Communications of the CCISA
Vol. 23 No. 4 Oct. 2017

個人資料管理系統驗證要求事項標準化進程初探：根基於 ISO/IEC JTC 1/SC 27 在 2017-01 公布的框架

蔡昀臻[1]、樊國楨[2*]
[1]國立交通大學管理科學研究所、[2]臺灣經濟新報文化事業股份有限公司
[1] yct1230@gmail.com、[2]kjf.nctu@gmail.com

摘要

個人資料保護法施行細則第 17 條闡明：「……所稱無從識別當事人，指個人資料以代碼、匿名、隱藏部分資料或其他方式，無從辨識該特定個人者」亦即通稱「去識別化(De-identification)」之議題，自 2014 年 11 月 17 日法務部法律字第 10303513040 號函的函釋：「去識別化之個人資料依其呈現方式已無從直接或間接識別該特定個人者即非屬個人資料」起，其「驗證(Certification)」成為我國標準化工作項目的優先項目。根基於此，本文探討包含前述「去識別化」之歐盟「一般資料保護條例」規範的「個人資料管理系統」驗證，其遵循之國際標準化組織(International Organization for Standardization, ISO)於此議題的標準化作業之脈絡及前景，並在最後提出本文的觀察與建議代為結論。

關鍵詞：驗證、個人可識別資訊、個人資料管理系統、資訊安全管理系統、標準化

Personal Information Management System Requirements Standardization and Implementation: Based on New Framework of ISO/IEC JTC 1/SC 27

Yun-Chen Tsai[1], Kwo-Jean Farn[2]
[1] Institute of Information Management Science, National Chiao-Tung University,
[2] Taiwan Economic Journal Co., Ltd.
[1] yct1230@gmail.com,[2] kjf.nctu@gmail.com

Abstract

Enforcement Rules of the Personal Information Protection Act Article 17 states that “the Act shall mean the personal information processed by ways of code, anonymity, hiding parts of information or other manners so as to fail to identify such a specific person.”, so as call the “De-identification” issue. Since 2014, Nov 17th the Ministry of Justice has explained that “De-identified personal information cannot identify directly or in-directly a specified individual.” certification has become our standardization primary issue. Thus, we discuss EU’s “General Data Protection Regulation” including “De-identification” mention before in “Personal information management system” certification, whose implementation follows International

*通訊作者：kjf.nctu@gmail.com

Organization for Standardization (ISO) standardization. The article is going to conclude with observation and suggestion to the status quo of protecting personal data in Taiwan subject to learning experience from the ISO standardization in striving for protecting personal data.

Keywords: Certification, Personally Identifiable Information (PII), Privacy/ Personal Information Management System (PIMS), Information Security Management System (ISMS), Standardization

壹、 前言

九十年代全球文明歷經了重大的轉變，品質、環境和職業安全衛生管理逐漸朝向一致化與標準化，而相關的國際標準也影響了許多國家經濟的發展以及組織管理與經營的方式，ISO 9000 品質管理和 ISO 14000 環境管理系列標準的遵循，就是最佳的佐證。2000 年 12 月 1 日，資訊安全管理系統(Information Security Management System，ISMS)控制措施之 ISO/IEC 17799:2000(E)公布，2002 年 12 月 5 日相對應之 CNS 國家標準正式頒布，建立 ISMS 並擴大推動驗證已成為資訊安全之工作項目的主軸之一。2006 年 6 月 16 日，經濟部標準檢驗局再公布了 ISO/IEC 27001:2005(E)之資訊安全管理系統的要求事項等國家標準，也成就了資安管理制度與國際化接軌的開端。

「讓過去與現在爭執不下，將錯失未來」，ISO/IEC JTC1/SC27 主席 Walter Fumy 先生，在世界資訊高峰會之邀請下，於 2004 年 9 月 24 日公布了 ISO 之深度防禦(Defense in Depth)的資訊安全管理模型觀點；其標準組件 ISO 27001 標準系列之 ISO/IEC 27003 已於 2010 年 2 月 1 日正式發行，ISMS 標準化的第一階段工作已樹立第 1 座里程碑。

鑑於管理系統日益增多，其標準系列宜加以規範，國際標準組織(International Standardization for Organization，ISO)自 2000 年起即分 3 階段進行管理系統標準(Management System Standards，MSS)之標準化工作；已正式納入 ISO 之強制性規範(Procedures specific to ISO)，期能在第 3 階段(2011~2015 年)完成各個管理系統要求事項的調和。ISO/IEC 27001 標準系列已遵循 MSS 逐步建立中，並納入個人資料/隱私管理系統(Personal/Privacy Information System，PIMS)安全規範之議題；以個人資料保護法施行細則第 17 條之規範為例，已公布 ISO/IEC 27009、ISO/IEC 29101、ISO/IEC 29191、ISO/IEC 20008 與 ISO/IEC 20009 標準系列，作為其 PIMS 中「前檯匿名、後檯實名」之實作要求事項的參考。2012 年 10 月，ISO/IEC JTC 1/SC 27 在進行為期 1 年之 2 階段的研究後，正式公布 PIMS 之要求事項遵循 ISO/IEC 27001，同時開展其標準系列(ISO/IEC 27009、ISO/IEC 27018、ISO/IEC 27017、ISO/IEC 29134、ISO/IEC 29101、ISO/IEC 29151 以及預備文件 SD 4、SD 5 等)的標準化計畫，已於 2017 年 8 月完成第 1 階段之工作項目；並根基於歐盟與美國聯邦政府實作意見分成「管理」、「實作」與「技術」3 個面向，進行第 2 階段的標準制訂之計畫。

研究「標準化」的人是需要有「同情」與「推理」兩種能力，所謂「同情」是指「標準」的制定者要有對等之情，那樣體驗的「標準」自然是立體、多元的；「同情」加上「推理」，則「標準」是活的，每一份「標準」的頒布是因或是果，是趨勢或是成績，「標準」的產生絕非偶然而是無數之努力的形成。「標準化」從長遠的角度來看，便可以體察出是有一股流勢，有無法阻擋的推移力量；MSS 與個人資料保護標準化及 ISMS&PIMS 的整

合性安全管理系統(Integrated(Information) Security Management System，IISMS)之進程僅為一端。國際認證論壇(IAF)自 2013 年 3 月 25 日起，已發行整合性安全管理系統(IISMS)之第三方稽核的強制性文件(IAF MD 11：2013)，除規範 ISMS 之第三方稽核的要求事項外並闡明其效益。根基於此與雲端服務(cloud services)已成為資訊社會之礎石，主責 ISMS&PIMS 標準化的 ISO/IEC JTC 1/SC 27 第一階段標準化之工作項目如圖 1.1 所示。

根基於此，本文在第 2 節闡明個人資料管理系統要求事項標準化之進程；於第 3 節，探討雲端運算與資料去識別化等的新議題及其已納入 ISO/IEC WD 27552.2 之擴增 ISO/IEC 27001 的 PIMS 驗證之要求事項進程的闡明；最後，在第 4 節提出借鏡個人資料管理系統標準化之進程與議題，作為我國 PIMS 及資料去識別化標準化藍稿的見解並代為本文之結論。

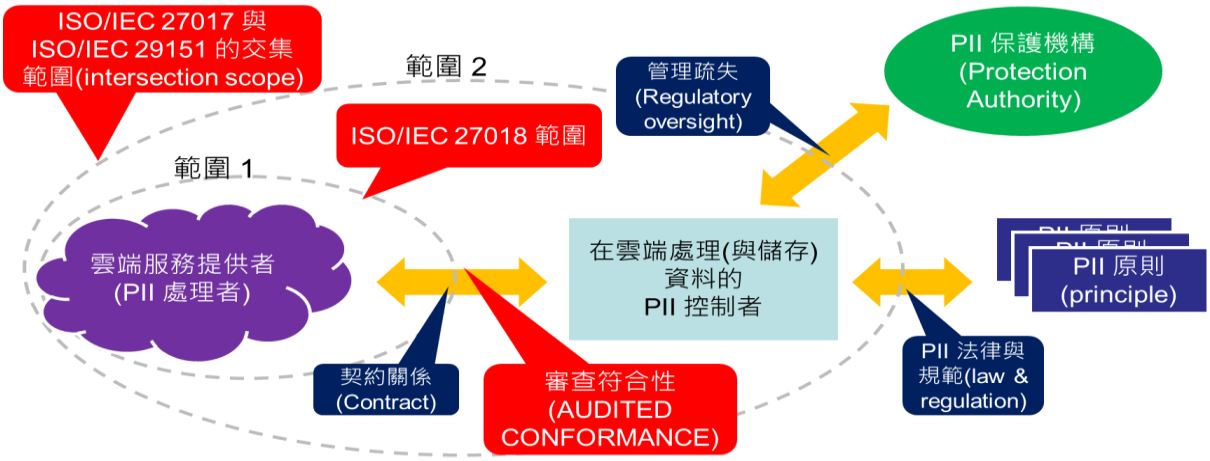

圖 1.1 雲端運算之 PIMS 控制措施的框架

說明：

1. PII 控制者(PII controller)(或稱為資料控制者(data controller)於某些管轄區(jurisdiction))意指決定個人資料處理或將要處理之目的(purpose)與方法(manner)之當事人(單獨一人、與他人共同)。
2. PII 處理者(PII processor) (或稱為資料處理者(data processor)於某些管轄區(jurisdiction)) 意指代表 PII 控制者處理資料之任何人(除了 PII 控制者的僱員外)。
3. 資料來源：Mitchell, C. (ISO/IEC 27018 編輯(editor)), Outsourcing personal data processing to the cloud(presentation),2012-02-16，圖中之「交集範圍(intersection scope)」係指「聚集(例：西江、北江與東江，三江匯流成為珠江)」。

貳、個人資料管理系統要求事項標準化之回顧與前瞻

2012 年 10 月，歷經 1 年 2 階段之研究，主責 PIMS 的要求事項之 ISO/IEC JTC 1/SC 27 的第 1 工作組(Working Group 1，WG 1)與主責隱私管理之第 5 工作組共同決定「個人資料管理系統」的要求事項根基於 ISO/IEC 27001 擴增之，同時立案進行其擴增

ISO/IEC 27002 控制措施的 ISO/IEC 29151 與擴增 ISO/IEC 27001 之規範的 ISO/IEC 27009 之標準化計畫；ISO/IEC 29151 已於 2016-12 進入 FDIS 階段，預定於 2017-07 正式發行，「資訊技術 – 安全技術 – ISO/IEC 27001 特定領域應用系統 – 要求事項(Information technology – Sector – specific application of ISO/IEC 27001-Requirements)」已於 2016-06-15 正式發行。為因應實作之需求， 2015 年 6 月 30 日，主責個人資訊安全標準化的 ISO/IEC JTC 1/SC 27/WG 5，根基於 ISO/IEC 27009 之標準化文件，先行公布擴增 ISO/IEC 27001 的 PIMS 要求事項之如圖 1 所示的第 5 號《於隱私領域中 ISMS 的應用指導綱要(Guidelines for the application of ISMS in the area of privacy)，簡稱 WG 5 SD5》之預備文件(Standing Document，SD)的徵求意見稿，並更新其標準化計畫框架如圖 2.1 所示；根基於此，公用雲(Public clouds)領域已據以(ISO/IEC 27001+ISO/IEC 27002+ISO/IEC 27018)進行驗證。2016 年 4 月，ISO/IEC JTC 1/SC 27/WG 1 根基於前述之 WG 5 SD5 之 PIMS 要求事項的「資訊技術 – 安全技術 – 於隱私管理之 ISO/IEC 27001 擴增- 要求事項(Information techniques – Security techniques – Enhancement (Extension) to ISO/IEC 27001 for privacy management – Requirements)」之 ISO/IEC 27552 之標準化計畫，並於 2016 年 12 月 5 日提出 ISO/IEC WD 27552.1 的票決版。2012 年 1 月，歐盟開始整合「個人資料保護指令(Directive 95/46/EC)」、「電子通訊隱私指令(Directive 2002/58/EC)」與「電信網路改革指令(Directive 2009/136/EC)」三大個人資料及隱私防護指令之法制，期以單一規則(Regulation)簡化機關/構以及企業的法規遵循義務並促進單一數位市場；2016 年 4 月 14 日經歐洲議會通過，於 2016 年 4 月 27 日公布之「一般資料保護規則(General Data Protection Regulation，GDPR)」，已提出個人資料「擬匿名化」之新定義並於條款 11 闡明「去識別化」的應然，條款 25 闡明應根基於「從設計以及預設機制著手保護個人資料(Data protection by design and by default)」實作 PIMS 之合適的「技術控制措施(technical measures)」與「組織控制措施(organizational measures)」。GDPR 於條款 40~43 規範其「行為準則及驗證(Codes of conduct and certification)」，認證機構遵循產品驗證標準規範驗證機構；根基於 GDPR，相關機構幾均公布採用 ISO/IEC 27001 作為其包含資料去識別化的 PIMS 合規之驗證要求事項的規範[16]。

「使用與應用 ISO/IEC 27001 在特定領域與服務之被認證的第 3 方規範(The Use and Application of ISO/IEC 27001 for Sector/Service-Specific Third-Party Accredited Certifications，ISO/IEC DIS 27009:2015-07-27)」之附錄 B(Annex B)，已以「個人資訊管理系統(Personal Information Management System, PIMS)」中的「隱私衝擊評鑑(Privacy Impact Assessment, PIA)」為例闡明 ISO/IEC 27009 之運用方式；依此，分別探討 ISO 個人資料保護標準化之進程以及整合性個人資料管理與資訊安全管理的「整合性安全管理系統(IISMS)」要求事項之脈絡。

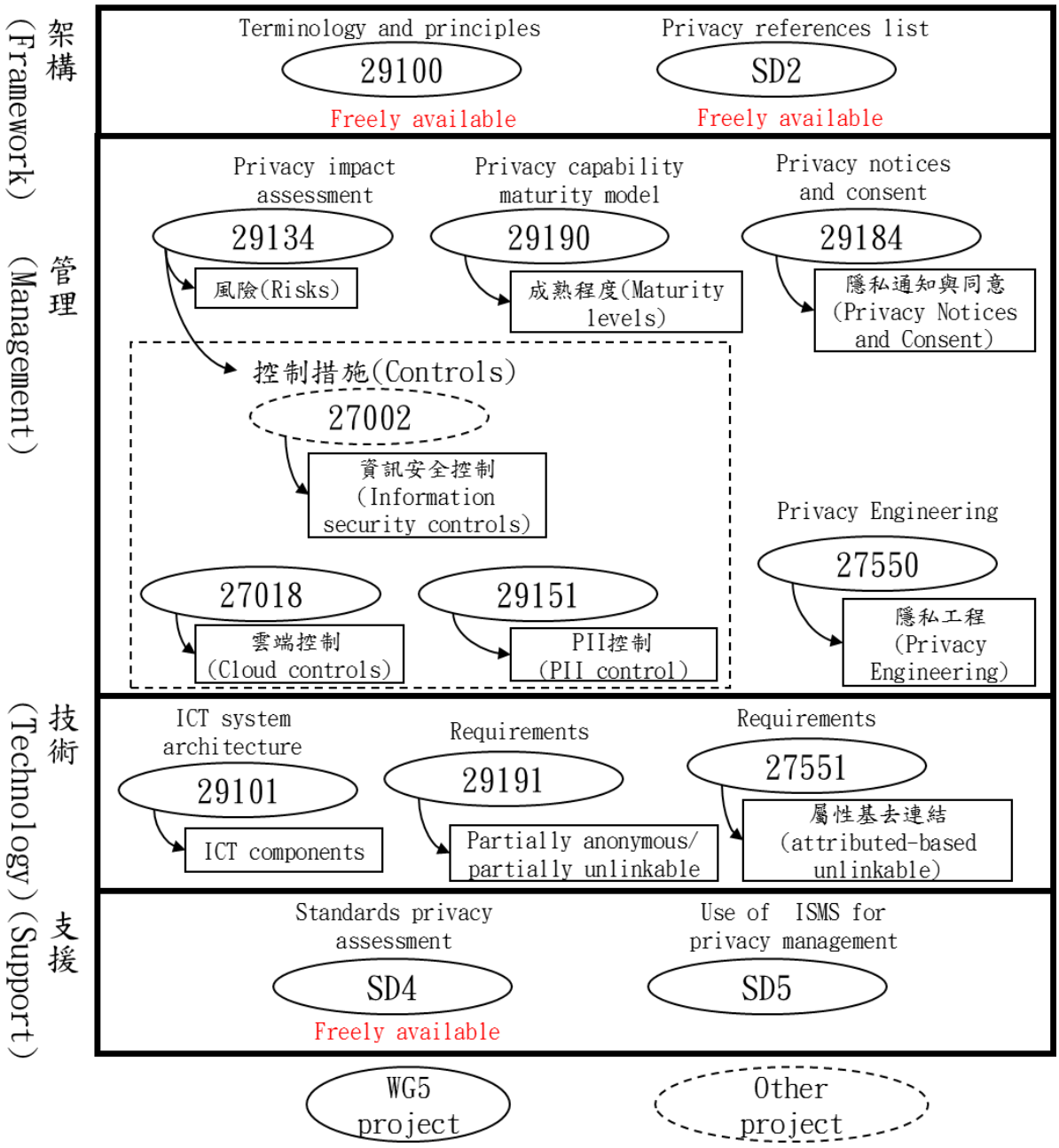

圖2.1 身分管理與隱私科技標準框架

說明：

1. 參考資料：Rannenberg, Kai (2015) Standards contributing to the protection of consumers' privacy and personal data, ISO/COPOLCO (2015). The connected consumer in 2020- empowerment through standards, 2015-05-13, Geneve, Switzerland.
2. ISO/IEC 27551為作者增列。

2002 年,美國先於「電子化政府法案(E-Government Act of 2002)」之第 208 節(Section)」中規範 PIA 的工作項目;2008 年,進一步於「聯邦資訊安全管理法案(Federal Information Security Management Act of 2002, FISMA 2002)」實作計畫中納入 PIA。2010 年 4 月美國國家標準與技術研究院(National Institute of Standards and Technology, NIST)公布「個人可識別資訊之機密性防護指引(Guide to Protecting the Confidentially of Personally Identifiable Information (PII))的 NIST SP(Special Publications) 800 – 122,作為 FISMA 實作計畫控制措施之規範;2013 年 4 月,根基並修訂 NIST SP 800 – 122 的內容後併入第 4 版之 FISMA 實作計畫控制措施規範「聯邦資訊系統與組織的安全與隱私控制措施(Security and Privacy Controls for Federal Information Systems and Organizations)」之 NIST SP 800 – 53 Revision 4 中,完成前述整合 ISMS 以及 PIMS 的標準化工作項目。2014 年 12 月 8 日,美國公布之「聯邦資訊安全現代法(Federal Information Security Modernization Act of 2014,FISMA 2014)的 3552(b)(3)(B)條款沿用 FISMA 2002 之 3542(b)(1)(B)條款,將「個人隱私(Personal Privacy)」納入;換言之,前述美國聯邦政府的「整合性安全管理系統」已建立法規依據[17]。

ISO 自 2000 年起,即以試作(Pilot: 2001~2005)、制定管理系統標準(MSS)之至次節的一致性高階規範程序(Procedures specific to ISO: 2006~2010)與完成各個管理系統之調合(2011~2015)的標準化工作項目;根基於此,ISO/IEC JTC 1/SC 27 於 2012 年 10 月決定 PIMS 直接使用 ISO/IEC 27001 之要求事項,並進行制定擴增其條款的 ISO/IEC 27009 之工作項目,在 2015-07-27 提出意見及投票之 ISO/IEC DIS 27009 的附錄 B 中已以 PIMS 之 PIA 為例,闡明如何擴增 ISO/IEC 27001 的條款;並考量時效性,於 2014 年 4 月 9 日,先行公布 PIA 之 ISO/IEC JTC 1/SC 27/WG 5 SD 4 的預備文件,圖 2.2 以及圖 2.3 分別是其示意說明。根基於此,各驗證機構紛紛公告以 ISO/IEC 27001 與 ISO/IEC 27009 作為 GDPR 之 PIMS 要求事項的驗證標準,應可作為我國落實「個人資料保護法」之參考[19]。

未雨綢繆,主責個人資料管理系統標準化(Personally Information Management System, PIMS)之 ISO/IEC JTC 1/SC 27/WG 5 於 2015-06-30 已公布遵循圖 2.3 之框架,如表 2.1 所示的資訊安全管理系統(Information Security Management System, ISMS)要求事項宜擴增的 PIMS 之論題及其隱私防護的攸關標準,表 2.2 是 PIMS 與 ISMS 間之用語對照。

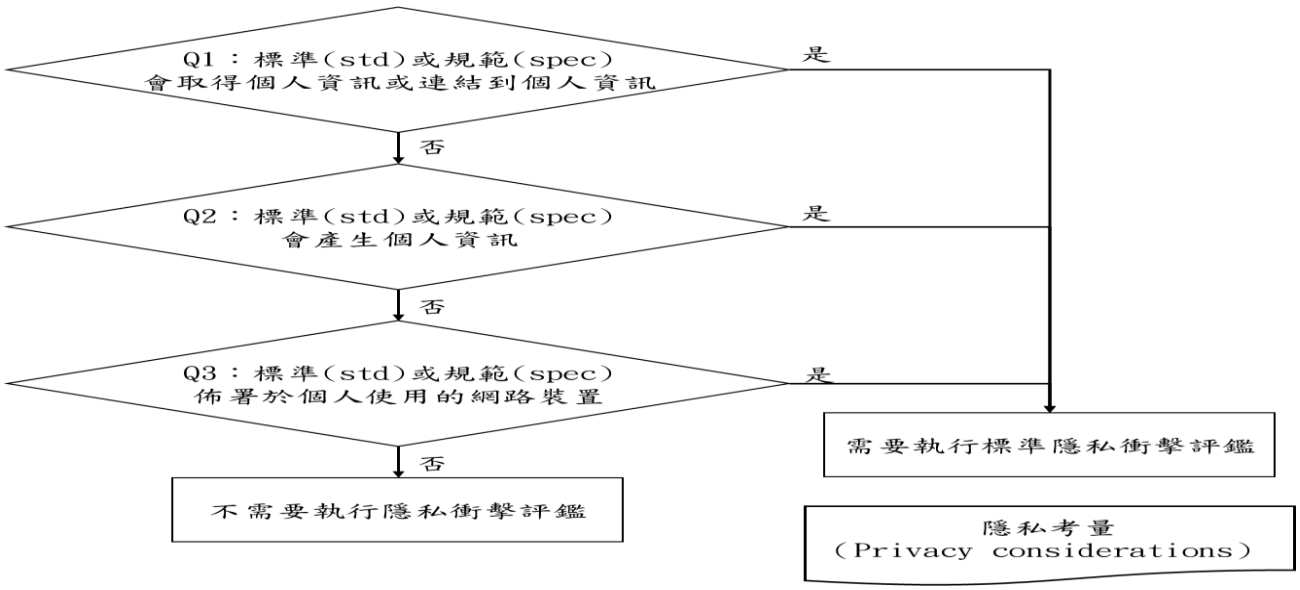

圖2.2 判斷何時需要執行標準隱私評鑑(Standards Privacy Assessment, SPA)
說明：ISO/IEC 29100：2012（E）中用語為：隱私衝擊評鑑（Privacy Impact Assessment, PIA）。
資料來源：ISO/IEC JTC 1/SC 27/WG 5 SD4: 2014

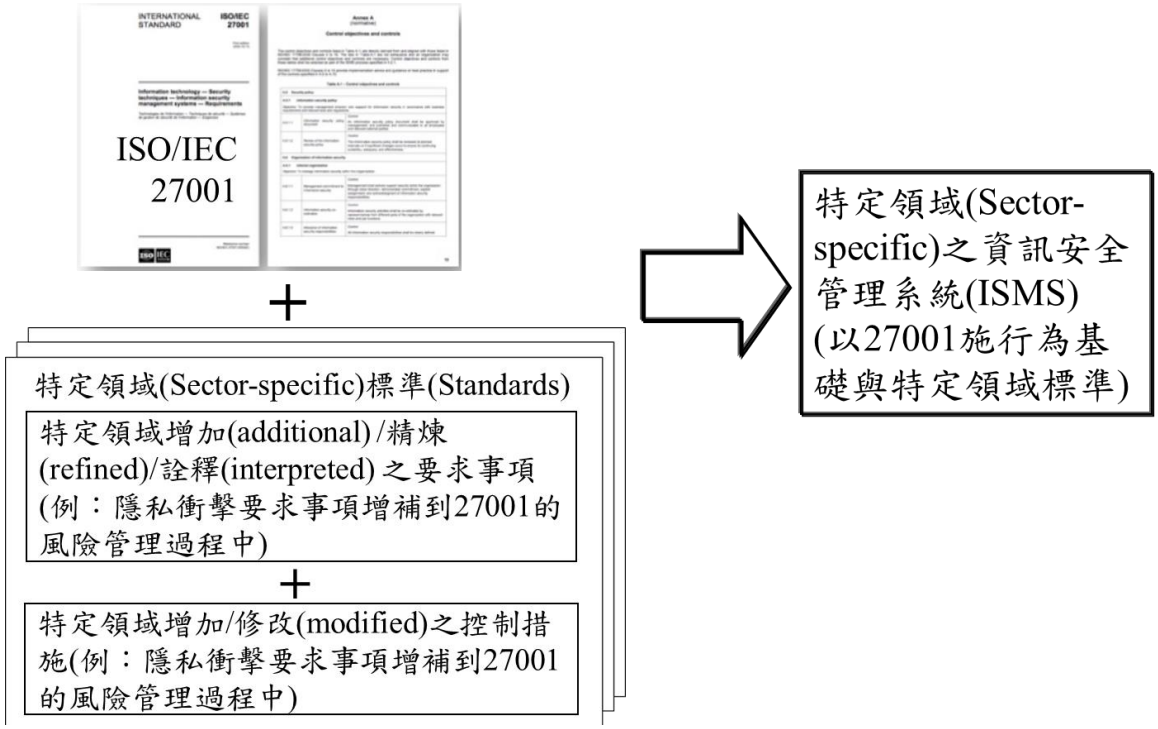

圖2.3 ISO/IEC 27009的應用
資料來源：ISO/IEC DIS 27009：2015-07-27.

表2.1 資訊安全管理系統要求事項與個人資料保護標準及論題之對應(ISO/IEC JTC 1/SC 27/WG 5 N110:2015-06-30)

條款節碼	ISO/IEC 27001:2013－要求事項	隱私攸關標準	論題
1	4. 組織全景 4.1 瞭解組織及其全景 4.2 瞭解關注方之需要及期望 4.3 決定資訊安全管理系統之範圍 4.4 資訊安全管理系統	ISO/IEC 29134 ISO/IEC 29100 ISO/IEC 29134	 隱私風險準則(Privacy risk criteria) 隱私保護要求事項(Privacy safeguarding requirements) 隱私利益相關者(Privacy stakeholder) 營運流程與目的(Business process and purpose) 個人可識別資訊流程, 隱私之支持資產(PII Flow, Privacy supporting assets)
2	5.領導作為 5.1 領導及承諾 5.2 政策 5.3 組織角色、責任及權限	 ISO/IEC 29100	 從設計著手/默認保護隱私(Privacy by Design/Default) 隱私政策(Privacy policy) 資料隱私管理官(Data Privacy Officer) 隱私風險擁有者(Privacy risk owners)
3	6.規劃 6.1 因應風險及機會之行動 6.2 資訊安全目標及其達成之規劃	ISO/IEC 29134	隱私衝擊評鑑(Privacy impact assessment) 隱私風險評鑑(Privacy risk assessment) 隱私風險處理(Privacy risk treatment)
4	7. 支援 7.1 資源 7.2 能力 7.3 認知 7.4 溝通或傳達 7.5 文件化資訊		 隱私事故管理(Privacy Incident Mgmt) 隱私意識(Privacy awareness) 隱私溝通, 透明化(Privacy communication, transparency)
5	8. 運作 8.1 運作之規劃及控制 8.2 資訊安全風險評鑑 8.3 資訊安全風險處理	 ISO/IEC 29134 ISO/IEC 29151	 隱私生命週期管理(Privacy Life cycle Mgmt) 隱私風險評鑑(Privacy risk assessments) 隱私風險處理(Privacy risk treatment)
6	9. 績效評估 9.1 監督、量測、分析及評估 9.2 內部稽核 9.3 管理審查	ISO/IEC 29151 *[ISO/IEC 29190[1]]*	隱私測量(Privacy measurement) 隱私能力成熟度*[Privacy capability maturity]*
7	10.改善 10.1 不符合項目及矯正措施 10.2 持續改善		

8	附錄 A(規定)參考控制目標及控制措施	ISO/IEC 29151 ISO/IEC 27018	隱私控制措施(Privacy controls)

說明1：編輯闡明，不適當待修定。

表2.2 對照CNS 29100概念與CNS 27000之隱私概念

CNS 29100 概念	對應 CNS 27000 概念
隱私權利害相關者	利害相關者
PII	資訊財產
隱私權違反	資訊安全事故
隱私控制措施	控制措施
隱私風險	風險
隱私風險管理	風險管理
隱私保全要求事項	控制目標

說明：個人可識別資訊(Personally Identifiable Information, PII)

為易於特定隱私全景中使用 CNS 27000 系列標準及整合 CNS 27000 之隱私觀念，CNS 29100 於其附錄 A 已列出其主要概念間之關係；惟以 CNS 27001 第 6.1.2 節(c)(2)的風險擁有者為例，於資訊安全，其對應之資訊資產的當事人(Principal)幾均在組織內，而 PII 當事人大多在組織外，其歧異處具攸關性；根基於此，CNS 29100 再將組織內之風險擁有者區分為 PII 控制者(PII controller)與 PII 處理者(PII processor)，於公用雲的 CNS 27018 即為其 PIMS 之 PII 處理者的擴增 CNS 27002 之控制措施標準，其與 2016 年 12 月 16 日提出之 ISO/IEC FDIS 29151 的票決版，已分別作為 2016 年 12 月 5 日提出之 ISO/IEC WD 27552.1 之強制性的「附錄 A：PII 控制者之控制目的與控制措施」以及「附錄 B：PII 處理者之控制目的與控制措施」之參考藍本，圖 2.3 所示的 PIMS 要求事項標準化第 1 階段如圖 2.4 之工作項目將於 2017 年完成，圖 2.5 是其實作過程的示意說明；ISO/IEC 27005 已確認存在缺失[10]，實作時，宜關注此議題。

2017 年 1 月，ISO/IEC JTC 1 SC 27/WG 5 公布了如圖 2.6 所示之下一階段的個人資料/隱私管理之標準化框架，針對「智慧手機應用程式提供者」、「智慧城市」與「物聯網」的雲服務，其新增之應用範圍均涉及大數據分析的資料去識別化之議題。除進行中的「資料去識別化」之 ISO/IEC 20889 標準化計畫，並新增「屬性基去連結」的 ISO/IEC 27551 以及線上(online)之「隱私聲明與許可」的標準化計畫，作為支持 PIMS 要求事項之準備；在另一方面，為因應 GDPR 規範之擬匿名化，針對 PII 去連結的需求與 PIMS 之控制措施應區分「PII 控制者」及「PII 處理者」等的不同之要求事項，立項進行 ISO/IEC 27552 的標準制定計畫[11]；換言之，內蘊資料去識別化的 PIMS 已成為數位社會之關鍵基礎建設。

2016 年 12 月 3 日，因應圖 2.4 中之 ISO/IEC 27005 的缺失(defect)，經 1 年研究期(study period)之求索，ISO/IEC JTC 1/SC 27/WG 1 已正式發出闡明 ISO/IEC 27001:2013(E) 第 6.1 節以及第 8 節「因應風險與機會之行動」的「資訊安全風險與管理指南」之 ISO/IEC 27005 新版的設計規範草案，圖 2.4 框架中之 ISO/IEC 27005 已更新其內蘊；根基於表 2.1 的 ISO/IEC 27552 之標準制定計畫亦同[8]。

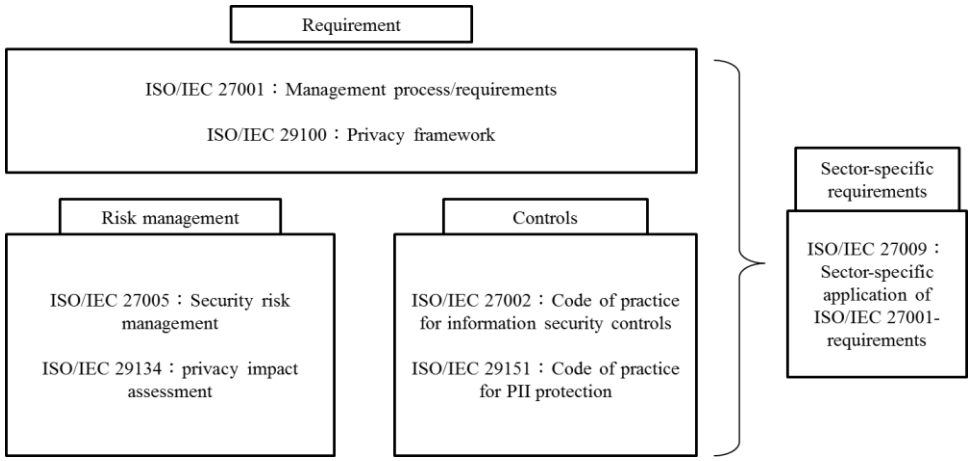

圖2.4 個人資料/隱私資訊管理系統驗證框架

說明：
1. 參考資料：ISO/IEC FDIS 29151, Figure 1, page X, 2016-12-20.
2. 隱私/個人資訊管理系統(Privacy/personal information management system, PIMS)。

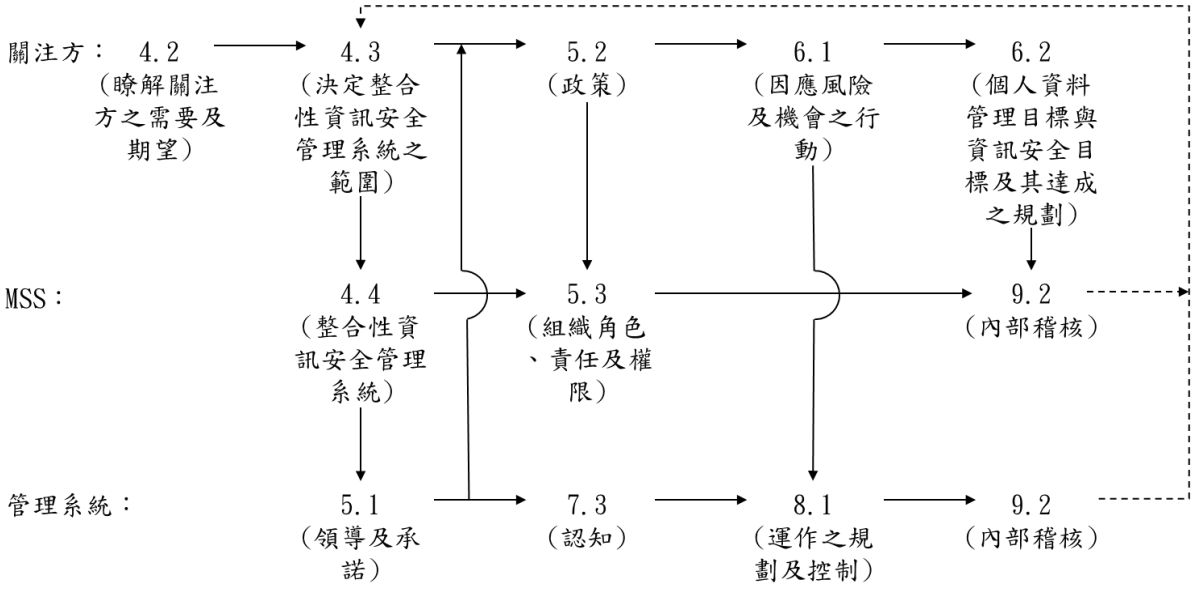

圖2.5 管理系統標準(Management System Standard, MSS)中之要求事項(Requirement)的分類與取徑示意(Approach)：根基於ISO/IEC 27001：2013(E)

說明：
1. 參考資料：Proposals for Management System Standards, ISO/IEC Directives Part 1, Consolidated ISO Supplement, Annex SL(Normative), 6th ed, 2015。
2. ISMS：Information Security Management System

ISO/IEC WD 27552.2 遵循 ISO/IEC 27009：2016-06-15，於 ISO/IEC 27001 本文部

分，參照 SD5，擴增第 4 節(組織全景)之 4.0~4.1、6.1.3c)(風險評鑑)與 6.1.3d)(風險處理)條款；於 ISO/IEC 27001 附錄 A(控制措施)部分，擴增 16 項控制措施；於 PII 控制者部分，增加 11 類共 47 項控制措施；於 PII 處理者部分，增加 11 類共 36 項控制措施；期於 PIMS 的實作，提供驗證之要求事項。舉例而言，於「資料去識別化」的工作項目，於 ISO/IEC WD 27552.2 第 6.2 節「PII 控制者的 ISO/IEC 27002 之增加」的 PIMS A 4.3 條款：「個人可識別資訊利用之外(PII beyond use)」中闡明由 PII 控制者主責，其實作指引敘明其技術參照 ISO/IEC 20889 中描述(雲端運算於透明性(transparency)等宜遵循 ISO/IEC 19944)，圖 2.7 是「資料去識別化」之「重新識別風險評鑑」與「隱私風險評鑑」關聯的參考[30]。

綜上所述，於現階段，PIMS 之實作除遵循 ISO/IEC 27001、ISO/IEC 27002、ISO/IEC 27005、ISO/IEC 27009、ISO/IEC 27018、ISO/IEC 29100、ISO/IEC 29134、ISO/IEC 29191 外、宜再增列 ISO/IEC WD 27552.2；若採行「從設計著手保護隱私(Privacy by design，PbD)」與「以預設機制保護隱私(Data protection by default 或 Privacy by default，PbD)」之原則，ISO/IEC 29101、ISO/IEC 27550 亦宜增列；於歐盟，前述 PbD 係法規(GDPR)的要求事項。

「他山之石，可以攻玉」，參照美國的 FISMA 實作計畫與歐盟 GDPR 之驗證規範，其以 ISO/IEC 27001 加 ISO/IEC 27009(ISO/IEC 27552)作為 PIMS(含去識別化：於 ISO/IEC WD/CD/DIS/FDIS/IS 29151 均將資料去識別化納入其資料最小化的控制措施之中)的「服務(services)」之要求事項，於「產品(products)」的安全功能則要求遵循 ISO/IEC 15408；綜上所述，針對 PIMS 驗證標準之要求事項及其實作的標準化之工作項目，應是我國宜面對之議題。

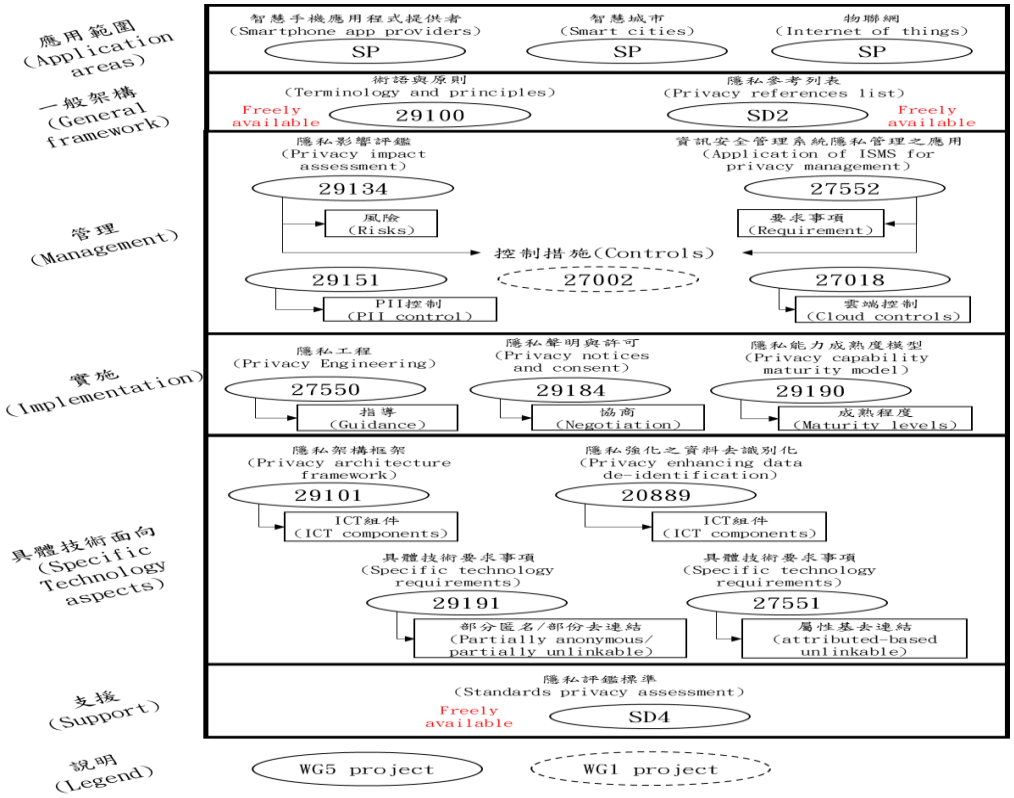

圖 2.6 個人資料管理要求事項之 ISO/IEC JTC 1/SC 27/WG 5 與 WG 1 的標準化框架 (2017-01)

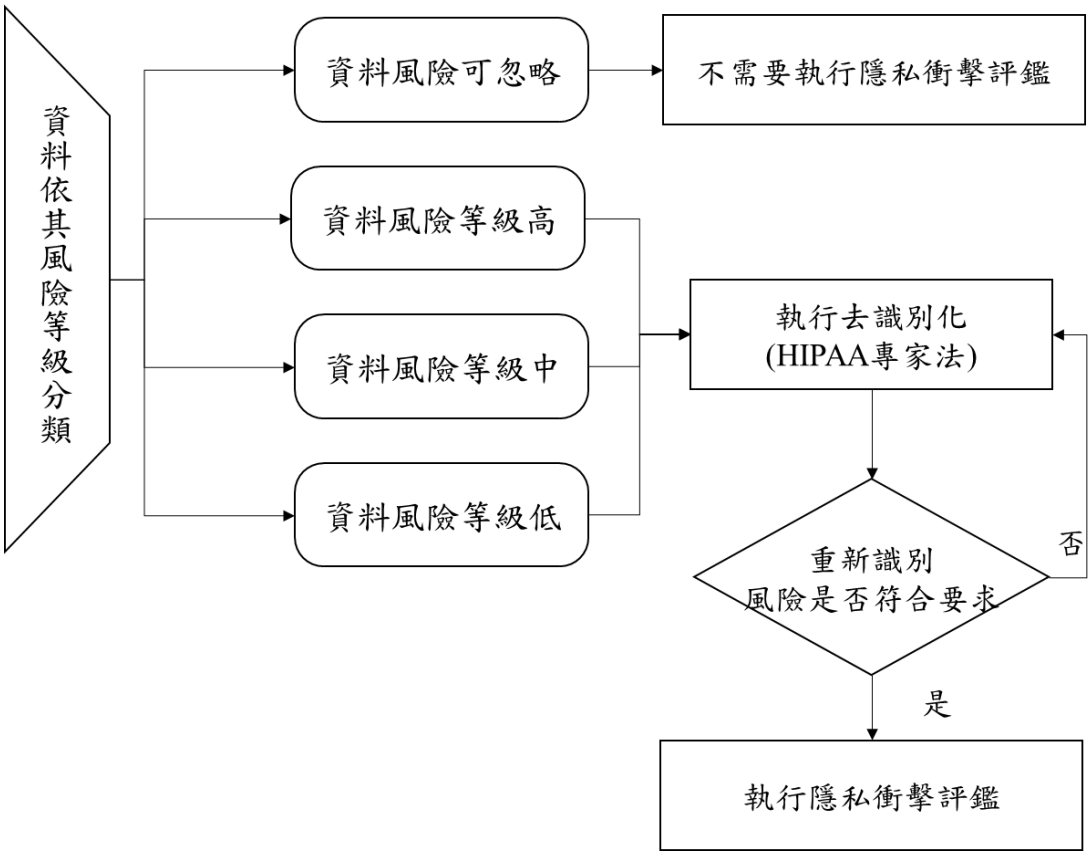

圖 2.7 HIPAA(Health Insurance Portability and Accountability)風險評鑑流程圖

參、雲端運算服務與個人資料管理之標準化初探

隨著雲端運算之日益普及，如何確保「雲服務客戶(Cloud service customer，CSC)」的個人資料安全，已成為「雲服務提供者(Cloud service provider，CSP)」與 CSC 必須共同面對之議題，亦為圖 2.6 中各個應用範圍的基石；在另一方面，大數據分析已勢不可當，如何在其分析之過程中確保個人隱私已成為 PIMS 的新課題，表 3.1 是雲服務標準化之此議題用語與資料去識別化標準化的對應；以雲服務先行者之網飛(Netflix)公司為例，其 75 %之影片瀏覽均來自「推薦服務(recommendation service)」；2013 年，網飛公司推出以政治權謀為主的第 1 部自製影片「紙牌屋」時，針對不同群組經由大數據分析設計了 7 種版本之預告片[6]；如何探勘顧客的喜好予以分群(例：同溫層(stratosphere))並產生推薦之剖繪(profile)，並且不侵犯隱私已成為「資料去識別化」求索的議題。2010 年 3 月 19 日，網飛公司即因推薦服務演算法競賽事宜，因前述議題遭到 4 位顧客提告，以 US$9,000,000 和解。

表3.1 ISO/IEC 19944與ISO/IEC 20889於資料去識別化用語之對應

ISO/IEC DIS 19944 資料識別限定符 (qualifiers)之資料狀態描述	隱私增強資料(Privacy enhancing data)之去識別技術，其應用產生的相對應狀態
識別資料 (Identified data)	包含識別符的原始、未處理的資料;換句話說，即是還沒有應用去識別化技術;對於其他限定符，識別符已被移除（遮蔽）。
擬匿名化資料 (Pseudonymized data)	使用具有可控制之重新識別的可能/實現之擬匿名化技術處理的資料。
不可連結之擬匿名化資料 (Unlinked pseudonymized data)	使用沒有可控制之重新識別的擬匿名化技術處理的資料。
匿名化資料 (Anonymized data)	使用概化(generalization)和/或隨機化(randomization)技術處理的資料。
聚集資料 (Aggregated data)	使用聚集(aggregation)技術處理的數據。

資料來源：ISO/IEC CD 20889.2：2016-12-02, Information technology – Security technology – Privacy enhancing data de-identification techniques, Annex B.

雲服務於 PIMS 之 CSC 與 CSP 的權責劃分如圖 3.1 所示，其中 CSC 是資料控制者，CSP 是資料處理者，圖 2.4 中的 ISO/IEC 29151 並未區分「PII 控制者之控制目的與控制措施」以及「PII 處理者之控制目的與控制措施」；2016 年 4 月，ISO/IEC JTC 1/SC 27 議決進行 ISO/IEC 27552 作為擴增 ISO/IEC 27001 之 PIMS 驗證要求事項的標準制定之工作項目。

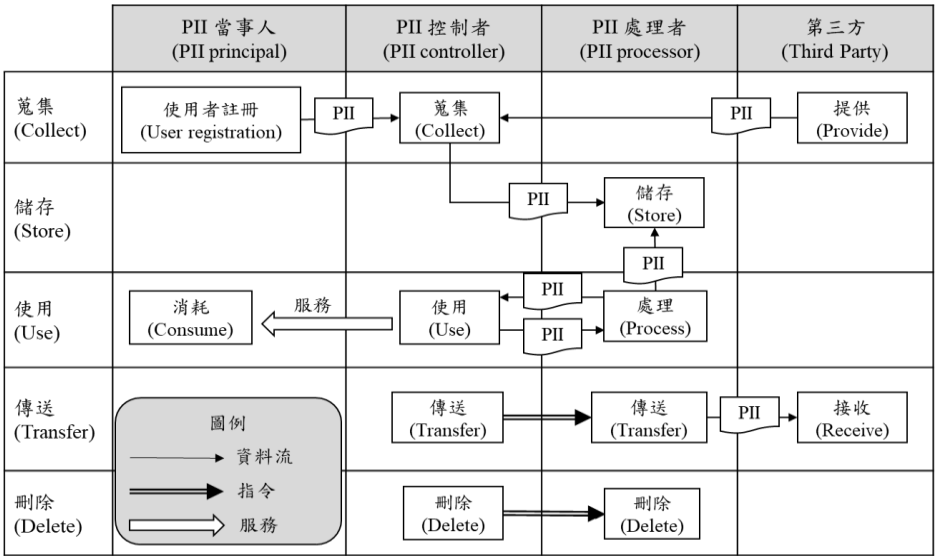

圖 3.1 PII 處理工作流程圖

說明：
1. PII：個人可識別資訊 (Personally identifiable information)
2. 資料來源：ISO/IEC 29134: 2017-06, Information technology – Security techniques – Privacy impact assessment – Methodology, p.41, Figure D.1(根據ISO/IEC 29134：2017(E)第6.4.1節) .

ISO/IEC JTC 1/SC 27 遵循 ISO/IEC 27009：2016-06-15，制定 ISO/IEC 27552，在 2017-06-01 公布之 ISO/IEC WD 27552.2，期於 PIMS 的實作，提供其驗證要求事項規範之準繩。舉例而言，於「資料去識別化」的工作項目，在 ISO/IEC WD 27552.2 之第 6.2 節：「PII 控制者的 ISO/IEC 27002 之增加」的 PIMS A.4.3 條款：「個人可識別資訊利用之外(PII beyond use)」中闡明由 PII 控制者主責，其實作指引並敘明其技術在 ISO/IEC 20889 中敘述[12][13]；在「雲服務及其裝備：資料流、資料分類與資料利用」的「透明性(transparency)」等，宜遵循 ISO/IEC 19944：2017-08。在另一方面，在 ISO/IEC WD 27552.2 之 PIMS A.8.4 條款：「蒐集或抹除(Correction or erasure)」，已關聯至「雲服務層級框架協議(Cloud service level(SLA) framework agreement)」的 ISO/IEC 19086-1：2016-09-21 第 10.7.2 與 10.12.8 節提出之如圖 3.2 所示的「資料淨化(Data sanitization)」中，「應用物理(physical)或邏輯(logical)之技術，確保標的資訊無法在實驗室之藝境(state of the art)中，致使其「回復(recovery)」的「廢止(purge)」中之「抹除(erase)」的邏輯技術[9][14]，表 3.2 是 ISO/IEC 27552 範疇合規之闡明，其中「抹除」於 GDPR 的「被遺忘權」之「實作(控制措施)」係指「廢止」中的「密碼式抹除」。

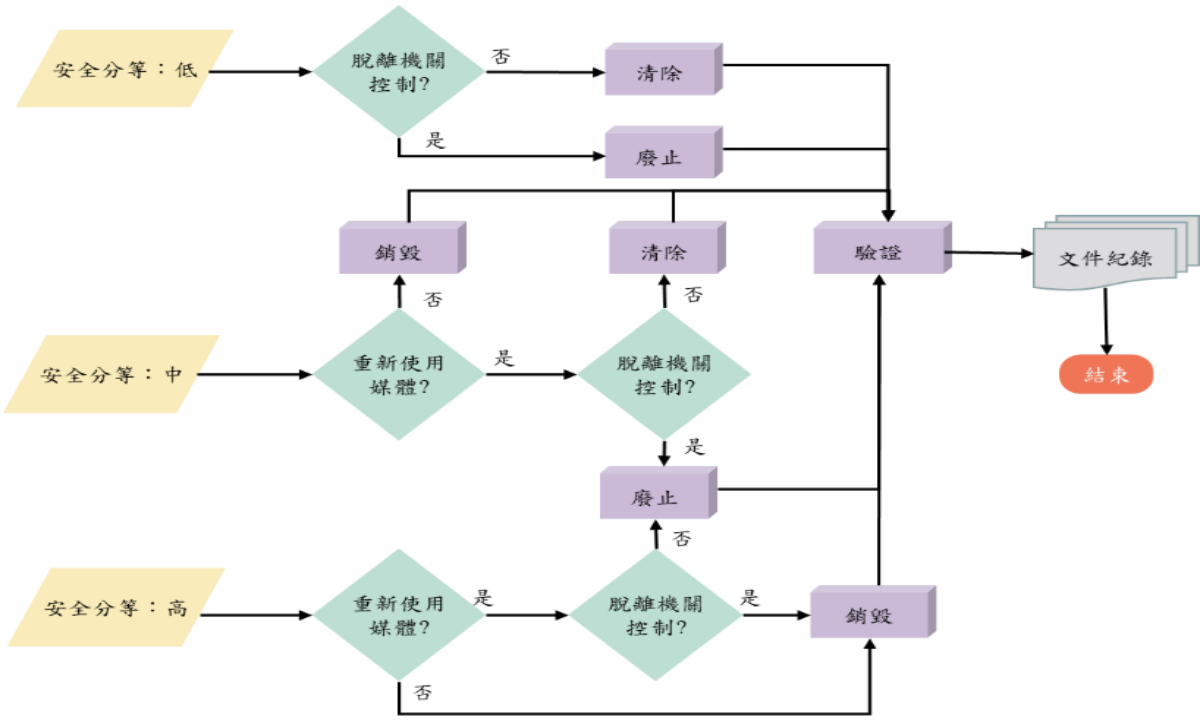

圖 3.2　資料清理(Sanitization)與處理(Disposition)決策流程

說明：

1. 清除(Clear)：使用邏輯性技術(logical techniques)來清理(sanitize)所有用戶可定位(user-addressable)之儲存位置(storage locations)的數據，以防止簡單的非侵入式(non-invasive)資料恢復技術。
2. 廢止(Purge)：使用最先進之實驗室的物理性(physical)或邏輯性技術，使目標資料無法恢復。
3. 銷毀(Destroy)：使用最先進的實驗室技術使目標資料無法恢復且使得後續無法使用該媒介(media)儲存資料。

資料來源：Kissel, Richard, et al. NIST SP 800-88 Rev. 1. Guidelines for Media Sanitization, National Institute of Standards & Technology,Figure 4.1,Page 17, 2014-12.

表3.2 ISO / IEC 27552 之組織證據(organizes evidence)

技術與組織之控制措施 (Technical & Organizational Measures)	● 去識別化(de-identification)(ISO/IEC 20889)與抹除(erasure)(ISO/IEC 27040)以支持資料最小化(data minimization) ● 接收(receiving)、記錄(documenting)和修改(modifying)同意書 ● 支援資料主體之權利(存取(access)、可攜帶(portability)、修正(correct)及抹除(erase)) ● 資訊安全遵照 ISO/IEC 27001、ISO/IEC 27002以及ISO/IEC 29151
記錄保存 (Record Keeping)	● 處理之目的 ● 處理之合法基礎 ● 對第三方單位之揭露(disclosure)與傳輸(transfer) ● 地理位置(geolocation) ● 為了負責(accountability)而保存紀錄
規範遵守之展示 (Demonstrate Adherence)	● 處理者之義務遵照 ISO/IEC 27018 ● 資料主體之風險遵照隱私影響評鑑(Privacy Impact Assessment)，即 ISO/IEC 29134，從設計著手及以預設機制進行保護資料(Data protection by design and by default，PbD)(ISO/IEC 29101以及ISO/IEC 27550) ● 同意與告知(online)(ISO/IEC 29184)、資料可攜性(ISO/IEC 19941)，自動決策以及剖析(profiling)（待定）
資料主體的透明性 (Transparency to data subjects)	● 資料主體之透明性遵照 ISO/IEC 19944 之資料使用之陳述(statements) ● 控制者、處理者之透明性遵照 ISO/IEC 19086

參考資料：Laura Lindsay, 2017, ISO/IEC JTC 1/ SC 27 Work in Support of Legislation, https://docbox.etsi.org/Workshop/2017/201706_SECURITYWEEK/01_STANDARDSandLEGISLATION/S01_SETTING_THE_SCENE/ISO_IECJTC1_SC27_LINDSAY.pdf

使用密碼學技術之「密碼式抹除(Cryptographic erase)」亦可執行「清除」與邏輯性技術「廢止」的工作項目，並提供「金鑰回復(Key Recovery)」之選項，提供系統停機時自動保護資料的控制措施；以磁碟機為例，具備前述之整合「存取控制(access control)」的「密碼式抹除」之整體功能者名為「自加密磁碟機(Self-Encrypting Drives，SED)」[14]，於「雲端運算服務水準協議」標準系列的 ISO/IEC 19086-1：2016(E)中之第 10.12.8.1 條款敘明可以圖 3.2 的「資料清理」過程代替「資料刪除(data deletion)」；換言之，於實作，SED 已是雲端運算供應者(Cloud Service Provider，CSP)「資料刪除組件(data deletion component)」的元件(element)之一[9]，圖 3.3 是「雲端運算服務」標準化的示意說明。

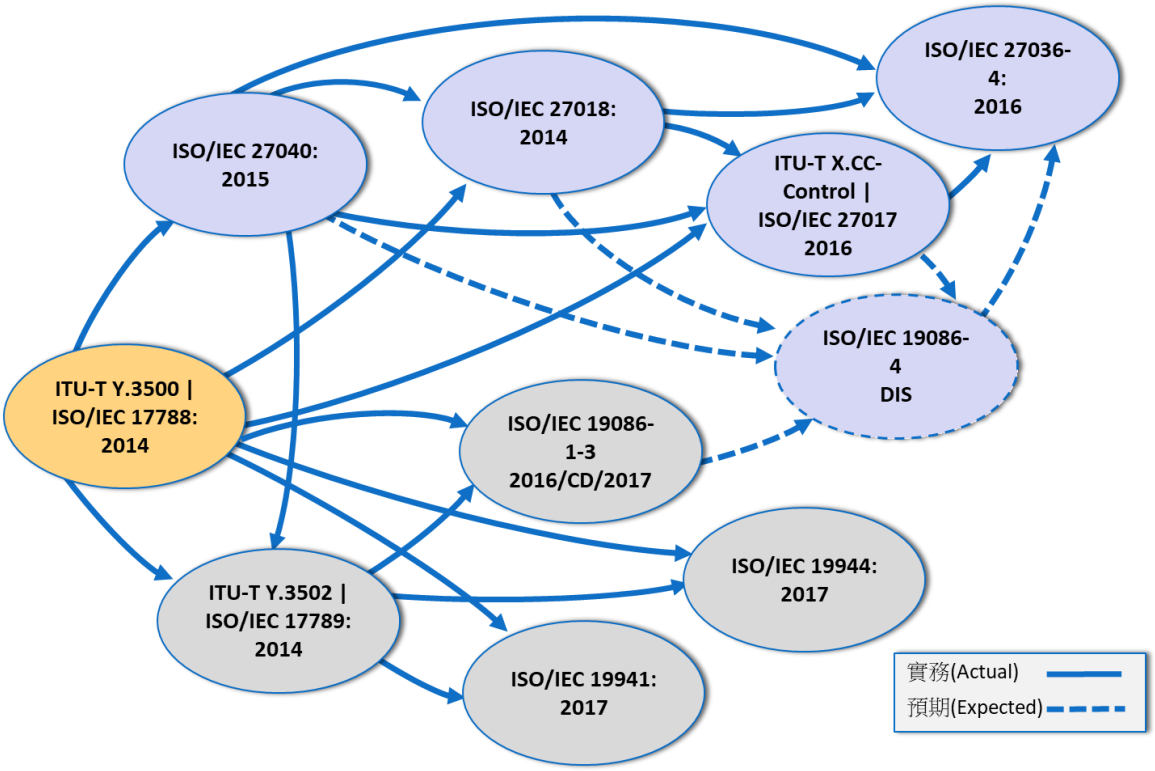

圖 3.3 雲端運算標準化(Standardization of Y.3500 (e.g., ISO))
參考資料：NIST&ISO&ITU,2017-08-23

於美國，健康、金融等領域，如表 3.3 所示，均以法規要求執行「資料清理」工作項目以保護個人資料，並制定 US$10,000~1,000,000 與「1%之資產(1% of assets)」等的未執行「資料清理」之相關罰則。

表3.3 要求執行資料清理之美國相關法規列表

法規名稱
健康保險可攜與責任法(Health Information Portability and Accountability Act，簡稱 HIPAA)
個人資訊保護與電子文件法(Personal Information Protection and Electronic Documents Act，簡稱 PIPEDA)
格雷姆-里奇-比利雷法案(Gramm-Leach-Bliley Act，簡稱 GLBA)，亦稱金融服務現代化法案(Financial Services Modernization Act)
加州資料隱私法案(California Senate Bill 1386)
沙賓法案(Sarbanes-Oxley Act, 簡稱 SBA)
美國證券交易委員會(United States Securities and Exchange Commission,簡稱 SEC)規定：第 17a 條(SEC Rule 17a)

資料來源：Hughes, Gordon, and Tom Coughlin. "Tutorial on disk drive data sanitization." cmrr.ucsd.edu/people/Hughes/DataSanitizationTutorial.pdf (2006).

「資料去識別化」同表 3.1 所示，ISO 尚在制定標準中[13]，表 3.4 是 GDPR 於個人資料保護層級之框架，表 3.5 是微軟公司(Microsoft)法務人員依據 ISO/IEC CD 20889.1 提出的去識化技術與大數據應用情境之框架，可作為其標準化法律遵循的參考。

表3.4 GDPR之層級

	已識別化 (Identified)	可識別化 (Identifiable)	Article 11 之去識別化 (De-Identified)	匿名化/彙集化 Anonymous /Aggregate
與識別資料(identifying data)直接連結(Directly linked)	是	否	否	否
已知(Known)、有系統性方法(systematic way)的(重新)識別((re)identify)	是	是	否	否
和特定對象(specific person)相關(Relates)	是	是	是	否

說明：

1. GDPR Article 11規範不須識別時資料的處裡程序，其包含兩個部分：
   a. 當個人資料無法(再)識別資料主體，管理者不應再強制維持、取得、處理額外資訊以識別資料主體。
   b. 當發生上述情形時，管理者應有能力展示其資料無法識別該資料主體，(若可能)並通知當事人。
2. 資料來源：Hintze, M. (2016). Viewing the GDPR Through a De-Identification Lens: A Tool for Clarification and Compliance.

圖3.1中，「PII控制者」與「PII處理者」之處理過程已與如圖3.4、表3.6所示的「資訊與通訊技術(Information and communication Technology，ICT)供應鏈風險管理(Supply Chain Risk Management，SCRM)」相關；圖3.5是ICT SCRM標準化之產品/系統/服務的供給面之關聯示意及其角色的說明，圖3.6是前述「密碼式抹除」使用之「密碼模組晶片」已建立的ICT SCRM之驗證框架，表3.7是其說明[29]。

表3.5 大數據應用情境及資料去識別化技術之隱私量測

		1	2	3	4	5	6	7	8	9
	共享情境 (Sharing scenario) / 去識別化(De-identification) 技術(technique)	資料僅限於基元合法實體(Data is restricted to an atomic legal entity)	資料存取權僅限於合法實體(Access to data is provided within a legal entity)	資料公開僅限於合法實體(Data is published within a legal entity)	存取資料由服務層級協議或合約規範(Access to data is provided under SLA or contract)	公開資料由服務層級協議或合約規範(Data is published under SLA or contract)	資料提供公開存取(Public access is provided to data)	資料對一般大眾公布(Data is published to the general public)	由個體蒐集去識別化資料(De-identified data is collected from individuals)	由個體蒐集原始資料(Raw data is collected from individuals)
1	無	O	R	R	R	R	I	I	NA	FFS
2	可控制的重新識別之擬匿名化(Pseudonymization with controlled re-identification)	C	O	O	R	R	I	I	NA	FFS
3	擬匿名化(Pseudonymization)	C	O	O	R	R	I	I	FFS	FFS
4	遮罩識別符 (Masking of identifiers)	C	O	O	R	R	I	I	FFS	FFS
5	遮罩離群值與選擇的部分識別符 (Masking of outliers and selective quasi-identifiers)	C	O	O	R	R	I	I	FFS	FFS
6	泛化選擇的部分識別符(Generalization of selective quasi-identifiers)	C	O	O	R	R	I	I	FFS	FFS
7	隨機選擇的部分識別符(Randomization of selective quasi-identifiers)	C	O	O	R	R	I	I	FFS	FFS
8	針對部分識別符實作K匿名模型(Implementing K-anomymity model for quasi-identifiers)	C	O	O	O	O	R	R	NA	FFS
9	產生合成資料(Creating synthetic data)	C	C	C	O	O	R	R	NA	FFS
10	泛化彙集的資料/數據Generating aggregated data/statistics	C	C	C	O	O	R	R	NA	FFS
11	實做差分隱私伺服器模式(Implementing DP server model	C	C	C	O	O	O	O	NA	FFS
12	實做差分隱私局部模式(Implementing DP local model)	C	C	C	O	O	O	O	O	NA

C	O	R	I	FFS	NA
保守 (Conservative)	選擇性 (Optional)	有風險 (Risky)	不適宜 (Inappropriate)	待研究 (For future study)	不適用 (Not applicable)

註：論文中敘明表中所示的潛在風險水平僅僅是根據作者的知識和經驗來舉例說明不同利益關係者如何使用該框架的方法。

說明：DP 是「差分隱私(differential privacy)」之縮寫。

資料來源：Orit Levin and Javior Salido (2016)The Two Dimensions of Data Privacy Measures, page 3, Corporate External and Legal Affairs, Microsoft.

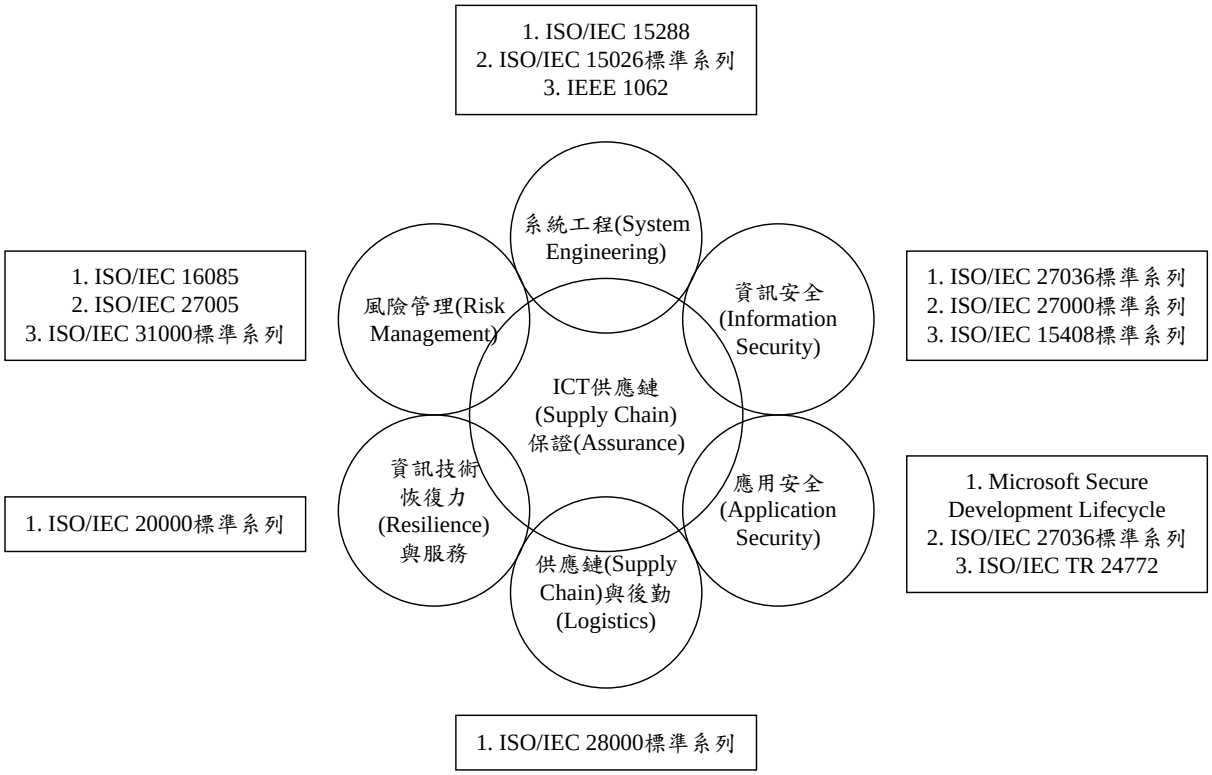

圖 3.4 資訊與通信技術(Information and Communication Technology，簡稱 ICT)供應鏈(Supply Chain)風險管理(Risk Management)要求規範之系列標準舉隅
資料來源：http://www.dhs.gov/ (2011-07-01)與本研究

表 3.6 ICT SCRM 系列標準(ISO/IEC 27036: Information Technology – Security Techniques – Information Security for Supplier Relationships)表列

Part 1	Overview and Concepts：2014-04-01。
Part 2	Requirements：2014-08-01。
Part 3	Guidelines for Information and Communication Technology Supply Chain Security：2013-11-15。
Part 4	Guidelines for Security of Cloud Services：2016-10-01。
備考：計畫於 2011 年公布，2016 年完成。	

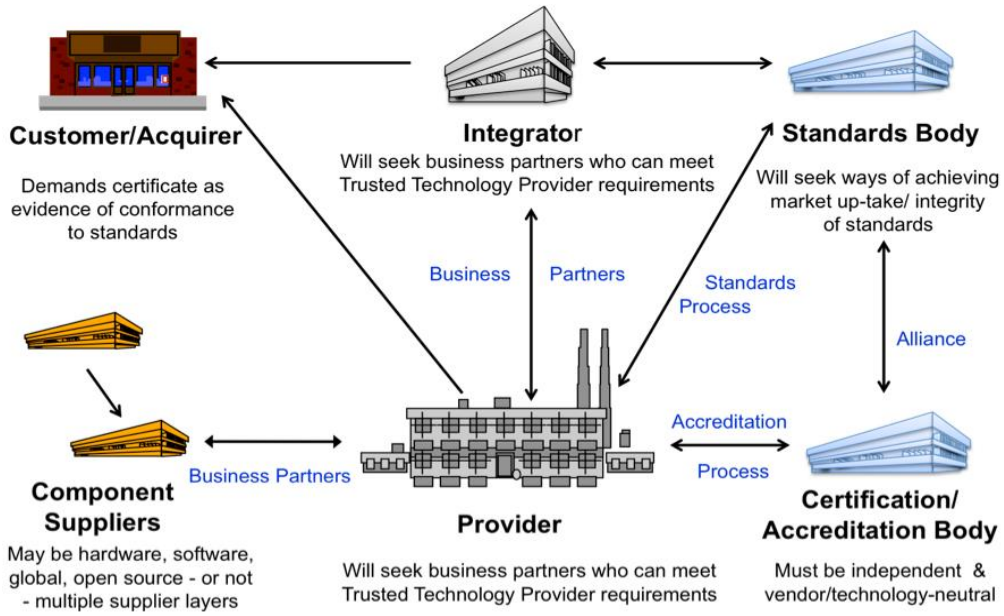

圖 3.5 ICT SCRM (Supply Chain Risk Management)標準化之產品/系統/服務的供給面之關連(ISO/IEC 27036-6)示意

參考資料：The Open Group (2012) Open Trusted Technology Provider Standard (O-TTPS)–Mitigating Tainted and Counterfeit Products (Snapshot), Figure 1, Page 5, February 2012。

圖 3.6 ISCI WG 2012 Contributors

資料來源：Dr. Gutau, W. and J. Noller (2012) Minimum Site Security Requirements for the Smart Secure Device Supply Chain (Presentation), Sept. 2012, 13 ICCC, Paris.

表3.7 資訊與通信供應鏈驗證例

1. ISCI: International Security Certification Initiative.
2. 遵循標準： 2.1 資訊安全管理系統(Information Security Management System，簡稱 ISMS)：ISO/IEC 27001。 2.2 ISMS 之控制措施：53 項僅為資訊，大部分是強制性(Mandatory)要求事項。 2.3 遵循 ISO/IEC 15408 標準系列之 Site Certification。

參考資料：CCDB (2007) Site Certification, Version 1.0, Revision 1, CCDB-2007-11-001, October 2007。

綜前所述，於現階段，PIMS 之實作，除遵循 ISO/IEC 27001、ISO/IEC 27002、ISO/IEC 27005、ISO/IEC 27009、ISO/IEC 27018、ISO/IEC 29100、ISO/IEC 29134、ISO/IEC 29151 外，宜再增列 ISO/IEC WD 27552.2；於雲端運算服務，則應再增列 ISO/IEC 19086-1、ISO/IEC 19086-3 與 ISO/IEC 19944 以及 ISO/IEC 27017。

肆、個人資料管理系統標準化進程及議題於我國之借鏡：代結論

2015 年 7 月 17 日，面對「開放資料」與「大數據」之「去識別化」議題，前行政院張善政副院長根基於經濟部標準檢驗局(Bureau of Standards, Metrology and Inspection，簡稱 BSMI)提出如圖 4.1 所示的方案規劃，公布如表 4.1 所示之行政院推動大數據發展的個人資料保護之標準化工作項目。「CNS(ISO/IEC 29191) 29191 有要求事項，無控制措施；而 CNS(ISO/IEC 29100) 29100 是保護個人可識別資訊的高階框架，可引用作為『去識別化』控制措施」，是 BSMI 對其執行圖 4.1 與表 4.1 之思路的說明[19][20][23][24][25][26] [27]，惟其實作尚待闡明之[28][30][31]。

表4.1 行政院推動大數據之個人資料保護相關的2項國家標準

標準	CNS 29100：2014-06-04	有關如何管理、確保隱私權之原則框架的國家標準
	CNS 29191：2015-06-10	有關如何去識別化之部分匿名與部分去連結的國家標準
推動作法		● 政院月底將出爐如何取得符合兩標準的標準程序作法 ● 第一步先鼓勵部會取得驗證，下一步鼓勵金融、電信業取得驗證
用處		● 去除外界擔心敏感個資外洩疑慮 ● 各部會與業界可以合理應用大數據

資料來源：2015年7月17日，大數據發展訂國家標準，經濟日報A1，記者林安妮/台北報導。

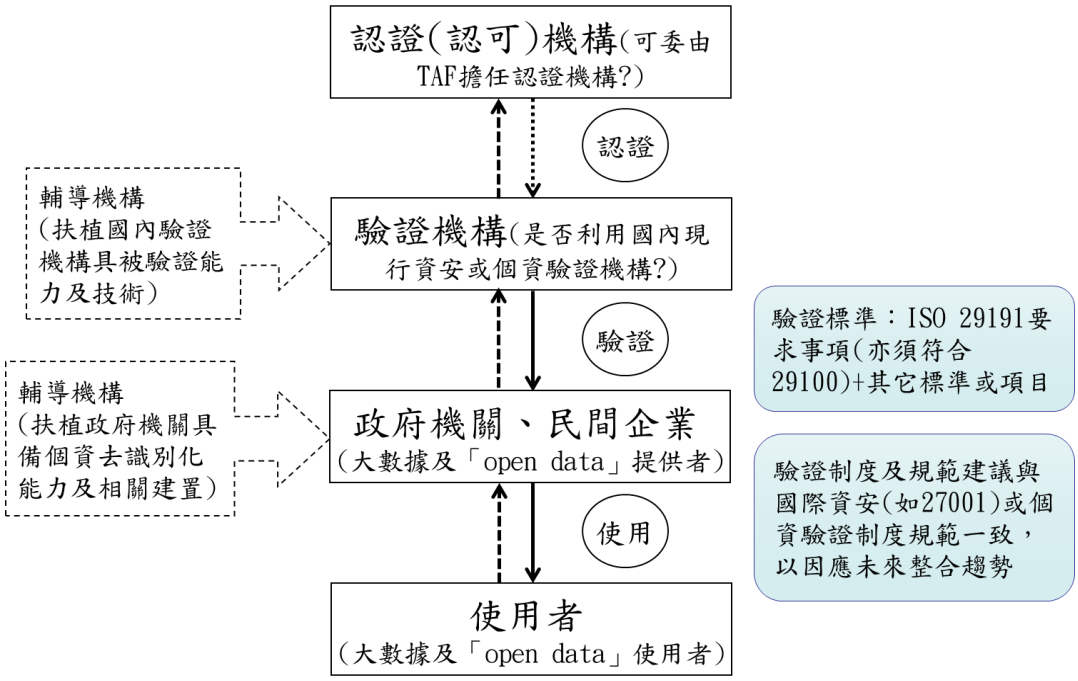

圖 4.1 個人資料去識別化方案規劃－個資去識別化驗證制度體系規劃
資料來源：個人資料去識別化之運作機制(簡報資料)，經濟部，2015-07-14《研商因應大數據潮流個人資料去識別化可行機制》會議(前經濟部標準檢驗局許景行組長簡報)。

因「個人資料去識別化」之「控制措施」宜參照「健康資訊資訊安全管理系統」驗證規範的 ISO 27799：2008-07-01 第 57 頁闡明其實作應遵循之 ISO/TS 25237：2008-10-01 內涵等的觀點，本文作者之一除持續提供資料供參考外，並於 2015 年 7 月 27 日 BSMI 召開的「研議政府機關個人資料去識別化之適用標準」會議中，提出先行加列其實作宜參考的已公布之 ISO/IEC 29101：2013-10-15 等標準的建議，獲採納，如圖 4.2 所示[26]。

2015 年 9 月 17 日，法務部提出「我國個人資料保護法有關去識別化之標準」的法律意見書，闡明「去識別化」於刑事、民事與行政責任之標準化實作的聯結性，提出遵循比例原則之風險管理及「開放資料(open data)」宜達「匿名化(Anonymised)資料(data)」與「不可逆(non-retraceable)之擬匿名化(Pseudonymised)資料」的見解；經濟部標準檢驗局提出「個人資料去識別化過程驗證要求及控制措施」之驗證規範，經「行政院」函知相關機關(構)[20]。

2015 年 12 月 21 日，「行政院國家資通安全會報第 29 次委員會議」，於會議紀錄中將「『個人資料匿名化、去識別化』分列」，同時要求相關機關善加推廣利用前述驗證規範[21]。

圖 4.1 中之 ISO/IEC 29100、ISO/IEC 29191 等標準與規範的用語並不一致，已如前述；其中 ISO/IEC 29191 僅為通稱「網路實名制」之「可控制的重新識別之擬匿名化」的管理控制措施之要求事項[7]。

圖 4.2 個人資料去識別化驗證標準規範
資料來源：http://vtaiwan.tw/personal-data-protection/「個人資料去識別化」驗證標準規範研訂及推廣，頁 12，《虛擬世界發展法規調適規劃方案》第 9 場會議，2016-02-23，簡報機關：經濟部標準檢驗局（檢索時間：2016-02-23)。

資料去識別化將面對之重新識別攻擊的攻擊者可能來自各方，他們可能是為了展示自己之理論正確性或是想從資料中獲益等。而其攻擊並不需要將資料庫完整重現才算成功的攻擊，攻擊者只要用各種方法取得相關之去識別化資料，包含向資料庫提出詢問(Query)以及直接取得去識別化資料集，而能夠在其取得的資料中分析出其目標即可以算是成功之攻擊。以目標分類的話，攻擊可以分為下列幾種：

1. 重新識別某筆紀錄是否在特定的資料主體中。
2. 重新識別特定資料主體中的特定紀錄。
3. 重新識別越多越好的紀錄與相對應的資料主體。
4. 重新識別特定資料主體是否落在資料集中。

任何重新識別之攻擊一般而言都會組合多種技術，並搭配可使用的外部資訊作為分析資料庫內容之工具。儘管攻擊的目標多變，評估哪些重新識別技術可能會被使用於去識別化資料庫之重新識別是相當重要的，表 4.2 是常用之重新識別的技術表列。

表 4.2 重新識別(Re-Identification)技術舉隅

技術(techniques)	實作方法
單獨挑出 (singling out)	透過觀察特定的特質，將單一資料或少數資料從資料主體(data principal)分離。
連結 (linking)	連接至少兩個以上在相關的資料主體中的紀錄，或是連接在不同資料集中的一組資料主體。
推斷 (Inference)	有不小的機率可以從某一組屬性(attribute)推斷出另一組屬性。
不可分辨之分析 (indistinguishability analysis)	針對特定資料，透過執行計算(computations)或詢問以確定其是否存在於搜尋的資料主體中。

註：資料主體(data principal) 在此指的是單一主體(個人、組織、設備、軟體程序、……)其需要保護的敏感資料總稱。
參考資料：ISO/IEC 2nd CD 20889：2017-06-09 第 7 節。

前述「不可逆之擬匿名化」於我國已有使用其理論上的弱點之重新識別風險大於1/30,000 的實證情境與資安事故[1][15][22][31]，且 GDPR 提出之新定義的擬匿名化亦不認定其為「開放資料」，前述的法律意見書宜修訂之。建議：

1.參照 GDPR 之「擬匿名化」的定義，重新定義我國「個人資料保護法有關去識別化之標準」中的「擬匿名化」。

2.闡明重新定義之「擬匿名化」為供研究等使用的「去識別化」資料。

3.敘明「重新識別風險評鑑」與「隱私風險評鑑」之過程。

綜前所述，PIMS 的「標準化」需要整合自然科學及社會科學之脈絡來解讀以及推理，才能融入文化與數位台灣混然為一體，參照 ISO/IEC CD 20889.2 徵求意見稿的思路，應先將「資料去識別化後之效用」與「差分隱私」納入前述「個人資料去識別化過程驗證要求及控制措施」的內容[13][18]；以及如圖 2.4 與圖 2.5 所示，進行擴增包含「資料去識別化」之「資訊安全管理系統的要求事項與控制措施之『個人資料管理系統』」的標準化之工作項目，並闡明「重新識別風險」與「隱私衝擊評鑑」之不同，不宜將前者作為後者的一項屬性，而僅實作隱私衝擊評鑑[2][3][12][20]；附錄一及附錄二分別是「PII 控制者」以及「PII 處理者」的 PIMS 控制措施之參考[11]。

2004 年 6 月 14 日，行政院院臺規字第 0930086121 號函頒之「行政院所屬各機關主管法案報院審查應注意事項」的第三點第(四)款規定：「法案衝擊影響層面及其範圍，包括成本、效益及對人權之影響等，應有完整之評估。」，以「個人資料去識別化過程驗證要求及控制措施」行政規則的法制作業之過程與試辦機關的實作結果評估，其「法規影響評估(Regulatory Impact Analysis，RIA)」作業宜精進之。

隨著「個人資料去識別化」等隱私防護議題實作之開展，僅確保資訊系統的機密性(Confidentiality，C)、完整性(Integrity，I)與可用性(Availability，A)並不足以確保民眾的數位生活福祉；2014 年 12 月，歐盟已正式發布將 CIA 擴增如後之目標(goals)：

1.去連結性(Unlinkability)：隱私相關之資料不能跨資料庫彼此連結。

2.透明性(Transparency)：可以在任何時間理解與重建，包含法規、技術以及組織 設置之所有隱私相關的資料處理。

3.可調解性(Intervenability)：對計畫與正在進行之隱私相關的資料處理，能進行合理的干預。

前述 CIA 定義之擴增目標，已納入於 2016 年 4 月成案的通稱為「從設計著手保護資料(Data protection by design)」之「隱私工程(Privacy engineering)」的 ISO/IEC 27550 標準化計畫之先期研究的內容之中[4]；2013 年 10 月 15 日公布的「隱私架構框架(Privacy architecture framework)」之 ISO/IEC 29101，通稱為「以預設機制進行資料保護(Data protection by default)」的標準，附錄三是其實作之闡明；前述「隱私工程」與「隱私架構框架」均為通稱「從設計著手保護隱私(Privacy-by-design, PbD)」的標準，PbD 與「資料極小化(Data minimization)」是個人資料防護實作之原則，PbD 已納入 GDPR[16]； 2017 年 1 月，美國亦公布同前述歐盟擴增 CIA 之「分離性(Disassociability)」、「可預測性

(Predictability)」及「可管理性(Manageability)」的 3 項目的(objects)之定義[2][3][17]，亦已納入前述 ISO/IEC 27550。「他山之石，可以攻玉」，前述 PbD 等如圖 2.6 所示的 PIMS 標準化之進程及其實作相關的法制，宜關注之。

[致謝]

本文作者謹在此對 ISO/IEC JTC 1/SC 27/WG 1 之友人提供 ISO/IEC 2nd CD 20889：2017-06-09 與 ISO/IEC WD 27552.2：2017-06-01 的盛情，與審稿者提升內容水平之意見，致衷心的謝忱！

參考文獻

[1] G.R. Blakley and I. Borosh, 1979, RSA Public Key Cryptosystems do not always conceal messages, Computers and Mathematics with Applications, Vol. 5, No. 3, pp. 169~178.

[2] S. Brooks, M. Garca, N. Lefkovita, S. Lightman and E. Nadeau, January 2017, Privacy Risk Management for Federal Information Systems, NISTIR 8062.

[3] ENISA(European Union Agency for Network and Information Security), 2014, Privacy and Data Prodevtion by Design from policy to engineering, December 2014.

[4] A. C. Garcia, N. N. McDonnell, C. Troncoso, D. L. Metayer, I. Kroener, D. Wright, J. M. del Alamo and Y. S. Martin, 2015, Privacy- and Security-by-Design Methodology Handbook(PRIPARE), TRiALOG, 31 December 2015.

[5] S. L. Garfinkel, October 2015, De-Identification of Personal Information, NIST IR 8053.

[6] INSIGHTS, 2014-03, http://www.wired.com/insights/2014/03/big-data-lessons-netflix/(2017-03-09 檢索)。

[7] ISO, 2012, ISO/IEC 29191:2012-12-15, Information technology-Security techniques-Requirements for partially anonymous, partially unlinkable authentication.

[8] ISO, 2016a, ISO/IEC JTC 1/SC 27/WG 1 N 715:2016-10-26, Draft design specitification for revision of ISO/IEC 27005.

[9] ISO, 2016b, ISO/IEC 19086-1：2016-09, Information technology – Cloud computing – Service level agreement(SLA) – Part 1：Overview and concepts.

[10] ISO, 2016c, ISO/IEC JTC 1/SC 27/WG 1 N 711:2016-12-08, Report of the meeting on N615(Defect Report on ISO/IEC 27005:2011) held in Abu Dhabi Oct 2016.

[11] ISO, 2017a, ISO/IEC WD 27552.2：2017-06-01, Information technology – Security techniques – Enhancement to ISO/IEC 27001 for privacy management – Requirements.

[12] ISO, 2017b, Disposition of comments report on document SC 27/WG 5 N16908(WG 5 N608) – ISO/IEC CD 20889：2017-06-09.

[13] ISO, 2017c,.ISO/IEC CD 20889.2：2017-06-09, Information technology – Security technology – Privacy enhancing data de-identification techniques.
[14] R. Kissel et al, 2014, Guidelines for Media Sanitization, NIST SP 800-88 Revision 1.
[15] A. K. Lenstra et al, 2012, Ron was wrong, Whit is right, ePrint(2012-064), http://eprint.iacr.org/2012/064.pdf/(2017-01-31 檢索)
[16] Official Journal of the European Union, 2016, General Data Protection Regulation (GDPR), REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016.
[17] OMB, 2016, Annual Report to Congress：Federal Information Security Modernization Act, March 18, 2016.
[18] 中華人民共和國國家質量監督檢驗檢疫總局/中國國家標準化管理委員會，2017，信息安全技術　個人信息去標識化指南(徵求意見稿)，2017-08-15。
[19] 行政院，2012，行政院院臺法字第 1010056845 號令(個人資料保護法除第 6 條及第 54 條條文外，其餘條文自 2012 年 10 月 1 日施行；2016 年 2 月 25 日，院臺法字第 1050154280B 號函，自 2016 年 3 月 15 日施行)。
[20] 行政院，2015，<我國個人資料保護法有關去識別化之標準>，院臺科字第 1040144764 號函(附件 1)；<個人資料去識別化過程驗證要求及控制措施>，院臺科字第 1040144764 號函(附件 2)。
[21] 行政院資通安全辦公室，2016，院臺護字第 1050150057 號函，2016-01-05。
[22] 周立平，2012，Cryptoanalysis in Real Life (Presentation), 2012-07-21 P.M. 13:00~13:45, HITCON 2012(備考：周教授於 2012-07-21 簡報中提出之脆弱性為-若取得一定數量的公鑰資料，則 n1=p1xq&n2=p2xq→q=gcd(n1，n2)，謹此敘明)。
[23] 法務部，2014，法律字第 10303513040 號函。
[24] 最高行政法院，2014，103 年度判字第 600 號判決(2014-11-13)。
[25] 最高行政法院，2017，106 年度判字第 54 號判決(2017-01-25)。
[26] 經濟部，2015，經標授字第 10420050540 號函。
[27] 臺北高等行政法院，2016，103 年度訴更一字第 120 號判決(2016-05-19)。
[28] 蔡昀臻、樊國楨，2016，大數據之資料去識別的標準化初探：根基於 ISO/IEC 2nd WD 20889：2016-05-30，資訊安全通訊，第 22 卷，第 4 期，頁 1~26。
[29] 樊國楨、韓宜蓁，2015，數位社會供應鏈風險管理的標準化(ISO/IEC 27036 系列標準)歷程初探，標準與檢驗，第 190 期，頁 65~74。
[30] 樊國楨、蔡昀臻，2016，隱私防護資料發布系統之保護剖繪初論：根基於個人資料去識別化的議題，前瞻科技與管理，第 6 卷，第 1 期，頁 47~114。
[31] 樊國楨、蔡昀臻，2017，擬匿名化的大數據之安全標準初探：根基於支付卡的安全事故與公開基礎建設之技術脆弱性的議題，資訊安全通訊，第 23 卷，第 2 期，頁 24~42。

附錄一：參考控制目標和控制措施（PII 控制者）

A.1 同意及選擇 目標：為確保在其他合法的處理不適用的情況下，PII 的收集和處理只有在 PII 當事人同意其一個或多個具體目的的處理的情況下進行。		
A.1.1	識別和記錄目的	控制措施 組織宜識別和記錄將被處理 PII 之一個或多個具體目的。
A.1.2	判定何時取得同意	控制措施 組織宜確定並記錄從 PII 當事人取得同意的時間和方式。
A.1.3	同意之取得與紀錄	控制措施 組織宜根據文件規定取得和記錄 PII 當事人的同意。
A.1.4	提供修改或撤銷同意的機制	控制措施 組織宜為 PII 當事人提供修改或撤銷其同意的機制。
A.1.5	提供反對處理的機制	控制措施 組織宜為 PII 當事人提供反對其 PII 處理的機制。
A.1.6	與第三方分享 PII 當事人同意之修改	控制措施 組織宜採取合理步驟，向分享 PII 的第三方通知 PII 當事人提交的任何修改、撤回或異議。
A.2 目的適法性及規定 目標：為確保 PII 處理之目的符合適用之義務且 PII 當事人知曉處理基礎。		
A.2.1	確定合法基礎	控制措施 組織宜依合法基礎判定、記錄和遵守確定目的之 PII 處理。
A.3 蒐集限制 目標：將 PII 的收集限制在適用之義務範圍內且嚴格必要的針對特定目的。		
A.3.1	蒐集限制	控制措施 組織宜將 PII 的蒐集限制為與識別目的相關、成比例且必要之最低限度。
A.4 資料極小化 目標：將 PII 的處理限制在與收集目的必要相關的。		
A.4.1	定義和記錄識別層級	控制措施 組織宜定義和記錄 PII 識別 PII 當事人的層級或將個人與 PII 識別的目所需相關的一組特徵聯繫起來。
A.4.2	符合識別層級	控制措施 組織宜識別與紀錄以及時方式處理 PII 到可以識別 PII 當事人的最低層級，或將個人與 PII 識別的目所需相關的一組特徵聯繫起來之機制。
A.4.3	PII 超出使用	控制措施 一旦原始 PII 不再需要用於識別的目的，組織宜以不允許識別 PII 當事人身份的形式提交 PII。
A.4.4	暫存檔	控制措施

		組織宜確保在代表客戶處理 PII 時創建的暫存檔與文件在特定、文件化之期限內被刪除或銷毀。
A.5 利用、持有及揭露限制 目標：限制 PII 的持有及揭露的使用和保存期間於必要之收集目的。		
A.5.1	限制利用、持有及揭露	控制措施 組織宜將 PII 的使用，持有和揭露（包括轉讓）限制在必要條件下，以實現具體、明確且合法的目的。
A.5.2	持有	控制措施 組織不宜為 PII 處理之目的保留 PII 超過必要的時間。
A.5.3	揭露	控制措施 組織宜有揭露 PII 之機制。
A.5.4	PII 向第三方揭露的記錄	控制措施 組織宜記錄對第三方之 PII 揭露，包括揭露之 PII、對象及時間。
A.6 精確性及品質 目標：為確保 PII 處理的準確性及品質，需考慮其收集目的。		
A.6.1	蒐集程序	控制措施 組織宜識別和記錄 PII 之收集機制以減少不準確的引導。
A.7 公開、透明及告知 目標：為 PII 當事人提供其 PII 的處理以及何時提供 PII 之適當訊息。		
A.7.1	確定 PII 當事人的資訊	控制措施 組織宜確定和記錄其提供給 PII 當事人關於其 PII 的處理以及何時提供 PII 的資訊。
A.7.2	向 PII 當事人提供資訊	控制措施 組織宜向 PII 當事人提供有關處理其 PII 的預期目的的資訊。
A.8 個人參與及存取 目標：確保 PII 當事人擁有行使其權利的權力。		
A.8.1	確定 PII 當事人的權利和行使	控制措施 組織宜確定 PII 當事人其處理 PII 有關的權利以及能夠行使其權利。
A.8.2	提供 PII 處理副本	控制措施 在 PII 當事人要求時，組織宜能夠提供 PII 處理的副本。
A.8.3	PII 處理者的支援	控制措施 組織宜確保代表其處理 PII 的任何 PII 處理者實施附錄 B.1.1 中規定的控制措施。
A.8.4	校正或抹除	控制措施 組織宜通過促進 PII 當事人行使存取、校正和/或抹除其 PII 的權利，實施校正或抹除被認定為不準確的 PII 之機制。
A.8.5	請求管理	控制措施

		組織宜有辦法處理 PII 當事人的合法要求。
A.8.6	自動化處理	控制措施 組織宜識別並處理由自動處理 PII 產生的 PII 當事人的任何義務，包括法律義務。
A.9 可歸責性 目標：確保可依據適用之義務證明 PII 已被處理。		
A.9.1	紀錄	控制措施 組織宜確定和維護必要的記錄，以支持證明其遵守處理 PII 的義務。
A.9.2	政策和程序記錄	控制措施 組織宜保留安全政策及運作程序之複本在取代（包括更新）時宜保留一特定、文件化之期限。
A.9.3	與 PII 處理者的契約	控制措施 組織宜確保 PII 處理者實施附錄 B.1.2 中規定的控制措施。
A.10 資訊安全 目標：確保 PII 依適當的安全措施進行處理。		
A.10.1	安全控制	控制措施 組織宜通過技術和組織措施保護 PII，以確保與其風險安全層級相符。
A.10.2	損害管理	控制措施 組織宜實施識別和記錄 PII 處理之安全損害，包括損害影響的評鑑和適當的通知的政策。
A.10.3	保密義務	控制措施 在組織控制措施下可存取 PII 之個人宜受保密義務限制。
A.10.4	紙本資料之構造 (construction)	控制措施 組織宜限制顯示 PII 之紙本資料的產生。
A.10.5	PII 之復原	控制措施 組織宜有 PII 復原工作之程序及其日誌。
A.10.6	轉移含有 PII 的媒體	控制措施 組織異地媒體之 PII 宜受授權程序之限制，且不宜被授權人員以外之人員存取。
A.10.7	未加密媒體	控制措施 除非無法避免，組織不宜使用不允許加密之可攜式實體媒體及可攜式裝置，同時宜記錄所有該等可攜式媒體及裝置之使用。
A.10.8	公眾網路上傳送	控制措施 組織宜將在公眾資料傳輸網路上傳送之 PII 在傳送之前予以加密。
A.10.9	紙本資料之毀壞	控制措施 組織宜有針對破壞任何紙本資料應採取之安全的毀壞程序。
A.10.10	個人登錄 ID	控制措施

		組織宜確保當有一人以上對儲存之 PII 有存取權限，則為識別、鑑別及授權之目的，每一人均宜有一相異的使用者 ID。
A.10.11	使用者之紀錄	控制措施 組織宜維護對資訊系統有授權存取權限的使用者之最新紀錄或使用者之剖繪。
A.10.12	重新利用使用者 ID	控制措施 組織不宜將撤銷或到期之使用者 ID 授與其他人。
A.10.13	與處理 PII 之分包商的契約	控制措施 組織與任何處理 PII 分包商間之處理 PII 契約宜明確規定達到組織資訊安全及 PII 保護義務之技術及組織的最少措施。
A.10.14	重新分配 PII 存儲空間	控制措施 組織宜確保不論資料儲存空間是否指派給顧客，任何先前駐存於該儲存空間之資料對該顧客均為不可見的。
A.11 隱私遵循 目標：確保 PII 依據適用之義務進行處理。		
A.11.1	隱私影響評鑑	控制措施 組織宜評估在計劃新的或改變的 PII 處理類型時之隱私影響評鑑的需要
A.11.2	PII 可能被轉移的國家	控制措施 組織宜規定及記錄 PII 可能被轉移的國家。
A.11.3	PII 傳輸控制	控制措施 組織使用傳輸 PII 之資料傳輸網路宜受限於設計用以確保資料抵達其預定目的地的適切控制措施。
A.11.4	記錄和傳輸 PII	控制措施 組織宜記錄 PII 向第三方轉移或從第三方轉移，並確保與其的合作以支持 PII 當事人未來的存取權。
A.11.5	聯合控制者	控制措施 組織宜確定與任何聯合 PII 控制者各自的職責。

資料來源：ISO, 2017a, ISO/IEC WD 27552.2：2017-06-01, Information technology – Security techniques – Enhancement to ISO/IEC 27001 for privacy management – Requirements, Annex A.
備考：因 A10.4 與 A10.9 之英文均為 'Destruction of hard copy materials'，表中 A10.4 的 'Construction'係作者自行更改。

附錄二：參考控制目標和控制措施（PII 處理者）

B.1 同意及選擇 目標：為確保在其他合法的處理不適用的情況下，PII 的收集和處理只有在 PII 當事人同意其一個或多個具體目的的處理的情況下進行。		
B.1.1	顧客對 PII 當事人的義務。	控制措施 組織宜提供顧客能履行義務容易行使 PII 當事人存取、修正及/或抹除有關其 PII 之權利的手段。

B.1.2	顧客合作協議	控制措施 組織宜確保處理 PII 的合約（有必要時，並考慮到處理的本質和組織可用的資訊）涉及組織作為 PII 控制者提供協助客戶義務之作用。
B.2 目的適法性及規定 目標：為確保 PII 處理之目的符合適用之義務且 PII 當事人知曉處理基礎。		
B.2.1	組織之目的	控制措施 組織應確保代表客戶處理的 PII 不得以任何目的進行處理且與顧客的文件指示獨立。
B.2.2	營銷與廣告使用	控制措施 組織不得在沒有明示同意的情況下使用根據合約處理之 PII 作為營銷和廣告的目的，也不得提供此類同意作為接受服務的條件。
B.2.3	侵權指示	控制措施 如其認為處理指示違反適用的立法或法規，組織應通知顧客。
B.2.4	處理活動記錄	控制措施 組織應保存代表 PII 控制者的客戶所進行的各類處理活動的記錄。
B.3 蒐集限制 目標：將 PII 的收集限制在適用之義務範圍內且嚴格必要的針對特定目的。		
B.3.1		無額外控制措施
B.4 資料極小化 目標：將 PII 的處理限制在與收集目的必要相關的。		
B.4.1	暫存檔	控制措施 組織宜確保在代表客戶處理 PII 時創建的暫存檔與文件在特定、文件化之期限內被刪除或銷毀。
B.5 利用、持有及揭露限制 目標：限制 PII 的持有及揭露的使用和保存期間於必要之收集目的。		
B.5.1	PII 揭露要求的告知	控制措施 除非法律另有規定，否則組織應通知顧客任何具有法律約束力揭露 PII 的請求。
B.5.2	PII 向第三方揭露的記錄	控制措施 組織宜記錄對第三方之 PII 揭露，包括揭露之 PII、對象及時間。
B.5.3	有關 PII 揭露的告知	控制措施 組織宜拒絕任何不具法律約束力 PII 揭露之要求、於法律允許時進行 PII 揭露之前諮詢對應的顧客、接受由對應的顧客授權之任何契約協議之 PII 揭露要求的契約保證。
B.6 精確性及品質 目標：為確保 PII 處理的準確性及品質，需考慮其收集目的。		
B.6.1		無額外控制措施
B.7 公開、透明及告知 目標：為 PII 當事人提供其 PII 的處理以及何時提供 PII 之適當訊息。		

B.7.1	分包 PII 處理之揭露	控制措施 組織宜在相關顧客使用之前對其揭露其使用分包商處理 PII。
B.7.2	分包商參與處理 PII	控制措施 組織宜提供合同承諾，不得在未經顧客事先具體或一般書面授權的情況下讓分包商處理 PII。
B.7.3	變更分包商處理 PII	控制措施 在通過書面授權的情況下，組織宜通知顧客關於加入或更換分包商處理 PII 的任何預期變更，從而使客戶有機會反對該變更。
B.8 個人參與及存取 目標：確保 PII 當事人可以存取他們的 PII 並得糾正不準確的 PII。		
B.8.1		無額外控制措施
B.9 可歸責性 目標：確保可依據適用之義務證明 PII 已被處理。		
B.9.1	PII 外洩之告知	控制措施 組織(必要時)於未經授權存取 PII 或未經授權存取處理設備或設施而導致 PII 之損失、揭露或改變事件時宜及時地告知相關顧客。
B.9.2	政策和程序記錄	控制措施 組織宜保留安全政策及運作程序之複本在取代（包括更新）時宜保留一特定、文件化之期限。
B.9.3	PII 之歸還、轉送及汰除	控制措施 組織宜有 PII 之歸還、轉送及汰除方面之政策，並宜在訂立 PII 處理合約之前使顧客可取得該政策。
B.10 資訊安全 目標：確保 PII 依適當的安全措施進行處理。		
B.10.1	保密義務	控制措施 在組織控制措施下可存取 PII 之個人宜受保密義務限制。
B.10.2	紙本資料之構造(construction)	控制措施 組織宜限制顯示 PII 之紙本資料的產生。
B.10.3	PII 之復原	控制措施 組織宜有 PII 復原工作之程序及其日誌。
B.10.4	轉移含有 PII 的媒體	控制措施 組織異地媒體之 PII 宜受授權程序之限制，且不宜被授權人員以外之人員存取。
B.10.5	未加密媒體	控制措施 除非無法避免，組織不宜使用不允許加密之可攜式實體媒體及可攜式裝置，同時宜記錄所有該等可攜式媒體及裝置之使用。
B.10.6	公眾網路上傳送	控制措施 組織宜將在公眾資料傳輸網路上傳送之 PII 在傳送之前予以加密。
B.10.7	紙本資料之毀壞	控制措施 組織宜有針對破壞任何紙本資料應採取之安全的毀壞程序。

B.10.8	個人登錄 ID	控制措施 組織宜確保當有一人以上對儲存之 PII 有存取權限，則為識別、鑑別及授權之目的，每一人均宜有一相異的使用者 ID。
B.10.9	使用者之紀錄	控制措施 組織宜維護對資訊系統有授權存取權限的使用者之最新紀錄或使用者之剖繪。
B.10.10	重新利用使用者 ID	控制措施 組織不宜將撤銷或到期之使用者 ID 授與其他人。
B.10.11	與客戶簽約	控制措施 組織與顧客之間宜規定技術及組織的最少措施，以確保備妥契約安全之安排，且不為任何與控制者指令無關之目的而處理資料。該等措施不宜受限於組織的單邊降低。
B.10.12	與處理 PII 之分包商的契約	控制措施 組織與任何處理 PII 分包商間之處理 PII 契約宜明確規定達到組織資訊安全及 PII 保護義務之技術及組織的最少措施。
B.10.13	重新分配 PII 存儲空間	控制措施 組織宜確保不論資料儲存空間是否指派給顧客，任何先前駐存於該儲存空間之資料對該顧客均為不可見的。
B.11 隱私遵循 目標：確保 PII 依據適用之義務進行處理。		
B.11.1	PII 可能被轉移的國家	控制措施 組織宜規定及記錄 PII 可能被轉移的國家。
B.11.2	PII 傳輸控制	控制措施 組織使用傳輸 PII 之資料傳輸網路宜受限於設計用以確保資料抵達其預定目的地的適切控制措施。
B.11.3	PII 傳輸的基礎	控制措施 組織宜通知顧客相關的 PII 傳輸基礎。
B.11.4	PII 控制者的義務	控制措施 組織宜向作為 PII 控制者的客戶提供必要的資訊來證明其履行義務。

資料來源：ISO, 2017a, ISO/IEC WD 27552.2：2017-06-01, Information technology – Security techniques – Enhancement to ISO/IEC 27001 for privacy management – Requirements, Annex A.
備考：因 B10.2 與 B10.7 之英文均為‘Destruction of hardcopy materials’，表中 B10.2 的‘construction’係作者自行更改。

附錄三：個人資料保護目標(Goals)與ISMS相關之資訊安全與意見連結表

隱私層面 (aspects)	個人資料保護層面連結特徵	連接到資訊安全	關於資訊安全管理系統(Information Security Management System, ISMS)實作的意見

去連結性(Unlinkability)	資料極小化 (Data minimization) 相關控制措施：ISO/IEC 27001 第.4 節、附錄一第 A.3/A.4/A.5 節、附錄二第 B.3/B.4/B.5 節	這不算資訊安全層面的一部分	這個特徵與組織的業務目的與使用個人資料之原因密切相關。 使用資料極小化可以降低風險，從而成為降低資訊安全的需求之一般方法，即使它不是資訊安全的一部分。
去連結性(Unlinkability)	知的必要/僅知原則 (Necessity / Need-to- know) 相關控制措施：ISO/IEC 27002 第 8.2.1/8.2.2/8.2.3/9/18.2.2 節	知的需要之概念經常用於資訊安全。 通常被認為是機密性(Confidentiality)的特徵。	關於個人資料保護層面它之意義更廣泛。 它同時指的是使用/提供服務之資料是完全必要的，以及為了執行該服務或任務而需要存取之人、事資訊的假定限制。
去連結性(Unlinkability)	目的綁定 (Purpose binding) 相關控制措施：ISO/IEC 27002 第 18.1.1/18.1.4 節、附錄一第 A.4 節、附錄二第 B.4 節	這是存取控制和/或使用控制的擴充。	這個特徵指的是在理想情況下，除了收集的目的之外，無法處理資料。 然而，這是很難實施的，因為通常需要技術和組織措施才能得到維護。
去連結性(Unlinkability)	權力分隔 (Separation of power) 相關控制措施：ISO/IEC 27002 第 6.1.1/6.1.2/8.1.2/9.2.3 節	角色和責任包括(資訊)資產之所有權。	所有資訊安全的責任應被定義與分配。 應分開職責及利益衝突之責任範圍，以減少未經授權或無意的修改或濫用組織資產之機會。 清單中的資產應有特定之所有者。
去連結性(Unlinkability)	可觀測性 (Observability) 相關控制措施：ISO/IEC 27002 第 18.2.3 節、附錄一第 A.4.4/A.10.1/A.10.4 節、附錄二第 B.4/B10.2 節	在某種意義上，這是一個機密性的問題，但指的是所進行的活動而不是實際的資訊。	根據共同準則(Common Criteria, CC)第 2 部 3.1 版之第 4 次修訂(CC PART2 V3.1R4)， 不可觀測性(un-observability)能確保使用者在沒有其他人（特別是第三方）能夠觀察到用戶正在使用資源或服務的情況下使用資源或服務。 在 ISMS 中，這應該被視為是為了減輕或減少與個人資料有關的風險而應考慮之一個層面，以及避免在不需要時創建個人資料的一種方法。
去連結性(Unlinkability)	不可偵測性 (Undetectability) 相關控制措施：附錄一第 A.4/A.7.1、附錄二第 B.4/B.10.2/B.10.6 節	這是事物存在之機密性的部分層面。 一妥善保護的資產應對未經授權的實體具有不可偵測性。	根據“ANON”v034 版，不可偵測性定義如下：從攻擊者之角度來看，利益項目(item of interest, IoI)的不可偵測性意味著攻擊者無法充分判斷它是否存在。在 ISMS 中，這應該被視為是為了減輕或減少與個人資料有關之風險而應考慮的一個層面，以及避免在不需要時創建個人資料之一種方法。
透明性(Transparency)	開放性 (Openness) 相關控制措施：ISO/IEC 27002 第 8.2.1 節、附錄一第 A5.1/A.8.1/A.8.3/A.8.4/A.8.5/A.10 節、附錄二第 B.1/B.10 節	開放性是資料主體和/或監督機構盡可能的要求文件、行動和活動開放且可理解的原則（另見政府開放性）。 這不是直接的資訊安全層面，而是間接影響 CIA 對公司相關資訊的要求。	在 ISMS 中，服務或處理之生命週期都應該被視為系統所有層面之要求。 它將影響必要的資訊安全控制措施以及將程序性活動/控制（如分類）之一部分的風險及需求納入考量。

透明性(Transparency)	可歸責性 (Accountability) 相關控制措施： ISO/IEC 27002 第 6.1.1/8.1.2 節、附錄一第 A.10/A.11 節、附錄二第 B.10/B.11 節	可歸責性與資訊安全層面無關。 在與透明性相關聯的方面，透明性是可歸責性特徵的先決條件。	這是在 ISM 內的組織。 與角色、責任與有關當局相關(如:資產所有權、治理、風險評鑑、供應商關係、監測、審計)。
透明性(Transparency)	可重製性 (Reproducibility) 相關控制措施：ISO/IEC 27002 第 14.1.3 節、附錄一第 A.8.3/A.8.4/A.8.5/A.10 節、附錄二第 B.10 節	這不是資訊安全的直接層面。 這個特徵是指重現資訊的處理方式以及其處理者的可能性。	在 ISMS 中，這將影響記錄流程、服務及系統之要求以及所需的可追溯性(traceability)與監控級別。 這很可能也會影響事件與其管理過程。 如果適當實行，這也可能協助處理需要描述與重新創建流程之商業連續性計畫。
透明性(Transparency)	通知與選擇 (Notice and Choice) 相關控制措施：ISO/IEC 27002 第 15.1.2 節、附錄一第 A.1/A.7 節、附錄二第 B.1/B.7 節	資訊安全沒有類似的層面。 通知通常指的是向資料主體提供關於正在收集個人資料以及如何使用和處理數據之行為，因此是透明性的一部分。 另一方面，選擇是指資料主體限製或同意收集和/或使用個人資料的能力。這就是調解性(Intervenability)特徵。	在 ISMS 中，服務或處理之生命週期都應該被視為系統所有層面的要求措施。 它將影響必要之資訊安全控制措施以及將程序性活動/控制（如分類）的一部分的風險及需求納入考量。
透明性(Transparency)	可審計性 (Auditability) 相關控制措施：ISO/IEC 27002 第 18.2 節、附錄一第 A.2/A.9.1/A.9.2/A.9.3 節、附錄二第 B.2/B.9.1/B.9.2/B.9.3 節	可審計性與與安全層面無直接關係，但對完整性(integrity)和可用性(availability)的依賴性很強。在與透明性相關聯的方面，透明性是可審計性特徵的先決條件。	在 ISMS 之概念中有控制等應具有可審計性之類似的基本要求。然而，在 ISMS 案例中著重於審計與 ISMS 或標準相一致之可能性；而在隱私案例中，核心重點為符合 GDPR 及同意處理個人資訊。 這兩方面對於可審計性的需要可能有不同之要求。
可調解性 (Intervenability)	自主決定性 (Self-determination) 相關控制措施：ISO/IEC 27002 第 7.1/7.2/7.3/15.1.2 節	自主決定性可以與資訊安全的完整性(Integrity)和機密性(Confidentiality)層面有關。 該面向涵蓋資料主體能夠決定其願意發布的資料的條件和用途的權利或能力。 它還藉由設計和資料極小化與隱私相關。	在 ISMS 中，服務或處理之生命週期都應該被視為系統所有層面的特定要求措施。 它將影響必要之資訊安全控制措施以及將程序性活動/控制（如分類）的一部分的風險和需求納入考量。
可調解性 (Intervenability)	使用者控制 (User control) 相關控制措施：ISO/IEC 27002 第 9.1/9.2/9.3/9.4 節	在隱私方面，這是指資料主體通過例如配置、流量管制或其他方式來控制個人資料使用的能力。它還藉由設計和資料極小化與隱私相關。	在 ISMS 中，這應被視為主要是為了設計、開發與取得流程及系統之要求以及風險來處理。 這種風險考量將影響必要的資訊安全控制措施以及將程序性活動/控制（如分類）的一部分的風險和需求納入考量。

可調解性 (Intervenability)	修正和抹除資料 (Rectification and erasure of data) 相關控制措施：ISO/IEC 27001 第 7.5 節、 ISO/IEC 27002 第 8.1.2/8.1.4/11.2.7 節、附錄一第 A.4.4/A.9.1/A.8.4/A.10.9 節、附錄二第 B.4.1/B.10.7 節	這與完整性和可追溯性有關。 但也是正確性(correctness)的概念。 實際上，它要求資料主體有權修正資料，並可能有權刪除其資料。	在 ISMS 中，應將其作為系統與服務之設計、開發及取得的要求措施以及技術與組織處理過程實施之要求措施來處理。
可調解性 (Intervenability)	同意撤回 (Consent withdrawal) 相關控制措施：ISO/IEC 27002 第 7.3.1 節、附錄一第 A.1/A.9.1/A.9.2 節、附錄二第 B.1/B.9.3 節	這與資訊安全層面沒有直接關係。 然而，同意撤回可能是設定完整性和可用性要求的前置作業。它還將對可追溯性甚至機密性產生影響，具體取決於所涵蓋的個人資料。	在 ISMS 中，應將此處理視為不可忽視之處理要求措施與與對商業模式的風險並透過其影響必要控制措施及將程序性活動/控制（如分類）之一部分的風險及需求納入考量。
可調解性 (Intervenability)	申索/損害控管 (Claim lodging / Dispute raising) 相關控制措施：ISO/IEC 27002 第 16 節	這不是資訊安全層面。然而，為了記錄事件發展，需要可追蹤性。	這是一個可能需要資訊安全管理之控制措施來處理風險的正式程序性活動。
可調解性 (Intervenability)	中斷處理 (Process Interruption) 相關控制措施：ISO/IEC 27002 第 16 節	停止或更改進程的能力能允許更改資訊，可被視為資訊安全的完整性和可用性層面。 但這算是資訊的需求而非保護。	這是一個可能需要資訊安全控制措施來處理風險及可能的事件之正式程序性活動。 所需的控制措施需遵循與 GDPR 相關之 ISMS 的要求事項將影響技術與組織控制措施。

資料來源：Veriscan Security AB, Information Security Management System (ISMS) and Handling of Personal Data Version 1.0.0.1, annex C, 2017-01-28.

說明(樊國楨、蔡昀臻，2016a)：

1. CC Part2 V3.1R4 是「 “Common Criteria for Information Technology Security Evaluation” 3.1 版第 2 部分(Part 2)之第 4 次修訂(Revision)，2017-04 已發行第 5 次修訂版；於 ISO，CC 即為 ISO/IEC 15408 Part 1(Introduction)、Part 2(Security functional components)與 Part 3(Security assurance components)。
2. ANON”v034 是 “A Terminology for Talking about Privacy by Data Minimization: Anonymity, Unlinkability, Unobservability, Pseudonymity, and Identity Management,” by A. ANON_Terminology_V0.34(2010-08-10)。
3. 表中之相關控制措施係作者自行加入。