以 BS 10012 為基礎評估組織導入個人資訊管理制度之研究

黃明達
淡江大學資訊管理學系教授
mdhwang@mail.tku.edu.tw

張書鳴
淡江大學資訊管理學系碩士班研究生
clio.chang@mail.im.tku.edu.tw

摘要

刑事警察局統計指出，2009年165反詐騙專線，網路購物個人資料(以下簡稱個資)外洩詐騙事件排名第一，佔全部詐騙數35%，顯示個資外洩情形嚴重。在個人資料保護法三讀通過後，組織一旦違法使用個資，將面臨高價求償金、刑責等問題，組織可能需開始著手規劃並實施針對個人資料的相關保護工作，降低個資法帶來的衝擊。

本研究以問卷調查方式，分析各組織個人資料保護現況。發現若不慎洩漏個資時，最多組織擔憂商譽受損的衝擊，但中小企業與非營利事業對於須自行舉證非組織本身洩漏個資的困擾更甚於商譽受損。本研究以BS 10012為基礎之「規劃」、「實行與運作」、「監督與審查」、「改善」等四構面，評估組織的個人資訊管理制度狀況，提供十種組織可優先加強構面之建議，如資訊服務業、金融業等組織在「規劃」構面、政府部門等在「實行與運作」構面、非營利組織等在「監督與審查」構面與電信業等在「改善」構面，建議強化個人資訊管理制度上的不足，使組織降低個資法將帶來的衝擊。

關鍵字：個人資料保護法、個人資訊管理制度、BS 10012、ISO 27001、PIMS

1.緒論

1.1 研究背景與動機

刑事警察局根據2009年統計資料指出，165反詐騙專線，接獲詐騙投訴電話，網路購物個人資料外洩詐騙事件排名第一，佔全部詐騙數的35%[6]，個人資料外洩情形嚴重[15]。玉山銀行之網路銀行於2010年4月遭駭客入侵，一萬多筆個資因此外洩，雖然金管會已對玉山銀行重罰400萬元[3]，但對於個資遭外洩的受害者來說，個資外洩的衝擊影響仍未獲得解決。根據NII產業發展協進會的「台灣網路安全信心調查」[1]中指出，國人對於網路安全信心不足，63.1%最擔憂個資外洩，且29.8%的受訪民眾最盼藉由法律嚴懲不法行為。

「個人資料保護法」[4]於2010年4月27日立法院三讀通過，立法之目的在於尋求個人資料隱私權與資料合理流通間一個利益平衡，加強了個資法前身「電腦處理個人資料保護法」[5]法律規範的不足。這也代表台灣有較全面的法律規範，保護國人的個人資料不遭濫用。

BSI (British Standards Institution, 英國標準協會)於2009年正式發佈BS 10012 :2009[14]個人資訊管理制度(Personal Information Management System, PIMS)；此標準具體說明對於個人資訊管理制度的各項要求，提供一套PDCA (Plan – Do – Check – Act)管理架構[11]，讓組織能維持和改善對資料保護法律及優良實務的遵循。

在個人資料保護法正式通過後，組織一旦違法使用個資，將面臨高價求償金，甚至可能有刑責問題，因此，組織可開始著手規劃個資安全與隱私的保護政策[20]，並針對個人資料保護，實施相關的防護工作[22]，參考國際標準[7]，詳實檢視現行工作流程中，個人資訊的處理細節[18]，結合預防和控制措施及程序，確認已有足夠的保護管理能力，降低個資法對組織帶來的衝擊。

1.2 研究目的

研究目的如下：

- 瞭解個人資料保護法通過後，整體組織對於個人資料的蒐集、處理及利用的因應現況。
- 針對各組織的個人資訊管理制度完成狀況進行差異比較，分析各組織對於個人資訊管理制度有哪些程度上的差異。
- 期望透過分析，提供目前各組織於個人資訊管理制度上可加強之建議，使組織降低個人資料保護法帶來的衝擊。

1.3 研究對象與限制

本研究為探討組織因應個資法的現況，因此研究對象以對於個人資訊管理制度有興趣的組織為主，資訊服務業、政府部門、金融業三者佔全部組織樣本的58.9%。

本研究樣本僅以出席BSI PIMS年會的組織為主，因無法預期出席年會之組織，故未包含所有組織，為本研究限制。

1.4 論文架構

本研究分為五章，第一章為緒論，含研究背景與動機及研究目的，第二章為文獻探討，第三章為研究方法，問卷設計與發放流程，輔助工具之說明。第四章為資料分析，資料整理分析，問卷問項結果彙總成表。第五章為結論與建議，整理本研究之研究結論，並對後續研究提出建議。

2. 文獻探討

2.1 個人資料保護法

我國為規範電腦處理個人資料，避免人格權受侵害，並促進個人資料之合理使用，研擬「電腦處理個人資料保護法」於民國八十四年八月十一日制定公布施行迄今。但由於電腦科技日新月異，利用電腦蒐集、處理、利用個人資料之情形日漸普遍，再加上各類型商務行銷廣泛大量蒐集個人資料[19]，對於個人隱私權之保護，造成莫大威脅；故政府當局整理國內學界及實務界之修法意見且參考APEC[13]和OECD[21]的隱私權綱領，擬具修正草案，名稱為「個人資料保護法」。

「個人資料保護法」於2010年4月27日立法院三讀通過，立法之目的在於尋求個人資料隱私權與資料合理流通間一個利益平衡。與現行「電腦處理個人資料保護法」最大差異，在於法律規範對象從原來的醫療、電信、金融等八大行業擴大至所有公民營機關，不限行業、自然人、法人或其他境外團體，個資法影響範圍更全面。

個資法規定蒐集個人資料時，不論直接或間接蒐集都要盡到告知的義務，包含詳細告知蒐集人是誰、資料使用目的及用途等等，並取得當事人書面同意。

當發生個資外洩的情況時，個資法第二十九條，規定組織須舉證說明並非組織自身的過失，否則無法脫責。在處罰的部分，個資法增加了二十人以上團體訴訟機制[9]，讓個資被外洩的被害人可進行團體訴訟及求償，團體求償金額從過去的上限兩千萬元提高至兩億元。

2.2 個人資訊管理制度

英國、日本等國家為強化個人資訊之保護，以國家個人資料保護法為基礎，開始推動結合個人資料保護法律及管理制度的「個人資訊管理制度」。與資訊安全管理制度ISO 27001[17]不同之處為ISO 27001廣泛針對組織保有的「資訊資產」進行管理，而個人資訊管理制度則強調「個人資料」的保護與法律的遵循[8]，關聯如圖2-1；由於個人資訊管理制度須遵循法律的規範，因此成功導入個人資訊管理制度且經過驗證的組織，可視為對個資有良善的管理且符合個人資料保護法律的要求。

對於組織個人資訊管理制度的建立，可參考國際標準，如英國的BS 10012、日本的JISQ 15001等，標準中有各項具體對於個人資訊管理制度的要求，讓組織能維持對個人資料保護法律的遵循。

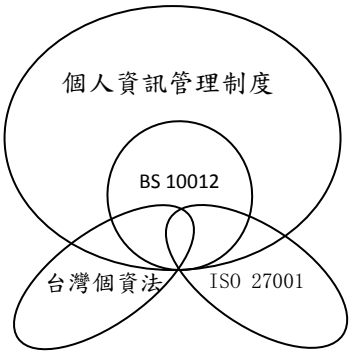

圖2-1：個人資訊管理制度關聯圖

2.3 BS 10012:2009 標準

BSI英國標準協會於2009年正式發佈BS 10012個人資訊管理制度；此標準具體說明對於個人資訊管理制度的各項要求，提供一套PDCA[23] (Plan – Do – Check – Act)管理架構,讓組織能維持和改善對資料保護法律及優良實務的遵循。

BS 10012內容共有7章，第0~2章為標準簡介、適用範圍與名詞定義，第3~6章則為個人資訊管理制度的PDCA架構，要求如下。

- 規劃 (Plan)：此章目標為規劃如何實行個人資訊管理制度，將提供方向，讓組織遵循資料保護法律及優良實務。
- 實行與運作 (Do)：內容為實作個人資訊管理制度的具體要求，也是標準中內容最多的一章。
- 監督與審查 (Check)：此章目標為確保個人資訊管理制度的有效性及效率受到監督和審查，因此組織必須制訂稽核計畫，定期實施內部稽核和管理階層審查會議，以掌握組織個資處理現況。
- 改善(Act)：此章目標為實施矯正措施，以改善個人資訊管理制度的有效性和效率，內容分為兩個方向，首先為組織針對可能違反法規的事件，在事先實施預防行動，並評估可能造成的問題來決定實施必要的矯正措施；其次為依據管理階層審查結果，針對不符合政策或標準要求的事項進行矯正，持續改善。

3. 研究設計

3.1 研究方法

本研究係採用資料蒐集方法中的調查研究法，選用自填式問卷調查方式。

3.2 問卷設計

本研究的問卷以BS 10012標準為基礎。採用BS 10012 PDCA四個章節，第3章到第6章的控制措施為內容，如表3-1所示，總共包含33題問項。

本研究中每個問項以「尚未考慮」、「考慮中」、「規劃中」、「部份完成」、「完全達成」五個答項方式[10] 來調查組織的個人資訊管理制度現況。

五個答項分別代表：尚未考慮：目前尚未考慮。考慮中：已考慮尚未規劃。規劃中：已規劃尚未執行。部份達成：已有部分執行。完全達成：已完全執行。

表 3-1：問卷涵蓋章節

章節	問項數
規劃 (Plan)	7
實行與運作 (Do)	19
監督與審查 (Check)	4
改善 (Act)	3
總數	33

3.3 問卷發放過程描述

問卷調查地點在2010年10月27日英國標準協會所舉辦的BSI 2011 PIMS年會會場。年會討論主題為個人資料保護法通過後，各組織將面臨的衝擊與影響；會中也公布BSI新制訂的標準BS 10012，此標準為國際專家學者所推薦為提供完整框架之標準及具體說明對個人資訊管理制度的各項要求，讓組織能維持和改善對資料保護及優良時務的遵循。

問卷發送於年會會場報到處，一併與年會資料交給參加年會者；問卷回收於年會中場休息時間及年會結束在會場出口處回收，並致贈一份小禮物答謝受訪者。

3.4 統計分析方法與工具

本研究使用統計分析方法如下：敘述統計用於計算問卷調查結果。交叉分析用以瞭解基本資料之間的關係。Cronbach α 係數則用以檢驗問卷信度。單因子變異數(One-Way ANOVA)分析用以檢測基本資料與問卷問項結果間是否有顯著差異。分析工具使用SPSS Statistics 17.0統計軟體。

4. 資料分析

4.1 問卷回收率分析

現場發放200份問卷，共回收106份，總回收率為53%。其中資料不全者的問卷有16份，故有效問卷為90份，有效回收率為45%。

4.2 受訪者基本資料分析及交叉分析

受訪者組織類別(表4-1)，「資訊服務業」、「政府部門」、「金融業」三者佔全部受訪者的58.9%。政府部門工作常需要經手大量民眾個人資料，金融業則持有許多客戶的個人資料，在個資法通過後，此兩種組織將面臨更嚴格的法律規範，受訪者可能藉參加此類型年會，掌握最新國際標準，強化組織內部原本個人資訊管理制度上的不足；另一方面，個資法的通過，對於資訊服務業來說，是一項很大的商機，可能藉參加此類型年會掌握客戶最新因應個資法通過後的需求，以便往後提供有效的解決方案給客戶。

在受訪者職位部分(表 4-2)，主管階層填答問卷的比例為 42.2%，本研究的問卷結果可做主管與員工之間的問卷差異度分析，檢視對於組織因應個資法的現況是否有認知上的落差。

受訪者組織資本額 (表4-3)，以「非營利事業」佔32.2%最多，主要由「政府部門」、「學術及研究機構」與「非營利組織」三者組成；資本額「一億元以下」的中小企業中[2]50%為「資訊服務業」(表4-4)，顯示中小企業受訪者參與年會目的可能不只局限於保護組織內的個資，有些資訊服務業者可能為了組織商業考量而參加。

表 4-1 受訪者組織類別統計表

	樣本數	百分比
政府部門	19	21.1
資訊服務業	20	22.2
金融業	14	15.6
電信業	2	2.2
IT製造業	6	6.7
國營公用事業	2	2.2
學校及研究機構	7	7.8
非營利組織	3	3.3
醫療生技業	3	3.3
通路物流業	5	5.6
其他	9	10
總和	90	100

表 4-2：受訪者職位統計表

	樣本數	百分比
資訊部門主管	20	22.2
資訊稽核主管	4	4.4
資訊部門人員	42	46.7
其他部門主管	14	15.6
其他	10	11.1
總和	90	100

表 4-3：受訪者組織資本額統計表

	樣本數	百分比
非營利事業	29	32.2
1億元以下(含)	16	17.8
1.1億元~10億元	12	13.3
11億元~50億元	13	14.4
51億元~100億元	1	1.1
101億元~300億元	2	2.2
301億元~1000億元	8	8.9
1001億元以上	9	10.0
總和	90	100

表 4-4：組織類別與資本額交叉表

		非營利事業	1億以下(含)	1.1~10	11~50	51~100	101~300	301~1000	1001億以上
政府部門	樣本數	19	0	0	0	0	0	0	0
	百分比	65.50%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%
資訊服務業	樣本數	0	8	6	4	0	0	0	2
	百分比	0.00%	50.00%	50.00%	30.80%	0.00%	0.00%	0.00%	22.20%
金融業	樣本數	0	0	1	4	1	2	3	3
	百分比	0.00%	0.00%	8.30%	30.80%	100.00%	100.00%	37.50%	33.30%
電信業	樣本數	0	0	0	1	0	0	1	0
	百分比	0.00%	0.00%	0.00%	7.70%	0.00%	0.00%	12.50%	0.00%
IT製造業	樣本數	0	2	0	0	0	0	3	1
	百分比	0.00%	12.50%	0.00%	0.00%	0.00%	0.00%	37.50%	11.10%
國營公用事業	樣本數	0	0	0	0	0	0	0	2
	百分比	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	22.20%
學校及研究機構	樣本數	6	0	1	0	0	0	0	0
	百分比	20.70%	0.00%	8.30%	0.00%	0.00%	0.00%	0.00%	0.00%
非營利組織	樣本數	3	0	0	0	0	0	0	0
	百分比	10.30%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%
醫療生技業	樣本數	1	0	1	1	0	0	0	0
	百分比	3.40%	0.00%	8.30%	7.70%	0.00%	0.00%	0.00%	0.00%
通路物流業	樣本數	0	1	1	3	0	0	0	0
	百分比	0.00%	6.30%	8.30%	23.10%	0.00%	0.00%	0.00%	0.00%
其他	樣本數	0	5	2	0	0	0	1	1
	百分比	0.00%	31.30%	16.70%	0.00%	0.00%	0.00%	12.50%	11.10%

受訪者組織的資訊部門員工數統計(表 4-5),「25 人以下」最多，其中「資訊服務業」與「政府部門」兩者佔 51.3%，此兩種類別組織較多，故造成 25 人以下的樣本數較高;「201 人以上」佔第二多，其中「金融業」佔 34.8%、「政府部門」佔 26.1%;組織類別交叉結果顯示(表 4-6),政府部門的資訊部門人數呈現兩極化，因政府部門不同層級，資訊人員編制不同，但不論人數多寡，均積極參與個資管理制度議題的年會。

表 4-5：受訪者組織資訊部門人數統計表

	樣本數	百分比
25 人以下	39	43.3
26~50 人	10	11.1
51~100 人	9	10
101~150 人	6	6.7
151~200 人	3	3.3
201 人以上	23	25.6
總　　和	90	100

表 4-6：組織類別與資訊部門人數交叉表

		25 以下	26~50	51~100	101~150	151~200	201 以上
政府部門	樣本數	8	2	2	1	0	6
	百分比	20.50%	20.00%	22.20%	16.70%	0.00%	26.10%
資訊服務業	樣本數	12	3	3	1	0	1
	百分比	30.80%	30.00%	33.30%	16.70%	0.00%	4.30%
金融業	樣本數	0	1	0	2	3	8
	百分比	0.00%	10.00%	0.00%	33.30%	100.00%	34.80%
電信業	樣本數	1	0	0	0	0	1
	百分比	2.60%	0.00%	0.00%	0.00%	0.00%	4.30%
IT 製造業	樣本數	2	0	1	0	0	3
	百分比	5.10%	0.00%	11.10%	0.00%	0.00%	13.00%
國營公用事業	樣本數	0	0	0	0	0	2
	百分比	0.00%	0.00%	0.00%	0.00%	0.00%	8.70%
學校及研究機構	樣本數	3	1	2	1	0	0
	百分比	7.70%	10.00%	22.20%	16.70%	0.00%	0.00%
非營利組織	樣本數	2	1	0	0	0	0
	百分比	5.10%	10.00%	0.00%	0.00%	0.00%	0.00%
醫療生技業	樣本數	2	0	0	0	0	1
	百分比	5.10%	0.00%	0.00%	0.00%	0.00%	4.30%
通路物流業	樣本數	3	2	0	0	0	0
	百分比	7.70%	20.00%	0.00%	0.00%	0.00%	0.00%
其他	樣本數	6	0	1	1	0	1
	百分比	15.40%	0.00%	11.10%	16.70%	0.00%	4.30%

在受訪者組織成立幾年部分(表 4-7),「41 年以上」佔最多,其中以「政府部門」、「金融業」與「學校及研究機構」三者佔了 73.3%(表 4-8)，此三種組織均在「電腦處理個人資料保護法」的涵蓋範圍中，在個資法通過後,受訪者藉參加此類型年會，掌握最新國際標準來加強組織內部個人資訊管理制度上的不足。

受訪者組織是否通過 ISO 27001 部分(表 4-9)，58.9%已通過 ISO 27001；組織類別與通過 ISO 27001 交叉分析（表 4-10）有顯著相關(P-value = 0.012),「政府部門」及「金融業」兩者佔已通過比例的 51%，主要因為政府部門與金融業主管機關有鼓勵導入 ISO 27001 認證的資安政策，故受訪者通過認證的較多；另一方面,「資訊服務業」通過的比例呈現兩極化，因資訊服務業的受訪者中，有 50%是中小企業，由於導入 ISO 27001 成本高，中小企業較難承擔導入成本，資訊服務業通過的受訪者組織，屬於較大型的資訊服務公司。

表 4-7：受訪者組織成立幾年統計表

	樣本數	百分比
10 年以下	11	12.2
11~20 年	22	24.4
21~30 年	20	22.2
31~40 年	7	7.8
41 年以上	30	33.3
總　　和	90	100

表 4-8：組織類別與成立幾年交叉表

		10 以下	11~20	21~30	31~40	41 以上
政府部門	樣本數	0	2	7	0	10
	百分比	0.00%	9.10%	35.00%	0.00%	33.30%
資訊服務業	樣本數	8	8	2	2	0
	百分比	72.70%	36.40%	10.00%	28.60%	0.00%
金融業	樣本數	0	1	5	2	6
	百分比	0.00%	4.50%	25.00%	28.60%	20.00%
電信業	樣本數	0	1	0	0	1
	百分比	0.00%	4.50%	0.00%	0.00%	3.30%
IT 製造業	樣本數	0	2	1	1	2
	百分比	0.00%	9.10%	5.00%	14.30%	6.70%
國營公用事業	樣本數	0	0	0	0	2
	百分比	0.00%	0.00%	0.00%	0.00%	6.70%
學校及研究機構	樣本數	0	0	0	1	6
	百分比	0.00%	0.00%	0.00%	14.30%	20.00%
非營利組織	樣本數	0	2	1	0	0
	百分比	0.00%	9.10%	5.00%	0.00%	0.00%
醫療生技業	樣本數	0	0	1	1	1
	百分比	0.00%	0.00%	5.00%	14.30%	3.30%
通路物流業	樣本數	1	2	2	0	0
	百分比	9.10%	9.10%	10.00%	0.00%	0.00%
其他	樣本數	2	4	1	0	2
	百分比	18.20%	18.20%	5.00%	0.00%	6.70%

表 4-9：受訪者組織通過 ISO 27001 統計表

	樣本數	百分比
已 通 過	53	58.9
建 置 中	6	6.7
考 慮 中	16	17.8
尚未考慮	15	16.7
總　　和	90	100

表 4-10：組織類別與通過 ISO 27001 交叉表

選項		已通過	建置中	考慮中	尚未考慮
政府部門	樣本數	16	0	3	0
	百分比	30.2%	0.0%	18.8%	0.0%
資訊服務業	樣本數	8	1	4	7
	百分比	15.1%	16.7%	25.0%	46.7%
金融業	樣本數	11	0	3	0
	百分比	20.8%	0.0%	18.8%	0.0%
電信業	樣本數	1	0	1	0
	百分比	1.9%	0.0%	6.3%	0.0%
IT 製造業	樣本數	3	0	0	3
	百分比	5.7%	0.0%	0.0%	20.0%
國營公用事業	樣本數	2	0	0	0
	百分比	3.8%	0.0%	0.0%	0.0%
學校及研究機構	樣本數	5	0	0	2
	百分比	9.4%	0.0%	0.0%	13.3%
非營利組織	樣本數	2	0	1	0
	百分比	3.8%	0.0%	6.3%	0.0%
醫療生技業	樣本數	1	1	1	0
	百分比	1.9%	16.7%	6.3%	0.0%
通路物流業	樣本數	2	1	2	0
	百分比	3.8%	16.7%	12.5%	0.0%
其他	樣本數	2	3	1	3
	百分比	3.8%	50.0%	6.3%	20.0%

在受訪者是否了解PIMS部分(表 4-11)，選擇「了解PIMS」的受訪者中，「資訊服務業」佔 33.3%(表 4-12)，印證顯示資訊服務業受訪者中，有些組織已了解PIMS，來參加年會以更了解國際標準，便於往後提供客戶解決方案。

表 4-11：受訪者了解 PIMS 分析表

	樣本數	百分比
非常了解	4	4.4
了　　解	24	26.7
部分了解	49	54.4
完全不瞭解	13	14.4
總　　和	90	100

表 4-12：組織類別與了解 PIMS 交叉表

		非常了解	了解	部分了解	完全不瞭解
政府部門	樣本數	1	4	10	4
	百分比	25.00%	16.70%	20.40%	30.80%
資訊服務業	樣本數	1	8	8	3
	百分比	25.00%	33.30%	16.30%	23.10%
金融業	樣本數	1	4	9	0
	百分比	25.00%	16.70%	18.40%	0.00%
電信業	樣本數	0	2	0	0
	百分比	0.00%	8.30%	0.00%	0.00%
IT 製造業	樣本數	1	1	2	2
	百分比	25.00%	4.20%	4.10%	15.40%
國營公用事業	樣本數	0	0	2	0
	百分比	0.00%	0.00%	4.10%	0.00%
學校及研究機構	樣本數	0	1	4	2
	百分比	0.00%	4.20%	8.20%	15.40%
非營利組織	樣本數	0	1	2	0
	百分比	0.00%	4.20%	4.10%	0.00%
醫療生技業	樣本數	0	0	3	0
	百分比	0.00%	0.00%	6.10%	0.00%
通路物流業	樣本數	0	0	3	2
	百分比	0.00%	0.00%	6.10%	15.40%
其他	樣本數	0	3	6	0
	百分比	0.00%	12.50%	12.20%	0.00%

在個資法通過後，當組織不慎洩漏客戶個人資料時，受訪者覺得對組織造成的最大衝擊部分(表 4-13)，「商譽受損」佔最多；選「自行舉證」的受訪者中，「中小企業」與「非營利事業」兩者佔 78.3%(表 4-14)，顯示人力與資源的利用在較小彈性情況下，對於不慎洩漏個資的衝擊，中小企業與非營利事業須自行舉證的困擾更甚於商譽受損。

個資法通過後，在電腦應用系統方面，受訪者組織考慮採用下列最主要的方式防止個人資料的外洩部分(表 4-15)，「加強內部稽核」佔 32.2%，但資本額「一億元以下」的中小企業 43.8%選擇「再購買資安設備加強系統之監督與稽核」(表 4-16)，顯示中小企業目前對於主要防止個資外洩的方式較偏好於購買現成的資安設備來防止個人資料外洩，也顯示個資法通過後將帶來的商機。

表 4-13：組織個資外洩面臨最大衝擊統計表

	樣本數	百分比
商譽受損	46	51.1
賠償金額	17	18.9
客戶流失	4	4.4
須自行舉證	23	25.6
總　　和	90	100

表 4-14：組織類別與個資外洩衝擊交叉表

		非營利事業	1 億以下(含)	1.1~10	11~50	51~100	101~300	301~1000	1001 億以上
商譽受損	樣本數	10	5	8	9	1	1	7	5
	百分比	21.70%	10.90%	17.40%	19.60%	2.20%	2.20%	15.20%	10.90%
賠償金額	樣本數	8	2	3	1	0	0	1	2
	百分比	47.10%	11.80%	17.60%	5.90%	0.00%	0.00%	5.90%	11.80%
客戶流失	樣本數	1	1	1	1	0	0	0	0
	百分比	25.00%	25.00%	25.00%	25.00%	0.00%	0.00%	0.00%	0.00%
須自行舉證	樣本數	10	8	0	2	0	1	0	2
	百分比	43.50%	34.80%	0.00%	8.70%	0.00%	4.30%	0.00%	8.70%

表 4-15：組織加強防止個資外洩方式統計表

	樣本數	百分比
再購買資安設備加強系統之監督與稽核	26	28.9
建立資料加解密機制	26	28.9
加強內部稽核	29	32.2
加強外部稽核	7	7.8
維持現狀	2	2.2
總和	90	100

表 4-16：資本額與加強防個資外洩交叉表

		非營利事業	1億以下(含)	1.1~10	11~50	51~100	101~300	301~1000	1001億以上
再購買資安設備加強系統之監督與	樣本數	7	7	1	4	0	1	2	4
	百分比	24.10%	43.80%	8.30%	30.80%	0.00%	50.00%	25.00%	44.40%
建立資料加解密機制	樣本數	9	3	4	6	0	0	2	2
	百分比	31.00%	18.80%	33.30%	46.20%	0.00%	0.00%	25.00%	22.20%
加強內部稽核	樣本數	11	4	5	2	0	1	3	3
	百分比	37.90%	25.00%	41.70%	15.40%	0.00%	50.00%	37.50%	33.30%
加強外部稽核	樣本數	1	2	1	1	1	0	1	0
	百分比	3.40%	12.50%	8.30%	7.70%	100.00%	0.00%	12.50%	0.00%
維持現狀	樣本數	1	0	1	0	0	0	0	0
	百分比	3.40%	0.00%	8.30%	0.00%	0.00%	0.00%	0.00%	0.00%

受訪者組織在因應個資法時，預計經費部分(表 4-17)，選擇「評估中」佔 41.1%為最多，「尚未評估」佔 20%居次。顯示受訪者組織超過 60%對於因應個資法通過，組織還沒有決定一個確切預算出來。

基於推行「個人資料保護法」所採取相關的因應措施，是否會迫使組織業務執行上的流程變得更為繁雜部分(表 4-18)，顯示超過 90%以上受訪者都同意組織因應個資法的措施會造成原本流程變為繁雜。

表 4-17：組織因應個資法預計經費統計表

	樣本數	百分比
尚未評估	18	20.0
評估中	37	41.1
100 萬元以下	10	11.1
101~1000 萬元	18	20.0
1001 萬元以上	6	6.7
不需要	1	1.1
總和	90	100

表 4-18：組織因應措施使流程變繁雜統計表

	樣本數	百分比
非常同意	20	22.2
同意	65	72.2
沒意見	2	2.2
不同意	3	3.3
總和	90	100

受訪者組織對於將面臨個資法之相關問題是否舉辦員工的訓練或說明會部分(表 4-19)，63.3%的受訪者組織有舉辦員工訓練或說明會，26.7%的受訪者組織考慮舉辦，顯示個資法通過後，組織積極讓員工瞭解個資法將為組織帶來的影響。

表 4-19：組織是否舉辦員工的訓練或說明會統計表

	樣本數	百分比
是	57	63.3
否	9	10.0
考慮中	24	26.7
總和	90	100

4.3 問卷效度與信度分析

效度方面：本研究依據標準BS 10012條文，設計 33 題問項，請資訊安全相關工作之專家，對問卷內容提出修正與建議，具有內容效度。針對「規劃」、「實行與運作」、「監督與審查」和「改善」等四流程進行因素分析，使用直交轉軸的最大變異轉軸法(Varimax rotation)，KMO值分別為 0.907、0.931、0.729 與 0.742(皆大於 0.7)，Bartlett's球體檢定結果均為 0.000，皆具顯著水準(P-value<0.001)，可進行因素分析。本研究分別進行因素萃取，皆萃取一個因素，因此分別命名為「規劃」、「實行與運作」、「監督與審查」和「改善」構面。

信度方面：本研究使用SPSS Statistics 17.0 計算四個構面問項的Cronbach α 係數以檢定問卷的信度，資料分析結果請參照表 4-20，四構面Cronbach α 係數皆大於 0.9，顯示本問卷的四個構面是一份可靠的測量工具。

表 4-20：四個構面的信度分析表

構面（問項數）	Cronbach α 係數
規劃 (7)	0.961
實行與運作 (19)	0.981
監督與審查 (4)	0.930
改善 (3)	0.913
所有構面	0.988

4.4 組織 PIMS 現況分析

組織 PIMS 四個構面的控制措施，整體現況調查相關統計數據請參照表 4-21。

表 4-21：整體組織 PIMS 現況列表

	尚未考慮	考慮中	規劃中	部分完成	完全達成
規劃	10.16%	20.16	32.04%	22.37%	15.23%
實行與運作	10.58%	14.15	29.00%	32.21%	14.03%
監督與審查	8.63%	14.43	29.73%	24.73%	22.50%
改善	7.07%	12.20	24.07%	37.80%	18.90%

- 規劃構面：

整體「規劃」構面的問項統計，受訪者組織「完全達成」(15.23%)，但深入分析問項(表 4-22)，發現在「貴組織由高階主管負責維護PIMS政策，並表態支持。」、「貴組織PIMS政策有說明需承諾遵守國內

個資法。」及「貴組織內的員工均被告知遵循PIMS政策，且了解在組織中自我的責任歸屬。」這三題問項中，「完全達成」的比例皆超過20%，另一方面，「貴組織有依照發展、實行、維護和持續改善等步驟將PIMS文件化。」(7.8%)及「貴組織有提供實作PIMS所需的資源。」(6.7%)這兩題問項中，「完全達成」的比例皆低於10%，呈現兩極化，顯示目前各組織十分積極規劃組織的PIMS政策，完全達成度高，但如何將組織所規劃的PIMS政策、實行步驟等文件化，受訪者組織的完成進度略慢，可能因為個資法通過不到一年，各組織還沒編列提供實作PIMS所需的資源，故造成「規劃」構面問項「完全達成」的比例不高。

● 實行與運作構面：

深入分析問項(表4-23)，發現「貴組織有具體指明處理個人資料之目的，且不用於目的外用途。」問項中，「完全達成」的比例達21.1%，另一方面，在「能確保當其他組織代表貴組織管理個人資料的處理程序有遵循個資法。」問項的調查結果，「完全達成」的比例僅8.9%，顯示各組織在個資法通過後，處理個人資料時，注重具體的指明個資使用目的以遵循法律規範，才能有如此高的完全達成率，但關於其他組織代表處理個資時，目前還未有一個公信驗證，故要確保其他組織如同自身一樣遵循個資法，是較難完全達成的部分。

整體上受訪者組織在「實行與運作」構面(32.21%)與「規劃」構面(22.37%)比較，發現「部分完成」的比例前者比後者高，顯示受訪者組織對於PIMS的實作並非從零開始，部分受訪者組織可能是接續組織已存在的制度、系統來做加強，轉變為PIMS的一部分，此為「實行與運作」的「部分完成」比例偏高的原因。

● 監督與審查構面：

此構面「舉行PIMS內部稽核」(36.7%)及「確保PIMS發生重大變更時可用性、充分性和有效性」(34.4%)兩題問項統計中(表4-24)，受訪者選擇「規劃中」的比例最高，顯示針對PIMS的稽核以往未納入組織的內部稽核範圍，因應個資法的通過，才將規劃PIMS加入組織內部稽核的重點目標。

「組織定期進行內部稽核並提供稽核報告給管理層」的問項調查中，「完全達成」的比例32.2%，顯示受訪組織定期舉行組織內部稽核且提供稽核報告給管理層有效執行比例高，這對於未來舉行PIMS內稽後，提供報告給管理層有正面幫助。

● 改善構面：

深入分析改善構面問項(表4-25)，「組織有防止不符合事項的措施」(62.3 %)及「定期進行風險評估」(62.3%)兩題問項中，「部分完成」及「完全達成」的合計比例均超過整體的60%，顯示現階段組織內部持續改善的行動周全，PIMS的PDCA週期能夠週而復始的循環下去，對於未來個資法實施細則公告後，PIMS能更快符合法律規範有正面幫助。

表 4-22：規劃構面問項統計表

	尚未考慮	考慮中	規劃中	部分完成	完全達成
1. 貴組織有依照發展、實行、維護和持續改善等步驟將 PIMS 文件化。	10.0%	27.8%	30.0%	24.4%	7.8%
2. 貴組織有定義 PIMS 的範圍和規定個人資料管理的目標。	7.8%	27.8%	33.3%	16.7%	14.4%
3. 貴組織由高階主管負責維護 PIMS 政策，並表態支持。	11.1%	15.6%	30.0%	21.1%	22.2%
4. 貴組織 PIMS 政策有說明需承諾遵守國內個資法。	12.2%	14.4%	32.2%	20.0%	21.1%
5. 貴組織內的員工均被告知遵循 PIMS 政策，且了解在組織中自我的責任歸屬。	11.1%	14.4%	33.3%	20.0%	21.1%
6. 貴組織有提供實作 PIMS 所需的資源。	10.0%	21.1%	31.1%	31.1%	6.7%
7. PIMS 是否有融入組織文化中，成為貴組織核心價值的一部分。	8.9%	20.0%	34.4%	23.3%	13.3%

表 4-23：實行與運作構面問項統計表

	尚未考慮	考慮中	規劃中	部分完成	完全達成
8. 貴組織的高階主管負責管理 PIMS，且有最佳實務顯示有遵循個資法。	13.3%	18.9%	28.9%	24.4%	14.4%
9. 貴組織有依照組織規模和處理個人資料之性質指派員工負起遵循 PIMS 政策的責任。	8.9%	18.9%	30.0%	26.7%	15.6%
10. 貴組織有推派代表在跨部門處理個人資料時，識別個人資料是否屬於高風險。	13.3%	15.6%	30.0%	26.7%	14.4%
11. 貴組織有明確的定義個人資料中有哪些資料是屬於高風險類別。	12.2%	12.2%	27.8%	35.6%	12.2%
12. 貴組織有舉辦教育訓練與意識提升,確保所有員工都能夠按照適當程序處理個人資料。	8.9%	13.3%	25.6%	34.4%	17.8%
13. 貴組織有對於處理個人資料的程序做過風險評估。	13.3%	11.1%	34.4%	31.1%	10.0%
14. 貴組織的 PIMS 能隨時維持在最新的狀態。	13.3%	16.7%	32.2%	28.9%	8.9%
15. 貴組織的 PIMS 有觸發通知的程序和確保能得到最新且準確的通知。	13.3%	15.6%	35.6%	26.7%	8.9%
16. 貴組織能確保個人資料受到公平合法的處理,且在開始處理前已清楚確認處理個人資料的法律基礎。	10.0%	16.7%	26.7%	34.4%	12.2%
17. 貴組織有具體指明處理個人資料之目的，且不用於目的外用途。	11.1%	11.1%	24.4%	32.2%	21.1%
18. 貴組織確保 PIMS 在蒐集和處理個人資料的適當性、相關性和不過度。	10.0%	13.3%	23.3%	36.7%	16.7%
19. 貴組織的 PIMS 能確保個人資料的完整性與正確性。	10.0%	13.3%	24.4%	33.3%	18.9%
20. 貴組織的 PIMS 有銷毀過期（或是不在保存範圍內）之個人資料。	8.9%	13.3%	32.2%	31.1%	14.4%
21. 貴組織的 PIMS 包含當處理個人資料時尊重當事人之意見，以及出現爭議時提供申訴管道之程序。	14.4%	14.4%	35.6%	23.3%	12.2%
22. 貴組織有實施適當技術或擬訂安全措施保護個人資料，防止遺失、損壞、擅自處理或非法處理。	6.7%	12.2%	22.2%	44.4%	14.4%
23. 貴組織能確保跨國個人資料轉移或處理有適當的保護措施。	5.6%	10.0%	26.7%	43.3%	14.4%
24. 貴組織與第三方合作時，能確保個人資料揭漏處於被管制的狀態。	7.8%	12.2%	23.3%	42.2%	14.4%
25. 能確保當其他組織代表貴組織管理個人資料的處理程序有遵循個資法。	7.8%	15.6%	33.3%	34.4%	8.9%
26. 貴組織的 PIMS 有定期維護，確保程序與技術元件的正確及能適當運作。	12.2%	14.4%	34.4%	22.2%	16.7%

表 4-24：監督與審查構面問項統計表

	尚未考慮	考慮中	規劃中	部分完成	完全達成
27. 貴組織有舉行內部稽核來監控及審查 PIMS 的有效性及效率。	8.9%	16.7%	36.7%	20.0%	17.8%
28. 貴組織內部稽核時，能為客觀及公正的稽核工作計畫挑選適當的稽核員。	6.7%	14.4%	27.8%	27.8%	23.3%
29. 貴組織有定期進行內部稽核且將稽核報告提供給管理層。	7.8%	12.2%	20.0%	27.8%	32.2%
30. 貴組織應定期或週期性審查 PIMS，當發生重大變更，應確保制度的可用性、充分性和有效性。	11.1%	14.4%	34.4%	23.3%	16.7%

表 4-25：改善構面問項統計表

	尚未考慮	考慮中	規劃中	部分完成	完全達成
31. 貴組織有防止潛在不符合事項發生的措施。	5.6%	11.1%	21.1%	46.7%	15.6%
32. 貴組織有定期進行風險評估，以確定立場是否改變和不符合事項是否需要矯正。	6.7%	11.1%	20.0%	35.6%	26.7%
33. 貴組織有持續透過預防和矯正措施來改善 PIMS。	8.9%	14.4%	31.1%	31.1%	14.4%

4.5 基本資料與四個構面差異分析

4.5.1 組織是否通過ISO 27001差異分析

為檢驗基本資料中「組織是否通過ISO 27001」與BS 10012 PDCA四大構面是否產生顯著差異。本研究使用單因子變異數(One-Way ANOVA)分析。分析結果，問卷33題問項中,6題問項與組織通過ISO 27001沒有顯著差異(顯著性>0.05)，分析結果請參照表4-26(僅列出無顯著差異部分)。

「規劃」構面中，唯一無顯著差異的控制措施—「PIMS是否有融入組織文化中，成為貴組織核心價值的一部分。」，顯示無論是否有通過ISO 27001的組織，個人資訊管理制度要融入到組織文化之中，沒有差異，可能因為ISO 27001的條文中，沒有控制措施指明組織制度與組織文化需融合，故通過ISO 27001在BS 10012此控制措施中，沒有顯著的差異。

「實行與運作」構面中，四項問項無顯著差異；「貴組織的高階主管負責管理PIMS，且有最佳實務顯示有遵循個資法。」、「貴組織有具體指明處理個人資料之目的，且不用於目的外用途。」、「貴組織確保PIMS在蒐集和處理個人資料的適當性、相關性和不過度。」及「貴組織的PIMS有銷毀過期（或是不在保存範圍內）之個人資料。」等控制措施中，由於BS 10012的PIMS與ISO 27001的ISMS所強調保護之資料屬性略有不同，有些控制措施是針對個資的處理做規範，比ISMS規範還要更仔細，故造成通過ISO 27001在「實行與運作PIMS」構面中部分控制措施無顯著差異。

「監督與審查」構面中，唯一無顯著差異的控制措施—「貴組織內部稽核時，

能為客觀及公正的稽核工作計畫挑選適當的稽核員。」，可能因為BS 10012與ISO 27001保護資料的目標不同，稽核員挑選沒有顯著差異。

整體上，「組織是否通過ISO 27001」與本研究問卷調查，81.8%的問項與通過ISO 27001有顯著差異。 可能因為ISO 27001的控制措施(A.15.1.4)「個人資訊的資料保護與隱私」中，有要求確保個人資訊的保護，且在ISO 27001的控制措施(A.11)存取控制的規範中，與BS 10012的「實行與運作」構面的控制措施有相似之規範，因此讓許多問項與「組織是否通過ISO 27001」有顯著差異。

表 4-26：與「通過 ISO 27001」無顯著差異問項

構面	無顯著差異問項	顯著性
規劃	**7.** PIMS 是否有融入組織文化中，成為貴組織核心價值的一部分。	0.104
實行與運作	**8.** 貴組織的高階主管負責管理 PIMS，且有最佳實務顯示有遵循個資法。	0.100
	17. 貴組織有具體指明處理個人資料之目的，且不用於目的外用途。	0.131
	18. 貴組織確保 PIMS 在蒐集和處理個人資料的適當性、相關性和不過度。	0.161
	20. 貴組織的 PIMS 有銷毀過期（或是不在保存範圍內）之個人資料。	0.097
監督與審查	**28.** 貴組織內部稽核時，能為客觀及公正的稽核工作計畫挑選適當的稽核員。	0.065

4.5.2 受訪者職位差異分析

受訪者職位與本研究問項做單因子變異數分析，研究主管層級與資訊部門人員是否有顯著差異，僅一題問項有顯著差異(顯著性<0.05)。

在「監督與審查」構面中的問項「貴組織應定期或週期性審查 PIMS，當發生重大變更，應確保制度的可用性、充分性和有效性」(顯著性 0.047)有顯著差異，可能因為組織內部已經開始規劃週期性的審查 PIMS，在未定案之前，主管尚未公告給資訊人員知道，所以造成顯著差異。

整體上，97.9%的問項與受訪者職位沒有顯著差異，本研究的研究推論可代表組織現況，研究結果不會因為職位不同而有顯著差異。

4.6 比較各組織與整體落差分析

● 「規劃」構面之落差(表4-27)：

本研究顯示「電信業」64.29%完全達成的比例最高，可見電信業者對於個人資料保護重視，能夠有這麼高的完全達成度，是累積而來，非一蹴可幾。

落後於整體平均的組織有「IT製造業」與「學校及研究機構」，但「IT製造業」的「完全達成」比例僅落後「考慮中」的2.38%，呈現兩極化的情況，主要原因為IT製造業受訪者組織資本額大小兩極化，資本額較小的組織對於規劃PIMS仍較多處於考慮中的情況，但另一方面資本額較大的組織對PIMS的規劃是較重視與支持，應該是組織內部提供較多資源發展PIMS的因素，造成此落差情況；「學術及研究機構」會落後於整體，顯示學術領域對於個資保護制度的規劃完成度不高，需要再加強，否則規劃部分不完善，個資法實行後將面臨的風險非常大。

表 4-27：各組織「規劃」構面統計表

選項		尚未考慮	考慮中	規劃中	部分完成	完全達成
政府部門	統計數	5	33	61	32	2
	百分比	3.76%	24.81%	45.86%	24.06%	1.50%
資訊服務業	統計數	20	32	37	23	28
	百分比	14.29%	22.86%	26.43%	16.43%	20.00%
金融業	統計數	10	18	40	20	10
	百分比	10.20%	18.37%	40.82%	20.41%	10.20%
電信業	統計數	0	0	2	3	9
	百分比	0.00%	0.00%	14.29%	21.43%	64.29%
IT 製造業	統計數	6	14	7	2	13
	百分比	14.29%	33.33%	16.67%	4.76%	30.95%
國營公用事業	統計數	0	0	8	6	0
	百分比	0.00%	0.00%	57.14%	42.86%	0.00%
學校及研究機構	統計數	6	17	11	8	7
	百分比	12.24%	34.69%	22.45%	16.33%	14.29%
非營利組織	統計數	0	0	12	7	2
	百分比	0.00%	0.00%	57.14%	33.33%	9.52%
醫療生技業	統計數	1	4	3	11	2
	百分比	4.76%	19.05%	14.29%	52.38%	9.52%
通路物流業	統計數	0	6	19	7	3
	百分比	0.00%	17.14%	54.29%	20.00%	8.57%
其他	統計數	16	3	2	22	20
	百分比	25.40%	4.76%	3.17%	34.92%	31.75%

● 「實行與運作」構面之落差(表 4-28)：

「電信業」領先各業，「其他」組織在此構面，呈現兩極化，「完全達成」及「尚未考慮」分別佔第一、第二多的百分比，

資本額大的組織與「顧問業」對於個人資料將對組織帶來的衝擊有較深的了解，故實際的保護動作較積極，完全達成比例相對的高。

「學校及研究機構」在實行與運作的構面落後於整體，顯示學術界在個人資訊管理制度上還有很大的進步空間，應該做的個資保護措施還有很多。

表 4-28：各組織「實行與運作」構面統計表

選項		尚未考慮	考慮中	規劃中	部分完成	完全達成
政府部門	統計數	18	74	132	125	12
	百分比	4.99%	20.50%	36.57%	34.63%	3.32%
資訊服務業	統計數	60	56	101	93	70
	百分比	15.79%	14.74%	26.58%	24.47%	18.42%
金融業	統計數	18	27	98	104	19
	百分比	6.77%	10.15%	36.84%	39.10%	7.14%
電信業	統計數	0	0	2	14	22
	百分比	0.00%	0.00%	5.26%	36.84%	57.89%
IT 製造業	統計數	18	10	21	35	26
	百分比	16.36%	9.09%	19.09%	31.82%	23.64%
國營公用事業	統計數	0	0	23	15	0
	百分比	0.00%	0.00%	60.53%	39.47%	0.00%
學校及研究機構	統計數	14	39	34	39	7
	百分比	10.53%	29.32%	25.56%	29.32%	5.26%
非營利組織	統計數	0	0	34	19	4
	百分比	0.00%	0.00%	59.65%	33.33%	7.02%
醫療生技業	統計數	1	12	10	26	8
	百分比	1.75%	21.05%	17.54%	45.61%	14.04%
通路物流業	統計數	4	9	30	40	10
	百分比	4.30%	9.68%	32.26%	43.01%	10.75%
其他	統計數	47	14	11	41	58
	百分比	27.49%	8.19%	6.43%	23.98%	33.92%

● 「監督與稽核」構面之落差(表 4-29)：

本研究顯示，在此構面各組織平均完成度都在「規劃中」之上，與基本資料的「組織加強防止個資外洩的方式」調查中最高比例為「加強內部稽核」的統計結果相證，組織期望透過內部稽核找出組織能夠改善個資保護之處。各組織不論規劃、實作PIMS的完成度如何，對於稽核PIMS構面的控制措施都相當的重視。

● 「改善」構面之落差(表 4-30)：

除了「學校及研究機構」落後於整體外，「國營公用事業」與「通路物流業」在「規劃中」的比例較高，雖略遜於整體平均的「部分完成」，但「考慮中」、「尚未考慮」的比例很小，顯示這兩組織雖在此構面起步較其他組織慢，但都很重視且正在進步中。

表 4-29：各組織「監督與稽核」構面統計表

選項		尚未考慮	考慮中	規劃中	部分完成	完全達成
政府部門	統計數	2	13	33	20	8
	百分比	2.63%	17.11%	43.42%	26.32%	10.53%
資訊服務業	統計數	10	11	19	24	16
	百分比	12.50%	13.75%	23.75%	30.00%	20.00%
金融業	統計數	3	11	18	14	10
	百分比	5.36%	19.64%	32.14%	25.00%	17.86%
電信業	統計數	0	0	0	1	7
	百分比	0.00%	0.00%	0.00%	12.50%	87.50%
IT 製造業	統計數	4	4	1	6	9
	百分比	16.67%	16.67%	4.17%	25.00%	37.50%
國營公用事業	統計數	0	0	7	0	1
	百分比	0.00%	0.00%	87.50%	0.00%	12.50%
學校及研究機構	統計數	3	8	9	6	2
	百分比	10.71%	28.57%	32.14%	21.43%	7.14%
非營利組織	統計數	0	0	8	2	2
	百分比	0.00%	0.00%	66.67%	16.67%	16.67%
醫療生技業	統計數	0	0	0	8	4
	百分比	0.00%	0.00%	0.00%	66.67%	33.33%
通路物流業	統計數	0	2	11	2	5
	百分比	0.00%	10.00%	55.00%	10.00%	25.00%
其他	統計數	9	3	1	6	17
	百分比	25.00%	8.33%	2.78%	16.67%	47.22%

表 4-30：各組織「改善」構面統計表

選項		尚未考慮	考慮中	規劃中	部分完成	完全達成
政府部門	統計數	0	9	18	22	8
	百分比	0.00%	15.79%	31.58%	38.60%	14.04%
資訊服務業	統計數	7	6	14	24	9
	百分比	11.67%	10.00%	23.33%	40.00%	15.00%
金融業	統計數	1	6	8	21	6
	百分比	2.38%	14.29%	19.05%	50.00%	14.29%
電信業	統計數	0	0	0	3	3
	百分比	0.00%	0.00%	0.00%	50.00%	50.00%
IT 製造業	統計數	3	2	2	3	8
	百分比	16.67%	11.11%	11.11%	16.67%	44.44%
國營公用事業	統計數	0	0	3	2	1
	百分比	0.00%	0.00%	50.00%	33.33%	16.67%
學校及研究機構	統計數	2	6	9	4	0
	百分比	9.52%	28.57%	42.86%	19.05%	0.00%
非營利組織	統計數	0	0	3	4	2
	百分比	0.00%	0.00%	33.33%	44.44%	22.22%
醫療生技業	統計數	0	0	0	8	1
	百分比	0.00%	0.00%	0.00%	88.89%	11.11%
通路物流業	統計數	0	1	7	3	4
	百分比	0.00%	6.67%	46.67%	20.00%	26.67%
其他	統計數	6	3	1	8	9
	百分比	22.22%	11.11%	3.70%	29.63%	33.33%

4.7 研究發現

1. 在受訪者組織類別部分(表4-1)，資訊服務業(22.2%)、政府部門(21.1%)、金融業(15.6%)三者佔全部受訪者的58.9%。政府部門工作常需要經手民眾個人資料，金融業則握有許多客戶的個人資料，在個資法通過後，此兩類組織將面臨更嚴格的法律規範，故受訪者藉參加此類型年會，掌握最新國際標準，強化組織內部個人資訊管理制度上的不足。另一方面，個資法的通過，對於資訊服務業來說，是一項很大的商機，可能藉參加此類型年會掌握客戶最新因應個資法通過後的需求，在受訪者是否了解PIMS部分(表4-11)，選擇「了解PIMS」的受訪者中，「資訊服務業」佔33.3%(表4-12)，印證顯示資訊服務業受訪者中，有些組織已了解PIMS，來參加年會為更了解國際標準與脈動，往後提供客戶個資保護解決方案。
2. 在個資法通過後，當組織不慎洩漏客戶個人資料時，受訪者覺得對組織造成的最大衝擊部分(表4-13)，「商譽受損」(51.1%)佔最多；選擇「須自行舉證」(25.6%)的受訪者中，「中小企業」(34.8%)與「非營利事業」(43.5%)兩者佔78.3%(表4-14)，顯示人力與資源的利用在較小彈性情況下，對於不慎洩漏個資的衝擊，中小企業與非營利事業須自行舉證的困擾更甚於商譽受損。
3. 在個資法通過後，在電腦應用系統方面，受訪者組織考慮採用下列最主要的方式防止個人資料的外洩部分(表4-15)，「加強內部稽核」佔32.2%，但資本額「一億元以下」的中小企業43.8%選擇「再購買資安設備加強系統之監督與稽核」(表4-16)，顯示中小企業目前對於主要防止個資外洩的方式較偏好於購買現成的資安設備來防止個人資料外洩，也顯示著個資法通過後將帶來的商機。
4. 在受訪者組織是否通過 ISO 27001 部分(表 4-9)，58.9%已通過 ISO 27001；組織類別與通過 ISO 27001 交叉分析 (表4-10)顯示有顯著相關(P-value = 0.012)，主要因為政府部門與金融業主管機關有鼓勵導入 ISO 27001 認證的資安政策，故通過認證的受訪者較多；另一方面，「資訊服務業」通過的比例呈現兩極化，因為資訊服務業的受訪者中，有 50%是中小企業，由於導入 ISO 27001 的成本高，故中小企業較難承擔導入的成本，資訊服務業通過 ISO 27001 認證的受訪者組織，都屬於較大型的資訊服務公司。
5. 深入分析「規劃」構面的問項(表4-22)，發現在「貴組織由高階主管負責維護PIMS政策，並表態支持。」、「貴組織PIMS政策有說明需承諾遵守國內個資法。」及「貴組織內的員工均被告知遵循PIMS政策，且了解在組織中自我的責任歸屬。」三題問項中，「完全達成」的比例皆超過20%，另一方面，「貴組織有依照發展、實行、維護和持續改善等步驟將PIMS文件化。」及「貴組織有提供實作PIMS所需的資源。」這兩題問項中，「完全達成」的比例皆低於10%，呈現兩極化，顯示目前各組織十分積極規劃組織的PIMS政策，完全達成度高，但將組織所規劃的PIMS政策、實行步驟等文件化，受訪者組織的完成進度略慢，可能因為個資法通過不到一年，各組織還沒編列提供實作PIMS所需的資源，故造成「規劃」構面問項「完全達成」的比例不高。
6. 分析「實行與運作」構面問項(表4-23)，發現「貴組織有具體指明處理個人資料之目的，且不用於目的外用途。」問項中，「完全達成」的比例達21.1%，另一方面，在「能確保當其他組織代表貴組織管理個人資料的處理程序有遵循個資法。」問項的調查結果，「完全達成」的比例僅8.9%，顯示各組織在個資法通過後，處理個人資料時，相當注重具體的指明個資使用目的以遵循法律規範，才能有如此高的完全達成率，但關於其他組織代表處理個資時，目前還未有一個

公信驗證，故要確保其他組織如同自身一樣遵循個資法，是較難完全達成的部分。

7. 「實行與運作」構面上與「規劃」構面完成度比較(表4-21)，會發現「部分完成」的比例前者比後者高，顯示受訪者組織對於PIMS的實作可能不是從零開始，部分受訪者組織可能接續組織已存在的制度、系統來做加強，轉變為PIMS的一部分，此為讓「實行與運作」構面部分完成的比例偏高的原因。
8. 分析「監督與審查」構面，「舉行PIMS內部稽核」(36.7%)及「確保PIMS發生重大變更時可用性、充分性和有效性」(34.4%)兩題問項統計中(表4-24)，受訪者選擇「規劃中」的比例最高，顯示針對PIMS的稽核，以往並未納入組織的內部稽核範圍，個資法的通過後，才將規劃把PIMS加入組織內部稽核的重點目標。
9. 分析「改善」構面，「組織有防止不符合事項的措施」(62.3%)及「定期進行風險評估」(62.3%)兩題問項，「部分完成」及「完全達成」兩者合計比例超過整體的60%，顯示現階段組織內部持續改善的行動周全， PIMS的PDCA週期能夠週而復始的循環下去，對於未來個資法實施細則公告後，PIMS能更快符合法律規範將有正面幫助。
10. 整體上，「組織是否通過ISO 27001」與本研究問卷調查，81.8%的問項與通過ISO 27001有顯著差異。 可能因為ISO 27001的控制措施(A.15.1.4)「個人資訊的資料保護與隱私」中，有要求確保個人資訊的保護，且在ISO 27001的控制措施(A.11)存取控制的規範中，與BS 10012的「實行與運作」構面的控制措施有相似之規範，因此讓許多問項與「組織是否通過ISO 27001」有顯著差異。
11. 「IT製造業」於「規劃」構面落後整體平均，但「IT製造業」的「完全達成」(30.95%)比例落後「考慮中」(33.33%)僅2.38%，呈現雙峰的情況，主要原因為IT製造業受訪者組織資本額大小兩極化，資本額較小的組織對於規劃PIMS仍較多處於考慮中的情況，但另一方面資本額較大的組織對PIMS的規劃則是較重視與支持，可能組織內部提供較多資源發展PIMS的原故，造成此落差情況。
12. 在「監督與稽核」構面 (表4-29)，各組織平均完成度都在「規劃中」之上，與基本資料的「組織加強防止個資外洩的方式」調查中最高比例為「加強內部稽核」(32.2%)的統計結果相證，多數受訪者組織期望透過內部稽核找出組織能夠改善個資管理制度之處。各組織不論規劃、實作PIMS的完成度如何，對於稽核構面的控制措施都相當的重視。
13. 「國營公用事業」(50%)與「通路物流業」(46.67%)在「改善」構面(表4-30)「規劃中」的比例較高，雖略遜於整體平均的「部分完成」，但兩者選擇「考慮中」、「尚未考慮」的比例很小，顯示這兩個組織雖在此構面起步較其他組織慢，但仍重視且正在進步中。
14. 電信業於BS 10012 PDCA四個構面當中，「完全達成」的比例相較於其他組織都是最高，顯示電信業已準備好個資法的來臨，做好較完整的準備。
15. 學校及研究機構與各組織比較，對於個資管理制度建置的完成度相對較低，受訪者在許多控制措施選擇「考慮中」比例仍佔大多數，因此還有很大的進步空間，能做的個資保護要點還有很多。

5. 結論與建議

5.1 結論

本研究有下列主要發現：

- 在個資法通過後，當組織不慎洩漏客戶個人資料時，受訪者覺得對組織造成的最大衝擊部分(表4-13)，「商譽受損」(51.1%)佔最多；選擇「須自行舉證」(25.6%)的受訪者中，「中小企業」(34.8%)與「非營利事業」(43.5%)兩者佔78.3%(表4-14)，顯示人力與資源的利用在較小彈性情況下，對於不慎洩漏個資的衝擊，中小企業與非營利事業須自行舉證的困擾更甚於商譽受損。
- 受訪者組織考慮採用最主要的方式防止

個人資料的外洩部分(表4-15),「加強內部稽核」佔32.2%，但資本額「一億元以下」的中小企業受訪者組織43.8%選擇「再購買資安設備加強系統之監督與稽核」(表4-16)，顯示中小企業目前對於主要防止個資外洩的方式較偏好於購買現成的資安設備來防止個人資料外洩，故個資法的通過，對於資訊服務業來說，是一項很大的商機。「資訊服務業」也藉參加此類型年會掌握客戶最新因應個資法通過後的需求，在受訪者是否了解PIMS部分(表4-11)，選擇「了解PIMS」的受訪者中，「資訊服務業」佔33.3%(表4-12)，印證顯示資訊服務業的受訪者組織中，有些組織已了解PIMS，來參加年會為更了解國際標準與脈動，往後提供客戶個資保護解決方案。

- 「實行與運作」構面上與「規劃」構面完成度比較(表4-21)，會發現「部分完成」的比例前者比後者高，顯示受訪者組織對於PIMS的實作可能不是從零開始，部分受訪者組織可能接續組織已存在的制度、系統來做加強，轉變為PIMS的一部分，讓「實行與運作」構面部分完成的比例偏高。加上「組織是否通過ISO 27001」與本研究問卷調查，81.8%的問項與通過ISO 27001有顯著差異。可能因為ISO 27001的控制措施(A.15.1.4)「個人資訊的資料保護與隱私」中，有要求確保個人資訊的保護，且在ISO 27001的控制措施(A.11)存取控制的規範中，與BS 10012的「實行與運作」構面的控制措施有相似之規範，因此讓許多問項與「組織是否通過ISO 27001」有顯著差異。
- 各組織 PIMS 優先加強構面建議(表5-1)：

表 5-1:對各組織 PIMS 優先加強構面之建議

類別	構面	加強原因
政府部門	實作與運行	此構面調查顯示「規劃中」比例最高，「部分完成」及「完全達成」的合計比例 37.95%，落後於整體平均的 46.24%，政府單位之業務須經手大量民眾個資，建議「規劃中」的控制措施盡早開始實作，讓民眾更有信心個資不外洩。
資訊服務業	規劃	此構面中，「尚未考慮」及「考慮中」的合計比例達 37.15%，相對高於資訊服務業其它三構面的比例，顯示在「規劃」構面的控制措施，仍有許多資訊服務業對於定義政策的部分還在觀望當中，建議有些控制措施還沒開始規劃的組織，能夠在參與此年會後，了解到 PIMS 的重要性，盡早開始作規劃。
金融業	規劃	「規劃」構面「完全達成」與「部分完成」的合計比例僅 30.61%，金融業手握大量客戶的個資，對於個資外洩的警覺須更高於其他組織，建議加快完成的腳步，盡早將控制措施完成。
電信業	改善	電信業於 PDCA 四個構面，相較於其他組織「完全達成」的比例都是最高，顯示電信業已積極準備好個資法的來臨，建議能再加強「改善」構面，因「部分完成」與「完全達成」各佔 50 %，如能完全達成，PIMS 的 PDCA 循環將更完善。
IT 製造業	規劃	「IT 製造業」於「規劃」構面落後整體平均，但「IT 製造業」的「完全達成」(30.95%)比例僅落後「考慮中」(33.33%)2.38%，呈現雙峰的情況，主要原因為 IT 製造業受訪者組織資本額大小兩極化，資本額較小的組織對於「規劃」構面仍較多處於「考慮中」的情況，建議資本額較小的組織，可盡快轉變「考慮中」為「規劃中」，及早規劃才能對個資法實施的來臨及早做好準備，降低風險。
國營公用事業	監督與審查	此構面「完全達成」與「部分完成」的合計比例(12.5%)遠低於其他組織，主要集中在「規劃中」(87.5%)，建議盡快導入控制措施，讓組織個人資訊管理制度的有效性及效率有受到監督與審查。

學校及研究機構	改善	學校及研究機構與各組織比較，對於個資保護制度建置的完成度相對較低，受訪者在許多控制措施選擇「考慮中」的比例仍佔大多數，因此還有很大的進步空間，應該做的個資保護還有很多。尤其建議「改善」構面的控制措施要優先加強，因「完全達成」與「部分完成」的合計比例僅 19.05%遠低於其他組織的合計比例。
非營利組織	監督與審查	此構面「完全達成」與「部分完成」的合計比例(33.34%)較低，主要集中在「規劃中」(66.66%)，建議盡快導入控制措施，讓組織個人資訊管理制度的有效性及效率有受到監督與審查。
醫療生技業	實行與運作	醫療生技業於四個構面「完全達成」與「部分完成」合計比例都僅次於電信業優秀，則可加強之處在「實行與運作」構面，因控制措施在「考慮中」(21.05%)的比例相較於其他三構面，較偏高，醫療生技業也會常經手大量的個人病歷等敏感性個資，比一般個資風險還要大，建議盡快轉變「考慮中」為「規劃中」，減少個資法對組織帶來的衝擊。
通路物流業	規劃	「規劃」構面「完全達成」與「部分完成」合計比例28.57%，主要集中在「規劃中」(54.29%)，建議盡快轉變「考慮中」為「規劃中」，及早規劃才能對個資法實施的來臨及早做好準備，降低風險。。

5.2 建議

對未來研究有以下建議：

- 本論文只針對個資法通過後作研究，但個資法施行細則尚未公布，後續研究可以在個資法實施後，再針對各組織類別作調查，研究各組織個資管理制度前後之差異。
- 未來研究可採用 BS 10012 為基礎，在個資法實施後，做不同組織類別的個案研究。
- 未來個資法實施後，可與國外個資法(譬如日本 JPIPA[12] 、英國 DPA[16])比較，研究各組織面臨的衝擊與改變是否有所差異。

致謝

特別感謝 BSI 蒲樹盛副總經理的大力幫忙，給本論文這麼好的機會在 BSI 盛大年會中，發放論文所需要的調查問卷，也非常感謝 BSI 全體人員的協助，非常感謝 BSI。

參考文獻

[1] 中華民國國家資訊基本建設產業發展協進會 NII，〝2007 台灣網路安全信心調查〞，網址：http://als.org.tw/article/new_paper_sg.asp?id=168，上網日期：2010 年 12 月。

[2] 台灣綜合研究院，〝中小企業定義〞，網址：http://www.tri.org.tw/ceo/，上網日期：2010 年 12 月。

[3] 行政院金管會，〝玉山銀行網路銀行資訊安全管理缺失處分案〞，網址：http://www.banking. gov.tw/ Layout/main_ch/News_NewsContent.aspx?NewsID=41372，上網日期：2010 年 12 月。

[4] 行政院法務部，〝個人資料保護法〞，網址：http://law.moj.gov.tw/LawClass/LawContent.aspx?pcode=I0050021，上網日期： 2010 年 10 月。

[5] 行政院法務部，〝電腦處理個人資料保護法〞，http://law.moj.gov.tw/LawClass/LawContent.aspx?pcode=I0050021，上網日期：2010 年 12 月。

[6] 李振瑋、江耀國，〝英國資料保護法中資料所有人權力之研究—兼論我國個資法之相關規範及案例〞，*中原財經法學報*，第二十四期，頁 29-84，2010 年 6 月。

[7] 翁清坤，〝論個人資料保護標準之全球化〞，*東吳法律學報*，第二十二期，頁 1-60，2010 年 7 月。

[8] 郭戎晉，〝國際個人資料保護制度鳥瞰〞，網址：http://gcis.nat.gov.tw/ec/knowledge/notes/doc_download.asp?DocID=1137，上網日期：2010 年 3 月。

[9] 張毓仁，〝新版個資法之影響與商機〞，

網址：http://mic.iii.org.tw/aisp/reports/reportdetail2.asp?sesd=685865671&docid=CDOC20100601006&doctype=RC&cate=&smode=1&countrypno，上網日期：2010 年 12 月。

[10] 曾淑惠，〝以 BS 7799 為基礎評估銀行業資訊安全環境〞，碩士論文，淡江大學資訊管理學系，2002。

[11] 蒲樹盛，〝創新科技環境下的資訊管理重點雲端資訊安全、個資隱私保護、營運持續服務〞，*中華民國品質學會月刊*，第 46 卷，第 7 期，頁 22-25，2010 年 7 月。

[12] Alston & Bird, "Japan's Personal Information Protection Act and its Key Guidelines to be Revised," *Asia-Pacific E-Commerce & Privacy Forum Policy Advisory*, 2006.

[13] APEC, "APEC Privacy Framework," http://www.ag.gov.au/www/agd/rwpattach.nsf/VAP/(03995EABC73F94816C2AF4AA2645824B)~APEC+Privacy+Framework.pdf/$file/APEC+Privacy+Framework.pdf, accessed 2011/1.

[14] BS 10012, "Data Protection - Specification for a Personal Information Management System, British Standards Institution," 2009.

[15] BSI Group, "Data Dilemma: One in Five Businesses Admit Breaching the Data Protection Act," http://www.bsigroup.com/About-BSI/ News-Room/BSI-News-Content/Disciplines/Information-Management/BS-10012-publication/, accessed 2011/1.

[16] ICO, "The Principles of the Data Protection Act in Detail," http://www.ico.gov.uk/upload/documents/library/data_protection/practical_application/the_guide_to_data_protection.pdf, accessed 2011/2.

[17] ISO/IEC 27001, "Information Technology – Security Techniques – Information Security Management Systems – Requirements," 2005.

[18] W. Jones, "Personal Information Management," *Annual Review of Information Science and Technology*, Vol. 41, Issue 1, 2007, pp. 453–504.

[19] L. Korba, "Privacy in Distributed Electronic Commerce," *Proceedings of the 35th Hawaii International Conference on System Science (HICSS)*, Vol. 9, Hawaii, USA, Jan. 2002, pp. 306.

[20] W. Lusoli & R. Compañó, "From Security Versus Privacy to Identity: an Emerging Concept for Policy Design?" *Info*, Vol. 12, Emerald Group Publishing Limited, 2010, pp. 80–94.

[21] OECD, "OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data," http://www.oecd.org/document/18/0,3746,en_2649_34255_1815186_1_1_1_1,00.html, accessed 2011/1.

[22] J. Raman, "European Court of Human Rights: Failure to Take Effective Information Security Measures to Protect Sensitive Personal Data Violates Right to Privacy," *Computer Law & Security Report*, Vol. 24, Issue 6, July 2008, pp. 562-564.

[23] Wiki, "PDCA," http://en.wikipedia.org/wiki/PDCA, accessed 2010/12.