個人資料保護與資訊安全管理探微

摘要：

在標準化之過程中，每一分標準的頒布是因或是果，是一個標準化趨勢之契機或是成績，標準化之過程是瞭解標準的「爲何」暨「如何」等探索時代脈動之綱目，「標準」從長遠的角度來看，是標準化過程中之里程碑。

隨著個人資料保護法在2010年5月26日之公布，個人資料保護的資訊安全管理議題已成爲眾所矚目之焦點；根基於此，本文以國際標準組織(International Organization for Standardization，簡稱ISO)已頒布與進行中的資訊安全管理系統(Information Security Management System，簡稱ISMS)之標準及標準化的工作項目爲核心，探討並提出合規於個人資料保護之ISMS標準化以及擴增控制措施實作的方法。

關鍵詞：

1. 資訊交換(Information Exchange)。
2. 資訊安全管理系統(Information Security Management System)。
3. 資訊分享(Information Sharing)。
4. 個人可識別資訊(Personally Identifiable Information)。
5. 標準化(Standardization)。

壹、前言

2010年4月27日立法院第7屆第5會期第10次會議通告：將「電腦處理個人資料保護法」名稱修正爲「個人資料保護法」，並修正全文，2010年5月26日業經總統公布[1]；其中如表1.1與表1.2所示，各個目的事業之已公布的法規及進行中之標準因涉及表1.3的財務風險，個人資料之資訊安全管理已成爲眾所矚目的資訊安全議題[1~5]。

表 1.1　個人資料保護法與資訊安全管理

1.　公務機關： 第１８條：公務機關保有個人資料檔案者，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。 2.　非公務機關： 第２７條：非公務機關保有個人資料檔案者，應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。 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。 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。

表 1.2　研修(個資法)施行細則之時程(隨時修正)

時程	6 月	7 月	8 月	9 月	10 月	11 月	12 月	100 年
法務部公聽會	*							
目的事業機關彙整研議	*	*	*					
第一階段會議				*	*			
第二階段會議						*	*	
第三階段預告公聽								*
資料來源：黃荷婷 (2010) 新版個資法施行細則預告與釋疑(簡報資料)，2010 年 6 月 22 日。								

表 1.3　隱私權集體訴訟案例

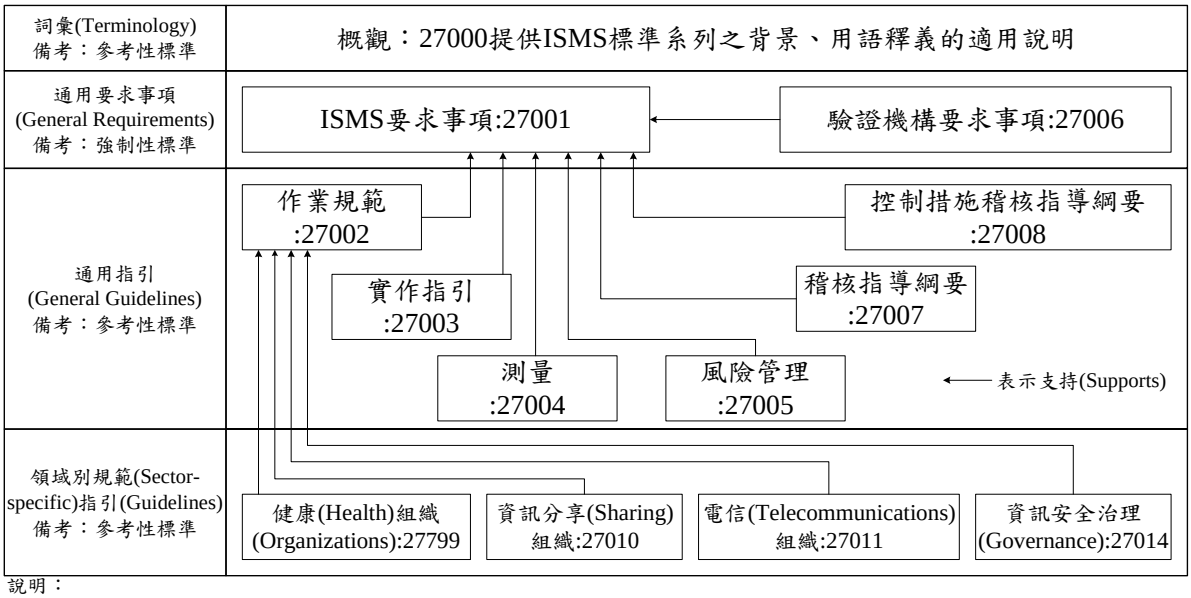
1. 資料來源：2010 年 9 月 5 日，聯合報 A9 (國際新聞)，鍾玉玨/綜合 4 日外電報導。
2. 美國加州舊金山一份法庭文件顯示，因一宗觸犯隱私權之集體訴訟，Google 已同意支付 U.S.$ 8,500,000.的合解金。
3. 7 位原告指控 Google 免費電子郵件服務之 Gmail 內建的 Buzz 社交網路工具，侵犯其隱私權。
4. Google 於 2010 年 2 月 9 日推出將 Gmail 連絡人自動掛到 Buzz 之連絡人名單中的新功能，引發網友疑慮；目前 Google 已改變其組態，Gmail 用戶必須在 Buzz 工具下，另建可以公開的連絡人名單，隨時可以瀏覽、編輯、隱藏或封鎖。
5. 和解金中 30%歸律師，7 位原先每人至多可獲得 U.S.$ 2,500.，其餘金額將存入專戶，資助致力於網路隱私或教育之相關機構。
6. 參考資料：http://zh.wikipedia.org/zh-tw/Google_Buzz/ (2010-09-11)。

隨著電子科技之一日千里，電腦與網路的結合在21世紀初已展現令人眩目之光芒，個人資料的安全維護將面對1980年9月23日經濟合作暨發展組織(Organization for Economic Co-operation and Development，簡稱OECD)公布之個人資料的跨國流通與隱私權保護指導綱要(Guidelines Governing the Protection of Privacy and Transporter Flows of Personal Data)不同之網路安全情境，惟其原則(Principles)除擴增「告知與預防損害原則」外仍同[1,6~10]。根基於此，在第2節與第3節分別闡明個人資料保護標準化的框架及以財稅(Finance)領域探討其研定個人資料資訊安全保護標準指導綱要(Guidelines)時宜擴增之控制措施項目，第4節是本文的結論。

貳、個人資料與資訊安全管理：

「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09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，如圖2.1與圖2.2所示之資訊安全管理系統(Information Security Management System，簡稱ISMS)標準化的第一階段工作已樹立第1座里程碑。



說明：
1. 資料來源：ISO/IEC 27000:2009-05-01，頁12，圖1；與本研究。
2. 備考：ISO/IEC 27001、ISO/IEC 27005均參照ISO 31000等修正中，預定於2012年5月完成。
3. 參考資料：2nd Working document for revision of ISO/IEC 27000, ISO/IEC JTC 1/SC 27 N9027, Page 15, Figure 1, 2010-11-23.

圖 2.1　資訊安全管理系統(Information Security Management System，簡稱 ISMS)標準系列(ISO/IEC 27001 屬別(Family))框架

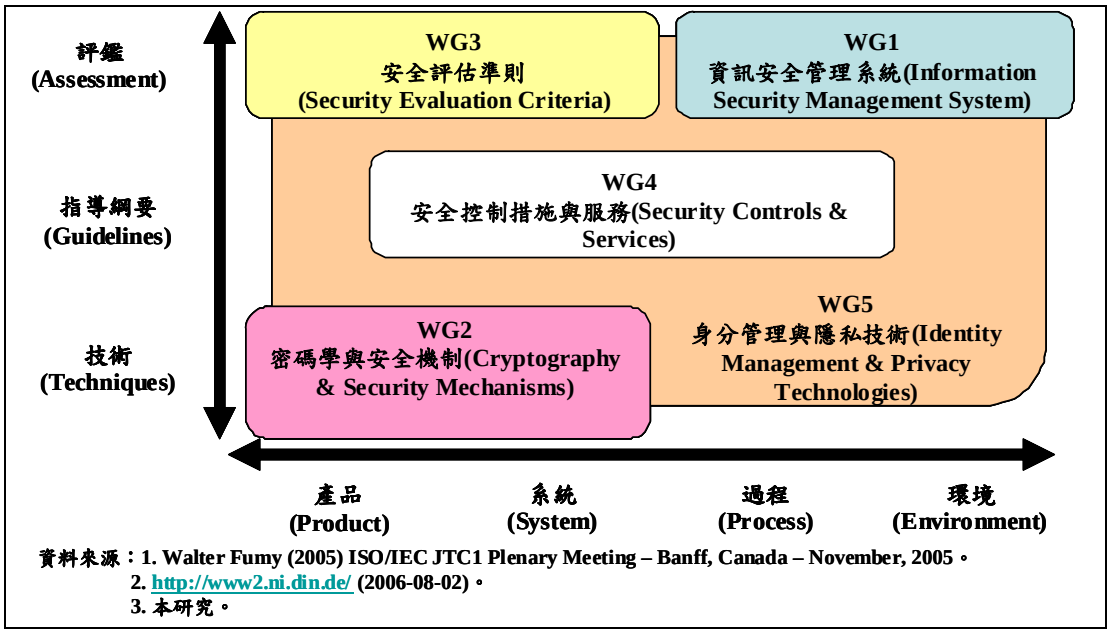
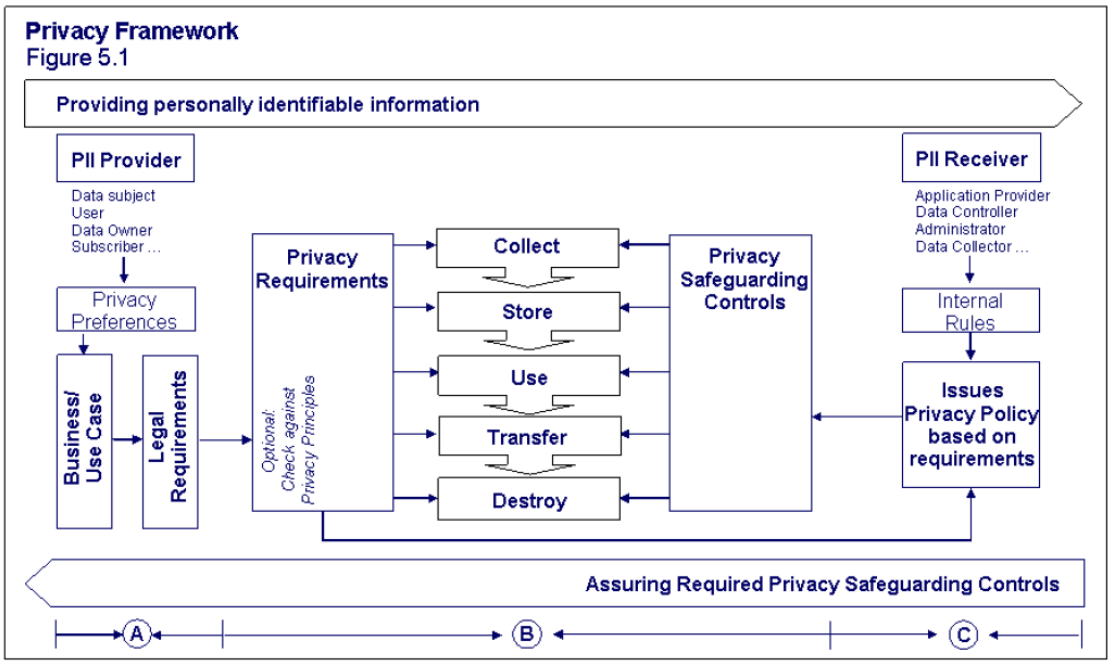


圖 2.2　ISO/IEC 安全標準工作框架調整現況(2005 年 5 月之後)

ISMS之國際標準提供在建立與維持管理系統時得以遵循的模型，ISMS模型(ISMS標準家族)納入資訊安全領域中各專家所達成共識的特性，以作爲國際之藝境。爲反映出ISMS標準家族在不同領域的實作宜進行之變更， ISO 27799與ISO/IEC 27011已分別頒布成爲健康(Health)及電信(Telecommunication)領域控制措施實作變更之規範。個人資料保護的施行，如圖2.3所示之ISO/IEC 29100等標準系列與ISMS的關連等均是建立ISMS稽核宜面對之議

題。

個人可識別資訊(Personally Identifiable Information，簡稱PII)是如表2.1所示之美國聯邦資訊安全管理法(Federal Information Security Management Act，簡稱FISMA)要求，爲強化ISMS有關個人資料安全的指引[11]，提出之概念；因具可操作性，自2003年10月研究起至2006年5月立項制定相關標準系列止，納入ISO/IEC JTC1/SC27 WG5如圖2.3所示的標準框架的核心組件，表2.2是PII之案例說明。



說明：

1. 資料來源：Rannenberg, K. (WG5 Convener), Sténuit, C. (Co-editor 24760), Yamada, A. (Editor 24761), and A.S. Weiss (Editor 29100/29101) (2007) Working Group 5 Identity Management and Privacy Technologies Within ISO/IEC JTC 1/SC 27 – IT Security Techniques (Presentation), 2007-09-30.
2. 24760 是身分識別之框架，24761 (已於 2009-05-11 出版)是生物量度的鑑別全景之標準。
3. 除 24761 外，於 2010 年 6 月 30 日均已至 CD 階段。

圖 2.3　ISO 29100 Privacy Framework Draft for Graphical Representation

表 2.1　個人資料保護與資訊安全管理已出版之相關標準

1. ISO/IEC 27001 資訊安全管理系統(Information Security Management System，簡稱ISMS)標準系列。
2. McCallister, E. et al. (2010) Guide to Protecting the Confidentiality of Personally Identifiable Information (PII), NIST Special Publication 800-122.
3. British Standard BS 10012 (2009) Data protection – Specification for a personal information management system.
4. Matthew, S. et al. (2008) An Introductory Resource Guide for Implementing the Health

Insurance Portability and Accountability Act (HIPPA) Security Rule, NIST Publication 800-66, Revision 1.
5. Payment Card Industry (PCI) Data Security Standard (DSS) Version 1.2.1 (2009).
6. 備考：ISO/IEC JTC1/SC27 WG5 主責隱私安全標準系列之制定。

表 2.2　個人識別資訊(Personally Identifiable Information，簡稱 PII)案例

1. 資料來源：2010 年 8 月 29 日，聯合報 A8(社會)，記者曹敏吉/高雄報導。
2. 2007 年 6 月，蘋果日報報導高雄縣某家美語補習班男教師涉嫌性侵 10 歲女童並搭配兩幅性侵(口交)動畫繪圖與性侵害時序表；及刊出眼部經馬賽克處理之男教師以及其妻子的合照，清楚表明補習班之地點。經高雄地檢署偵查，認定並非事實，前(2008)年底處分不起訴。
3. 男教師夫婦向蘋果日報及其 3 名記者各求償 N.T.$ 1,500,000.，法官認爲照片仍足以識別當事人身分，且報導內容大篇陳述性侵經過，僅簡單說明男教師否認性侵，實質並未平衡報導，一審判蘋果日報應賠償 N.T.$ 800,000.；二審判蘋果日報應賠償男教師 N.T.$ 1,000,000.與其妻子 N.T.$ 400,000.，合計 N.T.$ 1,400,000.。

前述PII之個人資料保護的ISMS控制措施，在圖2.1中之ISO/IEC 27001標準系列的ISO/IEC 27002第10.7.2節之實作指引中已有「宜考量聚合效應(Aggregation Effect)」等規範，表2.1中的標準規範應能提供實作時之參考。如前所述，PII等相關標準系列尚在制定中，惟遵循如表2.3所示之ISMS的規範，再參照ISO 27799、ISO/IEC 27012擴增之控制措施，應能建立可以適當保護個人資料的ISMS。

表 2.3　ISO/IEC 27001:2005(E)第 A.15.1.4 條款與 ISO/IEC 27002:2005(E)第 15.1.4 條款：「個人資訊的資料保護與隱私」之規範

A.15.1.4	個人資訊的資料保護與隱私	控制措施 應如同相關法令、法規及若適用的契約條文所要求的，確保資料保護與隱私。

實作指引

宜發展和實作組織的資料保護與隱私政策。此政策宜傳達給涉及處理個人資訊的所有人員。

爲遵循此政策與所有相關的資料保護法律及法規，需要有適切的管理結構和控制措施。通常最好指派如資料保護專員(data protection officer)的專人負責，來達成此目的，此人宜對管理者、使用者和服務提供者提供其各自的責任及宜遵照的特定程序之指引。處置個人資訊和確保資料保護原則認知的責任宜依據相關法律及法規處理。宜實作適當的技術與組織措施以保護個人資訊。

其他資訊

許多國家已經制定了法律，對個人資料(通常是有關個人的資訊，可依據這項資訊識別此人)的收集、處理及傳輸行爲採取控制措施。依個別的國家法律，此類控制措施可以強制這些收集、處理、散播個人資訊的個人負起責任，也可以限制向他國移轉該資料的能力。

前述ISMS之實作，以新竹市稅務局爲例，根基於立法院三讀通過的「個人資料保護法」明文規範之「公務機關」對個人資料的「資訊安全管理」事宜第十八條：「公務機關保有個人資料檔案者，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。」，在「個人資料保護法」第二條亦定義「處理：指爲建立或利用個人資料檔案所爲資料之記錄、輸入、儲存、編輯、更正、複製、檢索、刪除、輸出、連結或內部傳送。」，其個人資料之處理已包含儲存、參照相關規範[7~9]，分別定義如下：

一、 資訊保留政策(Information retention policy)：闡明機關(構)對個人資料之實體與電子文件的分類及機密等級、保存時間、方式以及保管人員之職責，應遵循的法規與內部稽核及資訊安全治理之要求。
二、 資料保留與處理政策(Data retention and disposal policy)：闡明機關(構)對資料保留及處理之實作的政策以及程序。

根基於前述定義，於新竹市稅務局爲保護納稅人等之個人資料已要求退稅、房屋稅、牌照稅等各項業務提出其資料保留與處理政策[1,7,10]，並提出如表2.4所示的ISMS之控制措施的要求及測試程序，供各個業務部門參考；參照表2.5之規範，圖2.4是諸如碟帶、磁碟等電磁紀錄物資料淨化(Sanitization)處理作業流程示意說明[1,7,10~12]。

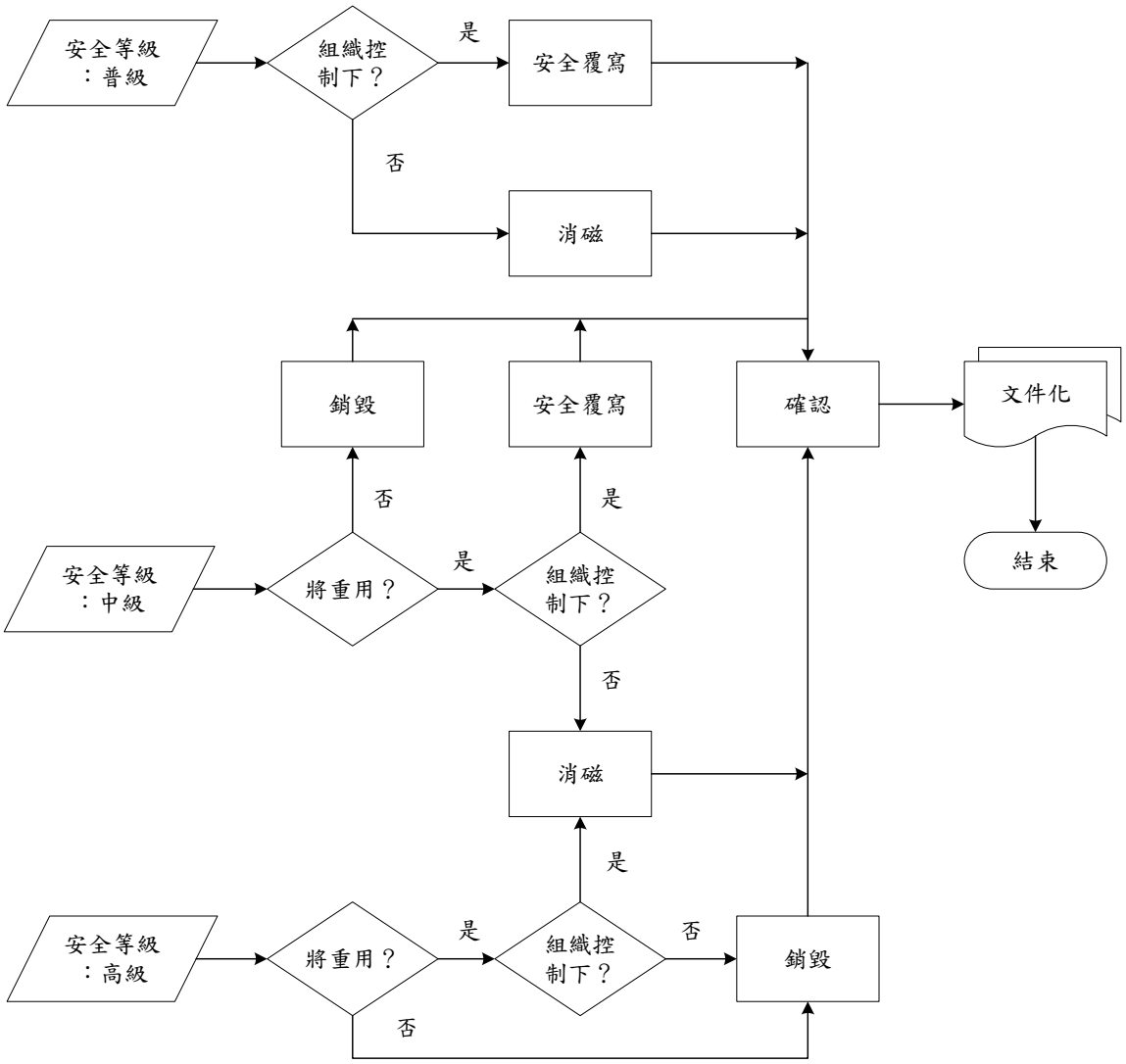
表 2.4　資料保留(Retention)與處理(Disposal)政策之要求與測試程序例

資訊安全管理控制措施要求	測試程序
使個人資料儲存與處理功能最小化。制定資料保留及處理政策。根據業務、法律及/或法規要求限制儲存之大小與保留以及處理功能時間，在資料保留與處理功能政策中進行記錄。	獲取並檢查機關(構)關於資料保留與處理功能之政策及程序，並且執行以下審查 1. 確認政策與程序包含資料保留及處理功能法律、法規以及業務要求，包括個人資料保留之具體要求（例如，個人資料因 Y 業務的原因需要保留 X 時長）。 2. 確認政策與程序包含不再因爲法律、法規或業務原因需要進行，包括個人資料在內之資料處理的規定。 3. 確認政策與程序包括媒體淨化(Media Sanitization)在內之所有個人資料儲存及處理功能的各個面向。 4. 確認政策與程序包含程式化（自動）程序以至少每個季度清除一次超過業務保留要求之個人資料，或者視檢查要求，至少每季進行一次，以確認儲存的個人資料沒有超過業務保留之要求及其處理。 5. 確認政策與程序包含程式化(自動)程序以至少每

	季審查一次超過業務要求之處理功能及其風險處理過程。
參考資料：支付卡產業資料安全標準 1.2.1 版，July 2009。	

表 2.5　ISO/IEC 27001:2005(E)第 A.9.2.6 條款與 ISO/IEC 27002:2005(E)第 9.2.6 條款：「設備的安全汰除或再使用」之規範

A.9.2.6	設備的安全汰除或再使用	控制措施 含有儲存媒體的設備，其所有項目在汰除前應加以檢核，以確保任何敏感性的資料與有版權的軟體已被移除或安全地覆寫。
實作指引 含有敏感性資訊的裝置宜實體銷毀，或宜以原始資訊將無法被擷取的技術毀損、刪除或覆寫資訊，而非僅使用標準的刪除或格式化功能。 其他資訊 含有敏感性資料的受損裝置可能需要作風險評鑑，以決定是否宜實體銷毀裝置而非僅修復或丟棄。 不慎的汰除或重複使用設備，其資訊可能遭致破解(備考：PII 之推論控制的脆弱性)。		



說明：

1. 資料來源：Kissel R. et al. (2006) Guidelines for Media Sanitization, NIST SP 800-88, September 2006。
2. 覆寫(Overwritten)過之磁碟仍能回復(資料來源：Garfinkel, S.L. and A. Shelat (2003) Remembrance of Data Passed: A Study of Disk Sanitization, IEEE Security & Privacy, Vol. 1, No. 1, pp.17~27.)。
3. NIST SP 800-88因應各種媒體(Media)之統一用語為清除(Clear)、刪除(Purge)與破壞(Destroy)。

圖 2.4　電磁紀錄物資料淨化(Sanitization)處理作業流程舉隅

「資訊安全因標準而不同，資安標準因實作而不同。」綜前所述，於臺灣地區若能遵循如圖2.1所示之ISMS標準系列框架所示之ISMS各項強制性或參考性標準系列，應能訂定合宜的「個人資料檔案安全維護計畫與業務終止後個人資料處理方法。」之指導綱要。

三、個人資料資訊分享宜擴增之資訊安全管理系統要求事項初探：

隨著個人資料保護法之公布，ISMS如何遵循法規而調整已成爲資訊安全管理的焦點之一。一個好的ISMS政策於實作ISMS之工作項目時能提供「水到渠成」的全景，讓執行者「舉止優雅」與「態度從容」；根基於此，在已建立之ISMS中，先於ISO/IEC 27001:2005(E)之下列條款：

1. 第4.2.1節(b)(2)：

考量營運與法律或法規要求，及契約之安全義務。

2. 第4.2.1節(c)(1)：

識別適合ISMS與已識別之營運資訊安全法律及法規要求的風險評鑑方法論。

3. 第5.2.1節(c)：

識別並因應法律與法規要求，及契約之安全義務。

4. 第7.3節(c)(4)：

影響資訊安全之程序與控制措施的必要時之修改，以回應可能衝擊ISMS之內部或外部事件，包括下列事項的變更：

(4)法律或法規各項要求。

備考：應配合「個人資料保護法」立法進程，於一定時間內完成修正。

5. 第A.15.1節：

目標：避免違反任何法律、法令、法規或契約之義務，與任何安全要求。

規範攸關「個人資料保護法」宜擴增的要求事項；於附錄A之「控制措施部分」，參照已出版與尚在進行中的標準，表3.1及表3.2分別是ISMS宜擴增以及列爲強制性控制措施之參考；表3.3、圖3.1與圖3.2是存取控制擴增之示意說明，囿於篇幅，僅就表3.1中的資產管理部分之共享資訊面向宜強制要求於其交換作業中確保存在適當之防護。

表 3.1 涉及個人資料之資訊分享(Information Sharing)宜參考之資訊安全管理系統(簡稱 IS-ISMS)要求事項初探

<table>
<tr><td colspan="4">ISO/IEC 27001:2005(E)本文第 4 節~第 8 節之釋義均擴增之</td></tr>
<tr><td colspan="4">5. 安全政策 [1,2,2,0,0]</td></tr>
<tr><td colspan="4">6.組織資訊安全 [2,11,2,0,0]</td></tr>
<tr><td colspan="4">7. 資產管理 [2,5,2,7,0] (備考：新增 1 控制目標)</td></tr>
<tr><td>8. 人力資源安全
[3,9,0,0,1]</td><td>9. 實體與環境安全
[3,13,13,6,3]</td><td>10. 通信與作業管理
[10,32,24,3,11]</td><td rowspan="2">12. 資訊系統獲取、開發及維護
[6,16,3,1,2]</td></tr>
<tr><td colspan="3">11. 存取控制 [7,25,10,2,6]</td></tr>
<tr><td colspan="4">13. 資訊安全事故管理 [2,5,2,1,1] (備考：新增 1 控制目標)</td></tr>
<tr><td colspan="4">14. 營運持續管理 [1,5,2,0,0]</td></tr>
<tr><td colspan="4">15. 遵循性 [3,10,3,0,0]</td></tr>
<tr><td colspan="4">備考：

1. [m,n,o,p,q] – D [控制目標數, 控制措施數, 擴增控制措施數, 新增控制措施數, 強制性控制措施數]
2. 控制目標於 ISO/IEC 3rd WD 27010:2010-05-27 中均擴增之。</td></tr>
</table>

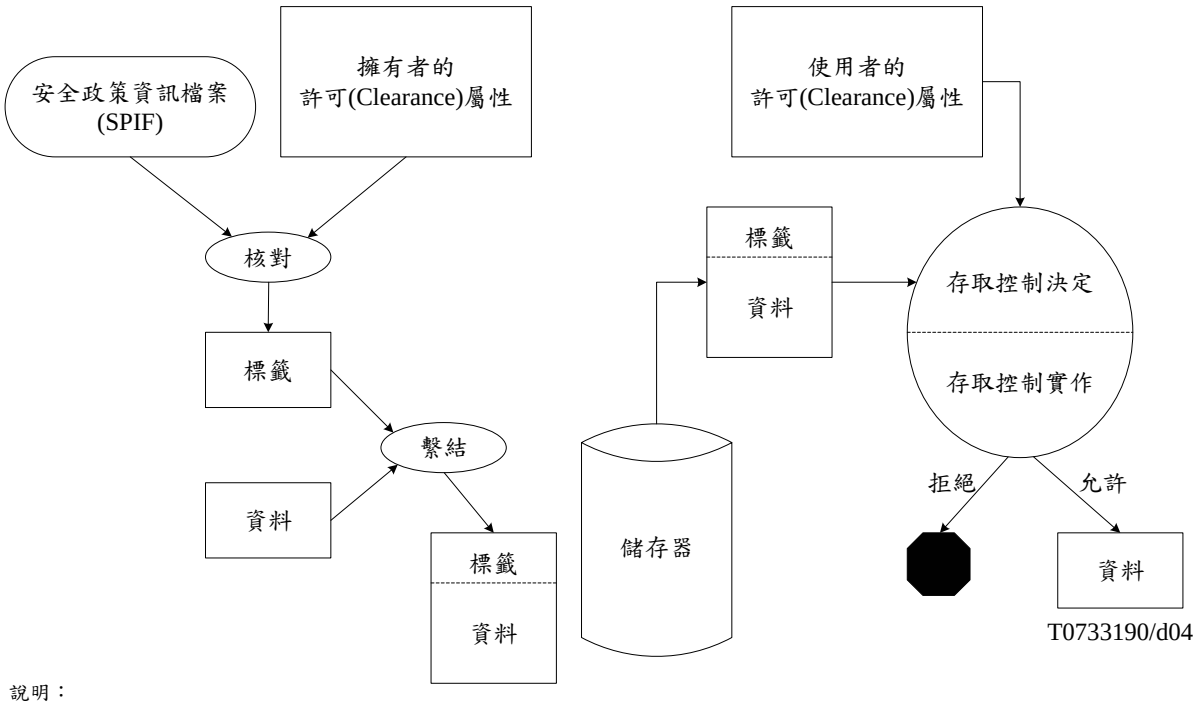
3. 資料來源：ISO/IEC 3rd WD 27010:2010-05-27、ISO/IEC 27011:2008-12-15 與 ISO 27799:2008-07-01。

表 3.2　IS-ISMS 敘述爲應(Shall)之強制性(Mandatory)控制措施表列初探

ISO/IEC 27002:2005(E)節碼	ISO/IEC 27002:2005(E)之節碼名稱
無	備考：於共享資訊交換作業中確保存在適當之防護
A.8.3.3	存取權限的移除
A.9.2.5	場所外設備的安全
A.9.2.6	設備的安全汰除或再使用
A.9.2.7	財產的攜出
A.10.1.2	變更管理
A.10.1.4	開發、測試及運作設施的分隔
A.10.3.2	系統驗收
A.10.4.1	對抗惡意碼的控制措施
A.10.5.1	資訊備份
A.10.7.2	媒體的汰除
A.10.7.3	資訊處理程序
A.10.8.1	資訊交換政策與程序
A.10.8.2	交換協議
A.10.10.3	日誌資訊的保護
A.10.10.6	鐘訊同步
無	備考：於存取控制之一般性(General)要求(Requirements)。
A.11.1.1	存取控制政策
A.11.2.1	使用者註冊
A.11.2.2	特權管理
A.11.6.1	資訊存取限制
無	備考：於共享資訊主題之唯一識別」
A.12.2.4	輸出資料確認
無	備考：建立早期預警系統(Early Warning System)提供資訊安全警示分享資訊

表 3.3　資訊系統間資訊交換存取控制政策

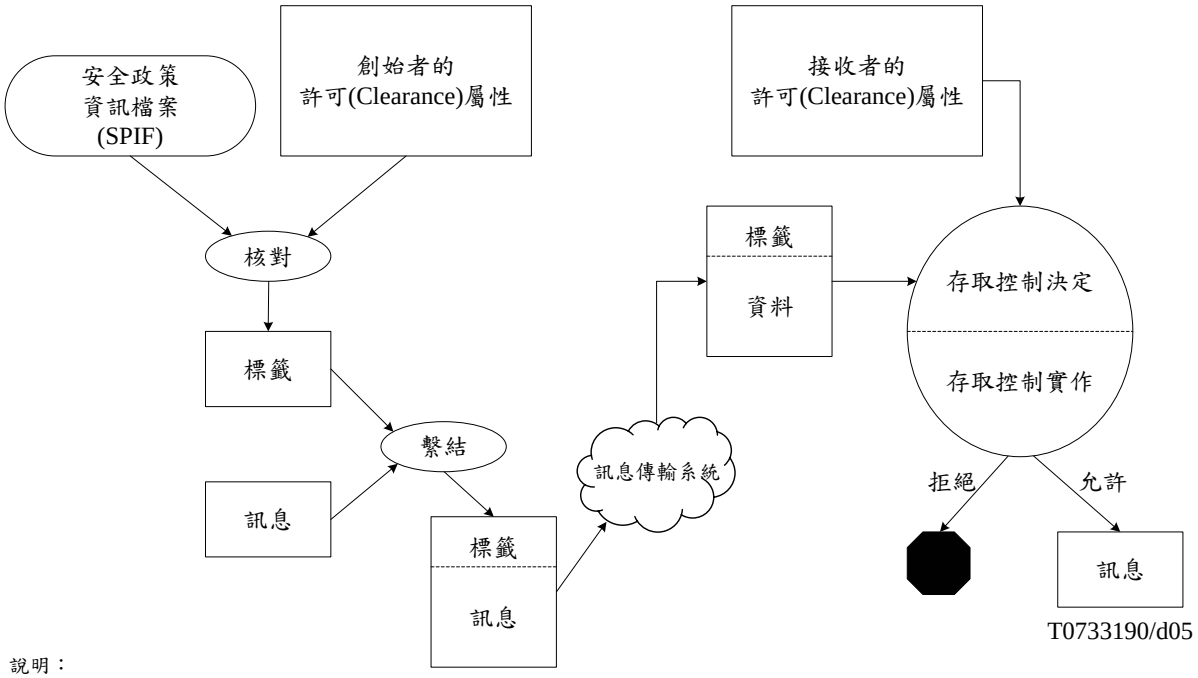
資訊系統使用其他系統之資料，必須由原資訊系統將必須提供的資料依經授權之檢索格式表列要求，使用暫存檔的方式提供。禁止直接萃取資料檔案或資料庫中之任何資料，僅允許經由介面程式轉檔後提供最小範圍的資料。



說明：

1. 繫結(Binding)方法，通常使用數位簽章(Digital Signature)或訊息鑑別碼(Message Authentication Code)之密碼演算法。
2. SPIF：Security Policy Information File。
3. 資料來源：ISO (2002) Information technology – Security techniques – Security information objects for access control, ISO/IEC 15816: 2002-02-01, Figure 4。

圖 3.1　資料儲藏之存取控制 (Data Storage Access Control)



說明：

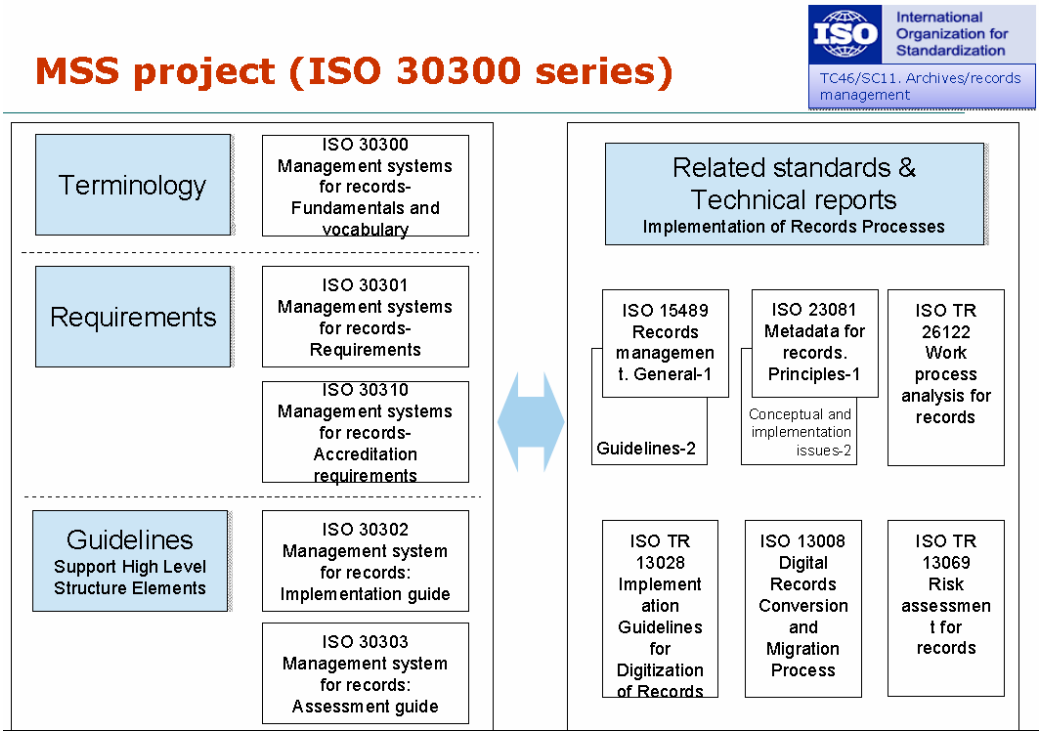
1. 繫結(Binding)方法，通常使用數位簽章(Digital Signature)或訊息鑑別碼(Message Authentication Code)之密碼演算法。
2. SPIF：Security Policy Information File。
3. 資料來源：ISO (2002) Information technology – Security techniques – Security information objects for access control, ISO/IEC 15816: 2002-02-01, Figure 5。

圖 3.2　檢索格式表列要求資訊交換情境

資訊交換防護(Information Exchanges Protection)之目的在於確保分享資訊之社群間資訊交換作業存在適當的防護，ISO/IEC 27002:2005(E)之第10.8節已提供建立資訊技術面向規範的良好指引，惟在實作上宜增加如後之控制措施：

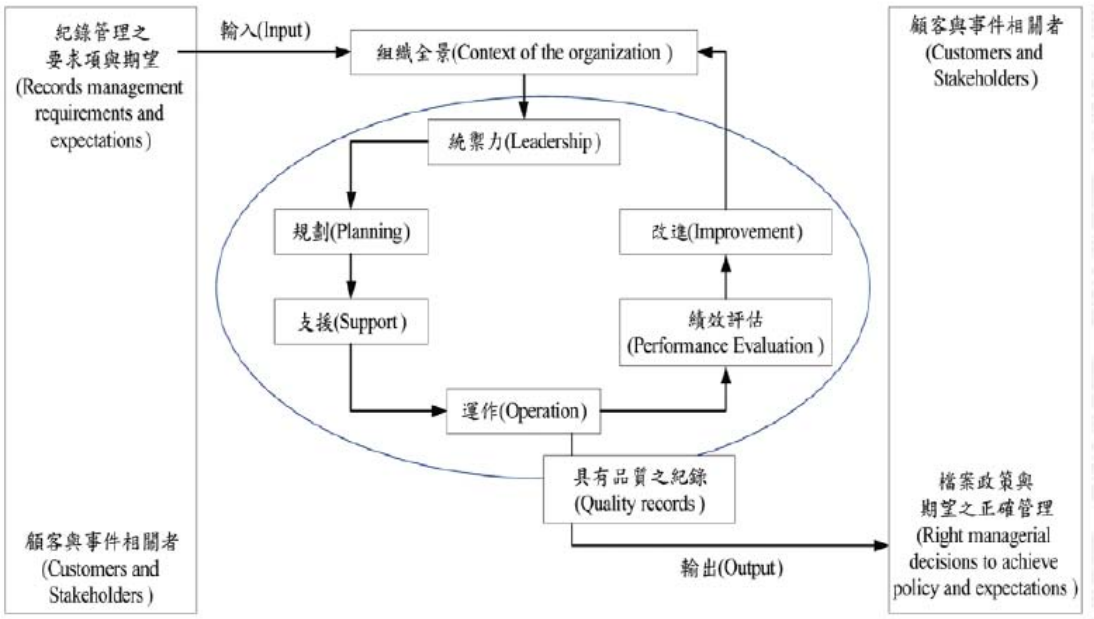
1. 分享資訊之分級標示：宜將分享資訊區分成「僅限當事人」、「僅限特定對象」、「僅限分享資訊社群」、「公開」等層級並明顯標。
2. 敏感性資訊之過濾：一分資訊提供不同層級之分享資訊時，宜將敏感性資料(例：犯罪剖繪之具體事實等)刪減或另行表述。
3. 設置被拒絕分享資訊之申訴窗口(Information Disclaimer)：宜提供當事人無法獲取資訊之特殊要求的傾聽、瞭解並澄清疑點與困難所在之管道。

綜上所述，參照圖2.1之ISMS標準系列框架中的規範與如圖3.3、圖3.4及圖3.5所示之紀錄管理系統標準系列的要求項目，型塑「個人資料保護法」合規之資訊安全管理的控制措施等，應是實作之議題。



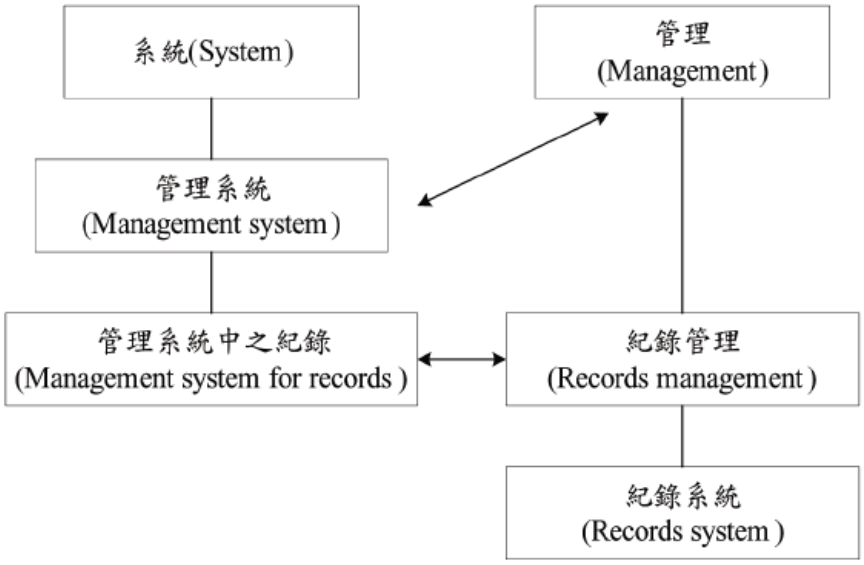
資料來源：Bustelo, C. (2010) Update ISO TC46/SC1 Current MSS Project, Buenos Aires, May 2010。

圖 3.3 管理系統標準(Management System Standards，簡稱 MSS)標準化(2001~2015?)與紀錄管理系統(Management System for Records，簡稱 MSR)標準系列



資料來源：ISO (2010) Information and documentation - Management system for records - Fundamentals and vocabulary, ISO DIS 30300:2010-05-21, Figure 3, p. 7.

圖 3.4　根基於過程導向之管理系統的紀錄模型(Process-based MSR model)



資料來源：ISO (2010) Information and documentation - Management system for records - Fundamentals and vocabulary, ISO DIS 30300:2010-05-21, Figure 3, p. 7.

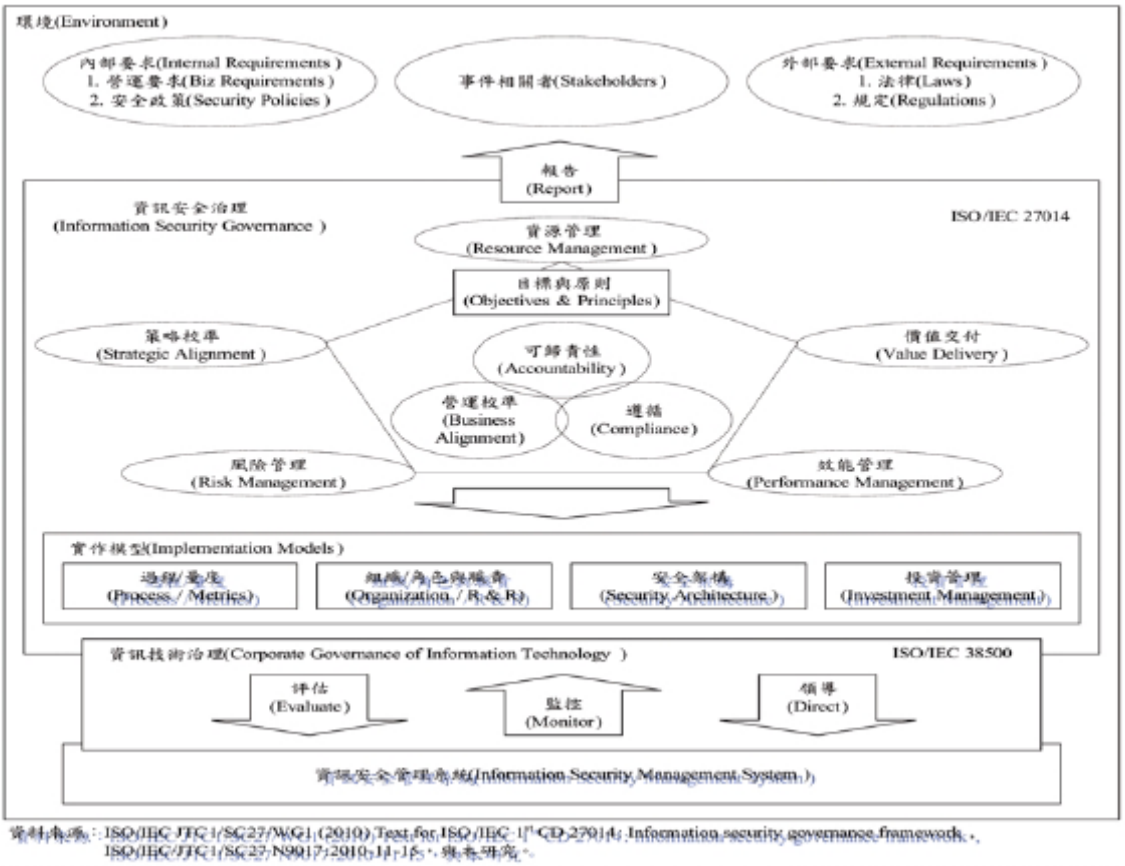
圖 3.5　管理系統與管理中之紀錄的關係

安全就像空氣，原本毫無價值，失去時才會痛苦覺察其存在，私密資訊外流，爲數位台灣投下了空前的威脅；查證費時，鑑識困難，甚至傳出犯罪集團已握有台灣民眾戶籍、兵籍、稅務等資料。在網路社會生活型態快速普及，資安威脅不斷使得人人自危之際，必須能讓社會大眾充分認知，惟有落實與時俱進的ISMS於日常生活中，才能成功邁向優質網路社會，確保人民生活之便利與安全；如何落實ISMS標準化之實作，是建立與驗證ISMS宜面對的議題。

肆、結論

標準(Standard)係指經由共識與某一公認的機構核准，提供一般或重複使用以提供各項活動或結果有關的規則、指導綱要或特性所建立之文件，期使在某一情況下獲致秩序的最佳程度；而標準化(Standardization)係指在一定的範疇內，針對實際或潛在的問題，建立共同而經常使用的條款之活動，以期達成秩序的最佳程度，此標準化活動，特別包括標準之制定、發行及實施等過程。換言之，標準是標準化的源池，標準化是標準之實踐；標準的發展宜以科學、技術與實踐之綜合成果爲基礎，以促進最佳的共同效益爲目的。

「建立我國通資訊基礎建設安全機制計畫」自行政院2001年1月17日核定通過後，資訊安全管理系統(Information Security Management System，簡稱ISMS)驗證是前2期(2001~2008年)工作的主軸之一，今(2009)年將進行2009年1月20日院台經字第0980080376號函核定更名爲「國家資通訊安全發展方案」之第3期(2009~2012)的相關計畫[3]，前述已奉核定之11項重要措施與30個行動方案(以下簡稱資安發展方案)中，「推動資訊與資訊系統分級資安稽核與推動ISMS驗證」是「落實電子化政府資安管理」之重要措施的9項行動方案之一，更成爲「政府機關(構)資訊安全責任等級分級作業施行計畫」的依據[4]。ISMS之實作不是一個事件或一種狀況，而是散布在ISMS作業中的一連串行動，這些行動隨處可見，甚至在管理階層營運之方式中，亦有其蹤跡。ISMS的過程，係經由規劃、執行、監督與改進等基本的管理過程力以治理。前述合規「個人資料保護法」之ISMS的實作宜已如圖4.1所示之ISO已公布的資訊安全治理框架[15]，據以制定分如圖4.2與圖4.3之能校準營運及資訊安全的ISMS計畫。



資料來源：ISO/IEC JTC 1/SC 27/WG 1 (2010) Text for ISO/IEC 1[1] CD 27014: Information security governance framework，ISO/IEC/JTC 1/SC 27 N9017 (2010-11-15)，與本研究。

圖 4.1　資訊安全治理框架之概念

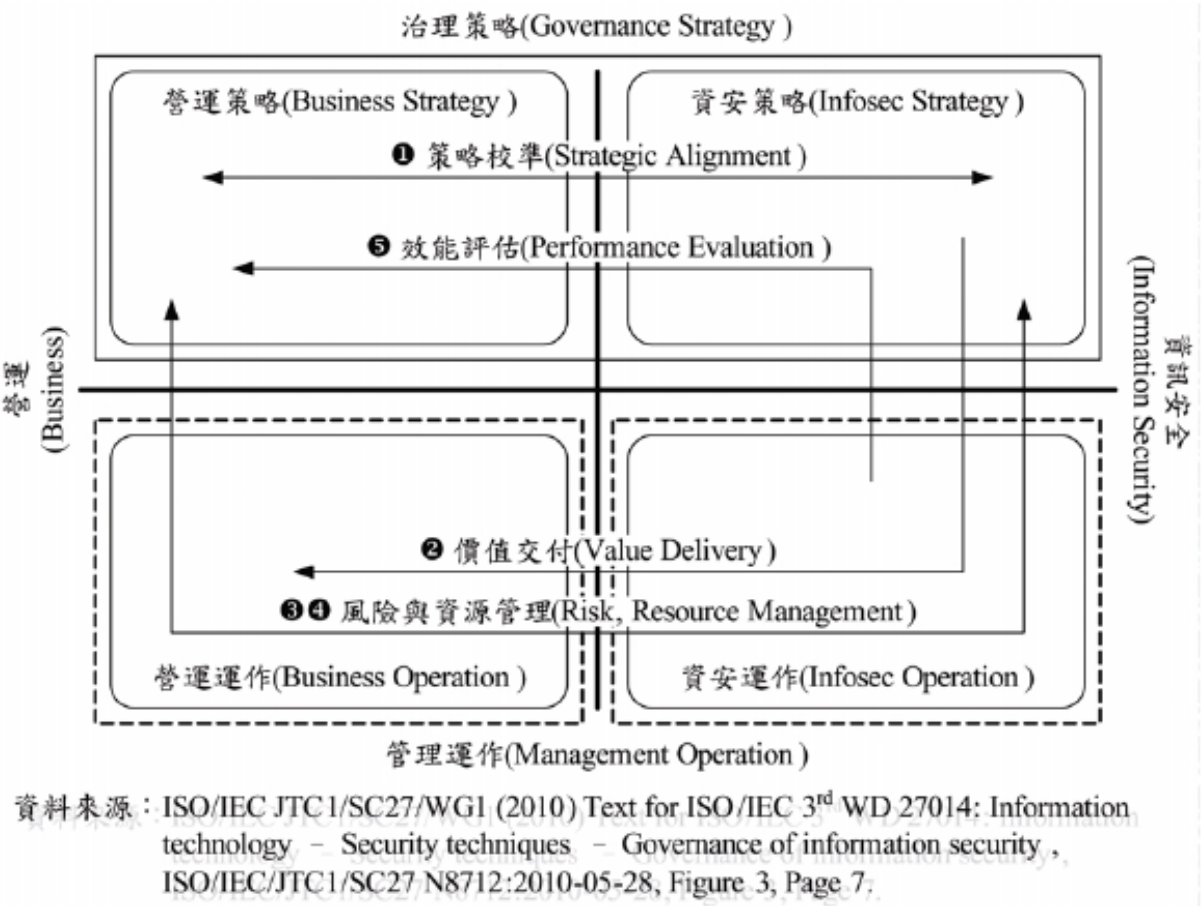


圖 4.2　資訊安全與營運間之校準領域

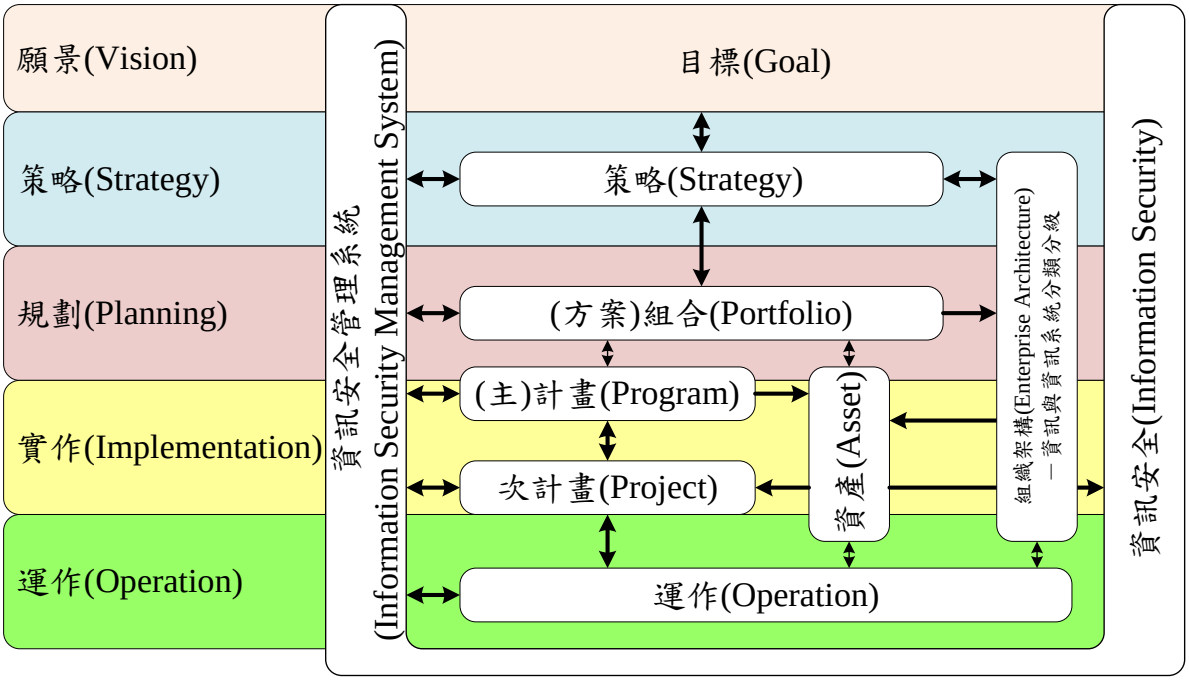


圖 4.3　資訊安全實作框架初探

標準可以累積知識與經驗，標準化則是冀求以系統的、共同協調一致之方法來強化標準的知識以供傳承。根基於ISMS標準化之進程及台灣的環境，本文參酌ISO/IEC 27001:2005(E)標準系列之發展軌跡據以裁適提出建立合規「個人資料保護法」ISMS實作的方法如前所述[9,11~15]；囿於水平，疏漏之處在所難免，尚望先進宏達不吝指正。

【參考文獻】

[1] 個人資料保護法 (2010) 中華民國 99 年 5 月 26 日華總一義字第 09900125121 號總統令公布。

[2] 黃荷婷 (2010) 新版個資法施行細則預告與釋疑(簡報資料)，2010 年 6 月 22 日。

[3] 國家資通安全會報 (2009) 國家資通訊安全發展方案(98~101 年)，行政院資安發字第 0980100055 號函，2009 年 2 月 5 日。

[4] 行政院國家資通安全會報 (2010) 資安發字第 0990100394 號函(資訊系統分類分級與鑑別機制參考手冊，2010 年 7 月)，2010-07-05。

[5] 行政院主計處電子資料處理中心 (2010) 中審字第 09990000855 號函，2010 年 7 年 28 日。

[6] 翁岳生等 (1985) 資訊立法之研究，行政院研究發展考核委員會編印。

[7] 法務部 (2009) APEC (Asia – Pacific Economic Cooperation) APEC 隱私權保護綱領(中英文對照)，2009 年 10 月。

[8] 財團法人金融聯合徵信中心 (2008) 澳洲隱私權法，2008 年 10 月。

[9] ISO (2010) Text for ISO/IEC 3rd WD 27001 – Information technology – Security techniques – Information security management systems – Requirements, ISO/IEC JTC1/SC27 N8700, 2010-08-17.

[10] Verizon Business (2010) 2010 Data Breach Investigations Report.

[11] McCallister E., Grance T., and Scarfone K. (2010) Guide to Protecting the Confidentiality of Personally Identifiable (PII), NIST Special Publication 800-122, April, 2010.

[12] ISO (2010) Text for ISO/IEC 3rd WD 27010 – Information technology – Security techniques – Information security management for inter-sector and inter-organizational communications, 2010-05-27.

[13] ISO (2008) Health informatics – Information security management in health using ISO/IEC 27002:2008-07-01.

[14] ISO (2008) Information technology – Security techniques – Information security management guidelines for telecommunications organizations based on ISO/IEC 27002:2008-12-15.

[15] ISO/IEC JTC1/SC27 (2010) Text for ISO/IEC 3rd WD 27014 – Information technology – Security techniques – Information security governance framework, ISO/IEC JTC1/SC27 N8712:2010-05-28.

（本文由國立交通大學資訊管理研究所/樊國楨教授、國立臺灣大學資訊管理學研究所/黃健誠、新竹市稅務局/廖菊芳 提供）