重視標準演進 提升網路安全

資安與個資法規的合規展現與相關國際標準發展

隨著新興科技如 IoT、Big data、AI、Blockchain 的蓬勃發展，國內外新興科技資安與個資相關法規與國際標準也陸續的發展，如何有效管理 Cybersecurity 的風險與事故更是刻不容緩。

文／梁日誠（第11屆CIO價值學院講師）

於2018年，國內外公告或實施了數個重要的資安與個資法規(例舉如表1)，也因此，如何進行合規展現便是各組織的 Chief Security Officer(CSO) 、Data Protection Officer (DPO) 與 Chief Compliance Officer (CCO)於2019年的重要課題。

國內的資安與個資法規

資通安全管理法與相關子法於2018年6月與11月相繼公告，也勾勒出了資通安全與個資保護的合規展現相關要求，例舉說明如下：

於資通安全責任等級分級辦法總說明中，可見：

- 「初次受核定或等級變更後之二年內，全部核心資通系統導入CNS 27001資訊安全管理系統國家標準、其他具有同等或以上效果之系統或標準，或其他公務機關自行發展並經主管機關認可之標準，於三年內完成公正第三方驗證，並持續維持其驗證有效性。」，此要求說明了國家標準CNS 27001驗證的重要性，也建議原只進行ISO 27001驗證的組織加驗CNS 27001，另可窺知可其它涵蓋CNS 27001驗證的國家標準如 ISO/CNS 27018與ISO/CNS 29151(制定中)等PIMS國家標準驗證可展現為「以上效果之系統或標準」，而其它外國標準如美國ANSI、英國BS、加拿大CAN、德國DIN等，除非經主管機關認可外，均不被接受。
- 「『公正第三方驗證』所稱第三方，指通過我國標準法主管機關委託機構認證之機構。」，此要求說明了唯有經全國認證基金會(TAF)認證的驗證機構進行的第三方驗證方可被接受。
- 第四條第四款中「業務涉及全國性民眾或公務員個人資料檔案之持有」及對應說明「第四款所稱全國性民眾或公務員個人資料檔案，指含括全國地域範圍內之絕大部分民眾或公務員之個人資料檔案」，已將個資列入分級的條件，也可窺知若核心資通系統中涉及個資，亦在資通安全管理法與相關子法的規範範圍之內。

於資通安全管理法施行細則總說明中，可見「為確保受託者辦理受託業務之程序及環境具安全性，並得妥善執行受託業務，爰為第一款及第二款規定。第一款所稱第三方，係指通過我國標準法主管機關委託機構認證之機構，其驗證標準可為國際、國家或團體標準。」，此要求說明了唯有國際(ISO)，國家(CNS)或團體標準(如IEC，IEEE或ITU)可被接受，其它外國標準(如美國ANSI，英國BS，加拿大CAN，德國DIN等)並非國際標準(ISO)而將不被接受。

表 1　近期發佈的資安與個資法規

地區	法規名稱
歐盟	General Data Protection Regulation (GDPR)
歐盟	Regulation on Privacy and Electronic Communication (ePrivacy)
美國加州	SB 327 Information privacy: connected devices
台灣	資通安全管理法與相關子法

資通安全管理法與相關子法公告後，也宣告國內一直以來被某些外國標準或驗證機構或前述機構的合作顧問機構主張其所推廣的某些外國標準可做為國內資安或個資的合規展現的亂象的終止，相對的，標準法主管機關對於資安與個資國家標準的制定與推動與TAF對於資安與個資驗證機構的認證方案的制定與推動就必須跟得上法規的腳步與市場的需求。各組織(包含提供資通安全管理法適用機構委外辦理資通系統之建置、維運或資通服務之提供商)在建立、維運與最佳化其ISMS/PIMS時也必須將資通安全管理法與相關子法的要求納入管理系統以有效的展現合規。

國外的資安與個資法規

歐盟的GDPR自2018年5月實施前就一直被關注著相關的發展，然而另一個與GDPR有個相同主管機構European Data Protection Board(EDPB)與相同高罰則的ePrivacy法規(Regulation)也不容忽視。GDPR與ePrivacy的主要異同點可見於表2。

因ePrivacy影響層面涉及國內廠商擅長之網通服務、網通設備、Smartphone/APP與IoT相關應用等領域或產業，宜及時準備對應的合規措施。於2019年

表 2　GDPR 與 ePrivacy 比較

GDPR	ePrivacy
涵蓋所有以各種不同方式傳輸的個人資料	涵蓋電子通訊與個人設備的個人資料與非個人資料的資訊的完整性
定義個人資料保護的權利	定義隱私與通訊機密性的權利
引入新的自然人的權利與公司的義務	確保所使用的手機 apps 或 Internet 服務於通訊中不被攔截，側錄，竊聽，擅入
於 2018 年 5 月 25 日實施	建議於 2018 年 5 月 25 日實施，將於完成立法程序後實施
主管機構為 EDPB	主管機構為 EDPB
罰則最高為歐元 20,000,000 或 4 % 全球營業額（取較高者）	罰則最高為歐元 20,000,000 或 4 % 全球營業額（取較高者）

1月，法國的個資主管機構(DPA) CNIL對Google因違反GDPR開罰歐元5,000萬的案例，也再次提醒了全球各GDPR適用單位對於法規遵循整備的迫切性，國內GDPR主政機構除積極與歐盟進行第三國適足性(Adequacy)協商外，也應儘速的整合GDPR相關資源，有效的協助企業面對GDPR的合規展現作為。

值的借鏡的是，依據2019年1月23日European Commission的公告文件”COMMISSION IMPLEMENTING DECISION “[pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate protection of personal data by Japan under the Act on the Protection of Personal Information]，日本的適足性(Adequacy)已被有條件的同意,日本申請適足性認定由2017年1月開始討論到2018年9月初步被接受，歷經GDPR的主管機構由Article 29 Working Party轉換為EDPB的組織性變動，歷時21個月。

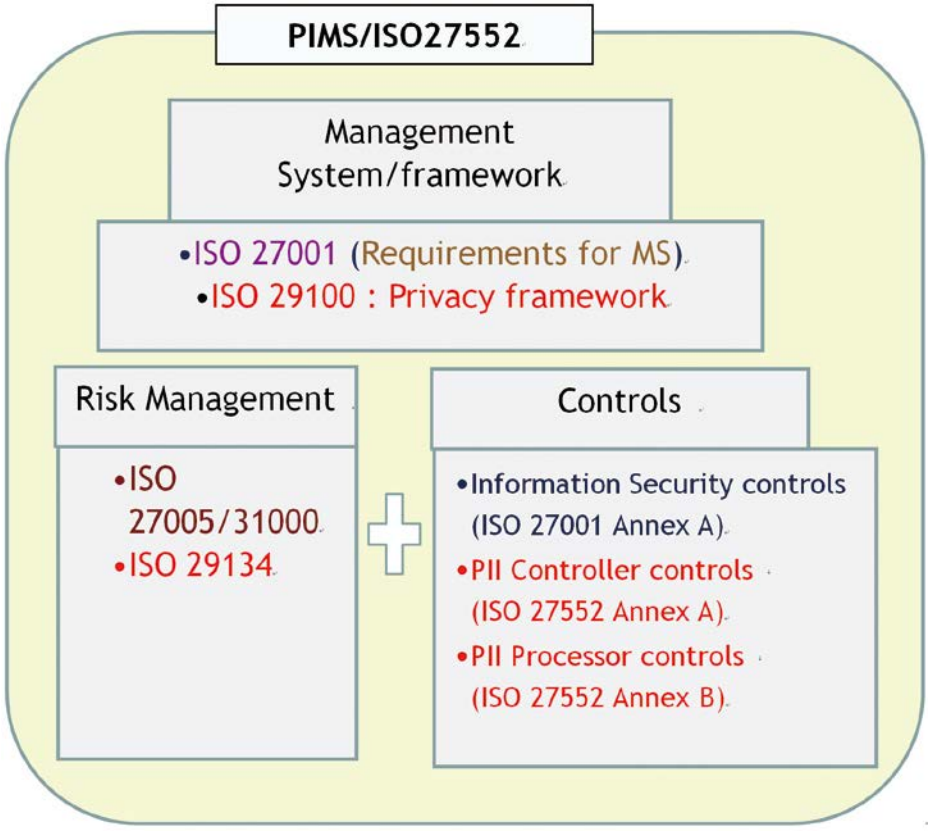

圖1　ISO/IEC 27552架構示意圖

國際(ISO)的PIMS驗證標準已經出現

國際間各國共同努力於ISO組織中推動的PIMS驗證標準ISO/IEC 27552已經於2018年年底公告其準國際標準(DIS)，於公告的準國際標準中可見ISO/IEC 27552整合了資訊安全管理系統與個資管理系統的要求於一個標準中，也代表通過ISO/IEC 27552驗證可展現同時符合資訊安全管理系統(ISMS)驗證(ISO/CNS27001)與個資管理系統(PIMS)驗證的要求，可作為符合國內資通安全管理法與相關子法精神(同時涵蓋資安與個資面象)最佳的合規展現。

ISO/IEC 27552是由ISO/IEC JTC1/SC27資訊技術安全技術組主責，歐盟GDPR主管單位EDPB參與SC27的WG5(第5工作組)共同推動制定，是目前唯一由EDPB支持的PIMS驗證的國際標準。於準國際標準的投票結果中，僅Japan (JISC)、Luxembourg (ILNAS)、Malaysia (DSM)與United States (ANSI)投下反對票，惟美國(ANSI)於協調後同意更新後的標準內容，改為同意準國際標準。此準國際標準的合意結果也代表了歐盟及國際間各國對ISO/IEC 27552的認可，可以預見此國際標準日後在個資保護合規展現的重要角色。ISO/IEC 27552由驗證觀點的架構示意如圖1，有意建置基於ISO標準的PIMS的組織可以於建置階段先參考ISO/IEC 27552準國際標準，再於ISO/IEC 27552國際標準公告後進行驗證。

隨著英國脫歐將近，筆者最近常被問到是否使用脫歐國家的標準與驗證機構可以展現GDPR的合規？此提問可由近期EDPB公布的二份指引文件「Guidelines 1/2018 on certification and identifying certification criteria in accordance with Articles 42 and 43 of the Regulation 2016/679」與「Guidelines 4/2018 on the accreditation of certification bodies under Article 43 of the General Data Protection Regulation (2016/679)」獲得釋疑，文件說明了歐盟會員國可以核准驗證標準(certification criteria)及認證(accredit)驗證機構(certification body)，以上若涉及多個歐盟會員國，則權責在於EDPB。

除了本文舉例的國內外資安與個資法規與國際標準外，隨著新興科技如IoT、Big Data、AI、Blockchain的蓬勃發展，國內外新興科技資安與個資相關法規與國際標準也陸續的發展，如何有效管理Cybersecurity的風險與事故，也成為各國刻不容緩的議題，筆者將再針對此主題說明新興科技相關的資安、隱私、風險管理的國際標準發展趨勢，期有助於新興科技產業發展。 CIO

梁日誠 Daniel Liang

- Standards Council of Canada (SCC) Canadian advisory committee on GDPR 加拿大國家GDPR諮詢委員會。
- Canada's Mirror Committee for ISO/IEC JTC1/SC27 IT Security Techniques.
- Canada's Mirror Committee for ISO/IEC JTC1/SC42 Artificial Intelligence.
- Canada's Mirror Committee for ISO/PC317 - Consumer protection: privacy by design for consumer goods and services.
- ISMS/PIMS/SMS/BCMS/QMS/MirrorLink Auditor/Assessor/Trainer.