Communications of the CCISA
Vol. 22 No. 1 Jan. 2016

個人資料管理系統標準化初論：根基於個人資料去識別化之議題

樊國楨[1]、蔡昀臻[2]
[1]國立交通大學資訊管理研究所、[2]國立交通大學管理科學研究所
[1]kjf.nctu@gmail.com 、[2]yct1230@gmail.com

摘要

個人資料保護法施行細則第 17 條闡明：「.....所稱資料經過處理後或依其揭露方式無從識別當事人，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」亦即通稱之「去識別化(De-identification)」的議題，自 2014 年 11 月 17 日法務部法律字第 10303513040 號函之函釋：「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，本文探討國際標準組織(International Organization for Standardization, ISO)於此議題之標準化作業的全景與我國宜實做之驗證方案。

關鍵詞：驗證、去識別化、個人資料管理系統、資訊安全管理系統、標準化

Standardization of Personal Information Management System: Based on Personal Information De-identification Issue

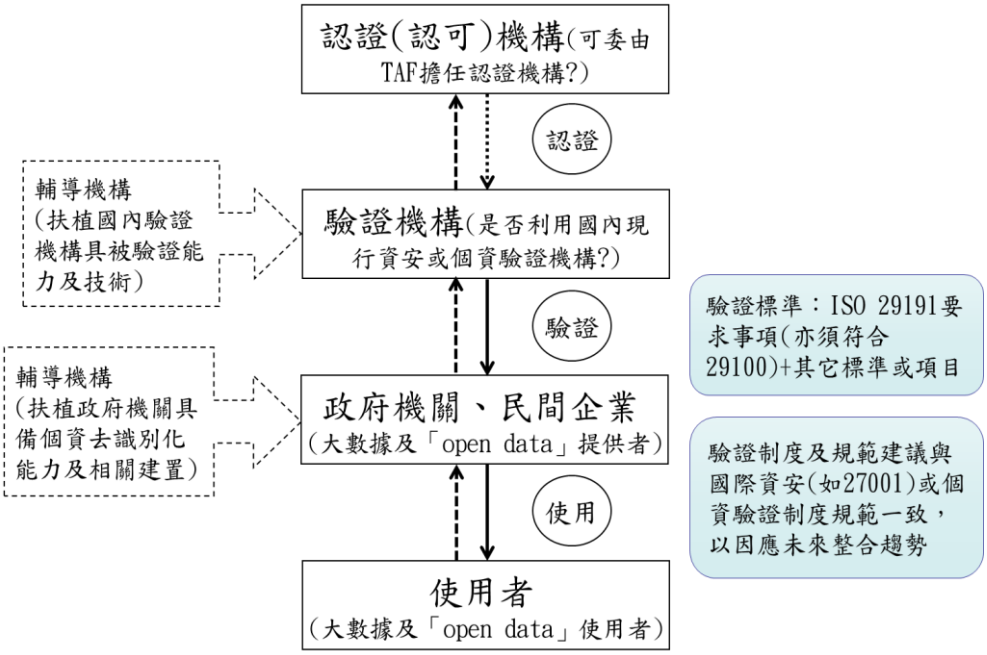
Abstract

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 what ISO’s standardize work and what we should do in certifications.

Keywords: Certification, De-identification, Personally Information Management System (PIMS), Information Security Management System (ISMS), Standardization

壹、前言

2015 年 7 月 17 日，面對「開放資料」與「大數據」之「去識別化」議題，行政院張善政副院長根基於經濟部標準檢驗局提出如圖一所示的方案規劃，公布如表一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 29191 有要求事項，無控制措施；而 CNS 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」的控制措施。是目前圖一與表一執行中之說明[19],[20],[25]~[27] 。



圖一：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：經濟部(2015)個人資料去識別化之運作機制(簡報資料)，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，經濟部標準檢驗局許景行組長簡報)

說明(2015-07-27，本文作者之一於會議中建議於CNS 27001增列的要求事項)：

1. 於第 6.1.1 節增列(f)：

(f) 隱私衝擊評鑑

(1) 組織履行之活動，以及與其他組織履行的活動間之介面，若使用或連結(link)個人資料、生成(generate)個人資料，以及經由網宇(cyber/network)連結個人(individual)裝置，則應於資訊安全風險評鑑中執行隱私衝擊評鑑。

(2) 隱私衝擊評鑑包含去識別化(de-identification)之風險評鑑。

備考 1.在 ISO/IEC 29134 公布前，隱私衝擊評鑑係指建立 ISO/IEC JTC 1/SC 27/WG 5 SD4[15]中所考量之過程。

備考 2.去識別化之技術要求事項係指 CNS 29191[13]第 5 節中之要求事項。

2. 於第 6.1.3 節(c)之備考增列：

備考 3.考量隱私衝擊評鑑結果，對所選定之資訊安全風險處理選項，本標準之使用者宜參照 ISO/IEC 29101。

表一：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

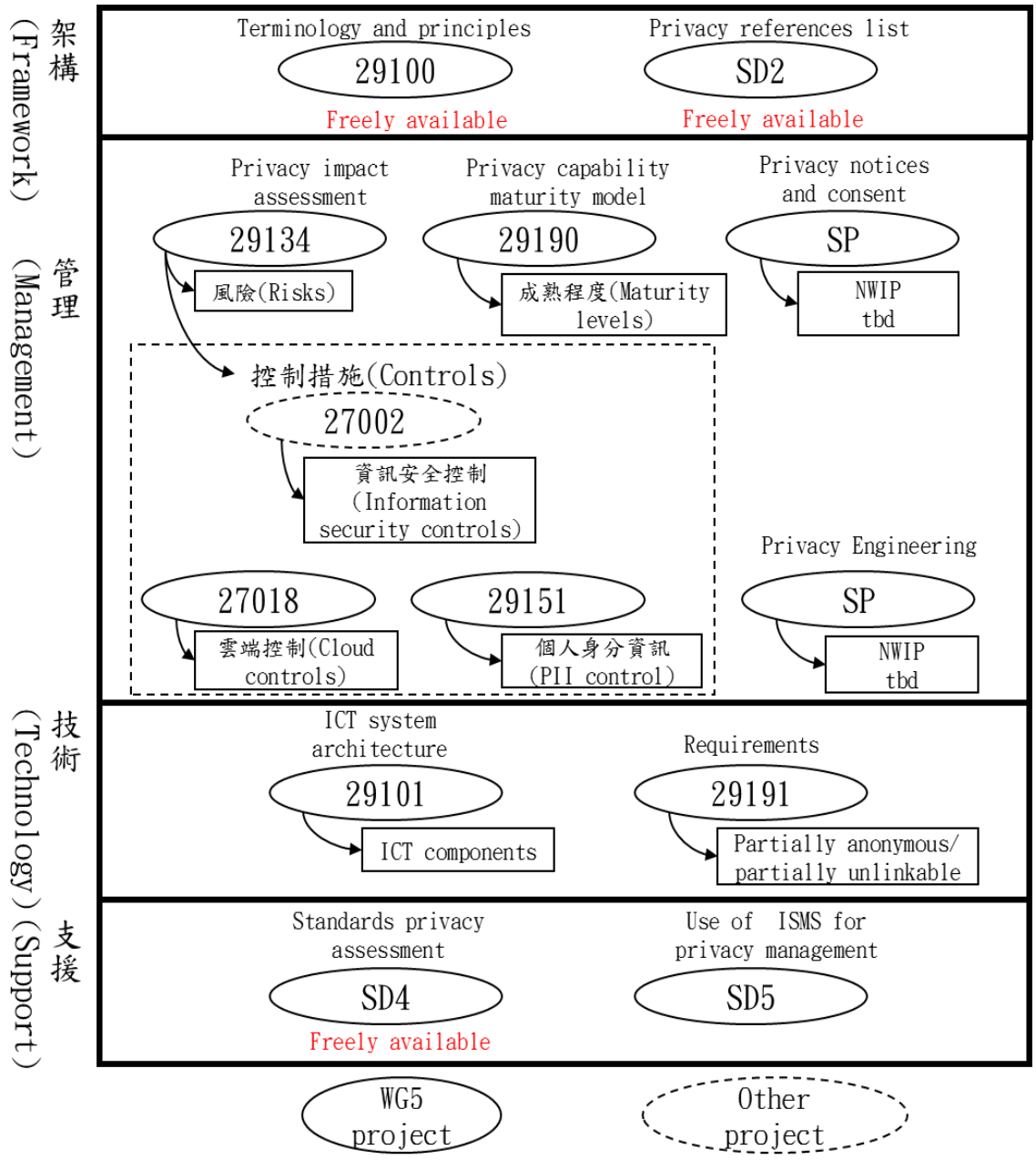
2015 年 9 月 17 日，法務部已提出「我國個人資料保護法有關去識別化之標準」的法律意見書，闡明「去識別化」於刑事、民事與行政責任之標準化實作的聯結性，提出遵循比例原則之風險管理的見解[2],[3],[19],[20],[22]~[24],[27],[32] 。根基於此，在第二節探討我國個人資料去識別化管理系統之框架；在第三節，提出遵循管理系統標準(Management System Standard, MSS)的前述框架之節次及其條文的包含去識別化之個人資料管理的整合性資訊安全管理系統(Integrated Information Security Management System, IISMS)之要求事項；在第四節，闡明去識別化實作的議題；最後，在第五節，提出本之結論[1]~[18],[21],[28]~[31]。

貳、推動個人資料去識別化驗證制度初探：根基於 ISO/IEC JTC 1/SC 27/WG 5 之標準化框架

2012 年 10 月 1 日是我國個人資料保護法(以下簡稱個資法)正式施行之初始日，揭示我國邁向資訊應用先進國家的新里程碑；個資法第二十七條第二項明定：「中央目的事業主管機關得指定非公務機關訂定個人資料檔案安全維護計畫或業務終止後個人資料處理方法。」，其第三項敘明：「前項計畫及處理方法之標準等相關事項之辦法，由中央目的事業主管機關定之。」自 2010 年 5 月 26 日個資法修正公布後，歷經 28 個月方制定公布的個資法施行細則第十七條闡明「去識別化(De-identification)：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」之應為，「個人資料」的資訊隱私權依司法院釋字第 603 號解釋，而受憲法第 22 條之保護；惟憲法對

其保障並非絕對，國家得於符合憲法第 23 條，在「為防止妨礙他人自由，避免緊急危難，維持社會秩序，或增進公共利益所必要者外」的意旨亦得以法律規定為適當之限制，故權利的行使仍有其界限[4],[7],[19],[23],[24],[32]，其與開放資料之競合已成為法制化之議題。

2014 年 11 月 13 日，最高行政法院判字第 600 號判決與 2014 年 11 月 17 日，法務部法律字第 10303513040 號函之函釋，開啟前述個資法施行細則第 17 條實作的「去識別化(De-Identification)」之標準化的議題(法務部，2014；最高行政法院，2014；張友寧，2015) [25],[26],[20]；擬匿名化自國際標準組織(International Organization for Standardization，ISO)於 2008-12-01 公布之 ISO/TS 25237：2008(E)Health informatics – Pseudonymization 國際標準起，已成為具攸關性的去識別化之技術控制措施；在 ISO/TS 25237 第 3.18 節，「去識別化 ：任一移除具識別性資料集與資料主體間關連的過程之一般用語(general term for any process of removing the association between a set of identifying data and the data subject)」，並於健康資訊的「資訊安全管理系統(Information Security Management System, ISMS)」擴增之控制措施標準的 ISO 27799：2008(E)Health information-Information security management in health using ISO/IEC 27002 第 57 頁，闡明「若有去識別化之需求，則參照 ISO/TS 25237：2008(E)實作之」。2015 年 6 月 30 日，主責資訊安全標準化的 ISO/IEC JTC 1/SC 27 之第 5 工作組(Working Group 5，WG 5)公布如圖二所示的第 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)》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。



圖二：身分管理與隱私科技標準框架

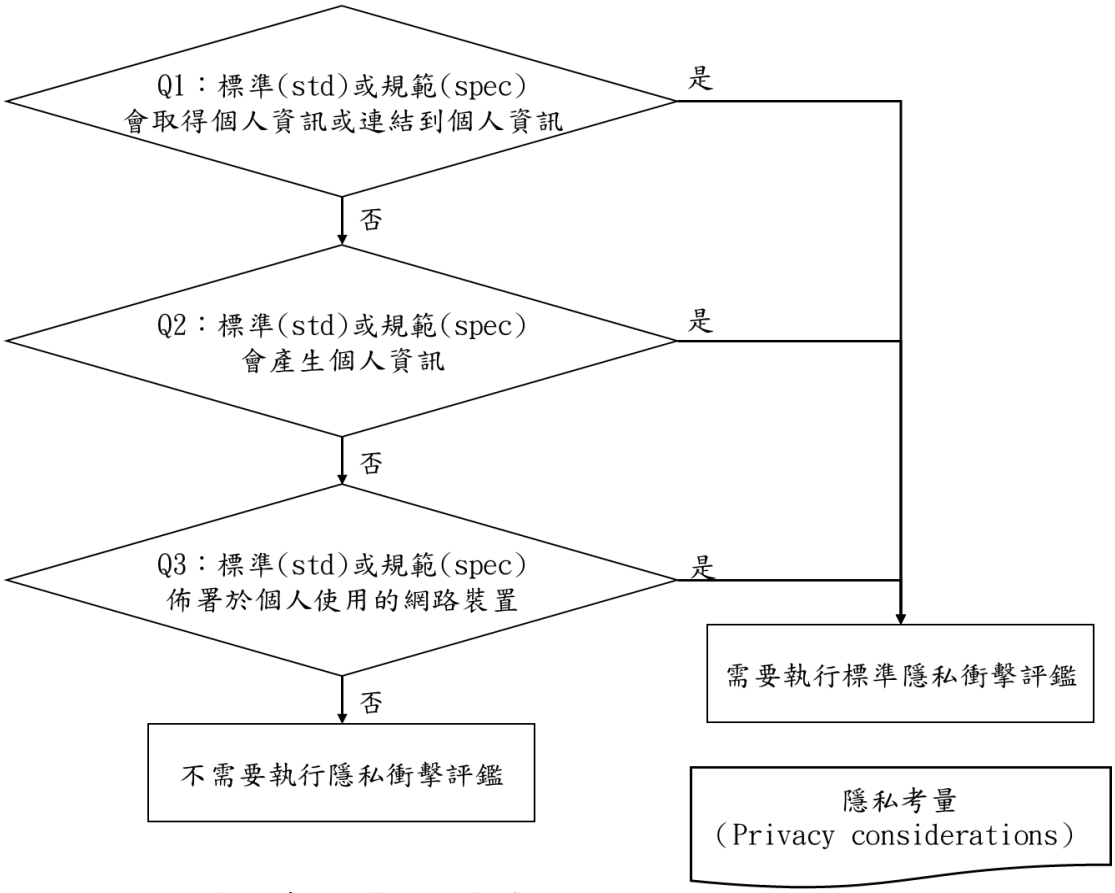
資料來源：Rannenberg, Kai (2015) Standards contributing to the protection of consumers' privacy and personal data, ISO/COPOLCO (2015). The connected consumer in 2020-empowerment through standards, 2015-05-13, Geneve, Switzerland.

「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及整合性安全個人資料管理與資訊安全的管理系統(Integrated Security Management System, ISMS)要求事項之脈絡[3],[4],[8],[11]~[13],[22],[30],[32]。

2002 年，美國先於「電子化政府法案(E-Government Act of 2002)」之第 2008 條(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。

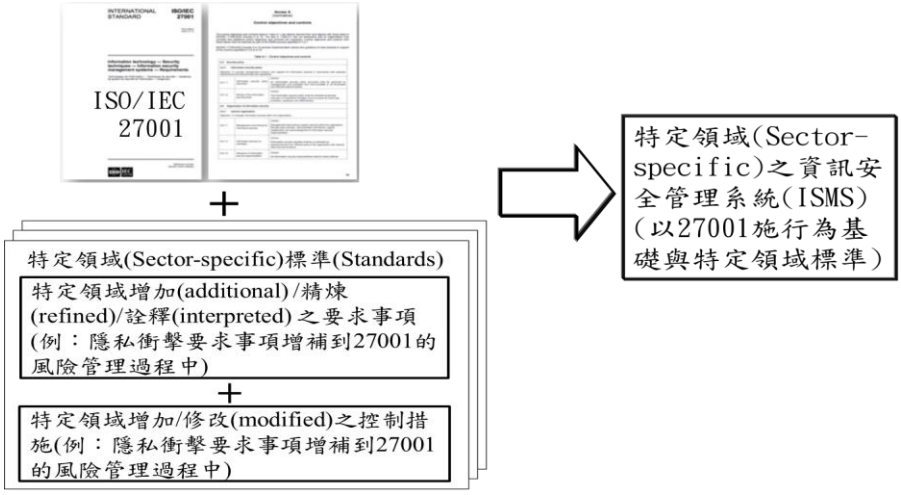
ISO 自 2000 年起，即以試作(Pilot：2001~2005)、制定管理系統標準(Management System Standards，MSS)之至次節的一致性高階規範程序(Procedures specific to ISO：2006~2010)與完成各個管理系統之調合(2011~2015)的標準化工作項目；根基於此，ISO/IEC JTC 1/SC 27 於 2012 年 10 月決定 PIMS 直接使用 ISO/IEC 27001 之要求事項，並進行制訂擴增其條款的 ISO/IEC 27009 之工作項目，在 2015-07-27 提出意見及投票之 ISO/IEC DIS 27009 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，圖三以及圖四分別是其示意說明[12],[13]。



圖三：判斷何時需要執行標準隱私評鑑(Standards Privacy Assessment, SPA)

資料來源：ISO/IEC JTC 1/SC 27/WG 5 SD4: 2014

說明：ISO/IEC 29100：2012（E）中用語為：隱私衝擊評鑑（Privacy Impact Assessment, PIA）



圖四：ISO/IEC 27009的應用

資料來源：ISO/IEC DIS 27009：2015-07-27

面對「去識別化」之議題，經濟部於 2015 年 7 月 14 日提出如圖一所示的「個人資料去識別化方案規劃－個資去識別化驗證制度認驗證體系規劃」之推動計畫，根基於圖一及我國管理系統與國際接軌的政策，本文作者之一於 2015 年 7 月 27 日的會議中提出前述之擴增 CNS(ISO/IEC 27001：2013(E))27001 第 6.1.1 節以及第 6.1.3 節的驗證規範，供相關機關(構)參考，並建議於 ISO/IEC 29151 完成前，先以 ISO/IEC 29101：2013(E)作為圖一之控制措施的參考標準[27]。

健康資訊安全管理系統控制措施之 ISO 27799：2008(E)第 57 頁闡明：「ISMS 之去識別化的實作，宜參照 ISO/TS 25237：2008(E)」，前述「去識別化之隱私衝擊評鑑」於 ISO/TS 25237：2008(E)第 6.6.2.7 節的用語為：「推論風險評鑑(inference risk assessment)」，並於附錄 B 闡明其 PIA 設計之要求事項[3],[8],[11]。

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 已公布遵循圖四之框架，如表二所示的資訊安全管理系統(Information Security Management System, ISMS)要求事向宜擴增的 PIMS 之論題及其隱私攸關標準[13]，表三是 PIMS 與 ISMS 間的用語對照。

表二：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映(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	隱私生命周期管理(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。

表三：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 之隱私關念，CNS 29100 於其附錄 A 已列出其主要概念間之關係；唯以 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[3],[14],[16],[18],[30] 。

參、 擴增CNS 27001本文之整合性資訊安全管理系統要求事項初探

自 2011 年起，管理系統標準已由 ISO 規範其共同結構、節次標題、文字、用語與核心定義，根基於表二，遵循 ISO/IEC DIS 27009 與 ISO/IEC JTC 1/SC 27/WG 5 SD 5 的徵求意見稿(2015-06-30)，擴增 CNS 之本文，以為整合個人資料管理系統於資訊安全管理系統的「整合性安全管理系統(Integrated Information Security Management System)」之要求事項，亦即型(Type)A 的管理系統標準(Management System Standard, MSS), 作為 PIMS 驗證之依據如後[2]~[13],[15],[20],[28]~[30] ：

1.適用範圍

本標準規定於組織全景內建立、實作、維持及持續改善整合性資訊安全管理系統之要求事項。本標準亦包括依組織需要而裁示之安全風險評鑑及處理的要求事項。本標準敘述之要求事項為通用的，旨在適用於所有組織，不論其型式、規模或性質。當組織宣稱符合本標準時，不得排除本標準第 4 節至第 10 節所規定之任何要求事項。

2.引用標準

下列標準因本標準所引用，成為本標準之一部分。下列引用標準適用最新版(包括補充增修)。

CNS 27000 資訊技術－安全技術－資訊安全管理系統－概觀及詞彙

CNS 29100 資訊技術- 安全技術 –隱私權框架

ISO/IEC 27009 Information technology – Security techniques – Sector – specific application of ISO/IEC 27001 - Requirements

3.用語及定義

CNS 27000 所規定之用語及定義適用於本標準。

CNS 29100 所規定之用語及定義適用於本標準。

ISO/IEC 27009 所規定之用語及定義適用於本標準。

4.組織全景

4.1 瞭解組織及其全景

組織應決定與其目的有關且影響達成其整合性資訊安全管理系統預期成果能力者之內部及外部議題。

備考：決定此等議題，係指建立於 CNS 31000[4]5.3 中所考量之組織內部及外部全景。

4.2 瞭解關注方之需要及期望

組織應決定下列事項。

(a)與整合性資訊安全管理系統有關之關注各方。

(b)此等關注方對個人資料管理與資訊安全之要求事項。

備考：關注方之要求事項可能包括法律及法規要求，以及契約義務。

4.3 決定整合性資訊安全管理系統之範圍

組織應決定整合性資訊安全管理系統之邊界及適用性，以建立其範圍。

於決定範圍時，組織應考量下列事項。

(a) 4.1 中所提及之內部及外部議題。

(b)4.2 中所提及之要求事項。

(c) 組織履行之活動與其他組織履行之活動間的介面及相依性。

範圍應以文件化資訊提供。

4.4 整合性資訊安全管理系統

組織應依本標準之要求事項，建立、實作、維持及持續改善整合性資訊安全管理系統。

5.領導作為

5.1 領導及承諾

最高管理階層應藉由下列事項，展現對整合性資訊安全管理系統之領導及承諾。

(a)確保已建立個人資料管理政策與資訊安全政策及個人資料保護目標及資訊安全目標，並與組織之策略方向相容。

(b)確保整合性資訊安全管理系統要求事項整合入組織之各項過程。

(c)確保整合性資訊安全管理系統所需之資源可取得。

(d)傳達有效之個人資料管理與資訊安全管理的重要性，以及符合整合性資訊安全管理系統要求事項之重要性。

(e)確保整合性資訊安全管理系統達成其預期成果。

(f)指導及支援人員，以促進整合性資訊安全管理系統之有效性。

(g)宣導持續改善。

(h)當適用其他相關管理角色之責任範圍時，加以支持以展現其領導權。

5.2 政策

最高管理階層應建立包含下列事項之個人資料管理政策與資訊安全政策。

(a)適合於組織之目的。

(b)包括個人資料管理目標與資訊安全目標(參照 6.2)或提供設定個人資料管理目標及資訊安全目標使用之框架。

(c)包括對滿足相關於從設計著手保護隱私等個人資料管理與資訊安全之適用要求事項的承諾。

(d)包括對持續改善整合性資訊安全管理系統之承諾。

個人資料管理政策與資訊安全政策應符合下列項目。

(e)以文件化資訊提供。

(f)於組織內傳達。

(g)適用時，提供給關注方。

5.3 組織角色、責任及權限

最高管理階層應確保個人資料管理與資訊安全相關角色之責任及權限已指派並傳達。

最高管理階層應指派下列責任及權限。

(a)確保整合性資訊安全管理系統符合本標準之要求事項。

(b)向最高管理階層報告整合性資訊安全管理系統之績效。

備考：最高管理階層亦可指派報告組織內整合性資訊安全管理系統績效之責任及權限。

6.規劃

6.1 因應風險及機會之行動

6.1.1 一般要求

於規劃資訊安全管理系統時，組織應考量 4.1 所提及之議題及 4.2 所提及之要求事項，並決定需因應之風險及機會，以達成下列事項。

(a)確保整合性資訊安全管理系統達成其預期成果。

(b)預防或減少非所欲之影響。

(c)達成持續改善。

組織應規劃下列事項。

(d)因應此等風險及機會之行動。

(e)執行下列事項之方法。

(1)將各項行動整合及實作於其安全管理系統過程之中。

(2)評估此等行動之有效性。

(f) 隱私衝擊評鑑

(1) 組織履行之活動，以及與其他組織履行的活動間之介面，若使用或連結(link)個人資料、生成(generate)個人資料，以及經由網宇(cyber/network)連結個人(individual)裝置，則應於資訊安全風險評鑑中執行隱私衝擊評鑑。

(2)隱私衝擊評鑑包含去識別化(de-identification)之風險評鑑。

備考 1.在 ISO/IEC 29134 公布前，隱私衝擊評鑑係指建立 ISO/IEC JTC 1/ SC 27/WG 5 SD4[6]4 中所考量之過程。

備考 2.去識別化之通訊匿名的技術要求事項係指 CNS 29191[7]5 中的要求事項。

備考 3.在 ISO/IEC 20889 與 ISO/IEC 29151 公布前，個人資料管理之控制措施宜參考 ISO/IEC 27018、ISO/TS 25237、ISO/IEC 27038、ISO/IEC 29101 與 ISO/IEC 29191。

6.1.2 資訊安全風險評鑑

組織應定義及應用資訊安全風險評鑑過程於下列事項中。

(a)建立及維持包括下列準則之資訊安全風險準則。

(1)風險接受準則。

(2)履行資訊安全風險評鑑之準則。

(b)確保重複之資訊安全風險評鑑產生一致、有效及適於比較之結果。

(c)識別隱私與資訊安全風險。

(1)應用資訊安全風險評鑑過程，以識別整合性資訊安全管理系統範圍內與漏失隱私及/或資訊之機密性、完整性及可用性相關聯之風險。

(2)識別隱私與資訊安全風險擁有者。

(d)分析資訊安全風險。

(1)評鑑若 6.1.2(c)(1)中所識別之風險實現時，可能導致之潛在後果。

(2)評鑑 6.1.2(c)(1)中所識別之風險發生的實際可能性。

(3)決定風險等級。

(4) 決定隱私衝擊評鑑等級。

(5) 決定去識別化等級。

(e)評估資訊安全風險。

(1)以 6.1.2(a)中所建立之風險準則，比較風險分析結果。

(2)訂定已分析風險之風險處理優先序。

組織應保存關於資訊安全風險評鑑過程之文件化資訊。

6.1.3 資訊安全風險處理

組織應定義並應用資訊安全風險處理過程，以達成下列事項。

(a)考量風險評鑑結果，選擇適切之資訊安全風險處理選項。

(b)對所選定資訊安全風險處理選項，決定所有必須實作之控制措施。

備考：組織可依要求設計控制措施，或由任何來源識別之。

(c)比較上述 6.1.3(b)中所決定之控制措施與附錄 A 中者，並確認未忽略必要之控制措施。

備考 1. 附錄 A 包括控制目標及控制措施之詳細清單。本標準之使用者參照附錄 A 以確保未忽略必要之控制措施。

備考 2. 控制目標隱含於所選定之控制措施中。附錄 A 中所列之各項控制目標及控制措施並未盡列，故可能需要額外之控制目標及控制措施。

備考 3.考量隱私衝擊評鑑結果，對所選定之資訊安全風險處理選項，在 ISO/IEC 20889 與 ISO/IEC 29151 公佈前， 本標準之使用者宜參考 ISO/TS 25237、ISO/IEC 27018、ISO/IEC 29101 與 ISO/IEC 29191。

(d)產生適用性聲明，包括必要之控制措施(參照 6.1.3(b)及(c))，且不論是否實作，提供納入之理由，以及由附錄 A 排除之理由。

(e)制訂資訊安全風險處理計畫。

(f)取得風險擁有者對資訊安全風險處理計畫之核准，以及對剩餘資訊安全風險之接受。

組織應保存關於資訊安全風險處理過程之文件化資訊。

備考：本標準中之資訊安全風險評鑑與處理過程與 CNS 31000[4]內提供之原則及通用指導綱要調和。

6.2 個人資料管理目標與資訊安全目標及其達成之規劃

組織應於各相關部門及層級建立個人資料管理目標與資訊安全目標。

個人資料管理目標與資訊安全目標應滿足下列事項。

(a)與個人資料管理政策及資訊安全政策一致。

(b)可量測(若可行時)。

(c)考量適用之資訊安全要求事項，以及風險評鑑及風險處理之結果。

(d)被傳達。

(e)於適當時，更新之。

組織應保存關於個人資料管理目標與資訊安全目標之文件化資訊。

於規劃如何達成個人資料管理目標與資訊安全目標時，組織應決定下列事項。

(f)待辦事項。

(g)所需資源。

(h)負責人員。

(i)完成時間。

(j)結果之評估方式。

7.支援

7.1 資源

組織應決定並提供建立、實作、維持及持續改善整合性資訊安全管理系統所需之資源。

7.2 能力

組織宜採取下列措施。

(a)決定於組織控制下執行工作，影響其個人資料管理與資訊安全績效人員之必要能力。

(b)確保此等人員於適當教育、訓練或經驗之基礎上能勝任。

(c)於適當時，採取取得必要能力之行動，並評估所採取行動之有效性。

(d)保存適切之文件化資訊，作為勝任之證據。

備考：適用之行動可能包括，例：對現有員工提供訓練、指導或重新指派，或是雇用或委外勝任人員。

7.3 認知

於組織控制下執行工作之人員，應認知下列事項。

(a)個人資料管理政策與資訊安全政策。

(b)其對整合性資訊安全管理系統有效性之貢獻，包括改善之個人資料管理與資訊安全績效的益處。

(c)未遵循整合性資訊安全管理系統要求事項之可能後果。

7.4 溝通或傳達

組織應決定，相關於整合性資訊安全管理系統之內部及外部溝通或傳達的需要，包括下列事項。

(a)溝通或傳達事項。

(b)溝通或傳達時間。

(c)溝通或傳達對象。

(d)溝通或傳達人員。

(e)進行有效溝通或傳達所採用過程。

7.5 文件化資訊

7.5.1 一般要求

組織之整合性資訊安全管理系統應包括下列內容。

(a)本標準要求之文件化資訊。

(b)由組織所決定對整合性資訊安全管理系統有效性，必要之文件化資訊。

備考：各組織之整合性資訊安全管理系統文件化資訊內容，可能因下列因素而異。

(a)組織規模，以及其活動之型式、過程、產品及服務。

(b)各過程及其互動之複雜度。

(c)人員之能力。

7.5.2 制訂及更新

於制訂及更新文件化資訊時，組織應確保適切之下列項目。

(a)識別及描述(例：標題、日期、作者或參引號碼)。

(b)格式(例：語言、軟體版本、圖形)及媒體(例：紙本、電子)。

(c)合宜性及適切性之審查及核准。

7.5.3 文件化資訊之控制

應控制整合性資訊安全管理系統及本標準要求之文件化資訊，以確保下列事項。

(a)其於需要處及需要時為可用及適用。

(b)其受適切保護(例：防止漏失機密性、不當使用或漏失完整性)。

為控制文件化資訊，組織應於適當時，闡明下列活動。

(c)派送、存取、檢索及使用。

(d)儲存及保存，包括可讀性之保存。

(e)變更之控制(例：版本控制)。

(f)留存及屆期處置(retention and disposition)。

於適當時，應識別及控制由組織所決定對整合性資訊安全管理系統之規劃及運作為必要之外部來源的文件化資訊。

備考：存取意謂關於文件化資訊僅可檢視之許可、或檢視及變更文件化資訊之許可及權限的決策等。

8.運作

8.1 運作之規劃及控制

組織應規劃、實作及控制達成個人資料管理與資訊安全要求事項所需之過程，並實作 6.1 中所決定之行動。組織亦應實作各項計畫，以達成 6.2 中所決定之個人資料管理及資訊安全目標。

組織應保存文件化資訊，其程度必須具有足以達成其過程已依規劃執行之信心。

組織應控制所規劃之變更，並審查非預期變更之後果，必要時採取行動以減輕任何負面效果。

組織應確保委外過程經確定並受控制。

8.2 資訊安全風險評鑑

組織應依規劃之期間，或當提議或發生重大變更時，考量 6.1.2(a)所建立之準則，執行資訊安全風險評鑑或隱私衝擊評鑑或去識別化風險評鑑。

組織應保存資訊安全風險評鑑結果之文件化資訊。

8.3 資訊安全風險處理

組織應實作資訊安全風險處理計畫。

組織應保存資訊安全風險處理結果之文件化資訊。

9.績效評估

9.1 監督、量測、分析及評估

組織應評估個人資料管理與資訊安全績效及資訊安全管理系統之有效性。

組織應決定下列事項。

(a)需要監督及量測之事項，包括個人資料管理與資訊安全過程及控制措施。

(b)監督、量測、分析及評估之適用方法，以確保有效的結果。

備考：所選擇之方法宜產生適於比較及可重製視為有效之結果。

(c)執行監督及量測之時間。

(d)監督及量測之人員。

(e)監督及量測結果應分析及評估之時間。

(f)分析及評估上述結果之人員。

組織應保存適切之文件化資訊，作為監督及量測結果的證據。

9.2 內部稽核

組織應依規劃之期間施行內部稽核，以提供整合性資訊安全管理系統之下列資訊。

(a)是否遵循下列事項。

(1)組織本身對其整合性資訊安全管理系統之要求事項。

(2)本標準之要求事項。

(b)是否有效實作及維持。

組織應採取下列作為。

(c)規劃、建立、實作及維持稽核計畫，包括頻率、方法、責任、規劃要求事項及報告。該稽核計畫應將所關注之重要過程及前次稽核之結果納入考量。

(d)定義各稽核之準則及稽核之範圍。

(e)選擇稽核員及施行稽核，以確保稽核過程之客觀性及公平性。

(f)確保稽核之結果對相關管理階層報告。

(g)保存文件化資訊作為稽核計畫及稽核結果之證據。

9.3 管理審查

最高管理階層應於規劃之期間，審查組織之資訊安全管理系統，以確保其持續的合宜性、適切性及有效性。

管理審查應包括對下列事項之考量。

(a)過往管理審查之議案的處理狀態。

(b)與整合性資訊安全管理系統有關之內部及外部議題的變更。

(c)個人資料管理與資訊安全績效之回饋，包括下列之趨勢。

(1)不符合項目及矯正措施。

(2)監督及量測結果。

(3)稽核結果。

(4)資訊安全目標之達成。

(d)關注方之回饋。

(e)風險評鑑結果及風險處理計畫之狀態。

(f)持續改善之機會。

管理審查之輸出應包括與持續改善機會有關之決策，以及任何對資訊安全管理系統變更之需要。

備考：最高管理階層宜考量整合性資訊安全管理系統之去識別化等級與隱私衝擊評鑑的持續改善之風險及機會。

組織應保存文件化資訊，以作為管理審查結果之證據。

10.改善

10.1 不符合項目及矯正措施

不符合項目發生時，組織應有下列作為。

(a)對不符合項目反應，並於適當時採取下列作為。

(1)採取行動以控制並矯正之。

(2)處理其後果。

(b)藉由下列作為，評估對消除不符合項目之原因的行動之需要，使其不再發生且不於他處發生。

(1)審查不符合項目。

(2)決定不符合項目之原因。

(3)決定是否有類似之不符合項目存在，或可能發生。

(c)實作所有所需行動。

(d)審查所有所採取矯正措施之有效性。

(e)若必要時，則對資訊安全管理系統進行變更。

矯正措施應切合所遇到之不符合項目。

組織應保存文件化資訊，以作為下列事項之證據。

(f)不符合項目之本質及後續採取之所有行動。

(g)所有矯正措施之結果。

10.2 持續改善

組織應持續改善整合性資訊安全管理系統之合宜性、適切性及有效性。

美國聯邦政府自 2008 年起經由「聯邦資訊安全管理法實作計畫」將 PIMS 併入

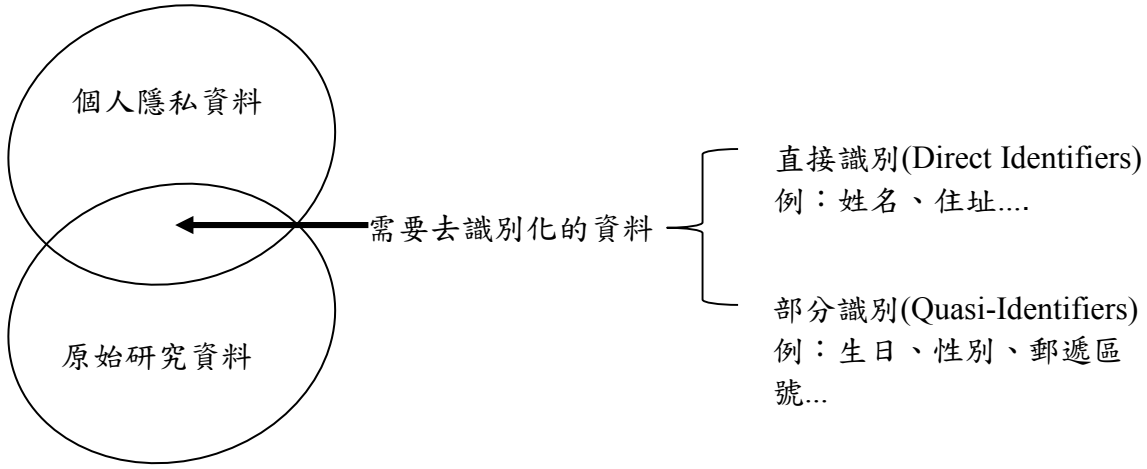
ISMS 中，2014 年 12 月 18 日，美國公布「聯邦資訊安全現代法(Federal Information Security Modernization Act of 2014, FISMA 2014)」之第 3552(b)(3)(B)條款，已將「個人隱私(Personal Privacy)」納入；換言之，IISMS 標準化之發展已勢不可當，本節淺見，供先進宏達參考，期待拋磚引玉。

肆、去識別化與資訊公開初探

根基「個人資料去識別化」之標準化的發展歷程，入微反思，先綜整其標準化之議題於後：

4.1. 何謂去識別化？

去識別化(de-identification)主要目的是在資料分析、研究與個人隱私中取得平衡之一種方法。在原始研究資料中有包含一部分和個人隱私相關的訊息，這些可能會損害到他人隱私之資料(需要去識別化的資料)又可以分為直接識別、部分識別兩種。直接識別資料指可以直接獲得個人資訊的項目；部分識別資料則指雖然單一項資料無法識別出 PII 當事人，但數個部分識別資料加在一起，如圖五所示，有一定的機會識別出 PII 當事人。



圖五： 個人資料去識別化之圖格

目前之對策：風險管理，線上型(例：網路交易)通常使用通稱「網路實名制」之控制措施[5],[6],[30]，在圖一中的「大數據及開放資料」面向，則使用如統計公開控制(Statistical Disclosure Control, SDC)方式，透過修改資料內容或遮蔽部分資料內容，使得能在效用損失以及揭露風險中取得平衡，常用方法舉隅如表四所示[1]。

表四： SDC 常用方法舉隅

方式名稱	實作方法例	SDC 評估
單元抑制 (Cell-suppression)	針對特別敏感的資料優先抑制其數據的讀取(Primary suppression)，其次如果數據可能造成優先抑制數據被識別，也需抑制其數據讀取(Secondary suppression)。判別資料是否為優先抑制讀取之敏感資料常見方法有： 1. (n, k)-dominance：如果資料中小於等於 n 個個體，卻對整體數值影響大於 k 比例，視為敏感資料 2. pq-rule：在未公開資訊前，個體對整體數值的影響估計在 p%內；公開後影響估計在 q%內，視為敏感資料。 3. p%-rule：當 q=100%時，為 pq-rule 的特例。	● 效用損失(Utility loss)：可以用次識別數據(Secondary suppression)被抑制的數量代表，並可加入重要性權重估計。 ● 洩漏風險(Disclosure risk)：計算敏感資料的破解可能性，如果在預設的安全值範圍內，視為安全。
微分隱私法框架 (Differential privacy framework)	在一定範圍內可以加入固定的雜訊(noise) ε，但仍然保持其原始的統計資訊。例如：可以利用動差生成函數(Moment Generation Function, MGF)控制，使得加入雜訊的動差生成函數與原來之要求(例：1~n 階的動差相差近於 0)相同，於實際上兩者存在誤差 ε 之系統化技術。	● 效用損失：可用修改後資料與實際資料的差距總合表示。 ● 洩漏風險：ε 可視為其被識別風險。
K 匿名框架 (k-Anonymity framework)	透過隱藏或是概略化部分類識別資訊，使得符合相同條件之個體數量有 k 個以上，並擴增至相關聯的資料屬性等(例：L-diversity 與 T-closeness)，以達到避免識別之目的之系統化技術。	● 效用損失：可以利用統計數值結果估算。 ● 洩漏風險：若僅使用 k-匿名法，則 k 可視為其風險值。

4.2.去識別化做法

先去除直接識別之資料，再將部分識別的資料依情況予以遮蔽或從本來之精確值改為一個範圍。另外，公開的資料除了需要經過去識別化外，也可以考慮限制可以取得資料的人員之存取權限。

存取權限之目前的對策：角色基(Role Based)與屬性基(Attribute Based)存取控制(Access Control)。

4.3. 現在去識別化遇到的困難

一般用來分析之資料可以分為3類：正規資料、敘述資料與圖片資料。下面，將簡述目前各種資料遇到的問題：

(1) 正規資料在單一資料庫的時候可以用程式之方法執行去識別化，但是如果遇到有心人士將兩個來源不一樣的資料庫資料放在一起分析，仍有一定的機會被識別出來。

(2) 敘述資料有些時候無法用電腦判斷是否該移除。例如：在診斷書裡面可能會提到病症名稱，而因為有些病症名稱是人名而被判定為私人資料刪除。

(3) 圖片資料中可能有些資訊電腦還無法辨識，可是肉眼可以，這樣的狀況下有可能會因為疏忽而損害個人隱私。

目前想到的解決方法：

(1) 執行去識別化。

(2) 不要公開有被識別疑慮的資料。

(3) 在不會影響資料分析的前提下，改動資料內容。

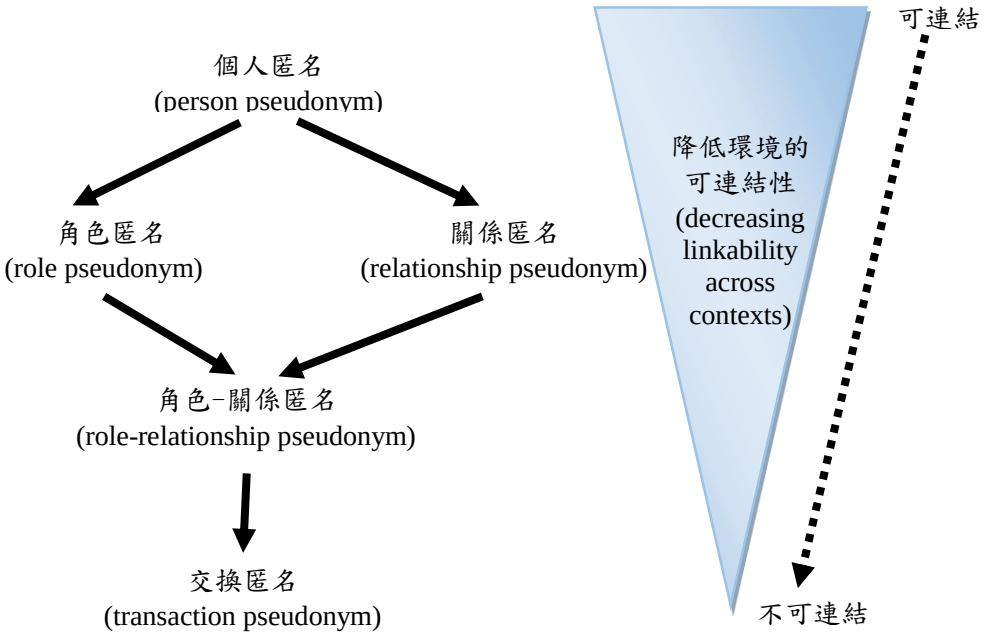
隨著資訊社會之進步，社會對於資訊公開的呼聲也逐漸增加。雖然資料庫之資料公開可以協助各種研究分析，可是同時資料之公開也會牽涉到是否會侵犯 PII 當事人隱私的問題。在這個情況下，資料庫之資訊安全越發的受到重視。針對資料庫裡面資料是否會侵害個人隱私之去識別化的安全分析主要有幾個重點，如表五所示[16]。

表五：去識別化之主要名詞與其反義詞定義

匿名性(Anonymity)： 攻擊者不能辨識出群體中之任一個體。	可識別性(Identifiability)： 攻擊者能辨識出群體中之一個體。
去連結性(Unlinkability)： 攻擊者不能連結群體中任兩個關注項目(Items of interest,IOI)：沒有足夠訊息判斷項目彼此之間是否相關。	可連結性(Linkability)： 攻擊者能連結群體中之兩個關注項目(Items of interest,IOI)：有足夠訊息判斷關注項目彼此間是否相關。
去偵測性(Undetectability)： 攻擊者沒有足夠資訊判斷任一關注項目(IOI)是否存在資料庫中。	可偵測性(Detectability)： 攻擊者有足夠資訊判斷一關注項目(IOI)是否存在資料庫中。
去觀察性(Unobservability)： 個體的每個關注項目都具有不可偵測性、而且所有個體均具有匿名性。	可觀察性(Observability)： 於語意上存在意指關注項目之許多的可能性。

資料來源：Pfitzmann, A. and M. Hansen(2013) ”A terminology for talking about privacy by data minimization: Anonymity, Unlinkability, Unobservability, Pseudonymity, and Identity Management”, V.0.34, page 35, 2010-08-10.

「去識別化」控制措施之實作，以表四中的「去連結化」為例，除了圖六中之個



圖六：去連結之框架示意

人匿名、角色匿名、關係匿名、角色-關係匿名與交易匿名外，尚有安全強度(Security strength)及匿名強度(Anonymity strength)的技術性議題須處理，方能滿足「我國個人資料保護法有關去識別化之標準」提出的「去識別化推論風險評鑑」之比例原則之應為[3],[5],[6],[14],[16],[18],[20],[30] 。

美國 FISMA 實作計畫將其 PII 之隱私特定(Privacy-Specific)防護(Safeguards)的控制措施分成：蒐集、利用與留存 PII 之最小化(Minimizing the Use, Collection, and Retention of PII)、經營隱私衝擊評鑑(Conducting Privacy Impact Assessment)、去識別化資訊(De-Identifying Information)與匿名化(Anonymization)4 個種類，均需擴增 CNS 27001 附錄 A 之控制措施[3],[8],[9],[11],[28]~[30] ；其中於去識別化資訊與匿名化控制措施的實作，於我國均為方起步之議題。「工欲善其事，必先利其器」，諸如於主機板及作業系統內嵌如表六所示的匿名化演算法與表四中之微分隱私框架(Differential privacy framework)的資料庫管理系統外掛模組(例：PINQ(Privacy Integrated Query))為例，如何使用宜考量之[18]。

表六：公開金鑰基礎建設(Public Key Infrastructure, PKI)與直接匿名認證(Direct Anonymous Attestation, DAA)之比較

	公開金鑰基礎建設 (Public Key Infrastructure, PKI)	隨機 B 之直接匿名認證 (Direct Anonymous Attestation, DAA)	命名 B 之直接匿名認證	隱私加強識別碼 (Enhanced Privacy ID, EPID)	群組簽章 (Group Signatures)
唯一公開金鑰 (Unique Public Key)	是	否	否	否	否
唯一私人金鑰 (Unique Private Key)	是	是	是	是	是
匿名 (Anonymous)	否	是	是	是	是
不可追蹤 (Untraceable)	否	是	是	是	否
不可連結 (Unlinkable)	否	是	否	是	是
檢查被揭露的私人金鑰 (Check for revealed private key)	是	是	是	是	具體方案 (Scheme specific)
撤銷簽名者的簽章 (Revoke the signer of a signature)	是	否	是	是	是
成員可審核撤銷 (Member Auditability of Revocation)	否	否	否	是	否

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。現階段「去識別化」之工作項目，ISO/TS 25237 宜作為其「匿名化資訊(Anonymizing Information)」控制措施實作

得參考標準；CNS 29191 是其「去識別化資訊(De-identification Information)」之控制標準，ISO/IEC 20008 與 20009 標準系列是其實作的參考標準。「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；資訊安全的「標準化」更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渾然為一體。2015 年 10 月 3 日，行政院蔡玉玲政務委員已公布我國「個人資料去識別化」驗證的「於 PIMS 中包含去識別化，其驗證均可」之方針[30]，「去識別化」標準的實作，宜進行深入之分析及探討，並制定適當的工作項目之行動方案。

伍、結論

個資法針對個人資料安全維護之要求事項，並無具體執行控制措施的規定，僅於其第 18 條要求公務機關應指定專人辦理安全維護事項，防止個人資料被竊取、竄改、毀損、滅失或洩漏；而在非公務機關方面，則於第 27 條要求必須採行適當之安全措施，防止個人資料被竊取、竄改、毀損、滅失或洩漏，惟各個中央目的事業主管機關，可以針對具攸關性之作業制定相關標準，指定其必須訂定個人資料檔案安全維護計畫等。並於個資法施行細則第 12 條，規範安全維護事項及適當之安全措施的原則性之規定事項；惟個資法要求的：「應注意，能注意而不注意之過失責任」，於公務機關是：「無過失責任」，非公務機關是：「抽象過失責任」，前述原則性之規定事項於「去識別化」宜遵循 ISO/TS 25237：2008(E)、CNS(ISO/IEC 29191：2013(E)29191 等標準化的進程，方能與國際接軌；惟無論是<匿名化資訊(Anonymizing information)>之控制措施(ISO/TS 25237)，還是<去識別化(De – identification)>的控制措施(CNS 29191)均較 CNS(ISO/IEC 27001)27001 附錄 A 之控制措施細緻，且前者於「資料庫管理系統」、後者在「作業系統/主機板(含手機)」均已有內嵌指令供其設計/實作使用，相關的推廣以及訓練攸關於我國「去識別化」工作項目之成本與效益[1],[2]~[4],[7],[8],[11]~[13],[18],[25],[27],[30]~[31]。

「資訊技術－安全技術－資訊安全管理－組織經濟學(Information techniques－Security techniques－Information security management－Organization economics)ISO/IEC TR 27016:2014-03-01」此標準提供方法論，使組織可以更加瞭解在經濟上如何更精確地評價其已識別的資訊資產、評鑑該等資產之潛在風險與清楚交付該等資訊資產的資訊保護控制措施之價值，以決定在保全該等資訊資產上的資源運用之最佳化[10][26]。

2005 年 9 月 28 日，行政院國家資通安全會報資安發字第 094100802 號函要求 C 級政府機關(構)應執行入侵偵測系統(Intrusion Detection Systems, IDS)之工作項目，於 2006-01-01 正式實施；2009 年 6 月 1 日，行政院國家資通安全會報資安發字第 0980100328 號函，停止前述的工作項目，其修正之說明為：「若無專責人員定期檢視，IDS 之實際效益不大，考量單位資源，刪除 C 級單位須建置 IDS 的要求」。在資訊安全

經濟學之考量下，美國聯邦政府資訊安全管理法實作計畫在 2003 年進行 IDS 的先導計畫並致力於改善 IDS 之可操作性議題，2008 年方以集中管理的框架建置 IDS 系統，同時開展態勢感知(Situational Awareness)之國家研究政策，2010 年正式實施資訊安全的連續性診斷與(風險)降低(Continuous Diagnostics Mitigation, CDM)之系列計畫；2012 年再擴增為入侵防護系統(Intrusion Prevention Systems, IPS)，並以「增進數位安全服務(Enhanced Cybersecurity Services, ECS)」等計畫，提供美國關鍵基礎設施(Critical Infrastructure, CI)等使用；在 IDS、IPS 及安全運作中心(Security Operation Center, SOC)的發展和建制之歷程，其思路以及推展的策略與我國截然不同。自 2002 年起，資訊安全預算是太多還是不足？一直是資訊安全經濟學國際研討會探討之議題，前述例證，發人省思。

在投資效益遞減的假設下：

資訊安全收益={[原始攻擊成功機率−安全投資後殘留之攻擊成功機率]×資訊資產的潛在損失值}−資訊安全投入

之資訊安全投入的參考值≅0.37×資訊資產之潛在損失值

是 2002 年發表的資訊安全經濟學著名之研究結果，並符合公共(福利)經濟學之學理，惟在我國至今幾無人求索亦乏人關注；當「組織經濟學(Organizational Economics)」正式成為 ISMS 要求事項的系列標準之一，開展去識別化認驗證體系宜如何遵循？是我國 ISMS 應面對的議題。

ISO/IEC TR 27016 以較廣泛的、組織運作於其中之社會環境全景下，經由在保護組織之資訊資產上加上經濟學觀點，並且藉由使用模型及範例，提供如何應用資訊安全之組織經濟學，強化資訊安全管理系統的實作 。綜上所述，隨著 ISO/IEC TR 27016 之發行，如何循序漸進，逐步落實 ISO/IEC 29101 的「從設計著手保護 PII」之「去識別化」的工作項目，宜對資訊安全經濟學進行更深入的研究。

「法規行為之所能落實與聚眾，必有其深厚的供應脈絡及功能應用。」2008 年 12 月 1 日，ISO/TS 25237 正式發行，成為第 1 份「去識別化」之「健康資訊 ISMS」PII 控制措施擴增的標準，參照 2011 年韓國儲存在雲端之個人資訊，90%均被竊取的情境，我國政府正執行之 10 朵雲中的「財政雲」、「健康雲」等均應遵守個資法施行細則第 17 條之要求，宜將「去識別化」的設計與實作納入「政府雲計畫」之進程，以落實個人資料保護的「供應脈絡」與「功能應用」及「基礎建設」。

致謝詞：作者謹在此對審查者提昇本文品質之貢獻，致衷心的謝忱！

參考文獻

[1] European Union Agency for Network and Information Security (ENISA), “Privacy and Data Protection by Design – from policy to engineering,” , 2014

[2] ISO, 2008a, “Health informatics – Information security management in health using ISO/IEC 27002” ISO 27799：2008-07-01.

[3] ISO, 2008b, “Health informatics – Pseudonymization”, ISO/TS 25237:2008-12-01(備考：2015-06-17，此份標準於 ISO/TC 215/WG 4 自 2012-08 起之審核，已完成行政程序，ISO 公佈結論：不修訂，繼續使用).

[4] ISO, 2013, “Information technology – Security techniques – Privacy architecture framework”, ISO/IEC 29101:2013-10-15.

[5] ISO, 2013a, “Information technology – Security techniques – Anonymous digital signatures – Part 1: General”, ISO/IEC 20008-1:2013-12-15.

[6] ISO, 2013b, “Information technology – Security techniques – Anonymous entity authentication – Part 1: General”, ISO/IEC 20009-1:2013-08-01.

[7] ISO, 2014a,WG 5 Standing Document 4(SD4) – Standard Privacy Assessment(SPA),ISO/IEC JTC 1/SC 27 N14174：2014-04-09.

[8] ISO, 2014b, “Information technology – Security techniques – Code of practice for protection of personally identifiable information(PII) in public clouds acting as PII processors, ISO/IEC 27018：2014-08-01.

[9] ISO, 2014c, “Information technology – Security techniques – Specification for digital redaction”, ISO/IEC 27038: 2014-03-15.

[10] ISO, 2014d, “Information technology – Security techniques – Information security management – Organization economics”, ISO/IEC TR 27016: 2014-03-01.

[11] ISO, 2015, “Proposal for management system standards” in “ISO/IEC Directives, Part 1: Consolidated ISO Supplement – Procedures specific to ISO(sixth edition), Annex Sh(normative) pp.116~137.

[12] ISO, 2015a, “Information technology – Security techniques – Sector – specific application of ISO/IEC 27001 – Requirements”,ISO/IEC DIS 27009：2015-07-27.

[13] ISO, 2015b, WG5 Standing Document(SD5) – Guidelines on the application of ISMS in the area of privacy, ISO/IEC JTC 1/SC 27/WG 5 N110：2015-06-30.

[14] B. Malin, “A De-identification Strategy Used for Shearing One Data Provider’s Oncology Trials Data through the Project Daya Sphere ® Repository,” 2013.

[15] E. McCallister, T. Grance, and K. Scarfone, “ Guide to Protecting the Confidentiality of Personally Identifiable Information(PII),” *NIST Special Publication 800 – 122,* 2010.

[16] A. Pfitmann, and M. Hansen, “A terminology for talking about privacy by data minimization: Anonymity, Unlinkability, Undectability, Unobservability, Pseudonymity, and Identity Management”, Version 0.34, Aug. 10, 2010.

[17] http://www.ithome.com.tw/news/98997 (2015/10/03)。

[18] http://www.trustedcomputinggroup.org (2015/08/15).

[19] 行政院，行政院院臺字第 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) ，2012。

[20] 行政院，*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 與附件 2)：2015-09-17，2015。

[21] 行政院，<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)，2015。
[22] 呂信瑩，*個人資料保護法上目的拘束原則之探討*，台北：台灣論證出版股份有限公司，2012。
[23] 法務部，*電腦處理個人資料保護法修正條文對照表*，總統華總一義字第 09900125121 號令公布，2010。
[24] 法務部，*個人資料保護法施行細則*，法務部令字第 1013107360 號，2012。
[25] 法務部，法律字第 10303513040 號函，2014。
[26] 最高行政法院，判字第 600 號，2014。
[27] 經濟部，經標授字第 10420050540 號函，2015。
[28] 經濟部標準檢驗局，*資訊技術－安全技術－資訊安全管理系統－要求事項* CNS27001：2014-04-24，2014。
[29] 經濟部標準檢驗局，*資訊技術－安全技術－隱私權框架*， CNS 29100：2014-06-04，2014。
[30] 經濟部標準檢驗局，*資訊技術－安全技術－部分匿名部分去連結鑑別之要求事項*，CNS29191: 2015-06-10，2015。
[31] 廖益鈞，“從環境及能源管理談企業社會責任”，*貨幣觀測與信用評等*，第116期，2015年11月，頁00~00，2015。
[32] 樊國楨、黃健誠、林樹國，“《個人資料保護法施行細則》第17條實作初論：根基於ISO/IEC 29100:2011-12-15標準系列”，*前瞻科技與管理*，5卷1期：頁43~83， 2015a。