# 個人資料保護標準化初探

一、前言

二、管理系統標準與個人資料保護

三、個人資料保護宜擴增之控制措施初探

四、隱私衝擊評鑑簡析

五、結論

異術科技股份有限公司資訊長
樊國楨

中華民國一〇一年一月十一日

# 資訊安全風險管理之典範轉移指標

1. 資料來源：

   1.1 ACFE (Association of Certified Fraud Examiners)：2011年全球(樣本：1,800以上)舞弊查核報告。

   1.2 Kroll：2011年全球(樣本：800以上)舞弊查核報告。

   1.3 備考：預防(Prevent)、遏止(Deter)、偵測(Detect)與調查(Investigate)是其防護方法。

2. ACFE：資訊舞弊首次超過財物舞弊。

3. Kroll：

   3.1 85%之舞弊是由新手(無前科紀錄)，15%的舞弊是累犯。

   3.2 40%經由「檢舉」揭發舞弊。

   3.3 大部分舞弊之源池是「受害者」：參見神鬼交鋒(Catch me if you can)影片。

# 個人資料資訊安全管理缺失事件例

1. 資料來源：2010年12月10日，聯合報A6(生活)，記者薛翔之/台北報導。

2. 2010年4月間玉山銀行網路銀行客戶反映網銀紀錄他們「登入失敗」之時段，他們並未「登入」；偵測並通報警方與金管會後發現係「駭客」入侵，盜取了16,001筆包括姓名、身分證字號及出生年月日等存戶個人資料，另有數千筆個人資料「盜取未遂」。

3. 2010年12月9日，金管會處分玉山銀行罰鍰N.T.$ 4,000,000.，並要求玉山銀行「立即改善」。

# 玉山銀行之裁罰依據－銀行法之保守秘密義務

**1.　第45條之1第1項**

銀行應建立內部控制及稽核制度；其目的、原則、政策、作業程序、內部稽核人員應具備之資格條件、委託會計師辦理內部控制查核之範圍及其他應遵行事項之辦法，由主管機關定之。

**2.　第48條第2項**

銀行對於客戶之存款、放款或匯款等有關資料，除有下列情形之一者外，應保守秘密：

一、法律另有規定。

二、對同一客戶逾期債權已轉銷呆帳者，累轉銷呆帳金額超過新臺幣五千萬元，或貸放後半年內發生逾期累計轉銷呆帳金額達新臺幣三千萬元以上，其轉銷呆帳資料。

三、依第一百二十五條之二、第一百二十五條之三或第一百二十七條之一規定，經檢察官提起公訴之案件，與其有關之逾期放款或催收款資料。

四、其他經主管機關規定之情形。

**3.　第129條**

有下列情事之一者，處新臺幣二百萬元以上一千萬元以下罰鍰：

七、未依第四十五條之一或未依第一百二十三條準用第四十五條之一規定建立內部控制與稽核制度、內部處理制度與程序、內部作業制度與程序或未確實執行。

十一、違反第四十八條規定。

# 個人資料保護與資安社群議題例－根基於日本Sony PSN (Play Station Network)遭駭客入侵事故

1. 資料來源：

   1.1 2011年4月28日，聯合報A17(國際)，編譯范振光、莊蕙嘉/報導。

   1.2 2011年4月29日，蘋果日報A8(要聞)，編譯歐陽梅芬。

   1.3 2011年5月4日，自由時報A7(國際新聞)，編譯林翠儀/綜合報導。

2. 日本Sony公司於2011-04-20得知，其遊戲網路PSN在2011-04-17~2011-04-19期間被非法入侵約77,000,000.筆包括姓名、出生日期、地址與信用卡資料在內之個人資料被盜取。

3. 日本Sony公司於2011-04-26公布前述事故，並提醒客戶其PSN與Qriocity線上音樂服務之會員防範身分及信用卡帳戶被人盜用的威脅。

4. 日本Sony公司於2011-04-13宣布已與今(2011)年初向兩名破解Play Station遊戲主機中之一名美國駭客George Hotz達成和解。

# 個人資料保護與資安社群議題例－根基於日本Sony PSN (Play Station Network)遭駭客入侵事故 (續)

5. Anonymous資安社群支持WikiLeaks，於2010年12月曾對關閉WikiLeaks帳戶之Visa、MasterCard、Amazon等公司的網站發動攻擊。
6. 2011年4月，Anonymous資安社群曾警示將對檔案分享軟體LimeWire提告侵權之華納兄弟公司發動攻擊。
7. 日本Sony公司可能因前述事故損失逾U.S.$ 1,500,000,000.-。
8. 日本Sony公司於2011-05-03通報位於美國加州之Sony線上娛樂公司(Sony Online Entertainment，簡稱SOE)亦被駭客入侵，全球約24,600,000.名用戶個人資料可能外洩。
9. George Hotz先生於2010-12在德國柏林之27屆CCC (Chaos Communication Congress)後，在2011-01-02其個人網站公開揭露PS3之用於程式簽章的金鑰(Root Key)與2隻範例程式，闡明可行性，並對27屆CCC之fail Overflow的演講等致謝。
10. 2011-04-06因PSN停用影響公眾活動，Anonymous資安社群要求停戰。

# 個人資料保護與電子商務交易安全事件例

1. 資料來源：謝明俊等 (2011) ○○○為省錢3度被駭，時報周刊，No. 1735，2011-05-20/26，頁46~48。

2. 經濟部自2011年起之6年N.T.$ 100,000,000.-預算的試辦廠商之一的○○○網路書店，於2011年1月起，疑被中國大陸直接入侵其網站並竊又資料庫內之客戶網路交易資料與原碼(Source Code)，並於同年3月再度入侵。

3. 2011年3月，165反詐騙案件量增異常，其中46名被害人均為前述網路書店；2011年4月最後2個星期，前述網路書店之客戶，高達77人遭到詐騙。

# 個人資料保護與電子商務交易安全事件例 (續)

4. 網路購物詐騙流程

4.1 民眾在商務網站購物交易。

4.2 駭客攻擊入侵商務網站，盜走客戶交易資料。

4.3 客戶交易資料轉賣給詐騙集團。

4.4 詐騙集團佯裝客服人員，騙稱因作業疏失，使先前交易勾選成分期付款。

4.5 詐騙集團再套取被害人金融卡、信用卡背面客服電話。

4.6 詐騙集團假冒金融機構客服人員，去電被害人要求至ATM進行消取分期付款作業。

4.7 被害人不查，遵從指示至ATM操作，誤將帳戶存款轉帳至詐騙集團人頭帳戶中。

4.8 詐騙集團車手迅速在30分鐘內，將轉帳款項提領一空。

# 個人資料保護管理與推論控制

1. 資料來源：

   1.1 2011年9月23日，聯合報，A15(社會)，記者王文玲/台北報導。

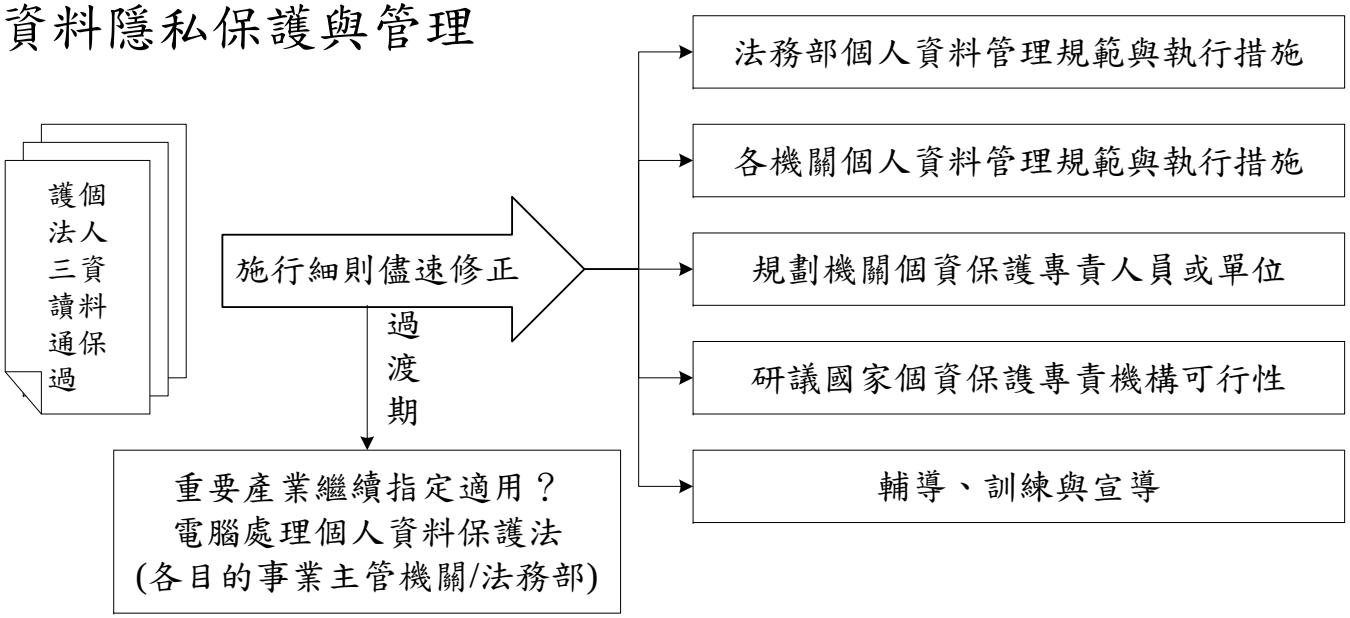
   1.2 2011年10月12日，聯合報，A10(話題)，記者王文玲、蕭白雪/台北報導。

2. 高等法院政風人員因注意到陳貽男庭長1個月查詢9件當事人之稅務、車籍、工商、勞保、電話通聯與戶役政資料，高於其他法官甚多，再調出兩年內紀錄比對，發現陳庭長違規查詢院方資料多達80幾筆，亦經由檢察官辦案系統查詢檢方資料近50筆，惟部分重複查詢，依「電腦處理個人資料保護法」目前無法可罰。

3. 陳庭長接受內部調查時，坦承違規，但說明因其妻子於2007年因故去世後，有人幫他介紹女友，或他想追求一些女同事，方「瀏覽」這些人的資料；查詢簽約對象，則是想確認對方有無不良紀錄。高院建議記過2次，司法院認定違失情節嚴重，決定加碼改記大過1次並免兼庭長。

# 法務部當前政策

1. 健全個人資料隱私保護與管理




1.1 建置完善之個人資料保護法制，協助公務及非公務機關採取適當之保護措施，同時協助各機關制定相關規範及制度，以因應個人資料保護之要求。

1.2 完善的法制尚需要配套之教育訓練與宣導，使觀念普及化，故將於方案當中逐年進行訓練與宣導推動。

2. 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。

# 研修(個資法)施行細則之方式

1. 第一階段：各目的事業主管機關彙整問題、研提修正意見及開會討論。

   1.1 各目的事業機關分別邀集業界開會研商。

   1.2 法務部邀集各目的事業機關召開研修會議。

2. 第二階段：學者專家研修小組會議

   2.1 學者專家之專業意見。

   2.2 主要目的事業機關之政策執行意見。

3. 第三階段：草案預告及公聽會

# 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 | | | | | | | | * |

說明：

1. 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 日與本研究。
2. 第 2 階段會議於 2011-02-15 召開第 1 次會議，2011-08-25 召開第 17 次會議後，會議結束。
3. 施行細則預告公聽期間：2011-10-27~2011-11-09。

# 公務機關辦理個人資料保護作業舉隅

1. 2010年12月31日：各機關完成「個人資料保護及管理規範」以及「個人資料保護專責人員及聯絡窗口」(2009年7月22日：法務部法律字第0980700516號函)。

2. 2011年7月31日：各機關完成「機關保有個人資料檔案清查作業」以及「特定目的與個人資料類別修正作業」(2011-05-13：法務部法律字第1000700352號函)。

3. 2011年11月18日：各機關於2011-12-19~2011-12-23完成諸如在電腦網站揭載供公眾查閱的「保有及管理個人資料項目之彙整表」的適當方式之行動措施(2011-11-18：法務部法律字第10007020280號函)。

# (機關、學校名稱)保有及管理個人資料之項目彙整表

| 項目<br>編號 | 個人資料檔案名稱 | 保有依據 | 個人資料類別 | 保有單位 |
|---|---|---|---|---|
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |

| | | |
|---|---|---|
| 聯絡方式 | 地址：新竹市◯◯路◯◯號 | |
| | ◯◯單位、◯◯單位、… | 電話：03-◯◯◯◯ |
| 保有及管理個人資料之特定目的 | | |

# 執行個人資料保護事項之「100年度執行計畫與具體行動措施」之執行情形

| 具體行動措施 | 辦理機關 | 完成期限 | 辦理情形 |
|---|---|---|---|
| (一)公開義務：<br>以適當方式公開（個人資料檔案名稱、保有機關名稱及聯絡方式、個人資料檔案保有之依據及特定目的、個人資料之類別），供公眾查閱（個人資料保護法第 17 條） | 各機關 | 100 年 12 月 19 日至 12 月 23 日 | 公開方式：以公開於電腦網站為原則，或以其他適當方式供公眾查閱（仍須符合常時揭載之精神）。 |
| (二)修正個人資料之特定目的與個人資料類別（個人資料保護法第 53 條） | 各中央目的事業主管機關 | 101 年 6 月 30 日（暫定） | 目前各機關仍陸續提報修正意見，請各機關依附件內容再予檢視。 |

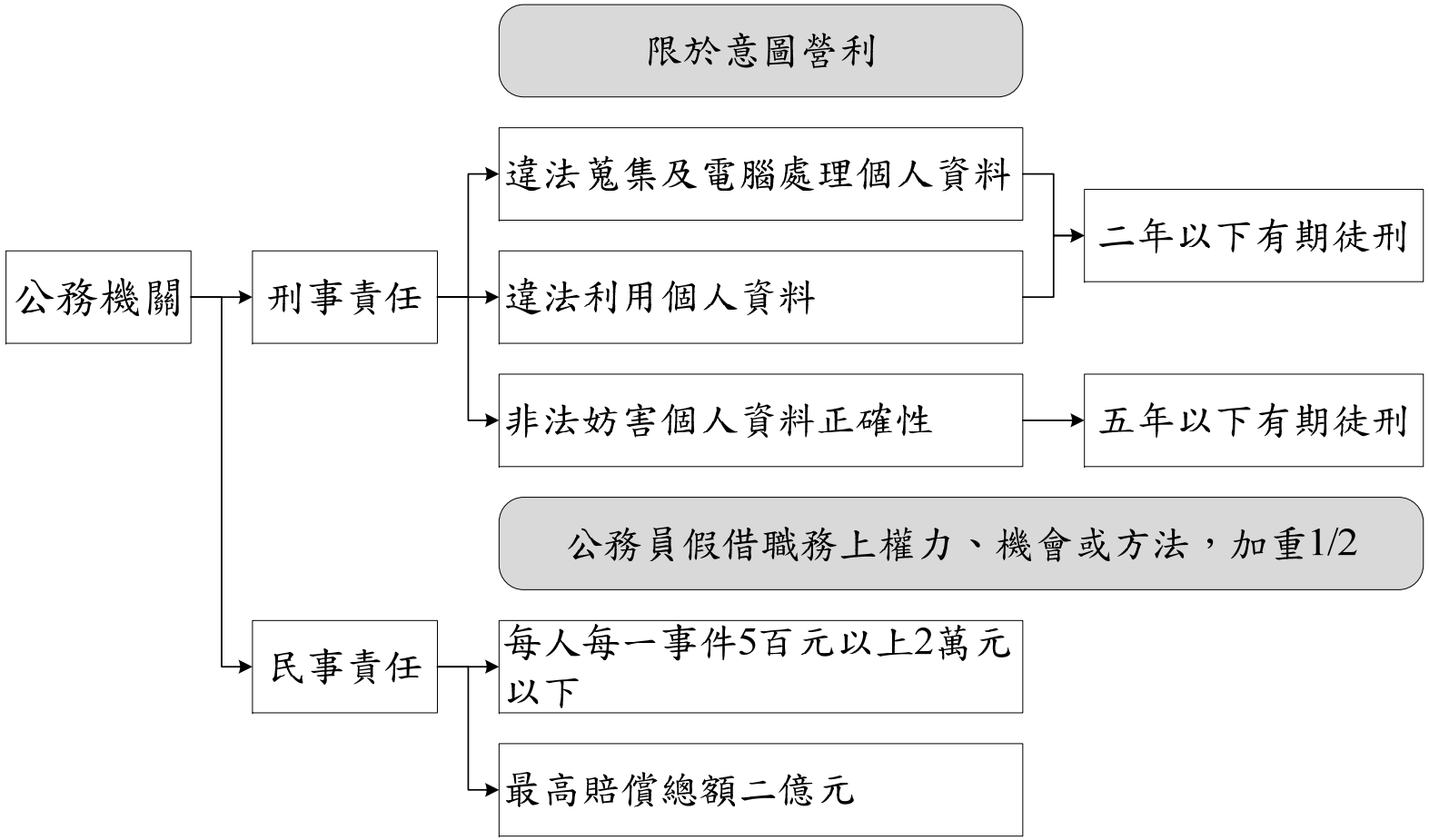
# 執行個人資料保護事項之「100年度執行計畫與具體行動措施」之執行情形 (續)

| 具體行動措施 | 辦理機關 | 完成期限 | 辦理情形 |
|---|---|---|---|
| (三)研訂或修正個資法相關授權法規命令<br>1、個人資料保護法第6條第2項之法規命令<br>2、個人資料保護法第27條第3項之法規命令 | 各相關中央目的事業主管機關 | 101年6月30日（暫定） | 本部已於100年10月就該2個法規命令（範本）草案召開座談會。 |
| 資料來源：法務部 (2011) 法律字第1000702028號函附件1，2011-11-18。 | | | |

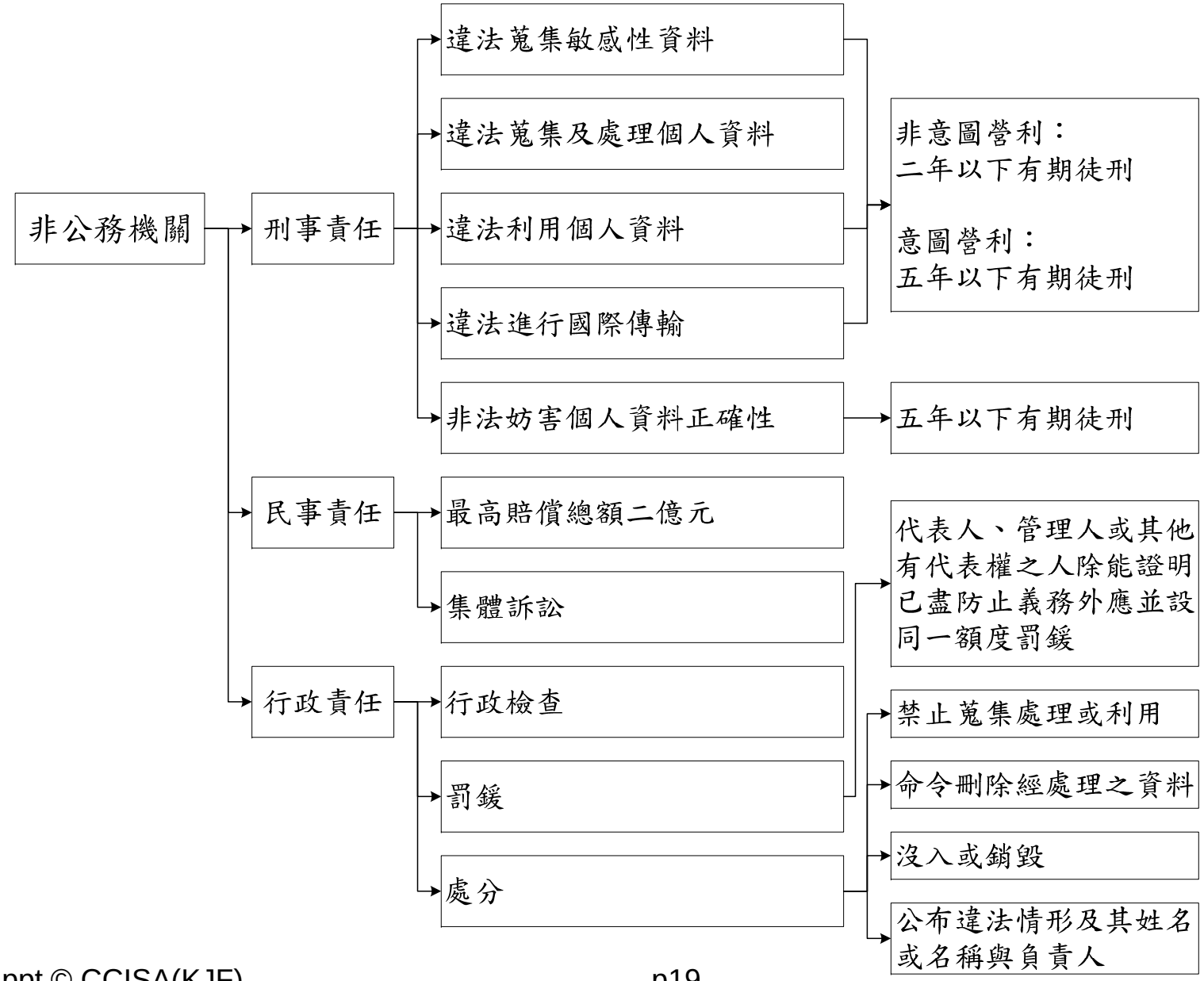
# 隱私權集體訴訟案例

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)。

# 違反個人資料保護法應負之相關法律責任－公務機關



# 違反個人資料保護法應負之相關法律責任－非公務機關



# 個人資料保護法與資訊安全管理

1. 公務機關：

   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。

2. 非公務機關：

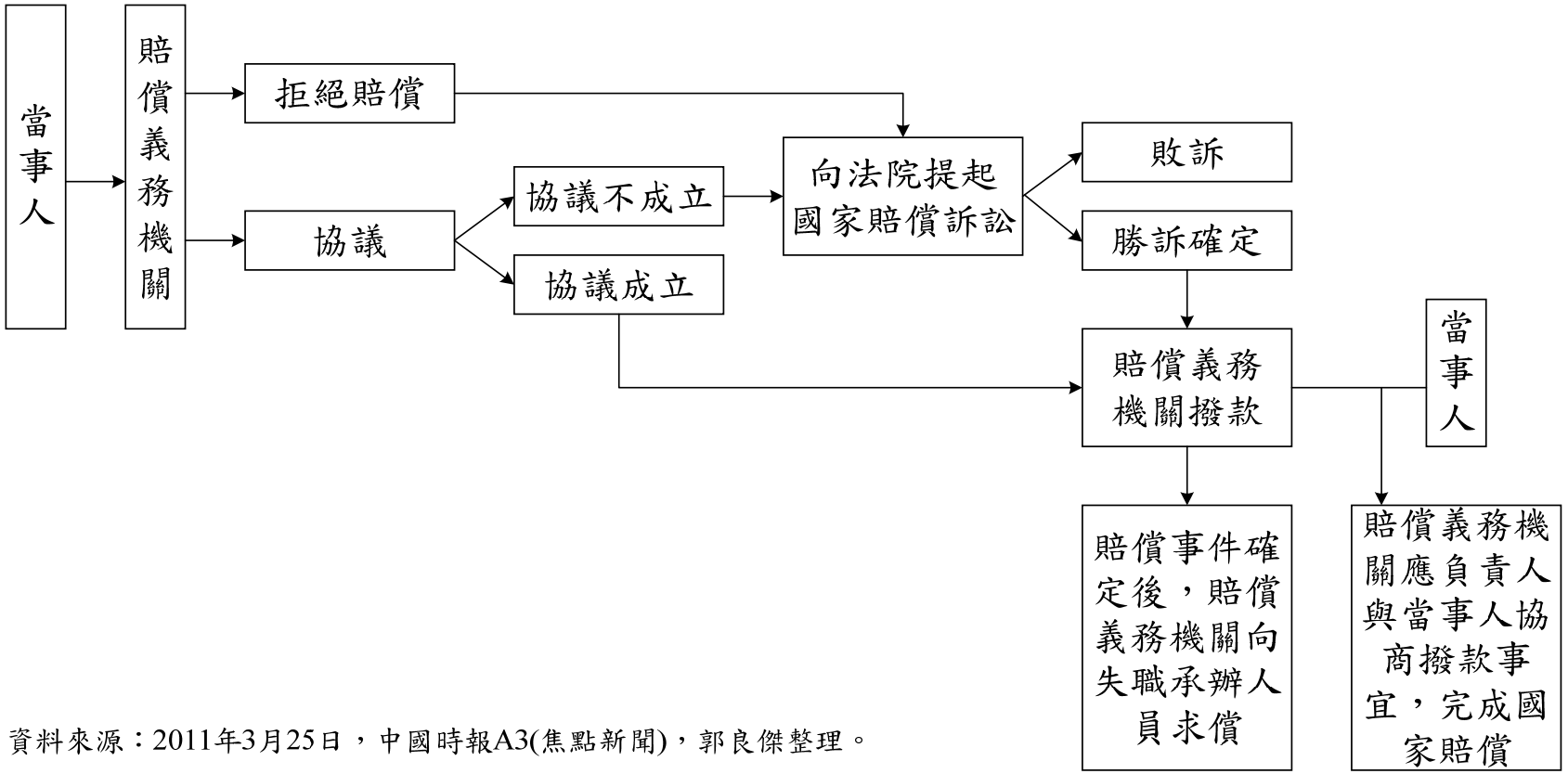
   第二十七條：

   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。

# 請求國家賠償流程圖




資料來源：2011年3月25日，中國時報A3(焦點新聞)，郭良傑整理。

# 公示送達與意思表示之解釋
# (民法第97條及第98條：2008-05-23)

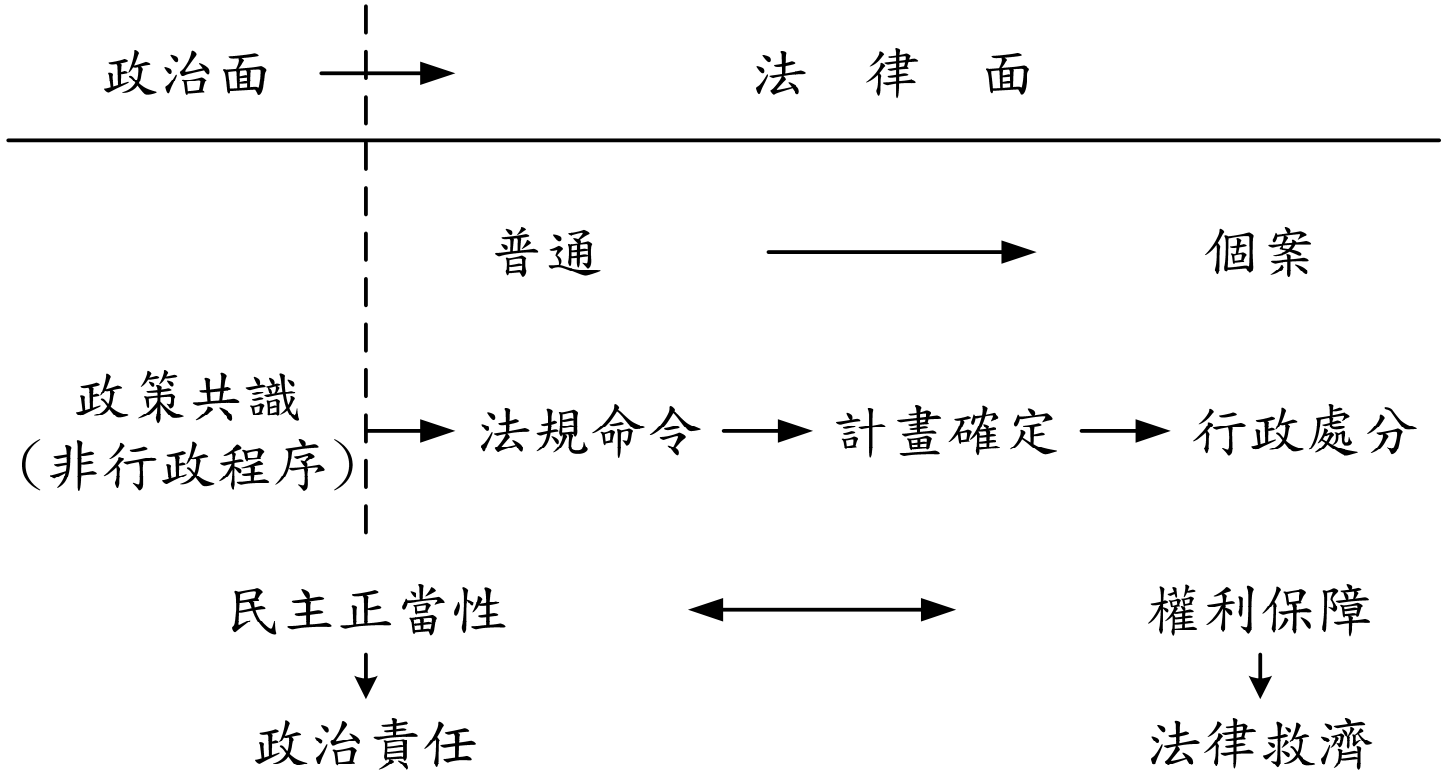
**第97條 (公示送達)**

表意人非因自己之過失，不知相對人之姓名、居所者，得依民事訴訟法公 示送達之規定，以公示送達為意思表示之通知。

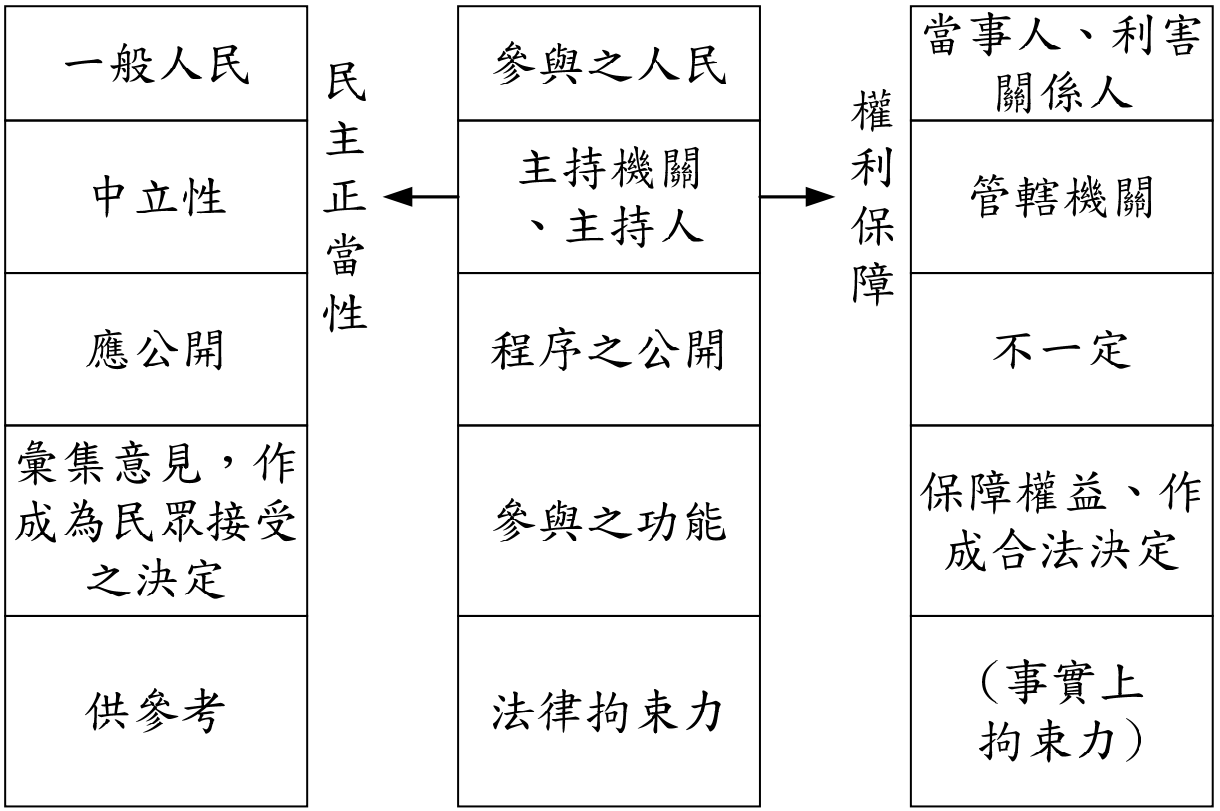
**第98條 (意思表示之解釋)**

解釋意思表示，應探求當事人之真意，不得拘泥於所用之辭句。

# 資訊安全管理立法與行政程序之一



# 資訊安全管理立法與行政程序之二



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

1. 資料來源：

   1.1 2010年8月29日，聯合報A8(社會)，記者曹敏吉/高雄報導。

   1.2 2010年11月27日，聯合報A17(社會)，記者王文玲、藍凱誠、陳俍任/連線報導。

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.，法官認為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.(侵害肖像權與名譽權)與其妻子N.T.$ 400,000.(侵害肖像權)，合計N.T.$ 1,400,000.；最高法院於2010-11-26判決蘋果日報敗訴定讞，除賠償N.T.$ 1,400,000.，還必須將報導之文字、圖片及照片，從「壹蘋果網路」上刪除。

# 個人資料保護法相關議題

1. 「指紋」宜屬「特種資料」？

2. 公立學校、醫院與其他中央及地方各級機關設立之實(試)驗、研究、文教機構等應適用公務機關或非公務機關的規範？

3. 「特種資料」得否為目的外之利用？

4. 公務機關對於個人資料之利用，如發生與「資訊公開法」間的競合時之適用性？

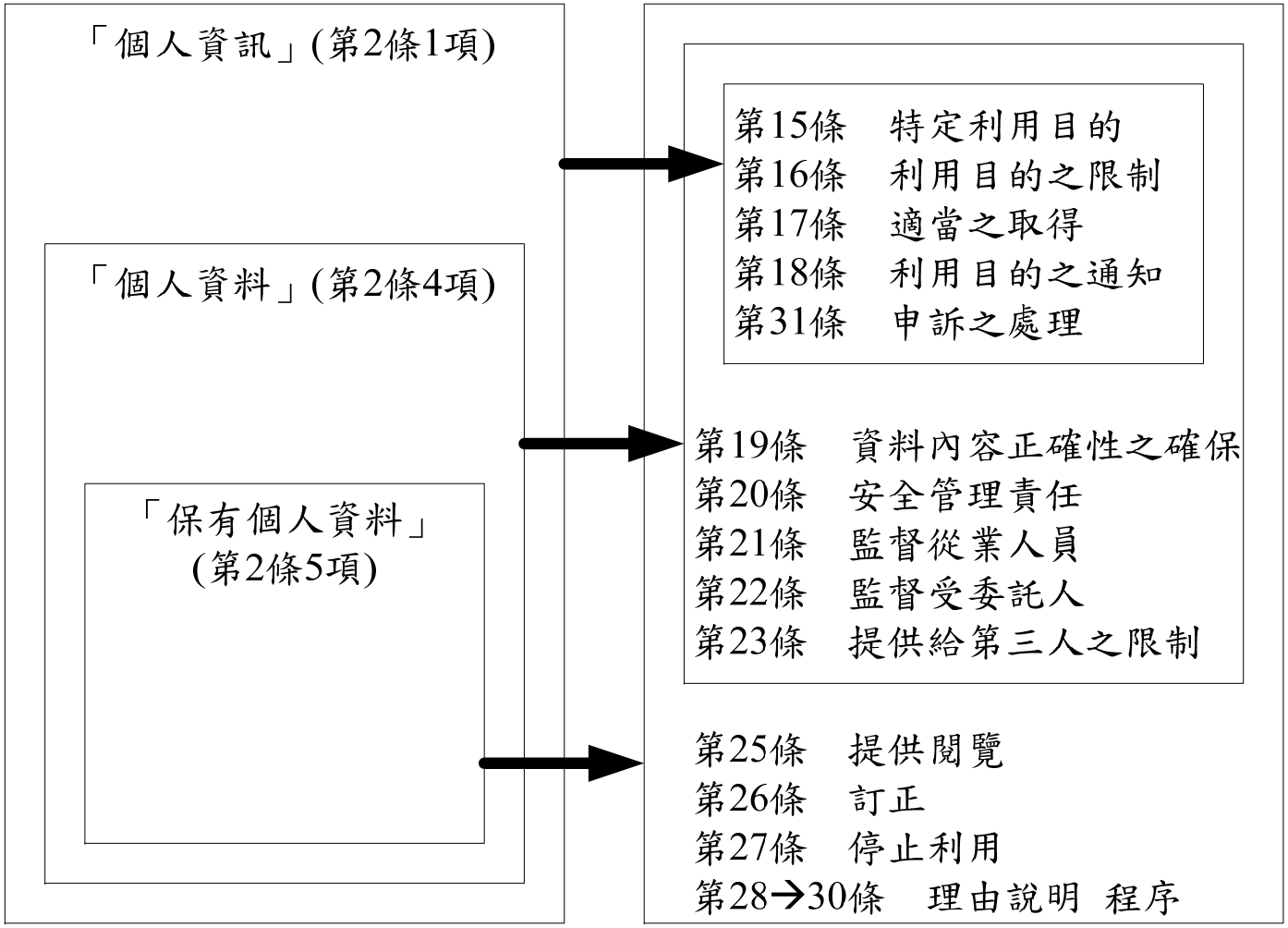
5. 「適當方式」通知當事人之執行？

6. 參考資料：


6.1 鄭菀瓊 (2011) 個人資料外洩通知與規範類型之探討，科技法律透析，頁50~61，2011-01。

6.2 林秀蓮 (2011) 個人資料保護法初探，萬國法律，第176期，頁2~13，2011-04。

# 日本個人資料保護法之層疊式義務簡表




資料來源：范姜真媺，日本個人資訊保護法對民間業者處理個人資料之規範，科技法律透析，2011-01，頁27~49。

# 不同類型資料外洩告知責任立法比較表

| | 類型一 | 類型二 | 類型三 |
|---|---|---|---|
| 代表立法 | 加州資料外洩通知責任法 | 美國跨金融部門未經授權近用消費者資訊告知責任綱領 | 研議中，代表人士為：<br>1. 芝加哥聯邦準對銀行主席 Michael H. Moskow<br>2. 重要隱私權學者 Paul M. Schwartz 教授 |
| 告知責任發生時點 | 顯名制之資料外洩通知責任<br>1. 資料外洩事實發生即成立通知責任 | 雙軌制之資料外洩告知責任<br>1. 資料外洩事件必須第一時間通報所屬主管機關 | 匿名制之資料外洩告知責任<br>1. 資料外洩事件集中通報第三方機構 |
| 通知責任發生時點 | 1. 不論外洩資料有無後續遭濫用風險皆須通報<br>2. 由資料外洩組織直接通知受害當事人 | 1. 僅外洩資料可能遭到濫用才需(以顯名方式)通知受害當事人 | 1. 若該外洩資料有遭濫用風險，再由該第三方機構以不顯示外洩組織身分之方式通報受害當事人 |
| 制度優勢 | 1. 以聲譽壓力促使消費者反映資安偏好 | 1. 避免資訊過載問題<br>2. 仍可適度課以組織資安聲譽壓力 | 1. 避免資訊過載問題<br>2. 降低資料外洩組織避免通知受害當事人之利益衝突問題 |
| 制度劣勢 | 資訊過載問題 | 外洩組織判斷資料是否有遭濫用風險時，存在利益衝突問題 | 無法發揮聲譽壓力 |
| 資料來源：鄭菀瓊(2011) 個人資料外洩通知與規範架構類型之探討，科技法律透析，2011-01，頁 50~61。 | | | |

# 個人資料保護相關保密法規條文

1. 職務秘密：
   - 1.1 公務員服務法第4條。
   - 1.2 刑事訴訟法第254條。
   - 1.3 稅捐稽徵法第33條。
   - 1.4 公害糾紛處理法規施行細則第17條。
   - 1.5 統計法施行細則第45條。
   - 1.6 勞動檢查法第11條。
   - 1.7 勞資爭議處理法第23條。
2. 人事秘密：
   - 2.1 典試法第28條。
   - 2.2 公務人員陞遷法第16條。
   - 2.3 公務人員考績法第20條。
   - 2.4 考績委員組織規程第7條。

# 個人資料保護相關保密法規條文(續)

3. 業務秘密：

3.1 中華民國刑法第316條。
3.2 醫師法第25條。
3.3 藥師法第141條。
3.4 護理人員法第28條。
3.5 助產人員法第31條。
3.6 醫療法第72條。
3.7 律師法第50-1條。
3.8 公設辯護人管理規則第11條。
3.9 銀行法第48條第2項。

# 行政罰法第15條
# (私法人之代表權人責任：2005-02-05)

1. 私法人之董事或其他有代表權之人，因執行其職務或為私法人之利益為行 為，致使私法人違反行政法上義務應受處罰者，該行為人如有故意或重大 過失時，除法律或自治條例另有規定外，應並受同一規定罰鍰之處罰。

2. 私法人之職員、受僱人或從業人員，因執行其職務或為私法人之利益為行 為，致使私法人違反行政法上義務應受處罰者，私法人之董事或其他有代 表權之人，如對該行政法上義務之違反，因故意或重大過失，未盡其防止 義務時，除法律或自治條例另有規定外，應並受同一規定罰鍰之處罰。

3. 依前二項並受同一規定處罰之罰鍰，不得逾新臺幣一百萬元。但其所得之 利益逾新臺幣一百萬元者，得於其所得利益之範圍內裁處之。

# OECD (Oranization for Economic Co-operation and Development)隱私權保護指導綱要(Guidelines)八大原則(Principles)：1980-09-23

1. 蒐集限制(Collection Limitation)
   個人資料的搜集必須經過當事人同意，基於合法且公平合理的目的。
2. 資料品質(Data Quality)
   個人資料必須與蒐集目的攸關，且須維持個資的正確性、完整性與即時性。
3. 目的明確(Purpose Specification)
   個人資料蒐集的目的必須清楚說明。
4. 使用限制(Use Limitation)
   除非經過法律授權或是當事人同意，否則個人資料的揭露與使用僅限於當初蒐集的目的。

# OECD (Oranization for Economic Co-operation and Development)隱私權保護指導綱要(Guidelines) 八大原則(Principles)：1980-09-23 (續)

5. 安全保護(Security Safeguards)
   個人資料必須受到合理的安全保護。
6. 公開(Openness)
   個人資料管理相關的政策以及個資問題的聯絡方式必須公開。
7. 個人參與(Individual Participation)
   個人資料當事人可以對所蒐集的資料進行確認，也必須被告知個人資料持有的合理時間與方式，當與當事人無法聯繫時，必須提供一各合理的理由，當個人資料蒐集目的完結後，資料應該被消除。
8. 可歸責性(Accountability)
   個人資料蒐集者必須設定可衡量的機制以確定有效地落實上述各項準則。

# 2005年11月亞太經濟合作組織(Asia-Pacific Economic Cooperation，簡稱APEC)公布之APEC隱私保護框架(Privacy Framework)的原則(Principles)

1. 預防損害(Preventing Harm)：目的在於防止個人資料遭到濫用以及因此所生之損害。
2. 告知(Notice)：確保當事人能夠知悉其個人資料已遭蒐集及其被利用之目的。
3. 蒐集限制(Collection Limitation)：將個人資料之蒐集限於與蒐集目的相關者。
4. 個人資料之利用(Use of Personal Information)：規定個人資料之利用限於與蒐集目的一致或相關的範圍內。
5. 當事人自主(Choice)：確保當事人有機會就其個人資料之蒐集、利用、傳遞與揭露進行選擇，惟當個人資料管理者所蒐集者為其公開可獲得資料時，本原則之規定不適用。
6. 個人資料完整性(Integrity of Personal Information)：個人資料應正確、完整並依利用目的為必要之更新。
7. 安全管理(Security Safeguards)：本原則旨在說明當事人對於其個人資料將受到安全之保護一事應能有合理的期待。
8. 查閱與矯正(Access and Correction)：就隱私之保護而言，查閱與矯正個人資料並不是一個絕對的權利。本原則詳細規範個人查閱與矯正個人資料之合理的權利與條件，以及個人資料管理者應盡之責任及義務。
9. 可歸責性(Accountability)：個人資料管理者應確保前述各原則之實踐及於其傳遞資料的第3方。

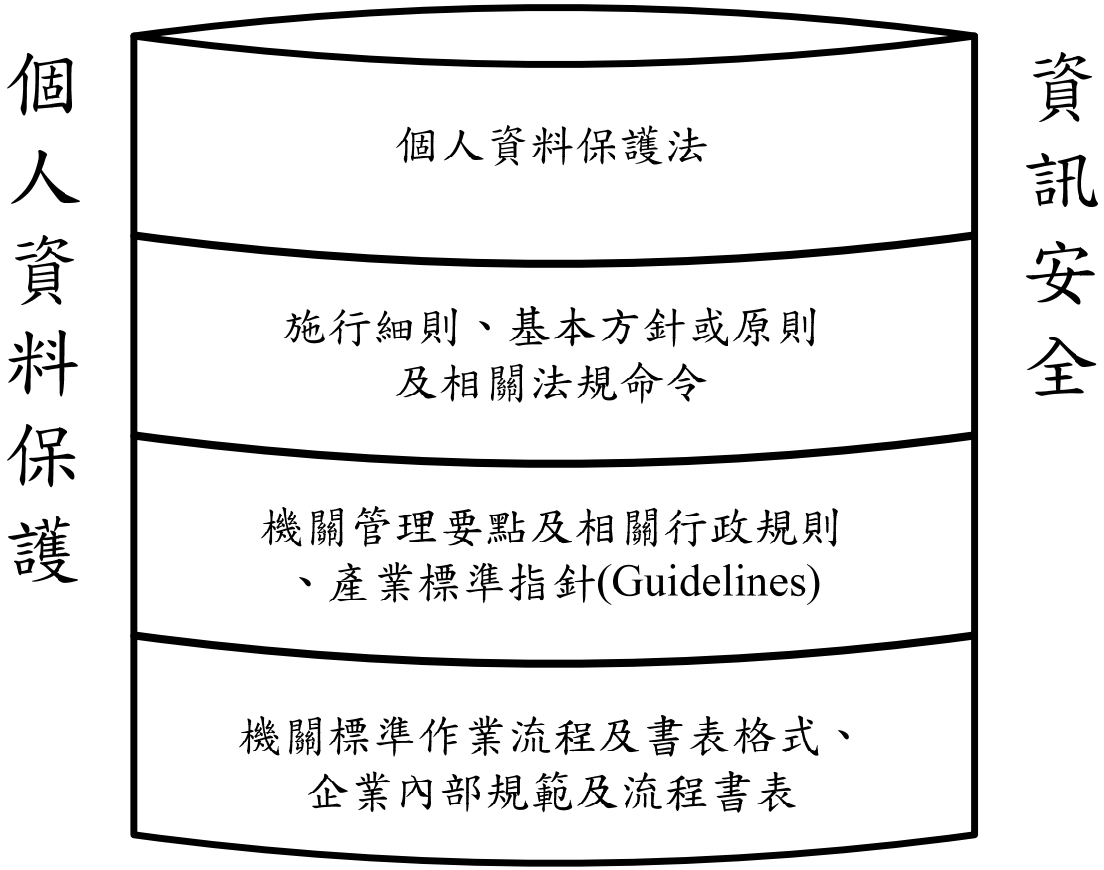
# 個人資料保護法施行細則修正草案之適當安全維護事項(2011-10-27~2011-11-09預告公聽版)

第九條：本法所稱適當安全維護措施或安全維護事項或適當之安全措施，係指公務機關或非公務機關為防止個人資料被竊取、竄改、毀損、滅失或洩漏，以善良管理人之注意義務，採取技術上與組織上之必要措施。

前項必要措施，應包括下列事項：
一、成立管理組織，配置相當資源。
二、界定保有個人資料之範圍。
三、個人資料之風險評估及管理機制。
四、事故之預防、通報及應變機制。
五、個人資料蒐集、處理及利用之內部管理程序。
六、資料安全管理及人員管理。
七、認知宣導及教育訓練。
八、設備安全管理。
九、資料安全稽核機制。
十、必要之使用紀錄、軌跡資料及證據之保存。
十一、個人資料安全維護之整體持續改善。

第一項必要措施，以所須支出之費用與所欲達成之個人資料保護目的符合適當比例者為限。

# 法務部之建置個資保護制度的體系

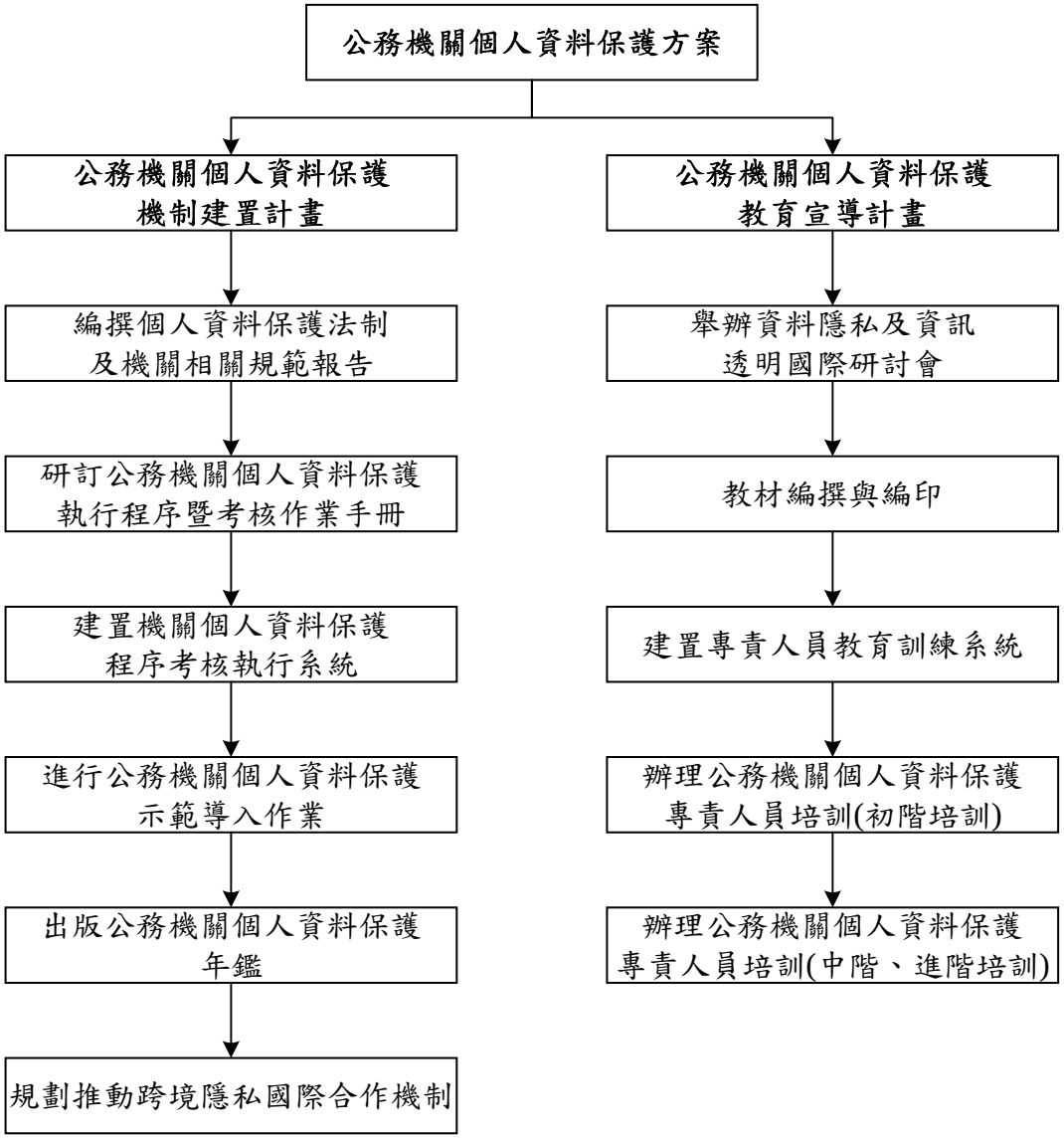



資料來源：法務部法律事務司 (2010) 個人資料保護之政策與作法，2010-11。

# 法務部執行「公務機關個人資料保護方案」之行政院國科會科技發展基金補助計畫

1. 經費：1360萬5千元整。
2. 執行期程：1年6個月。
3. 內容：「建置公務機關個人資料保護機制」並「落實公務機關個人資料保護教育宣導」為兩大主軸，打造完善之公部門個人資料保護環境，並利國內(非公務機關)及國際執行合作。

# 法務部之「公務機關個人資料保護方案」整體架構



# ISO資訊安全管理模型與WSIS

1. 2003瑞士日內瓦召開之資訊社會世界高峰會(World Summit on the Information Society，簡稱WSIS )：提出原則性聲明(Declaration for Principles)與行動計畫(Plan of Action)中，要求ISO制定相關資訊安全標準。

2. WSIS與資訊安全管理模型相關之原則性聲明與行動計畫的主要項目:

   a) 「建立通資訊技術的信賴與安全」。

   b) 「建立各層面足以發展的環境」。

3. 2004年10月24日，ISO主責資訊安全之ISO/IEC JTC1/SC27(簡稱SC27)主席公布SC27的資訊安全管理模型觀點，並宣布因應WSIS之要求，SC27將進行組織再造。

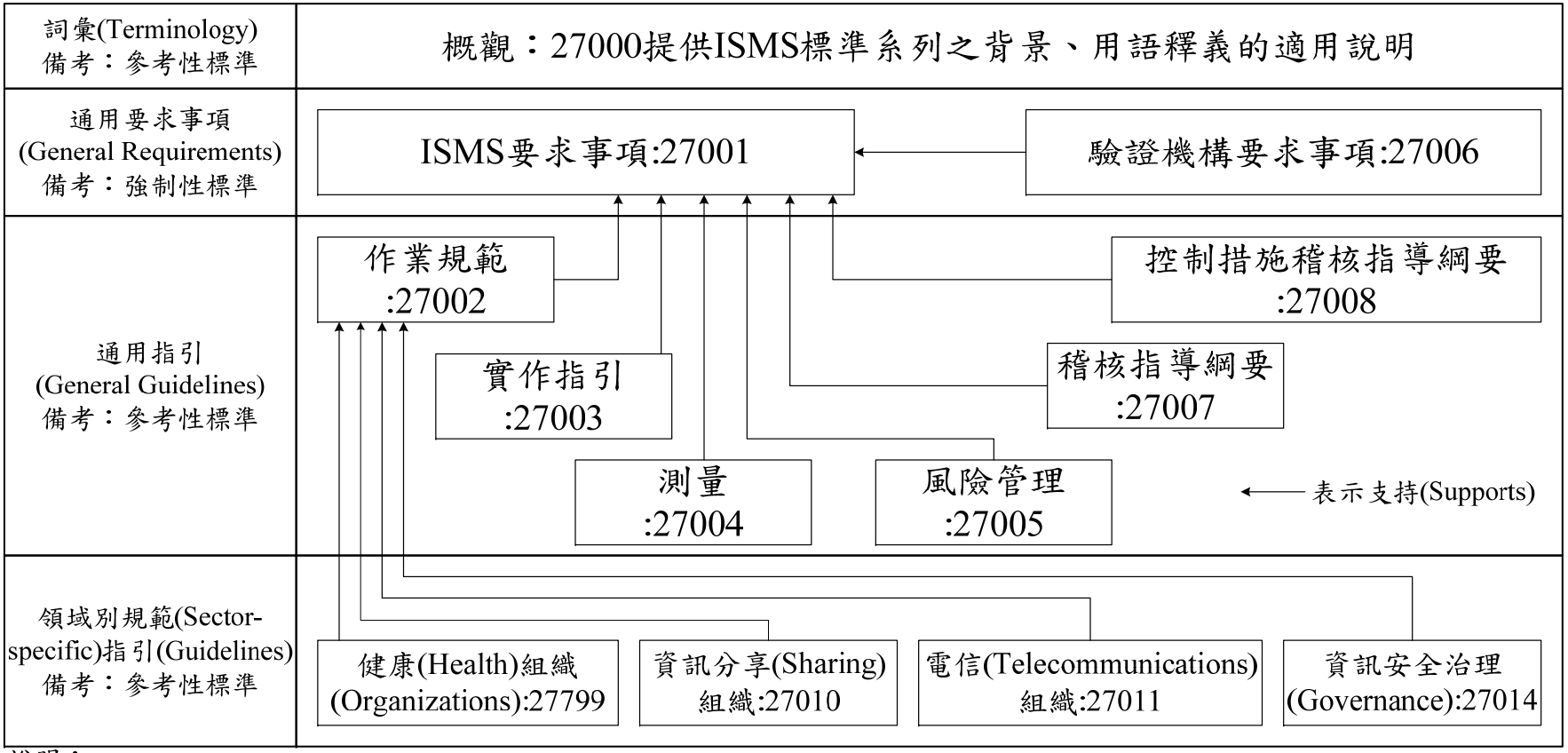
4. 2005年5月，SC27將原有之3個工作組調整成5個。

5. 2005年10月15日出版之「資訊安全管理系統需求(ISO/IEC 27001:2005(E))」成為ISO/IEC 27000系列標準之第1份標準。

# ISO/IEC JTC1/SC27資訊安全管理模型觀點之CNS標準對照

| 分類 | 標準與原則 | 對照之CNS標準 |
|---|---|---|
| 名詞暨使用指導綱要 | 1. 風險管理詞彙暨標準使用指導綱要：ISO/IEC Guide 73:2010(E/F)。<br>2. 資訊安全管理系統之概觀與詞彙：ISO/IEC 27000:2009(E)。 | 1. CNS 14889 (ISO/IEC Guide 73:2002 (E/F))於2005年2月10日出版。<br>2. 2010年1月已完成草案。 |
| 一般性指引 | 1. 資訊安全管理原則。<br>2. OECD(請參見備考)。 | 備考：宜遵循OECD於2002年7月25日公布之「資訊系統安全指導綱要」的「資訊系統與網路安全指導綱要--朝向安全之文化」。 |
| 原則與框架 | 1. 資訊安全管理框架：ISO/IEC 13335-1:2004(E)。<br>2. 資訊安全管理系統要求事項：ISO/IEC 27001:2005(E)。 | 1. CNS 14929-1於2008年12月26日修訂公布。<br>2. CNS 27001於2006年6月16日出版，2007年12月24日修訂公布。 |
| 標準元件 | 1. 資訊安全管理系統要求事項：ISO/IEC 27001:2005(E)。<br>2. 資訊安全管理之作業規範：ISO/IEC 27002:2005(E)。<br>3. 資訊安全管理系統實作指引：ISO/IEC 27003:2010(E)。<br>4. 資訊安全管理量度(Metrics)與測量：ISO/IEC 27004:2009(E)。<br>5. 資訊安全風險管理：ISO/IEC 27005:2011(E)。<br>6. 稽核與驗證機構要求ISO/IEC 27006:2007(E)。<br>7. 資訊安全管理系統稽核指導綱要：ISO/IEC 27007。<br>8. 資訊安全管理系統控制措施稽核指引：ISO/IEC TR 27008 :2011(E)。 | 1. CNS 27001於2006年6月16日出版，2007年12月24日修訂公布。<br>2. CNS 27002於2007年10月24日出版。<br>3. 2011年7月已完成草案研擬。<br>4. 2011年5月已完成草案。<br>5. CNS 27005於2010年2月出版(2008(E))，第2版(2011(E))尚在蒐集資料中。<br>6. CNS 27006於2010年2月出版。<br>7. 尚在蒐集相關資料中。<br>8. 尚在蒐集相關資料中。<br>9. 備考：ISO/IEC 17799:2005(E)於2007年7月1日改號成為ISO/IEC 27002:2005(E)。 |
| 應用指引與增補 | 1. 醫療：ISO 27799:2008(E)。<br>2. 資訊分享：ISO/IEC 27010。<br>3. 電信：ISO/IEC 27011: 2009(E)。<br>4. 電子化政府：ISO/IEC 27012。<br>5. 資訊技術服務：ISO/IEC 27013。<br>6. 資訊安全治理：ISO/IEC 27014。<br>7. 金融與保險服務：ISO/IEC 27015。 | 1. 尚在蒐集資料中。<br>2. 尚在蒐集資料中。<br>3. 尚在蒐集資料中。<br>4. 尚在蒐集資料中。<br>5. 尚在蒐集資料中。<br>6. 尚在蒐集資料中。<br>7. 於財務方面於2002年5月16日參照ISO TR 13569:1997(E)公布CNS 14644。 |
| 技術工具盒 | 1. 資訊安全事故管理：ISO/IEC TR 18044:2004(E)。<br>2. IT入侵偵測框架：ISO/IEC TR 15947:2002(E)。<br>3. 網路安全：ISO/IEC 27033。<br>4. 可信賴第三方服務指導綱要：ISO/IEC TR 14516:2002(E)。<br>5. 入侵偵測系統之選取、布署與實作、運作與管理：ISO/IEC 27039。<br>6. 營運持續之資訊與通信技術整備指導綱要：ISO/IEC 27031:2011(E)。 | 1. CNS 15215於2008年12月26日出版 。<br>2. CNS 14992於2006年6月1日出版。<br>3. 尚在蒐集資料中。<br>4. 尚在蒐集資料中。<br>5. 尚在蒐集資料中。<br>6. 尚在蒐集資料中。<br>7. 備考：ISO/IEC JTC 1/SC 27/WG 4尚在進行ISO/IEC 27034等標準系列制定工作中。 |
| 資料來源：ISO/IEC JTC1/SC27 (IT Security Techniques) Chairman, Mr. Walter Fumy, 2004-10-04，暨本研究自行整理。 | | |

# 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



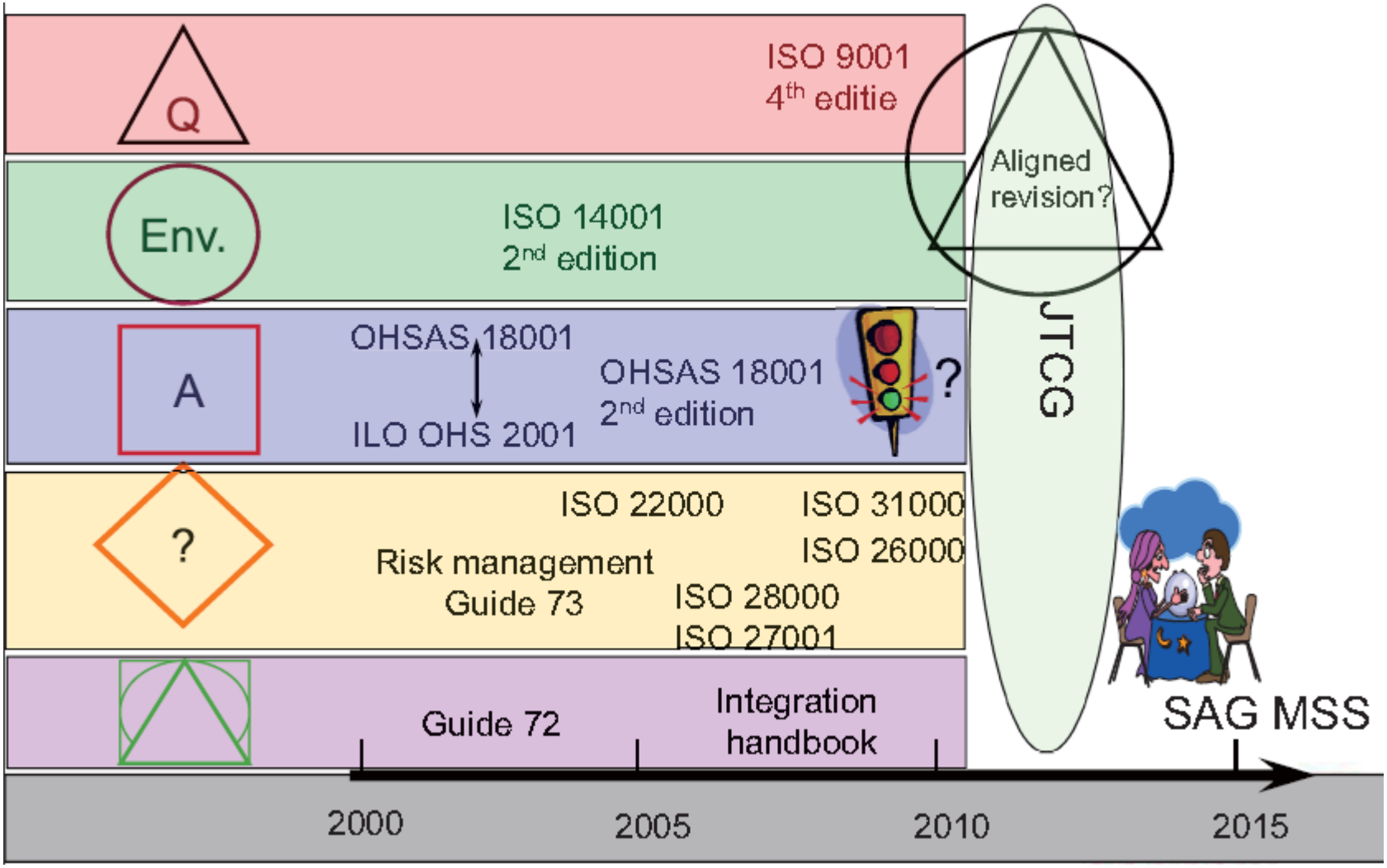

說明：

1.資料來源：ISO/IEC 27000:2009-05-01，頁12，圖1；與本研究。

2.備考：ISO/IEC 27005已參照ISO 31000等修正，預定於2012年6月1日頒布新版。

3.參考資料：Working document for revision of ISO/IEC 27000, ISO/IEC JTC1/SC27 N8718, Page 21, Figure 1, 2010-05-27.

# 管理系統之校準(Alignment)－未來：2010~?




資料來源：Waumans, R. (2010) JTCG Introduction, Buenos Aires, May 2010。

# ISO/IEC 27001:2005(E)第A.15.1.4條款

| | | |
|---|---|---|
| A.15.1.4 | 個人資訊的資料保護與隱私 | 控制措施<br><br>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。 |

# 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

控制措施

宜如同相關法律、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。

為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、處理及傳輸行為採取控制措施。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。

# ISO/IEC 27002:2005(E)之第10.8節：資訊交換

10.8 資訊交換

目標：維護組織內及與任何外部個體所交換資訊與軟體的安全。

組織間資訊和軟體的交換宜基於正式的交換政策，依交換協議進行，且宜遵循所有相關法律(參照第15節)。

宜建立程序與標準以保護資訊與包含輸送中資訊的實體媒體。

# 資訊交換防護(Information Exchange Protection)
## 控制措施舉隅

1. 目的：確保分享資訊之社群間資訊交換作業存在適當的防護。

2. 控制措施：

   2.1 分享資訊之分級標示。

   2.2 敏感性資訊之過濾。

   2.3 設置拒絕分享資訊之申訴窗口(Information Disclaimer)。

3. 參考資料：ISO/IEC FCD 27010 Information technology – Security techniques – Information security management for inter-sector and inter-organizational communications, 2011-05-05。

# IS-ISMS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<br>[3,9,0,0,1]</td><td>9. 實體與環境安全<br>[3,13,13,6,3]</td><td>10. 通信與作業管理<br>[10,32,24,3,11]</td><td rowspan="2">12. 資訊系統獲取、開發及維護<br>[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：<br>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 ]<br>2. 控制目標於 ISO/IEC FCD 27010:2011-05-05 中均擴增之。<br>3. 資料來源：ISO/IEC FCD 27010:2011-05-05、ISO/IEC 27011:2008-12-15 與 ISO 27799:2008-07-01。</td></tr>
</table>

# IS-ISMS涉及個人資料之資訊分享之資訊安全管理系統的敘述為應(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 |

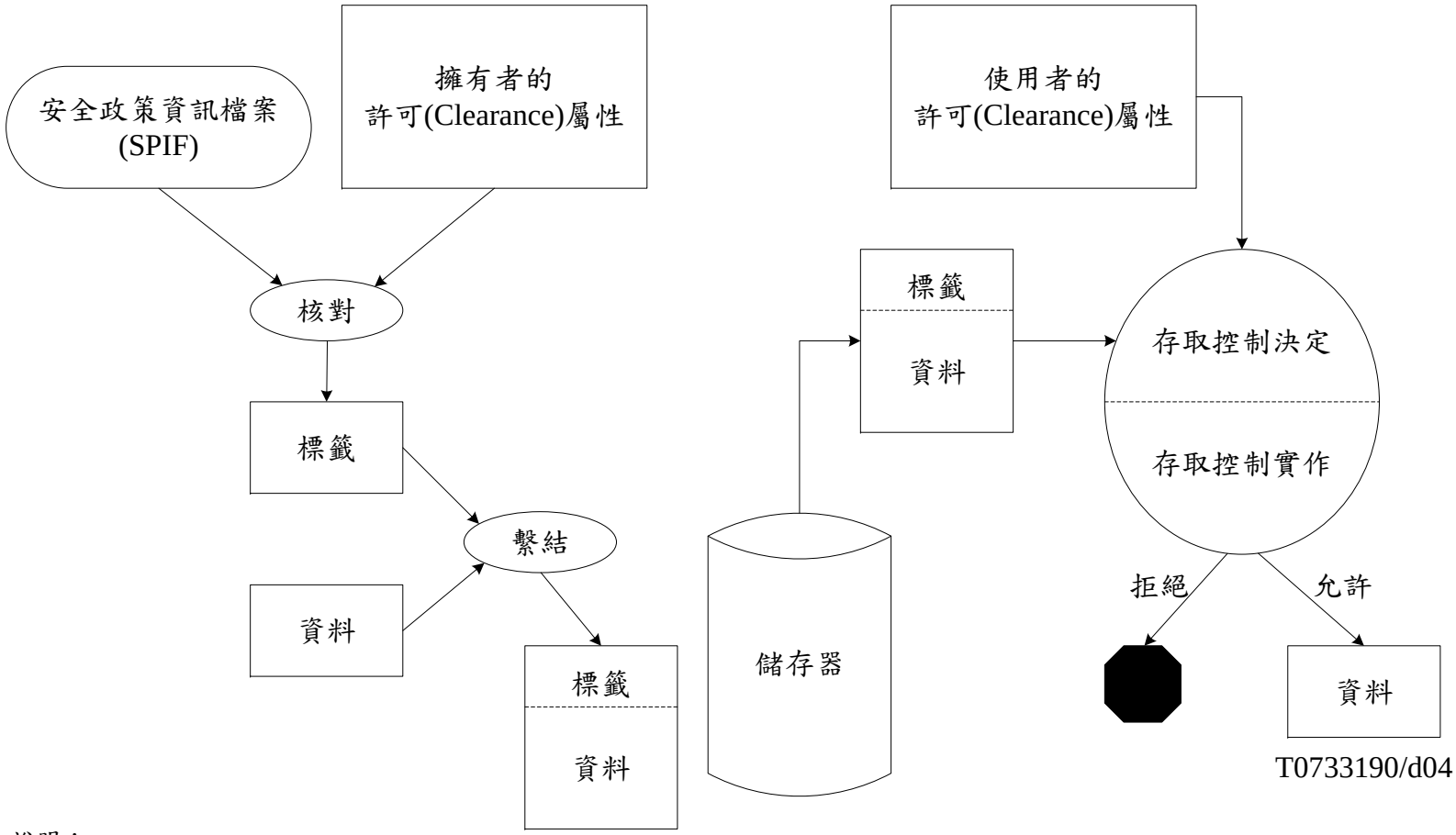
# IS-ISMS涉及個人資料之資訊分享之資訊安全管理系統的敘述為應(Shall)之強制性(Mandatory)控制措施表列初探 (續)

| ISO/IEC 27002:2005(E)節碼 | ISO/IEC 27002:2005(E)之節碼名稱 |
|---|---|
| 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 |

# 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。

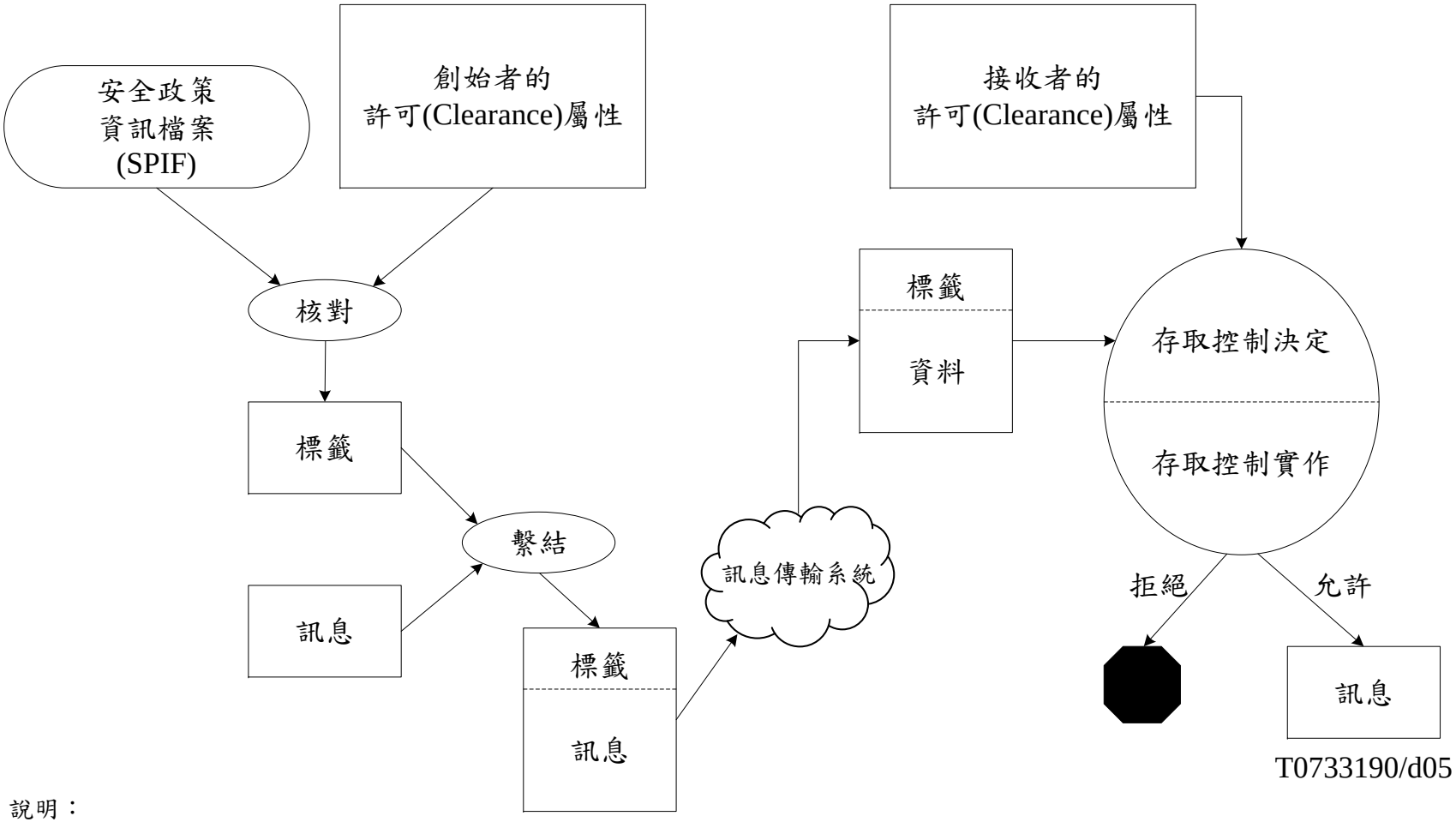
# 資料儲藏之存取控制 (Data Storage Access Control)




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 4。

# 檢索格式表列要求資訊交換情境




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。

# 資訊分享通訊協定例

1. 分享層級：

   1.1 紅色(Red)：指定資訊揭露之對象。

   1.2 琥珀色(Amber)：遵循僅知原則，資訊對特定團體揭露。

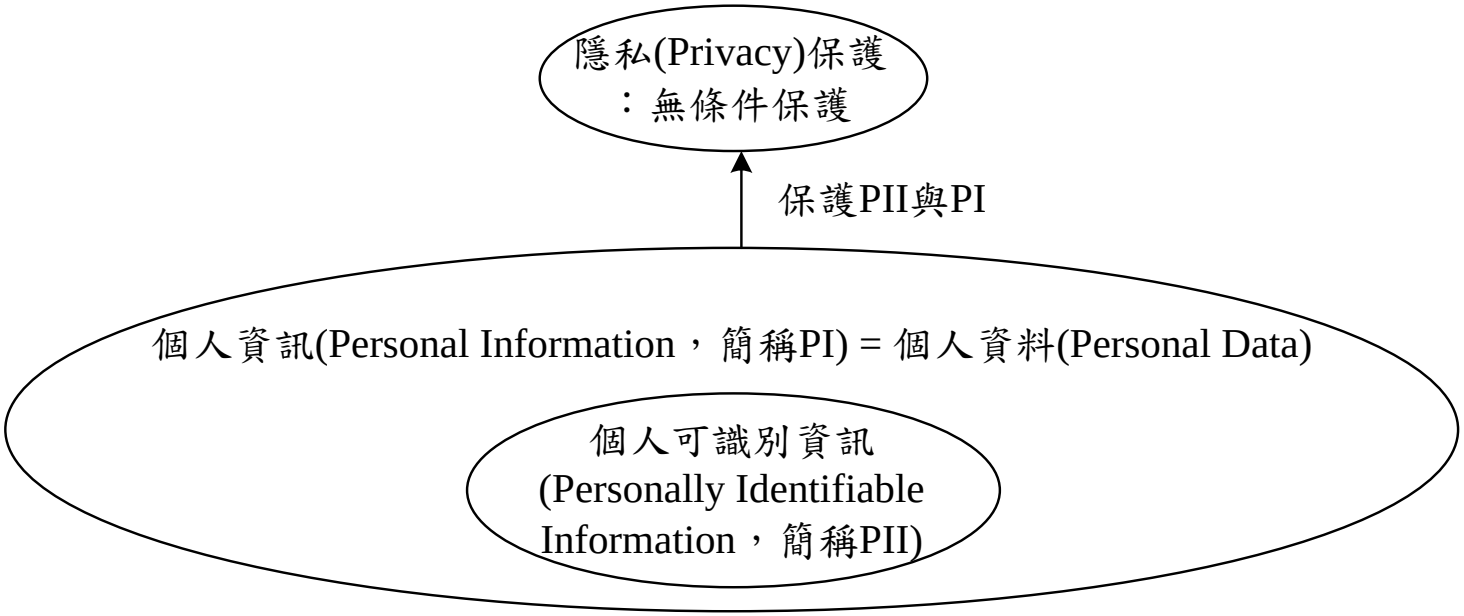
   1.3 綠色(Green)：資訊僅對會員揭露。

   1.4 白色(White)：公開之資訊。

2. 資料來源：ENISA (European Network and Information Security Agency), Good Practice Guide Network Security Information Exchanges, 2009-07。

3. 參考資訊：http://warp.gov.uk (2010-10-15)。

# 個人資訊、個人可識別資訊與隱私




備考：

1. PII之公領域基本4資訊：姓名、住址、出生年月日、性別(於本人闡明有應保護之特別事由時，始不公開)。
2. PI之私領域資訊(例：工作狀況、社交資訊)與公益之比較衡量：公益之正當性與必要性→對PI之不公開本人有應受保護的利益存在→公益之保護優越於當事人之利益。

# 個人資料保護法及其施行細則
# (2011-10-27~2011-11-09預告公聽版)
# 宜考量擴增之控制措施初探

| | 種類別 | 控制措施 |
|---|---|---|
| 1 | 授權、目的與遵循管理 | 7 |
| 2 | 資料極小化與保留 | 2 |
| 3 | 利用與限制 | 3 |
| 4 | 資料品質與限制 | 3 |
| 5 | 資訊安全 | 2 |
| 6 | 可歸責性、稽核與風險管理 | 7 |

# 授權(Authority)、目的(Purpose)與遵循(Complaint)管理

1. 同意(Consent)。
2. 存取(Access)。
3. 糾正(Redress)。
4. 蒐集(Collect)之授權(Authority)。
5. 特定目的(Purpose Specification)。
6. 個人資料與隱私保護計畫之公告(Notice)與傳播(Dissemination)。
7. 遵循性(Compliance)管理。
8. 相關條文：
   8.1 個人資料保護法第3條、第6條、第7條、第8條、第9條、第10條、第11條、第12條、第15條、第16條與第17條。
   8.2 個人資料保護法施行細則修正草案(2011-10-27~2011-11-09預告公聽版)第8條、第9條與第21條。

# 資料(Data)極小化(Minimization)與保留(Retention)

1. 個人可識別資訊(Personally Identifiable Information，簡稱PII)之極小化。

2. 資料保留與處理(Disposal)。

3. 相關條文：

   3.1 個人資料保護法第11條、第18條(公務機關)或第27條(非公務機關)。

   3.2 個人資料保護法施行細則修正草案(2011-10-27~2011-11-09預告公聽版)第5條、第6條、第9條與第21條。

# 利用(Use)與限制(Limitation)

1. 內部(Internal)利用。
2. 資訊分享(Information Sharing)。
3. 系統設計(Design)與開發(Development)。
4. 相關條文：

   4.1 個人資料保護法第2條、第14條、第17條、第18條(公務機關)或第27條(非公務機關)。

   4.2 個人資料保護法施行細則修正草案(2011-10-27~2011-11-09預告公聽版)第5條、第7條、第8條、第9條與第21條。

# 資料(Data)品質(Quality)與完整性(Integrity)

1. 資料品質。
2. 資料完整性。
3. 相關條文：

   3.1 個人資料保護法第2條、第3條、第5條、第6條、第11條與第17條。

   3.2 個人資料保護法施行細則修正草案(2011-10-27~2011-11-09預告公聽版)第8條、第9條與第21條。

# 資訊安全(Information Security)

1. 個人可識別資訊(PII)之存貨(Inventory)。
2. 隱私(Privacy)事故回應(Incident Response)。
3. 相關條文：

   3.1 個人資料保護法第2條、第14條、第17條、第18條(公務機關)或第27條(非公務機關) 。

   3.2 個人資料保護法施行細則修正草案(2011-10-27~2011-11-09預告公聽版)第8條、第9條與第21條。

# 可歸責性(Accountability)、稽核(Audit)與風險管理(Risk Management)

1. 治理(Governance)與個人可識別資訊(PII)及隱私保護計畫。
2. 隱私衝擊與風險評鑑。
3. 合約商(Contractors)與服務提供者(Service Providers)之隱私要求。
4. 隱私保護之監視(Monitoring)與稽核。
5. 隱私保護之認知(Awareness)與訓練。
6. 隱私保護之報告(Reporting)。
7. 相關條文：

   7.1 個人資料保護法第2條、第3條、第6條、第7條、第8條、第9條、第10條、第11條、第12條、第15條、第16條、第17條、第21條(非公務機關)、第28條、第29條(非公務機關)、第41條(非公務機關)與第47條(非公務機關) 。

   7.2 個人資料保護法施行細則修正草案(2011-10-27~2011-11-09預告公聽版)第8條、第9條與第21條。

# 資訊傳播的三個層次(Warren W. Weaver, Recent Contributions to Manthematical Theory of Communication, 1949)

1. 技術問題(The technical problem)：如何將資料正確的傳輸。
2. 語意問題(The sematic problem)：如何使收受資訊者能精確地明白欲傳達的訊息。
3. 效果問題(The effectiveness problem)：如何讓傳達的資訊達到預期的效果。

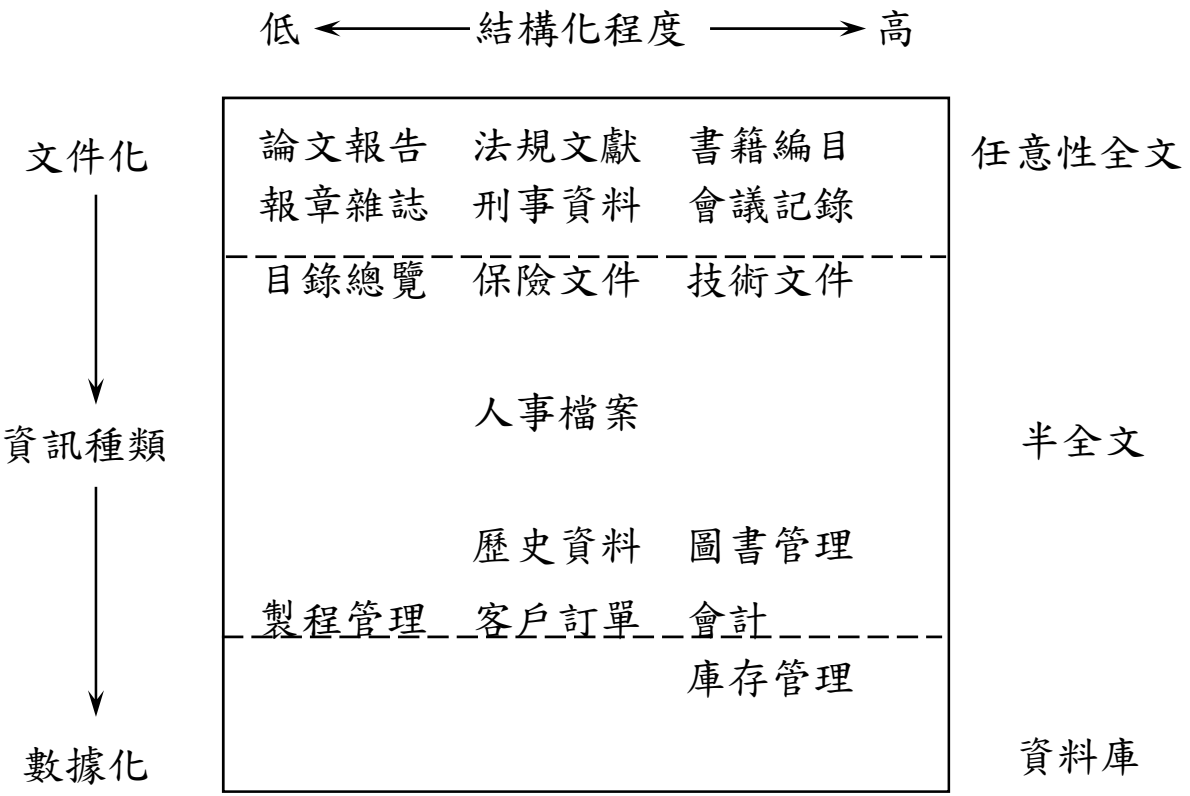
# 資訊是什麼？

1. 資訊並不是事物本身，而是事物內容、狀態及其運動特徵。

2. 資訊是事物的運動狀態及關於事務運動狀態的陳述。

3. 事物運動狀態的本身是直接的資訊，而關於其狀態的陳述是間接的資訊。

# 由資料的觀點來說明應用系統的範圍



# 隱私衝擊評鑑(Privacy Impact Assessment，簡稱PIA)－根基於2011-02之美國司法部(Department of Justice，簡稱DOJ)的PIA型式(Form)

1. 描述(Description)資訊系統－提供非技術(non-technical)之系統整體(overall)描述以闡明(address)：

   1.1 紀錄(records)與/或(and/or)系統設計之欲達成的特定目的(purpose)。

   1.2 欲達成特定目的之系統運作方式。

   1.3 經由系統蒐集(collected)、處理(maintained)、利用(used)或傳播(disseminated)之資訊(information)的型式(type)。

   1.4 在系統中存取(access)資訊之人(含機關/構)。

   1.5 使用者在系統中如何萃取(retrieved)資訊。

   1.6 系統如何傳輸(transmitted)資訊。

   1.7 與其他系統之任何互相連絡(interconnections)。

# 隱私衝擊評鑑(Privacy Impact Assessment，簡稱PIA)－根基於2011-02之美國司法部(Department of Justice，簡稱DOJ)的PIA型式(Form) (續)

2. 系統中之資訊：

2.1 經由查檢表說明系統中被蒐集、處理或傳播之資訊(分成：識別碼(Identifying numbers)、一般個人資料(General personal data)、工作相關資料(Work–related data)、辨別特徵(Distinguishing features)/生物量測(Biometrics)系統管理(System admin)/稽核資料(Audit data)、其他資訊(詳加敘述)(Other information specify) 6類)。

2.2 經由查檢表說明系統中資訊來源之全部(Check all that apply)：分成取得方式、源自政府、源自民間3類。

2.3 分析(Analysis)：識別與評估前述資訊之隱私的潛在威脅及描述將採用預防或降低其隱私威脅之組件(component)。

# 隱私衝擊評鑑(Privacy Impact Assessment，簡稱PIA)－根基於2011-02之美國司法部(Department of Justice，簡稱DOJ)的PIA型式(Form) (續)

3. 系統之特定目的(purpose)與使用(use)：

3.1 經由查檢表說明系統中資訊之蒐集、處理或傳播的特定目的之全部(Check all that apply)。

3.2 分析：解釋如何利用資訊之規範與其達成特定目的之理由。

3.3 經由表檢表說明系統中資訊被蒐集之法規、政策或協議的引證(citation)/參考文獻(reference)之全部。

3.4 闡述為達成特定目的，資訊保留之期間與到期資訊將如何處理(若能夠，則提出保留時程之國家檔案與紀錄管理的參考文獻)。

3.5 分析：描述各個組件利用資訊結果的潛在威脅，與確保適當地操縱(handled)、保留(retained)、與處置(disposed)資訊之控制措施(controls)的安置(例：系統使用者之強制性訓練，資訊淨化的自動化設施等)。

# 隱私衝擊評鑑(Privacy Impact Assessment，簡稱PIA)－根基於2011-02之美國司法部(Department of Justice，簡稱DOJ)的PIA型式(Form) (續)

4. 資訊分享(Information Sharing)：

4.1 經由查檢表說明分享系統中資訊之單位(whom the component)，及其分享的方式(分成個案(Case-by-case)、整批傳輸(Bulk transfer)、直接存取(Direct access)與其他(詳加敘述(Other (Specify))) 4類)。

4.2 分析：描述因分享資訊所增加的衍生風險，與預防或降低隱私威脅其之組件的控制措施之安置。

# 隱私衝擊評鑑(Privacy Impact Assessment，簡稱PIA)－根基於2011-02之美國司法部(Department of Justice，簡稱DOJ)的PIA型式(Form) (續)

5. 告知(Notice)、同意(Consent)與更正(Redress)：

5.1 經由查檢表告知資料當事人，經由系統之其資訊被蒐集、處理或傳播的全部。

5.2 經由查檢表詳述當事人有無拒絕提供資訊之方法或理由。

5.3 經由查檢表詳述當事人有無拒絕同意其特別(particular)利用其資訊之方法或理由。

5.4 分析：當事人資訊被蒐集與利用之告知/免為告知、同意與更正權利的清晰及明顯地之資訊公開以及解釋。

# 隱私衝擊評鑑(Privacy Impact Assessment，簡稱PIA)－根基於2011-02之美國司法部(Department of Justice，簡稱DOJ)的PIA型式(Form) (續)

6. 資訊安全(Information Security)：

6.1 是否已進行安全風險評鑑。

6.2 詳述已識別與實作之經由安全風險評鑑識別出的風險之適當地安全控制措施。

6.3 詳述預防資訊誤用(misuse)之保護機制的監視、測試或評估之保證(undertaken)。

6.4 資訊已達到遵循(美國)聯邦資訊安全管理法要求之安全性，並提供近期的驗證與認證(Certification and Accreditation)報告。

6.5 已有確保已遵循安全標準之稽核程序，並包含角色基(role-based access)與預防資訊誤用之測量(measures)。

6.6 存取系統之受委託人的契約已存在遵守隱私權法(Privacy Act)之條款。

# 隱私衝擊評鑑(Privacy Impact Assessment，簡稱PIA)－根基於2011-02之美國司法部(Department of Justice，簡稱DOJ)的PIA型式(Form) (續)

6. 資訊安全(Information Security) (續)：

6.7 存取系統之受委託人的契約已存在遵守司法部要求之資訊安全規範。

6.8 被授權存取或接收系統資訊之使用者應要求接受下列訓練：

(1) 資訊安全之一般性訓練。

(2) 被授權使用系統之單位內人員的規範性訓練。

(3) 被授權使用系統之單位外人員的規範性訓練。

(4) 其他(詳加敘述)。

# 隱私衝擊評鑑(Privacy Impact Assessment，簡稱PIA)－根基於2011-02之美國司法部(Department of Justice，簡稱DOJ)的PIA型式(Form) (續)

7. 隱私權法：

7.1 經由查檢表確定系統中的紀錄之合法性。

7.2 分析：描述系統中之資訊為何合法。

7.3 備考：涉及美國隱私權法之條文處，均省略。

8. 說明：

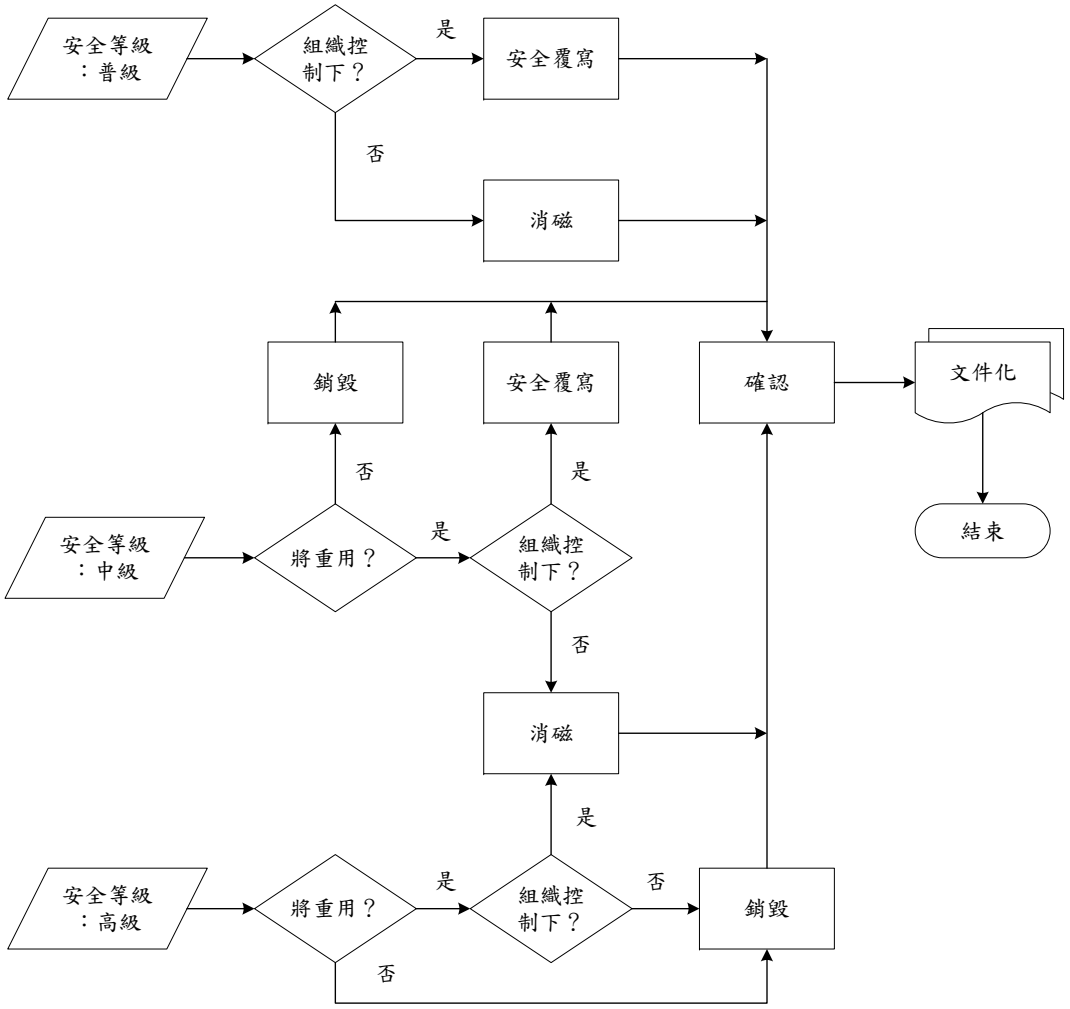
8.1 2002年12月17日，美國公布之電子化政府法(E-Government Act of 2002)中的第208節(Section)之隱私條款(Privacy Provisions)明文規範PIA。

8.2 金融服務領域(Financial services)於2008年已出版Financial Services – Privacy impact assessment (2008(E)):2011-09-17。

# 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<br>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）。<br>2. 確認政策與程序包含不再因為法律、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。<br>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。<br>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。<br>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 2.0 版，2010-10-28。 | |

# 電磁紀錄物資料淨化(Sanitization)處理作業流程舉隅




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：Garfinked, 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)。

# 個人資料保護標準制定工作項目簡述

1. 2003年10月：ISO/IEC JTC1成立隱私技術研究組(Study Group on Privacy Technologies，簡稱SGPT)，進行至2004年10月為期1年之標準化需求(Standardization needs)識別(Identity)的研究。
2. 2004年10月(JTC1之豫解(Resolved))：

   2.1 解散SGPT。

   2.2 指正SC 27進行隱私技術標準制定工作，於2006年11月向JTC 1提出報告。
3. 2005年5月：提出識別管理框架(A framework for identity management: ISO/IEC 24760)之新工作項目建議書(New Work Item Proposals，簡稱NWIP)。
4. 2006年5月：

   4.1 成立SC 27之第5工作組(Working Group)，主責識別管理與隱私技術(Identity Management and Privacy Technologies)的標準制定工作。

   4.2 提出隱私框架(A Privacy Framework: ISO/IEC 29100)與隱私參考架構(A Privacy Reference Architecture: ISO/IEC 29101)之NWIP。

# 個人資料保護標準制定工作項目簡述(續)

5. ISO/IEC JTC 1/SC 27 WG5進行中之工作項目：

5.1 框架與架構(Framework & Architecture)：

5.1.1 ISO/IEC 29100:2011-12-05。

5.1.2 ISO/IEC 29101。

5.1.3 識別管理框架(A framework for identity management: ISO/IEC 24760 Part 1:2011-12-07、Part 2 and Part 3)。

5.1.4 存取管理框架(A framework for access management: ISO/IEC 29146)。

5.1.5 實體鑑別保證框架(Entity authentication assurance framework: ISO/IEC 29115)。

# 個人資料保護標準制定工作項目簡述(續)

5. ISO/IEC JTC 1/SC 27 WG5進行中之工作項目 (續)：

5.2 保護概念(Protection Concepts)：

5.2.1 生物量測保護(Biometric template protection: ISO/IEC 24745:2011-06-17)。

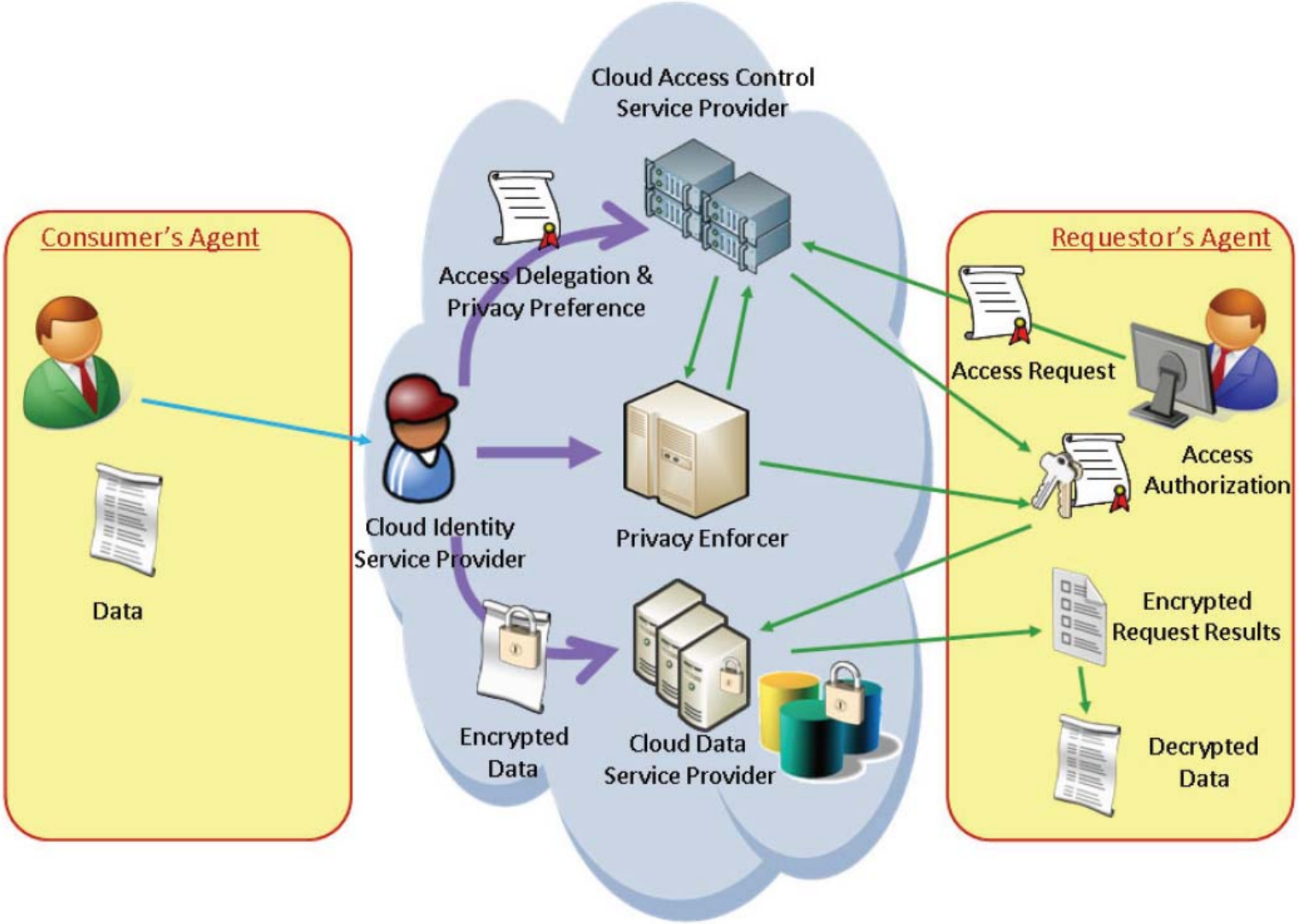
5.2.2 關於匿名之識別信託的要求項目－使用群簽章之鑑別與授權模型(Requirements on relative anonymity with identity escrow – model for authentication and authorization using group signatures: ISO/IEC 29191)。

5.3 脈絡與評鑑指南(Guidance on context and assessment)：

5.3.1 生物量測鑑別脈絡(Authentication context for biometrics: ISO/IEC 24761:2009-05-11)。

5.3.2 隱私能力成熟度模型(Privacy capability maturity model: ISO/IEC 29190)。

# 資料委外運作與隱私保護宜建立之雲計算架構




資料來源： Modelling Cloud Computing Architecture without Compromising Privacy, Figure 3, P. 13, ISO/IEC JTC 1/SC 27 N9326:2010-09-22.

# 個人資訊管理系統(Personal Information Management System，簡稱PIMS)建議之結構(Structure)

1. multi-part standard
   - ISO/IEC 27xxx Information technology — Security techniques — Personal information security and privacy:
     - Part 1 : Requirements
     - Part 2 : Code of practice for security controls
     - Part 3 : Code of practice for data protection controls
     - Part 4 : Auditing Guidelines
2. multiple standards
   - ISO/IEC 27xxx Information technology — Security techniques — Requirements for personal information management system
   - ISO/IEC 27xxx Information technology — Security techniques — Code of practice for security controls for personal information management
   - ISO/IEC 29xxx Information technology — Security techniques — Code of practice of data protection controls for the personal information management
   - ISO/IEC 27xxx Information technology — Security techniques — Auditing guidelines for the personal information management

# 個人資訊管理系統(Personal Information Management System，簡稱PIMS)建議之結構(Structure) (續)

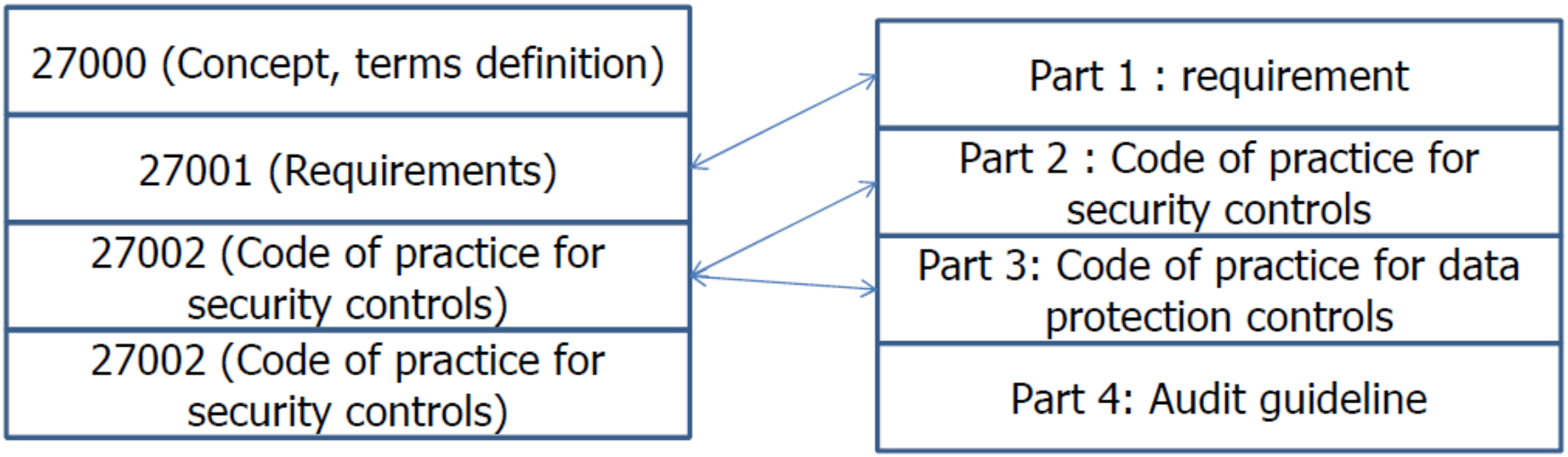
3. 說明：

3.1 PIMS之標準制計畫於2011-10由ISO/IEC JTC 1/SC 27的WG1與WG5共同主責。

3.2 資料來源：Heung Youl Youm (2011) Personal information management system in Korea (Presentation), RAISE 2011 in Seoul, 2011-11-24。

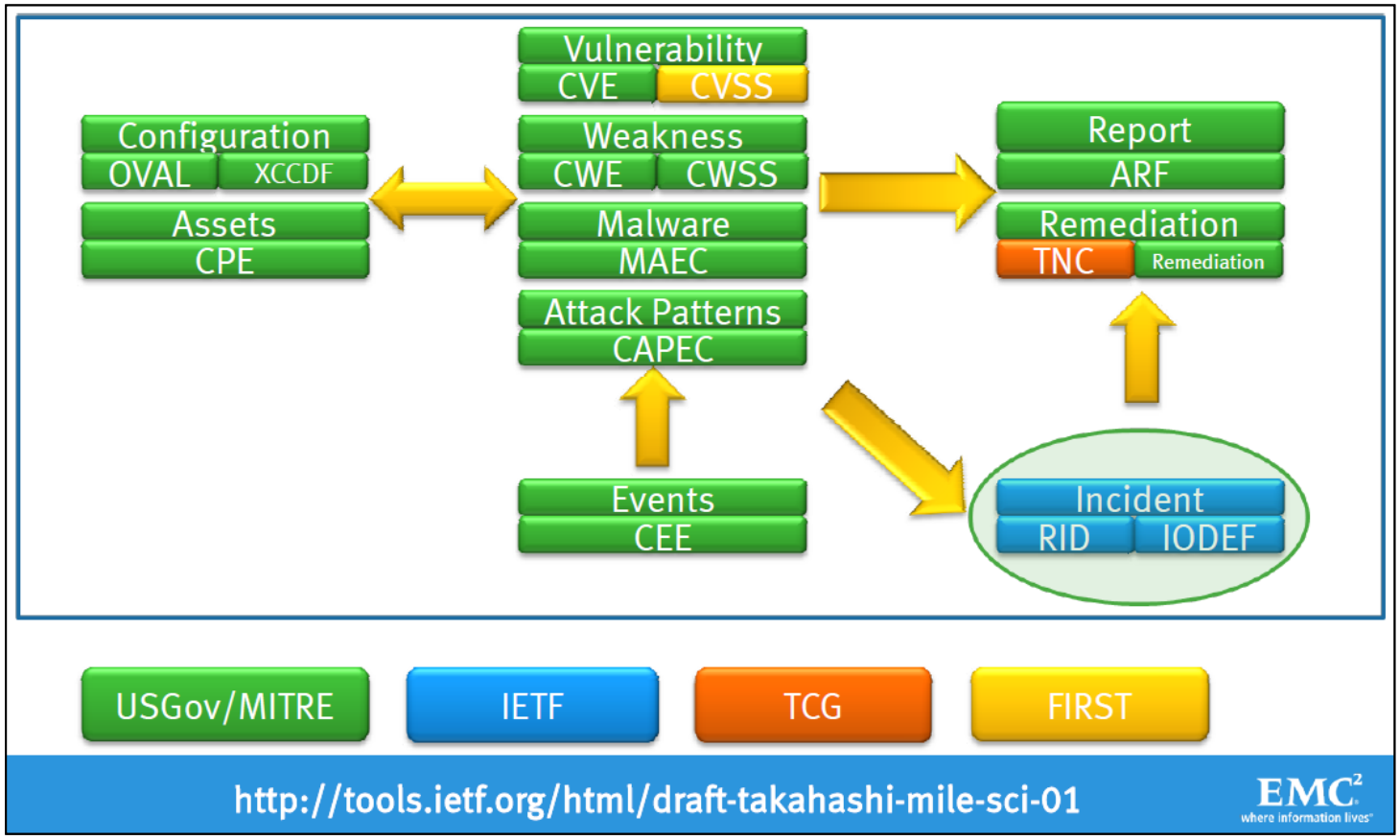
3.3 備考：WG5為2005年5月新增，WG4為原WG1中特定控制措施標準化工作項目移出之工作組。

# 資訊安全管理系統標準系列
# 與個人資訊管理系統標準系列之關連




資料來源：Heung Youl Youm (2011) Personal information management system in Korea (Presentation), RAISE 2011 in Seoul, 2011-11-24。

# 結構化數位安全標準系列(Structured Cyber Security Standards: Protocols and techniques encompassed in CYBEX and now IODEF)




資料來源：Kathleen M. Moriarty (2011) IETF MILE: Improving Incident and Information Sharing Standards, Managed Incident Lightweight Exchange (MILE) Working Group, 2011-11-01。

# CYBEX (Cybersecurity Information Exchange Framework)與MILE (Managed Incident Lightweight Exchange)技術規範表列

| | | |
|---|---|---|
| CVE | Common Vulnerabilities and Exposures | What |
| CVSS | Common Vulnerability Scoring System | What |
| CWE | Common Weakness Enumeration | What |
| CWSS | Common Weakness Scoring System | What |
| OVAL | Open Vulnerability and Assessment Language | How |
| OCIL | Open Checklist Interactive Language | How |
| XCCDF | eXtensible Configuration Checklist Description Format | How |
| CPE | Common Platform Enumeration | What |
| CCE | Common Configuration Enumeration | How |
| ARF | Assessment Result Format | How |
| CEE | Common Event Expression | What |
| IODEF | Incident Object Description Exchange Format | How |
| CAPEC | Common Attack Pattern Enumeration and Classification | What |
| MAEC | Malware Attribution Enumeration and Characterization Format | What |
| CybOX | Cyber Observable Expression | What |
| PFAM | Phishing, Fraud and Misuse Format | How |
| RID | Real-time Inter-network Defence | How/What |
| TNC | Trusted Network Connect | How/What |

說明：

1. RID 係 MILE 提出，TNC 為 MILE 擴增。
2. 資料來源：http://measureable.mitre.org/ (2011-12-01)與本研究。
3. TNC 使用 SCAP。

# 資訊安全管理系統(Information Security Management System，簡稱ISMS)與資訊安全管理過程

<table>
<tr><td>管理</td><td colspan="2">運作</td><td>技術</td></tr>
<tr><td rowspan="2">創建 ISMS 政策</td><td colspan="3">監視(Monitor)與測度(Measure))</td></tr>
<tr><td colspan="2">資訊安全政策</td><td>資訊安全(系統)政策</td></tr>
<tr><td>建立目標(Goals)</td><td colspan="3">發展資訊安全管理剖繪(Profile)</td></tr>
<tr><td>識別標的(Targets)</td><td colspan="3">資訊安全管理評鑑合規</td></tr>
<tr><td colspan="4">稽核：<br>1. ISMS 里程碑與改進計畫。<br>2. ISMS 有效性之實作計畫。<br>3. ISMS 持續改進之查證結果的回饋機制。</td></tr>
<tr><td colspan="4">資料來源：<br>1. ISO/IEC 27001 標準系列。<br>2. ISO/IEC 15408 標準系列。<br>3. 本研究。</td></tr>
<tr><td colspan="4">備考：<br>1. 遵循管理系統標準(Management System Standards)之進程，於 ISO/IEC 4th WD 27001:2010-11-15「ISMS 政策」已改名「資訊安全政策」，「資訊安全政策」改名「資訊安全特定政策(Information Security Specific Policy)」。<br>2. 於 ISO/IEC 4th WD 27001 中，規範資訊安全風險管理取徑(Approach)與資訊安全規則(Rules) 2 資訊安全特定政策之文件化。<br>3. 資訊安全(系統)政策係本研究之用語。</td></tr>
</table>

# ISMS驗證與認證及資訊安全護理

資訊安全管理標準化之研究必須設法超越，彷彿不證自明的資訊安全管理系統(Information Security Management System，簡稱ISMS)之驗證與認證空間建構，其標準化所以成立的關鍵在如何跨越現有之ISMS驗證的空間，使之成為資訊社會運作的空間。在2000年前後形成之ISMS驗證的空間，所以成為具有社會意義之空間仍是因為相互競爭的行動者將之「挪為己用」，或典雅些，「經營」之，而形成的。此社會空間的存在預設了不同利益關係之行動者所共同參與的場域。共同在場者，藉由其在場域內不同結構位置所引致之利益及所連結的資源，進行策略性之行動，從而鞏固或改變既存的秩序。國家作為一個控制資訊安全管理之集中式權力，它對ISMS驗證的需求影響到其標準化之進程，資訊安全護理(Healthcare)的結構化數位安全之標準系列的實作形塑了美國資訊安全管理法之ISMS的驗證方式，其對ISMS標準化之制約以及影響是一個值得關心的議題。

# 奧瑪.開儼(11~12世紀波斯學者)四行詩之一

我將靈魂送往蒼穹，

探索那來世的奧秘，

不料他卻回來傾訴，

你的自身就是天堂與地獄。

I sent my Soul through the Invisible,

Some letter of that After-life to spell;

And by and by my soul return'd to me,

And answer'd, "I Myself am Heav'n and Hell."

Edward Fitz Gerald (1809~1883)英譯

# 元　日
## (王安石先生 1069年間作)

爆竹聲中一歲除，春風送暖入屠蘇。

千門萬戶瞳瞳日，總把新桃換舊符。

# 染　雲
## (王安石先生 1078~1081年間作)

染雲為柳葉，剪水作梨花。

不是春風巧，何緣有歲華。

# 敬 請 指 教