度又更具公信力。

ISO 27701相當強調數位證據，如紀錄、軌跡資料的保存，又比如說誰可以存取、誰不行存取，以及保存的時間與方式。企業在運作ISO 27701管理制度時，須定義紀錄保存期限到底要多長，如果有適法性的因素存在，就應按照適法性的要求處理。梁日誠以民眾向公家單位求償為例指出，由於會涉及到國家賠償法，此時就會去參考國家賠償法裡面的賠償請求權，在民事部分也是一樣，都有相關規定。

此外，證據必須是可追溯的，紀錄也要維持它的唯一可識別性，這些管理系統的特性一旦經過稽核，作為證據的可信度相對就會增加。屆時只要發生的事件只是單一偶發事件，且企業又能證明已經作好良善管理，現有的管理制度客觀上無法防止，

但在法庭上的攻防就能獲得比較有利的結果。

梁日誠表示，現在比較常看到的狀況，就是企業錯用標準、缺乏管理制度，或是沒有按照中央目的事業主管機關的規定去建立相關防護機制，很明顯地當沒有建立管理制度的時候，很容易就會輸掉訴訟。



ISO-27701 在合規展現上的示意圖。

用ISO 27701可對應個資安全維護計畫

梁日誠指出，近期有些洩漏個資的案例在法院上攻防時，如果沒有建立「個人資料檔案安全維護計畫」就導致敗訴；就算有作資訊安全防護如防火牆，但是沒有建立管理制度也還是敗訴；還有一個案例是某企業委託資安公司做弱點掃描，也有導入PCI-DSS（支付卡產業資料安全標準），但最後法院是以「缺乏個資保護的有效性」而被判敗訴。也就是雖然你做了資安，但是洩漏的是個資，而且不是只有一次，因此法官認定為無效，最終還是敗訴。

所以選擇適當的國際標準以及對應的稽核機制很重要，也就是個資法規定的「適當安全維護措施」有沒有達到一定合理的程度。除了法律條文規定之外，中央目的事業主管機關如果已經明文規定，要制定個資防護計畫，就會看企業有無對應的證據佐證是否已經做到。

在企業的個資安全維護計畫中，通常包含了人員配置、個人資料蒐集處理利用的作業程序、受理當事人權利行使作業程序、個人資料盤點風險評估、事故預防通報應變、認知宣導、個人資料安全管理作業使用紀錄、委外監督及持續改善等規定，每個規定和中央目的主管機關的規定或許會有些許不同，但可以做為基本範疇。ISO 27701可以跟個資安全維護計畫的各個項目做出對應，導入符合ISO 27701的個資管理系統並通過公正第三方驗證，就是建立適當安全維護措施的最佳展現方法。

轉成國家標準社會大眾受惠

梁日誠表示，以前就算有個資安全維護計畫，企業也都是自己去琢磨，怎樣去達到目標，現在因為有了ISO 27701國際標準，只要按照標準要求去作，而且都能夠對應上，之後並提供第三方稽核程序的合規展現，就能很快地找出相關證據體現。加上通過第三方稽核，可信度又會更高一些。

因為ISO 27701是ISO會員國的國際專家所議決出來的標準，就不用企業自己去論證及陳述信效度，能夠有效降低不可預知的風險。ISO 27701正式公告後，做為ISO/IEC JTC1/SC27的參與成員，基於推廣國際標準的立場，相關的機構也會去推廣及宣導。也只有國際標準，才有機會及早轉成CNS國家標準，讓更多的機構及社會大眾受惠。