以BS 10012為基礎評估大專校院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

鄒宛璉
淡江大學資訊管理學系碩士班研究生
s698630091@mail.im.tku.edu.tw

摘要

根據趨勢科技於「2010上半年全球資安威脅報告」中指出，教育界在上半年所感染的惡意程式數量最多，幾乎有50%的感染出現於學校和大專院校，對擁有大量個人資料的學校而言，不僅會使校內個人資料外洩，造成校譽受損，更影響學校永續發展。因此本研究以「BS 10012個人資訊管理制度」之「規劃」、「實行與運作」、「監督與審查」、「改善」四構面作為參考，以了解目前大專校院的個人資訊管理制度。

研究發現若個人資料不慎外洩，64.6%的電算中心管理層認為校譽受損衝擊最大，多考慮再加強內部稽核。而目前大專校院的個人資訊管理制度，多處於「規劃」和「實行與運作」構面，對於「監督與審查」和「改善」構面較缺乏控管。若依地區劃分比較，各區域的學校在四構面中都無顯著差異，僅北區學校在職員的教育訓練表現較佳；若依電算中心專任職員人數規模劃分，10人以上的學校發展較佳。最後，本研究依大專校院落後的控制措施，提出改善建議。

關鍵詞：電腦處理個人資料保護法、個人資料保護法、個人資訊管理制度、BS 10012、PIMS。

1. 緒論

1.1 研究背景與動機

根據趨勢科技公布的「2010 上半年度全球資安威脅報告」中指出[13]，亞太地區所感染的惡意程式數量最多，位居第一。若依行業別劃分，2010 上半年度感染惡意程式數量最多的是教育界，幾乎有 50%的感染出現於學校和大專院校。而惡意程式的攻擊目標多為資料竊取，常是導致個人資料外洩的原因，對於擁有大量個人資料的學校而言，透過惡意程式其竊取資料的行為，不僅使校內個人資料外洩，更可能造成相關人員負上刑責、校譽受損，影響學校永續發展。

我國政府為維護個人資料的安全，於民國99年4月27日三讀通過「個人資料保護法」（以下簡稱個資法），但由於目前新版個資法施行細則尚未公布，國內也未有與個資相關的管理制度或驗證標準，因此本研究透過英國標準協會BSI所發佈之BS 10012：2009個人資訊管理制度(Personal Information Management System, PIMS)，作為校內落實個人資訊管理制度之參考，並搭配新版個資法之檢核，來達到適法性的要求。

1.2 研究目的

在個資法公告後，為因應將實施的個資法，本研究希望能了解各大專校院目前的個人資訊管理制度，進而達到下列目的：

- 了解各大專校院目前是否有在施行個人資訊管理制度及其現況。
- 分析在不同地區與不同電算中心人數規模下，各大專校院目前於個人資訊管理制度上的差異。
- 針對目前各大專校院個人資訊管理制度提出改善建議，以供日後改進之參考。

1.3 研究對象

因學校內電算中心之業務為維護全校資訊系統，接觸學生或教職員個人資料情況十分的頻繁，故研究對象以各大專校院電算中心主任為主，並調查電算中心各部

門組長和職員。

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、研究目的與研究對象，第二章為文獻探討，描述個資法及 BS 10012 之介紹，第三章為研究方法、問卷設計、問卷調查過程以及統計工具之說明。第四章為研究分析，依問卷樣本資料進行各種面向之分析，第五章為結論與建議，總結本研究之結果，並且對後續研究提出建議。

2. 文獻探討

2.1 個人資料保護法

2.1.1 立法背景

我國於民國 84 年公佈實施「電腦處理個人資料保護法」，是臺灣唯一一個針對個人資訊安全的法律規範。然而，時下利用電腦處理或傳遞個人資料情形普遍，此法早已不合時宜。因此我國政府彙整國內學者與實務界之建議，參考 APEC[16]和 OECD[22]的隱私權綱領，於民國 99 年三讀通過個資法。

2.1.2 修正要點

個資法共計 56 條，其修法重點如下：

- 擴大保護客體：個資法於第一條規定不再侷限於經電腦處理之個人資料[21]，並將較隱私的資料納入保護。而個人資料定義包括：自然人之姓名、出生年月日、國民身分證統一編號、護照號碼、特徵、指紋、婚姻、家庭、教育、職業、病歷、醫療、基因、性生活、健康檢查、犯罪前科、聯絡方式、財務情況、社會活動及其他得以直接或間接方式識別該個人之資料[2]。
- 擴大適用對象：以往電腦處理個人資料保護法只侷限於八大行業[3]；個資法於第二條規定適用對象不限行業、自然人、法人或其他團體[2]。
- 增加行為規範：個資法規定在蒐集個人資料時，需盡到告知的義務，且於第五條規定個人資料的蒐集或使用，都應正當合理並尊重當事人之權益，如：(1)告知蒐集資料之目的、利用方式、資料的類別…等；(2)取得當事人書面同意；(3)資料外洩時通知當事人…等[2]。
- 高額賠償金：個資法將賠償金額從以往的二千萬元提高為二億元。
- 加重刑責：以往電腦處理個人資料保護法只有意圖營利者才需負刑責，且需有確切證據[3]；個資法不論是否意圖營利皆處刑責，因此須自行舉證已盡保管責任[2]。

2.2 個人資訊管理制度

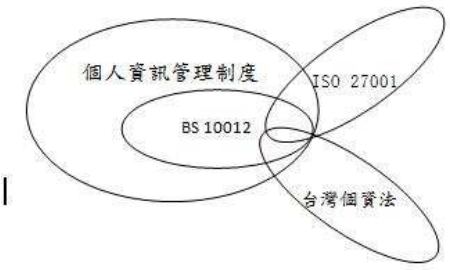

圖2-1：ISO 27001、BS 10012、個人資訊管理制度、個資法之四者關聯圖

個人資訊管理制度主要是透過結合國家的個資法和管理制度，進而達到保護個人資訊安全的目的，如英國BS 10012和日本JISQ 15001制度要求，皆可作為組織導入個人資訊管理制度之參考。而由圖2-1可知，ISO 27001資訊安全管理制度與個人資訊管理制度的主要差異在於，前者是管理組織內的資訊資產；後者是在保護個人資料，並能同時遵循法律規範[8]。因此導入個人資訊管理制度且通過驗證的組織，不僅能確保個人資料相關的業務流程受到妥善監控與保護外，也符合國家法規之要求。

2.3 BS 10012：2009 個人資訊管理制度

2.3.1 背景介紹

英國標準協會 BSI 於 2009 年 6 月正式公布 BS 10012，其內容主要是透過規劃（Plan）、實行與運作（Do）、監督與審查（Check）與改善（Act）的管理流程[12]，

具體說明各項資料保護之要求，是一套可依循的個人資訊管理框架。

2.3.2 內容介紹

BS 10012 內容分為 7 章，前三章為標準簡介、適用範圍與名詞定義，主要內容則按照 PDCA 順序編排在第 3 至 6 章[14]。以下簡述 PDCA 章節內容：

- 規劃：提供符合國家法規和實務之良好做法。先確立個人資訊管理制度的範圍與目標，再制定個人資訊管理政策，並由高階管理小組負責維護和支持，幫助職員盡速了解政策及其責任，並能提供資源，讓制度可長久發展，最終融入組織文化。
- 實行與運作：提供實作個人資訊管理制度的具體要求，包括：指派適當人員推行個人資訊管理政策、識別並記錄個人資料的用途及其風險、對職員進行個人資訊管理訓練…等多項目標。
- 監督與審查：透過監控及審查方式，確保組織內的個人資訊管理制度具有效性與效率。因此組織應制定稽核計畫，挑選適當人選作為稽核員，定期執行內部稽核，提供管理層稽核報告。且需定期進行管理審查，確保發生重大變化時，能維持個人資訊管理制度的可用性、充分性和有效性。
- 改善：實施矯正措施，改善個人資訊管理制度的有效性與效率。當個人資訊管理制度進行變更前，需先評估是否符合組織內部政策或國家相關法令之規定，持續透過稽核結果或其他方式，改善個人資訊管理制度之效益。

3.研究設計

3.1 研究方法

本研究採用資料蒐集方法中的調查研究法，以自填式問卷調查方式蒐集資料。

3.2 問卷設計

本研究問卷架構是以 BS 10012 標準為基礎，提出 33 項基本要求，作為問卷題項。而各章節的問項題數如表 3-1 所示。

表 3-1：各章節之問項題數

章節名稱	問項題數
規劃	7
實行與運作	19
監督與審查	4
改善	3
總數	33

本研究問卷各題答項皆以「完全達成」、「部份完成」、「規劃中」、「構思中」、「尚未考慮」來調查學校目前導入個人資訊管理制度的現況[10]。基本資料的部份則採用名目尺度作為衡量方式。各答項定義如下：

- 尚未考慮：此項控制措施目前尚未考慮。
- 構思中：已構思尚未規劃。
- 規劃中：已規劃尚未執行。
- 部份達成：此項控制措施已有部分執行。
- 完全達成：此項控制措施已完全執行。

3.3 統計方法與工具

本研究選用 SPSS Statistics 統計應用分析軟體進行統計分析，在考慮問項特性與研究需求後，採用的統計方法有敘述性統計分析、交叉分析、信度分析、因素分析與單因子變異數分析。

3.4 問卷調查過程

全國大專校院電算中心主任研討會，每年由教育部委託各大專院校電算中心輪流舉辦，今年度的研討會為元智大學承辦，於民國99年11月22日至23日舉行，研討會主題為「新世代校園資訊服務所面臨之挑戰與因應」[1]，其中也涵蓋了個資法相關講座。本研究問卷是由研討會報到處統一發放，於講座中場休息時間，現場進行回收，並致贈每位受訪者一份精美小禮物。

4.研究分析

4.1 問卷回收率分析

本研究問卷經元智大學電算中心范書愷資訊長同意後，調查於民國 99 年 11 月 22 日所舉辦的年度「全國大專校院電算中

心主任研討會」上發放。共發放 160 份問卷，總共回收 71 份，總回收率為 44.38%。扣除資料填寫不完整者 6 份，調查實際有效問卷為 65 份，實際有效回收率為 40.6%。

4.2 基本資料分析

在本研究中共有 65 份有效樣本，而這些樣本的分布情形如下：

- 受訪者職位分析：70.8%的多數受訪者職位為電算中心主管。總計共 92.3%受訪者職位是屬於管理層（含主管和組長），顯示此份問卷大部份是由管理階層負責填答（表 4-1）。

表 4-1：「受訪者職位」統計表

	樣本數	百分比%
電算中心主任/處長/資訊長	46	70.8
電算中心部門組長	13	20.0
其他部門主管	1	1.5
電算中心職員	3	4.6
其他	2	3.1
總計	65	100

- 電算中心專任職員人數分析：92.3%的受訪者所屬學校內，電算中心專任職員人數在 20 人以下佔多數。而其中又多集中於「10 人以下」，佔 63.1%（表 4-2）。

表 4-2：「電算中心專任職員人數」統計表

	樣本數	百分比%
10 人以下	41	63.1
11-20 人	19	29.2
21-30 人	3	4.6
31-40 人	0	0.0
41-50 人	1	1.5
51-60 人	0	0.0
61-70 人	0	0.0
71 人以上	1	1.5
總計	65	100

- 電算中心成立年數分析：73.8%受訪者所屬學校電算中心成立年數為20年以下。而其中又以成立了「11-20年」的電算中心居多，佔56.9%（表4-3）。

表 4-3：「電算中心成立年數」統計表

	樣本數	百分比%
10 年以下	11	16.9
11-20 年	37	56.9
21-30 年	13	20.0
31-40 年	2	3.1
41 年以上上	2	3.1
總計	65	100

- 是否通過第三方資安驗證分析：64.2%的受訪者所屬學校已有通過第三方資安驗證，17.9%目前正在進行驗證中。由於為加強教育單位人員的專業資訊安全技能，並落實校園資訊安全，因此教育部規定大專院校在2008年必須通過第三方資安認證。此外，為使各級學校能以低成本及時間，建構良好的資訊安全環境，因此教育部於2007年公布「教育體系資通安全管理規範」[7]。顯示教育部對於學校落實資訊安全制度的重視，透過導入相關管理標準和第三方驗證，確保校內實施的資安措施是有效的。而在此項調查中有2所學校同時通過「ISO27001」與「教育體系資通安全管理規範」，因此樣本數總計為67位（表4-4）。

表 4-4：「是否已通過第三方資安驗證」統計表

	樣本數	百分比%
ISO27001	18	26.9
教育體系資通安全管理規範	25	37.3
進行中	12	17.9
否	12	17.9
總計	67	100

- 個人資訊管理制度了解程度分析：0%受訪者對個人資訊管理制度「非常了解」，此是由於個資法的通過，使個人資訊管理更顯重要，但因個資法才通過不到一年的時間，且個人資訊管理制度是一套新標準，國內並無相關完善制度，因此對於詳細的規範與作法尚未能完全了解，也仍有18.5%受訪者選填「不了解」與 3.1%受訪者選填「完全不了解」（表 4-5）。

表 4-5：「個人資訊管理制度了解程度」統計表

	樣本數	百分比%
非常了解	0	0.0
了解	27	41.5
有些了解	24	36.9
不了解	12	18.5
完全不了解	2	3.1
總計	65	100

- 個人資料外洩對學校的衝擊分析：若個人資料不慎外洩，69.2%過半數受訪者認為「校譽受損」對學校造成的衝擊最大（表4-6）。且受訪者職位與對學校造成的衝擊交叉分析具有顯著相關（P-value=0.000），其中認為「校譽受損」對學校衝擊最大的受訪者，64.6%皆為電算中心管理層（表4-7）。顯示受訪者由其是電算中心管理層，普遍認為學校形象是靠長久累積而來，一旦個人資料外洩，將造成學校的形

象受損、招生率下降，而此不良的社會形象，也將影響學校的永續發展。其次，認為對學校造成的衝擊最大為 18.5%「賠償金額」(表 4-6)，此是由於個資法將罰鍰提高為二億元，對擁有上千筆甚至到上萬筆個人資料的學校而言，所承擔的風險不容小覷，一旦個人資料不慎外洩，將造成學校營運上的衝擊。

表 4-6：「對學校的衝擊」統計表

	樣本數	百分比%
校譽受損	45	69.2
賠償金額	12	18.5
招生率下降	1	1.5
須自行舉證	7	10.8
總計	65	100

表 4-7：受訪者職位與對學校的衝擊交叉表

受訪者職位		對學校造成的衝擊				總計
		校譽受損	賠償金額	招生率下降	須自行舉證	
電算中心主任/處長/資訊長	樣本數	34	9	0	3	46
	百分比	52.3%	13.8%	0.0%	4.6%	70.8%
電算中心部門組長	樣本數	8	3	0	2	13
	百分比	12.3%	4.6%	0.0%	3.1%	20.0%
其他部門主管	樣本數	1	0	0	0	1
	百分比	1.5%	0.0%	0.0%	0.0%	1.5%
電算中心職員	樣本數	2	0	0	1	3
	百分比	3.1%	0.0%	0.0%	1.5%	4.6%
其他	樣本數	0	0	1	1	2
	百分比	0.0%	0.0%	1.5%	1.5%	3.1%
總計	樣本數	45	12	1	7	65
	百分比	69.2%	18.5%	1.5%	10.8%	100%

- 防止個人資料外洩方式分析：56.9%受訪者所屬學校考慮採取防止個人資料外洩的方式為「加強內部稽核」(表 4-8)。且防止個人資料外洩方式與電算中心專任職員人數交叉分析具有顯著相關（P-value=0.048），可發現不論學校規模大小，多考慮採取「加強內部稽核」(表 4-9)。此是由於內部稽核成本較一般外部稽核來得低，能降低營運成本，並可透過檢查之方式確認內部控制是否有確實執行，能在合理管理成本下加強控制，因此考慮採用比例最高。其次，考慮採取防止方式為 27.7%「再購買資安設備，加強系統(含資料庫)之稽核與監督」，由於以往資安設備皆在加強內部系統之安全，而個資法通過後，主要是防止從資料庫外洩資料，因此部份學校考慮購買現成資安設備，加強監控資料的流向及其使用行為[15]。此外，0%的受訪者所屬學校選擇「維持現狀」，可見個資法所帶來的衝擊效應，各校皆認為有必要重新檢視校內的個人資料保措施，對目前的資安控制措施，都未能有滿足個資法規範的信心，因此皆考慮採取可行之防範措施，加強保護(表 4-8)。

表 4-8：「防止個人資料外洩方式：」統計表

	樣本數	百分比%
再購買資安設備加強系統(含資料庫)之稽核與監督	18	27.7
建立資料加解密機制	6	9.2
加強內部稽核	37	56.9
加強外部稽核	4	6.2
維持現狀	0	0.0
總計	65	100

表 4-9：專任職員人數與防止外洩方式交叉表

電算中心專任職員人數		防止個人資料外洩方式					總計
		再購買資安設備	建立資料加解密機制	加強內部監督	加強外部監督	維持現狀	
10 人以下	樣本數	12	3	23	3	0	41
	百分比	18.5%	4.6%	35.4%	4.6%	0.0%	63.1%
11-20 人	樣本數	4	3	12	0	0	19
	百分比	6.2%	4.6%	18.5%	0.0%	0.0%	29.2%
21-30 人	樣本數	1	0	2	0	0	3
	百分比	1.5%	0.0%	3.1%	0.0%	0.0%	4.6%
31-40 人	樣本數	0	0	0	0	0	0
	百分比	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%
41-50 人	樣本數	0	0	0	1	0	1
	百分比	0.0%	0.0%	0.0%	1.5%	0.0%	1.5%
51-60 人	樣本數	0	0	0	0	0	0
	百分比	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%
61-70 人	樣本數	0	0	0	0	0	0
	百分比	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%
71 人以上	樣本數	1	0	0	0	0	1
	百分比	1.5%	0.0%	0.0%	0.0%	0.0%	1.5%
總計	樣本數	18	6	37	4	0	65
	百分比	27.7%	9.2%	56.9%	6.2%	0.0%	100%

- 預計所需經費分析：在個資法公告後，44.6%學校已對施行個人資訊管理制度進行經費評估，期望能在可負擔的成本下，選擇最佳的保護方式（表 4-10）。且預計所需經費與防止個人資料外洩方式交叉分析具有顯著相關（P-value=0.029），選擇「加強內部稽核」防止個人資料外洩的學校，多數還在評估需投入多少經費。推估採取內部稽核的學校，因需加強職員對個人資料保護的認知，所以必須對職員進行相關訓練活動，將花費大量的成本及人力，因此多數學校尚在評估能提供多少經費。而已預計好所需經費的學校，多選擇為「再購買資安設備，加強系統(含資料庫)之稽核與監督」，加強電腦應用系統，達到防止個人資料外洩的目的（表 4-11）。再者，由於目前個資法施行細則尚未公布，為確保學校能完全符合法令規範，部份學校選擇等到個資法施行細則公布後，再進

行經費的評估，因此尚有 30.8%受訪者所屬學校「尚未評估」所需經費（表 4-10）。

表 4-10：「預計所需之經費」統計表

	樣本數	百分比%
尚未評估	20	30.8
評估中	29	44.6
100 萬元以下	7	10.8
100 萬元(含)-500 萬元	7	10.8
500 萬元(含)-1,000 萬元	2	3.1
1,000 萬元(含)以上	0	0.0
總計	65	100

表 4-11：預計所需經費與防止資料外洩方式交叉表

預計所需經費		防止個人資料外洩方式					總計
		再購買資安設備	建立資料加解密機制	加強內部監督	加強外部監督	維持現狀	
尚未評估	樣本數	5	0	13	2	0	20
	百分比	7.7%	0.0%	20.0%	3.1%	0.0%	30.8%
評估中	樣本數	4	4	19	2	0	29
	百分比	6.2%	6.2%	29.2%	3.1%	0.0%	44.6%
100 萬元以下	樣本數	4	0	3	0	0	7
	百分比	6.2%	0.0%	4.6%	0.0%	0.0%	10.8%
100 萬元-500 萬元	樣本數	5	2	0	0	0	7
	百分比	7.7%	3.1%	0.0%	0.0%	0.0%	10.8%
500 萬元-1,000 萬元	樣本數	0	0	2	0	0	2
	百分比	0.0%	0.0%	3.1%	0.0%	0.0%	3.1%
1,000 萬元(含)以上	樣本數	0	0	0	0	0	0
	百分比	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%
總計	樣本數	18	6	37	4	0	65
	百分比	27.7%	9.2%	56.9	6.2%	0%	100%

- 認為校務執行程序變得繁雜分析：共計有 93.9%受訪者所屬學校，「同意」或「非常同意」推行個資法所採取的相關因應措施，將會使校務執行程序變得更為繁雜。因為了要符合個資法的規範，校務程序必須重新被檢視，在資料處理的流程上需加入許多規範或是管控措施，且也會加強各職員的權責歸屬，因此普遍認為個資法的推行會使校務程序更為繁雜（表 4-12）。

表 4-12：「校務執行程序變得繁雜」統計表

	樣本數	百分比%
非常同意	28	43.1
同意	33	50.8
沒意見	4	6.2
不同意	0	0.0
非常不同	0	0.0
總計	65	100

- 舉辦職員教育訓練分析：44.6%受訪者所屬學校有舉辦職員的教育訓練或說明會，由於多數學校已了解個資法帶來的影響，因此有透過舉辦相關的訓練活動，向校內推廣個人資料保護意識，以加強職員在資訊安全方面的相關技能（表 4-13）。且職員教育訓練與對個人資訊管理制度了解程度交叉分析具有顯著相關（P-value=0.031），顯示有舉行職員訓練的學校，多數能達到其目的，受訪者對個人資訊管理制度已「了解」或「非常了解」（表 4-14）。僅 6.2%的受訪者所屬學校沒有舉辦職員的教育訓練（表 4-13）。

表 4-13：「舉辦職員教育訓練」統計表

	樣本數	百分比%
是	29	44.6
否	4	6.2
考慮中	32	49.2
總計	65	100

表 4-14：職員訓練與個人資訊管理制度了解程度交叉表

職員教育訓練		個人資訊管理制度了解程度					總計
		非常了解	了解	有些了解	不了解	完全不了解	
是	樣本數	0	17	7	5	0	29
	百分比	0.0%	26.2%	10.8%	7.7%	0.0%	44.6%
否	樣本數	0	1	1	1	1	4
	百分比	0.0%	1.5%	1.5%	1.5%	1.5%	6.2%
考慮中	樣本數	0	9	16	6	1	32
	百分比	0.0%	13.8%	24.6%	9.2%	1.5%	49.2%
總計	樣本數	0	27	24	12	2	65
	百分比	0.0%	41.5%	36.9%	18.5%	3.1%	100%

表 4-15：「學校所在區域」統計表

	樣本數	百分比%
北	26	40.0
中	11	16.9
南	20	30.8
東	4	6.2
離島	1	1.5
未填	3	4.6
總計	65	100

表4-16：學校所在區域與職員教育訓練交叉表

職員教育訓練		學校所在區域					總計
		北區	中區	南區	東區	離島	
是	樣本數	17	2	8	1	0	28
	百分比	27.4%	3.2%	12.9%	1.6%	0.0%	45.2%
否	樣本數	3	0	0	0	0	3
	百分比	4.8%	0.0%	0.0%	0.0%	0.0%	4.8%
考慮中	樣本數	6	9	12	3	1	31
	百分比	9.7%	14.5%	19.4%	4.8%	1.6%	50.0%
總計	樣本數	26	11	20	4	1	62
	百分比	41.9%	17.7%	32.3%	6.5%	1.6%	100%

- 學校所在區域分析：此次全國大專校院主任研討會，參與者 40.0%為「北部」學校的電算中心主管與職員（表 4-15）。且學校所在區域與職員教育訓練交叉分析具有顯著相關（P-value=0.034），27.4%的北區學校已有舉行職員教育訓練（表 4-16）。顯示北區學校對於職員是否具備對個資法的認知，與了解校內個人資訊管理制度相當重視，因此能較其他地區優先舉行職員訓練，並積極推動校內資料保護意識，透過教育訓練的方式，讓職員能了解個資法對學校以及個人所帶來的影響，以降低職

員因認知不足與疏失所造成的個人資料外洩事件。而其他地區的學校，對於是否舉行教育訓練或相關說明活動，多在「考慮中」，相對北區之發展較為緩慢。此項調查中有 4.6%的受訪者未填選此題問項（表 4-15）。

表4-17：區域與個人資訊管理制度了解程度交叉表

學校所在區域		個人資訊管理制度了解程度					總計
		非常了解	了解	有些了解	不了解	完全不了解	
北	樣本數	0	14	4	7	1	26
	百分比	0.0%	22.6%	6.5%	11.3%	1.6%	41.9%
中	樣本數	0	3	8	0	0	11
	百分比	0.0%	4.8%	12.9%	0.0%	0.0%	17.7%
南	樣本數	0	9	6	5	0	20
	百分比	0.0%	14.5%	9.7%	8.1%	0.0%	32.3%
東	樣本數	0	0	3	0	1	4
	百分比	0.0%	0.0%	4.8%	0.0%	1.6%	6.5%
離島	樣本數	0	1	0	0	0	1
	百分比	0.0%	1.6%	0.0%	0.0%	0.0%	1.6%
總計	樣本數	0	27	21	12	2	62
	百分比	0.0%	43.5%	33.9%	19.4%	3.2%	100%

- 學校所在區域與個人資訊管理制度了解程度交叉分析：學校所在區域與個人資訊管理制度了解程度交叉分析具有顯著相關（P-value=0.015），位於北區的學校，對個人資訊管理制度較「了解」(表4-17)。顯示北區因優先舉辦教育訓練，所以對個人資訊管理制度的了解，能比其他地區來好的。

4.3 效度分析

本研究以BS 10012標準為依據，設計33題問項，而此標準為多位專家設計而成，因此已具內容效度。且本研究針對「規劃」、「實行與運作」、「監督與審查」和「改善」四個流程進行因素分析，並使用直交轉軸的最大變異轉軸法。檢定結果KMO值分別0.873、0.919、0.833與0.773，皆大於0.7；Bartlett's球體檢定結果皆具顯著水準(P-value<0.001)，可進行因素分析。而本研究四個流程分別進行因素萃取，各萃取一個初始特徵值大於1的因素，所以無法解釋轉軸，並將因素分別命名為「規畫」、「實行與運作」、「監督與審查」和「改善」構面。而各因素負荷量皆大於0.6，總解釋變異量%皆在60%以上，均為不錯之結果。

4.4 信度分析

本研究採用 Crobach α 分析方法衡量各構面下問卷題項的一致性。根據Cronbach α值的意義，可知一般α係數 0.5~0.7 便可稱其具有信度，若 α 值愈大則可信度也愈高[11]。本研究問卷分成規畫、實行與運作、監督與審查、改善和整體五個部份，分別計算其信度（表 4-18），而本份問卷各構面與整體的α值皆在 0.9 以上，故本研究問卷具有十分良好的信度。

表 4-18：問卷信度表

測量構面	測量題數	Crobach α 係數
規劃	7	0.929
實行與運作	19	0.967
監督與審查	4	0.953
改善	3	0.952
整體	33	0.981

4.5 大專校院個人資訊管理制度整體現況分析

本研究問卷統計大專校院目前在個人資訊管理制度上之整體表現，分別算出四個構面中各答項佔全體總數之比例，與在四個構面中各自的比例（表 4-19），並探討四個構面中「完全達成」比例較高之問項（表 4-20 至表 4-23）。

- 整體現況分析（表 4-19）：目前大專校院在個人資訊管理制度中四個構面的發展，多處於規劃與實行階段，而在「規劃」和「實行與運作」構面的整體問項統計，發現目前受訪者學校的個人資訊管理制度中，多集中於「部份完成」與「規劃中」，其中又以「實行與運作」構面發展最佳，19.6%「部份完成」與 18.7%「規劃中」此兩答項佔全體比例較高，可能與原先已有存在相關的規範或資安制度，如：電腦處理個人資料保護法、ISO27001、教育體系資通安全管理規範…等制度。顯示目前大專校院有在因應個資法，也有施行部份管控措施，降低個人資料外洩風險，但是因為個資法施行細則尚未公布，國內也未有相關可依循的標準，因此在「實行與運作」構面的發展並未完善。而「監督與審查」與「改善」構面之整體比例較低，多處於「規劃

中」，發展較為落後，而「改善」構面更是四個構面中發展最為緩慢的，也顯示目前大專校院較缺乏此兩構面的控管，還有待加強。

表 4-19：個人資訊管理制度整體現況統計表

		完全達成	部分完成	規劃中	構思中	尚未考慮	總計
規劃	樣本數	41	160	134	98	22	455
	構面%	9.0%	35.2%	29.5%	21.5%	4.8%	100%
	整體%	1.9%	7.5%	6.2%	4.6%	1.0%	21.2%
實行與運作	樣本數	69	420	402	296	48	1235
	構面%	5.5%	34.0%	32.6%	24.0%	3.9%	100%
	整體%	3.2%	19.6%	18.7%	13.7%	2.3%	57.5%
監督與審查	樣本數	18	70	102	56	14	260
	構面%	6.9%	26.9%	39.2%	21.6%	5.4%	100%
	整體%	0.8%	3.3%	4.8%	2.6%	0.7%	12.2%
改善	樣本數	16	52	66	51	10	195
	構面%	8.2%	26.7%	33.8%	26.2%	5.1%	100%
	整體%	0.7%	2.4%	3.1%	2.4%	0.5%	9.1%
總計	樣本數	144	702	704	501	94	2145
	構面%	6.7%	32.8%	33.0%	23.2%	4.3%	100%
	整體%	6.6%	32.8%	32.8%	23.3%	4.5%	100%

以下深入探討各構面中特殊問項：

- 規劃構面分析（表 4-20）：深入分析在「部份完成」的問項，發現僅「貴校將定義個人資訊管理制度的範圍和規定個人資訊管理的目標。」此問項處於「規劃中」，其餘問項皆處於「部份完成」。顯示雖然大專校院以往有電腦處理個人資料保護法的規範，但因為個資法提高更多在個人資料保護方面的責任與義務，因此需要重新規劃保護範圍，並制定詳細的管理目標，所以多數受訪者學校目前還在規劃中。

深入分析在「完全達成」的問項，發現「貴校將由高階主管負責維護個人資訊管理政策，並表態支持。」，以及「貴校個人資訊保護政策將說明需承諾遵守國內個資法。」此兩問項中，「完全達成」比例遠比其餘問項在「完全達成」比例高，皆超過10%，而其餘問項皆低於10%。推估是因為在一般資訊安全環境的建置中，需由高階主管帶領組織，擴及至所有職員，所以高階主管的支持與具備較高的資訊安全意識，如能較快了解個資法及其衝擊，對於學校在資訊安全的活動，可以帶來正面的影響。且從以往資安政策相關的研究中可知，若獲得高階主管的支持，在資安政策推動上也會較為成功[20]。

再者，深入分析在「尚未考慮」的問項，發現「貴校內的職員將被告知遵循個人資訊管理政策，且了解在組織中自我的責任歸屬。」此問項調查結果中，「尚未考慮」之比例為0%，為本構面在「尚未考慮」此答項中，比例最低之問項。可見各校皆認為告知職員遵守個資法，除了有助於「規劃」構面的發展外，重要的是能強化職員了解與工作相關的個人資料保護規範，及其職責，因此是必要施行的措施[18]。

- 實行與運作構面分析（表 4-21）：深入分析在「完全達成」的問項，發現 15.4%「貴校與第三方合作時，將能確保個人資料揭漏處於被管制的狀態。」、12.3%「貴校將具體指明處理個人資料之目的，且不用於目的外用途。」，以及 10.8%「貴校的個人資訊管理制度將有銷毀過期（或是不在保存範圍內）之個人資訊。」此三問項中，「完全達成」比例遠比其餘問項在「完全達成」比例高，皆超過 10%，而其餘問項皆低於 10%。推估是因為學校以往在電腦處理個人資料保護法中，是被規範的對象之一，因此存在相關的管制措施，如：電腦處理個人資料保護法中第十八條與第七條規定，非有特定目的或符合法律之規範，不得為之。再者，因為教育部規定學校需通過第三方資安驗證，所以採用 ISO 27001 和教育體系資通安全管理規範比例高，校內也存有資訊安全的框架，因此在此三問項能表現得較好。

深入分析在「尚未考慮」的問項，發現「貴校將舉辦教育訓練與意識提升，確保所有職員都能夠按照適當程序處理個人資料。」、「貴校將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。」，以及「貴校的個人資訊管理制度將能確保個人資料的完整性與正確性。」的問項調查結果中，「尚未考慮」比例皆為 0%，為本構面在「尚未考慮」此答項中，比例最低的問項。推估此是因受訪者所屬學校意識到個資法所帶來的衝擊，因此對於職員能否具備資保護意識、在個人資料的處理上是否能遵循一定的程序，降低人員疏失造成資料外洩的情形[23]，以及能否維護個人資料的完整性與正確性…等能力都相當重視，像是較敏感的個人資料在存入電腦資料庫前，需進行核對確認[17]。因此三問項皆有被列入

考量。因此三問項皆有被列入考量。

- 監督與審查構面分析（表 4-22）：本構面的 4 題問項在「規劃中」比例最高，推估雖然以往在法規中已有相關規定，如：電腦處理個人資料保護的施行細則 [5]、私立學校及學術研究機構電腦處理個人資料管理辦法第 12 條[4]。也都有規範學校應建立個人資料檔案稽核制度，但卻未再有詳細的規訂，因此大專校院原先對個人資訊未存在完善的監督基礎，加上個資法的保護範圍較廣、規範較為詳細，因此需重新規劃對於個人資料監督之目標與範圍，且因個資法施行細則尚未公布，所以多數學校仍在規劃當中。
- 改善構面分析（表 4-23）：深入分析在「完全達成」的問項，10.8%「貴校將持續透過預防和矯正措施來改善個人資訊管理制度。」此問項，遠比本構面中其餘問項在「完全達成」之比例高，皆超過 10%，而其餘問項皆低於 10%。且本研究發現，此問項選填為「完全達成」的受訪者，其所屬學校內四個構面整體達成度相較其他學校好。推估是因為這些學校已有實施個人資訊管理制度，為了要確保所施行的內部控制仍能達到所預期的目標，因此須透過內部矯正措施，持續改進個人資訊管理制度的缺失，以及預防措施降低發生潛在個人資訊外洩的風險，幫助學校的個資保護制度符合法律規範，也因此完成度較高。

表 4-20：規劃構面之問項統計表

題目	完全達成		部分完成		規劃中		構思中		尚未考慮	
	樣本數	百分比	樣本數	百分比	樣本數	百分比	樣本數	百分比	樣本數	百分比
1 貴校將依照發展、實行、維護和持續改善等步驟將個人資訊管理制度文件化。	2	3.1%	25	38.5%	20	30.8%	17	26.2%	1	1.5%
2 貴校將定義個人資訊管理制度的範圍和規定個人資料管理的目標。	1	1.5%	21	32.3%	27	41.5%	15	23.1%	1	1.5%
3 貴校將由高階主管負責維護個人資訊管理政策，並表態支持。	12	18.5%	20	30.8%	17	26.2%	13	20.0%	3	4.6%
4 貴校個人資訊管理政策將說明需承諾遵守國內個資法。	11	16.9%	24	36.9%	15	23.1%	13	20.0%	2	3.1%
5 貴校內的職員將被告知遵循個人資訊管理政策，且了解在組織中自我的責任歸屬。	4	6.2%	27	41.5%	21	32.3%	13	20.0%	0	0.0%
6 貴校將提供實作個人資訊管理制度所需的資源。	3	4.6%	22	33.8%	19	29.2%	16	24.6%	5	7.7%
7 個人資訊管理制度將成為貴校核心價值的一部分。	6	9.2%	22	33.8%	18	27.7%	13	20.0%	6	9.2%

表 4-21：實行與運作構面之問項統計表

題目	完全達成		部分完成		規劃中		構思中		尚未考慮	
	樣本數	百分比	樣本數	百分比	樣本數	百分比	樣本數	百分比	樣本數	百分比
1 貴校的高階主管將負責管理個人資訊管理制度，且有最佳實務顯示有遵循個資法。	3	4.6%	20	30.8%	20	30.8%	19	29.2%	3	4.6%
2 貴校將依照組織規模和處理個人資料之性質指派職員負起遵循個人資訊管理政策的責任。	2	3.1%	24	36.9%	20	30.8%	16	24.6%	3	4.6%
3 貴校將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。	0	0.0%	16	24.6%	26	40.0%	16	24.6%	7	10.8
4 貴校將明確的定義個人資料中有哪些資料是屬於高風險類別。	3	4.6%	25	38.5%	15	23.1%	21	32.3%	1	1.5%
5 貴校將舉辦教育訓練與意識提升，確保所有職員都能夠按照適當程序處理個人資料。	2	3.1%	23	35.4%	27	41.5%	13	20.0%	0	0.0%
6 貴校將對處理個人資料的程序做風險評估。	1	1.5%	19	29.2%	22	33.8%	18	27.7%	5	7.7%
7 貴校的個人資訊管理制度將隨時保持在最新的更新狀態。	2	3.1%	26	40.0%	18	27.7%	17	26.2%	2	3.1%
8 貴校的個人資訊管理制度將有觸發通知的程序和確保能得到最新且準確的通知。	1	1.5%	18	27.7%	29	44.6%	12	18.5%	5	7.7%
9 貴校將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	2	3.1%	19	29.2%	27	41.5%	17	26.2%	0	0.0%
10貴校將具體指明處理個人資料之目的，且不用於目的外用途。	8	12.3%	23	35.4%	21	32.3%	12	18.5%	1	1.5%
11貴校將能確保個人資訊管理制度在蒐集和處理個人資料的適當性、相關性和不過度。	3	4.6%	23	35.4%	22	33.8%	15	23.1%	2	3.1%
12貴校的個人資訊管理制度將能確保個人資料的完整性與正確性。	5	7.7%	24	36.9%	22	33.8%	14	21.5%	0	0.0%
13貴校的個人資訊管理制度將銷毀過期（或是不在保存範圍內）之個人資料。	7	10.8%	15	23.1%	21	32.3%	15	23.1%	7	10.8%
14貴校的個人資訊管理制度將包含當處理個人資料時尊重當事人之意見，以及出	4	6.2%	16	24.6%	25	38.5%	17	26.2%	3	4.6%
15貴校將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	2	3.1%	26	40.0%	21	32.3%	14	21.5%	2	3.1%
16貴校將能確保個人資料轉移或處理有一適當的保護措施。	3	4.6%	25	38.5%	19	29.2%	17	26.2%	1	1.5%
17貴校與第三方合作時，將能確保個人資料揭漏處於被管制的狀態。	10	15.4%	23	35.4%	16	24.6%	13	20.0%	3	4.6%
18能確保當其他組織代表貴校管理個人資料的處理程序將會遵循個資法。	6	9.2%	25	38.5%	18	27.7%	14	21.5%	2	3.1%
19貴校的個人資訊管理制度將定期維護，確保程序與技術元件的正確及能適當運作。	5	7.7%	22	33.8%	22	33.8%	14	21.5%	2	3.1%

表 4-22：監督與審查構面之問項統計表

題目	完全達成		部分完成		規劃中		構思中		尚未考慮	
	樣本數	百分比	樣本數	百分比	樣本數	百分比	樣本數	百分比	樣本數	百分比
1 貴校將舉行內部稽核來監控及審查個人資訊管理制度的有效性及效率。	5	7.7%	21	32.3	22	33.8	13	20.0	4	6.2%
2 貴校對個人資訊管理制度進行內部稽核時，將能為客觀及公正的稽核工	4	6.2%	18	27.7%	21	32.3%	17	26.2%	5	7.7%
3 貴校的個人資訊管理制度將定期進行內部稽核且將稽核報告提供給管理層。	5	7.7%	11	16.9	25	38.5	17	26.2	7	10.8%
4 貴校將定期或週期性審查個人資訊管理制度，當發生重大變更，應確保	4	6.2%	20	30.8%	20	30.8%	15	23.1%	6	9.2%

表 4-23：改善構面之問項統計表

題目	完全達成		部分完成		規劃中		構思中		尚未考慮	
	樣本數	百分比	樣本數	百分比	樣本數	百分比	樣本數	百分比	樣本數	百分比
1 貴校的個人資訊管理制度將有防止潛在不符合事項發生的措施。	4	6.2%	19	29.2	20	30.8	17	26.2	5	7.7%
2 貴校的個人資訊管理制度將定期進行風險評估，以確定立場是否改變和	5	7.7%	15	23.1%	23	35.4%	19	29.2%	3	4.6%
3 貴校將持續透過預防和矯正措施來改善個人資訊管理制度。	7	10.8%	18	27.7%	23	35.4%	15	23.1%	2	3.1%

表 4-24：電算中心專任職員人數規模與「規劃」構面的 ANOVA 表

題目	F 值	顯著	平均值		平均值的 95%信賴區間			
			10 人以下	10 人以上	10 人以下		10 人以上	
					下界	上界	下界	上界
1貴校將依照發展、實行、維護和持續改善等步驟將個人資訊管理制度文件化。	14.848	0.000*	2.85	3.67	2.58	3.12	3.35	3.99
2貴校將定義個人資訊管理制度的範圍和規定個人資料管理的目標。	10.733	0.002*	2.85	3.50	2.59	3.11	3.22	3.78
3貴校將由高階主管負責維護個人資訊管理政策，並表態支持。	7.765	0.007*	3.10	3.88	2.72	3.48	3.52	4.23
4貴校將提供實作個人資訊管理制度所需的資源。	24.673	0.000*	2.61	3.75	2.30	2.92	3.44	4.06

表 4-25：電算中心專任職員人數規模與「實行與運作」構面的 ANOVA 表

題目	F 值	顯著	平均值		平均值的 95%信賴區間			
			10 人以下	10 人以上	10 人以下		10 人以上	
					下界	上界	下界	上界
1 貴校將依照組織規模和處理個人資料之性質指派職員負起遵循個人資訊管理政策的責任。	14.848	0.000*	2.78	3.63	2.58	3.12	3.35	3.99
2 貴校將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。	10.733	0.002*	2.59	3.13	2.59	3.11	3.22	3.78
3 貴校將明確的定義個人資料中有哪些資料是屬於高風險類別。	7.765	0.007*	2.93	3.46	2.72	3.48	3.52	4.23
4 貴校將舉辦教育訓練與意識提升，確保所有職員都能夠按照適當程序處理個人資料。	24.673	0.000*	2.95	3.67	2.30	2.92	3.44	4.06
5 貴校將對處理個人資料的程序做風險評估。	14.848	0.000*	2.66	3.29	2.58	3.12	3.35	3.99
6 貴校的個人資訊管理制度將隨時保持在最新的更新狀態。	10.733	0.002*	2.85	3.63	2.59	3.11	3.22	3.78
7 貴校的個人資訊管理制度將有觸發通知的程序和確保能得到最新且準確的通知。	7.765	0.007*	2.68	3.46	2.72	3.48	3.52	4.23
8 貴校將具體指明處理個人資料之目的，且不用於目的外用途。	24.673	0.000*	3.10	3.88	2.30	2.92	3.44	4.06
9 貴校將能確保個人資訊管理制度在蒐集和處理個人資料的適當性、相關性和不過度。	14.848	0.000*	2.95	3.50	2.58	3.12	3.35	3.99
10貴校的個人資訊管理制度將能確保個人資料的完整性與正確性。	10.733	0.002*	3.10	3.67	2.59	3.11	3.22	3.78
11貴校的個人資訊管理制度將銷毀過期（或是不在保存範圍內）之個人資料。	7.765	0.007*	2.78	3.38	2.72	3.48	3.52	4.23
12貴校的個人資訊管理制度將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。	24.673	0.000*	2.78	3.42	2.30	2.92	3.44	4.06
13能確保當其他組織代表貴校管理個人資料的處理程序將會遵循個資法。	10.733	0.002*	2.02	3.75	2.59	3.11	3.22	3.78

表 4-26：電算中心專任職員人數規模與「監督與審查」構面的 ANOVA 表

題目	F 值	顯著	平均值		平均值的 95%信賴區間			
			10 人以下	10 人以上	10 人以下		10 人以上	
					下界	上界	下界	上界
1貴校將舉行內部稽核來監控及審查個人資訊管理制度的有效性及效率。	8.866	0.004*	2.88	3.63	2.54	3.22	3.30	3.95
2貴校對個人資訊管理制度進行內部稽核時，將能為客觀及公正的稽核工作計挑選適當的稽核員。	10.459	0.002*	2.65	3.50	2.36	3.01	3.13	3.87
3貴校的個人資訊管理制度將定期進行內部稽核且將稽核報告提供給管理層。	12.568	0.001*	2.51	3.42	2.21	2.81	2.97	3.86
4貴校將定期或週期性審查個人資訊管理制度，當發生重大變更，應確保制度的可用性、充分性和有效性。	6.966	0.010*	2.76	3.46	2.41	3.10	3.06	3.85

表 4-27：電算中心專任職員人數規模與「改善」構面的 ANOVA 表

題目	F 值	顯著	平均值		平均值的 95%信賴區間			
			10 人以下	10 人以上	10 人以下		10 人以上	
					下界	上界	下界	上界
1貴校的個人資訊管理制度將有防止潛在不符合事項發生的措施。	7.236	0.009*	2.71	3.42	2.40	3.02	2.95	3.88
2貴校的個人資訊管理制度將定期進行風險評估，以確定立場是否改變和不符合事項是否需要矯正。	10.609	0.002*	2.71	3.50	2.40	3.02	3.23	3.87
3貴校將持續透過預防和矯正措施來改善個人資訊管理制度。	11.111	0.001*	2.88	3.75	2.58	3.18	3.37	4.13

4.6 大專校院所在區域與各構面之關係

為了解不同區域的在大專校院在個人資訊管理制度之現況上是否有差異存在，本研究以學校所在區域劃分為北、中、南、東和離島五個區域，再與四個構面分別進行單因子變異數分析。而結果證明不同區域的學校,在個人資訊管理制度下之PDCA構面檢定，結果皆不顯著。此結果表示不同區域的學校，目前在個人資訊管理制度下之 PDCA 構面中的導入程度，並無顯著差異存在。

4.7 電算中心專任職員人數與各構面之關係

為了解不同電算中心專任職員人數規模，對於目前個人資訊管理制度的發展是否有差異存在，透過「電算中心專任職員人數」統計表（表 4-2）發現，電算中心專任職員人數多集中於「10 人以下」，所以本研究將電算中心專任職員人數，劃分成為「10 人以下」與「10 人以上」兩個群體，與個人資訊管理制度 33 題問項進行單因子變異數分析，結果僅列出有達顯著水準（P-value≤0.05）的問項（表 4-24 至表 4-27），並再深入了解電算中心職員人數規模於 PDCA 四構面中，顯著差異的問項。

- 規劃構面分析（表 4-24）：本構面共 4 題問項達顯著水準，此結果表示不同電算中心專任職員人數規模，對個人資訊管理制度的文件化、範圍與目標定義、高階管主管表態支持，及提供資源皆有差異存在。

為了解電算中心專任職員人數規模，於「規劃」構面有何差異，深入探討具顯著差異的問項。電算中心專任職員人數在「10 人以上」的學校，在「規劃」構面各問項的平均值皆高於「10 人以下」的學校，由此顯示目前規模大的學校在個人資訊管理制度「規劃」構面發展較快。再者，透過兩群體在「貴校將有提供實作個人資訊管理制度所需的資源。」此問項的平均值可知，電算中心專任職員人數在「10 人以上」的學校完成度較佳，顯示規模大的學校部份已有提供發展個人資訊管理制度所需資源。第三，電算中心專任職員人數與預計所需經費交叉分析具有顯著相關（P-value=0.003），電算中心專任職員人數在「10 人以上」的學校，58.3%尚在評估所需經費，而已預計好經費僅 37.5%；「10 人以下」的學校，46.3%還未評估所需經費（表 4-28）。因此綜合上述結果，推估因個資法已勢在必行，為了要符合法規的要求，並降低學校的營運風險，規模大的學校高階主管能較快表態支持，所以可獲得的資源較為充足，能幫助個人資訊管理制度的發展，而其對個人資訊管理制度的範圍、目標，以及文件化的發展速度上，都比「10 人以下」的學校表現好，因此規模大的學校能在「規劃」構面表現較佳。

表 4-28：電算中心專任職員人數與所需經費交叉表

電算中心專任職員人數		所需經費						總計
		尚未評估	評估中	100 萬元以	100 萬元 - 500 萬元	500 萬元-1,000 萬元	1,000 萬元含)以上	
10 人以下	樣本數	19	15	3	2	2	0	41
	百分比	46.3%	36.6%	7.3%	4.9%	4.9%	0.0%	100%
10 人以上	樣本數	1	14	4	5	0	0	24
	百分比	4.2%	58.3	16.7%	20.8%	0.0%	0.0%	100%
總計	樣本數	20	29	7	7	2	0	65
	百分比	30.8%	44.6%	10.8%	10.8%	3.1%	0.0%	100%

- 實行與運作構面分析（表 4-25）：本構面共 13 題問項達顯著水準，此結果表示不同電算中心專任職員人數規模，對個人資訊管理制度中，指派職員負起遵循責任、公平處理個人資料、舉辦職員教育訓練、有觸發通知程序…等皆有差異存在。

為了解電算中心專任職員人數規模，於「實行與運作」構面有何差異，深入探討具顯著差異的問項，發現電算中心專任職員人數在「10 人以上」的學校，在「實行與運作」構面各問項平均值皆高於「10 人以下」的學校。

透過在「貴校將依照組織規模和處理個人資料之性質指派職員負起遵循個人資訊管理政策的責任。」、「貴校將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。」、「貴校將對處理個人資料的程序做風險評估。」，與「貴校的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。」此 4 題問項中發現，電算中心專任職員人數在「10 人以上」的學校完成度較佳，此是由於規模大的學校，因為人力資源較為充足，所以能指派較多職員負責個人資訊管理政策的相關事宜，或是能推派合適的職員負責跨部門資料處理與風險識別，或是負責校內有關個人資料的申訴問題。也因此能在「貴校將明確的定義個人資料中有哪些資料是屬於高風險類別。」、「貴校將具體指明處理個人資料之目的，且不用於目的外用途。」，與「貴校的個人資訊管理制度將銷毀過期（或是不在保存範圍內）之個人資料。」此 3 題問項上連帶表現較佳。

在「能確保當其他組織代表貴校管理

個人資料的處理程序將會遵循個資法。」此問項中，電算中心專任職員人數在「10人以上」的學校幾乎都通過了第三方資安驗證，僅極少數3.1%尚在進行驗證（表4-29），而在這些資安驗證中，如：ISO 27001控制目標A.15.1「與法律法規要求的符合性」[19]，與教育體系資通安全管理規範控制目標A.15.1「法規之遵守」[7]，都有規定需遵循相關法律和法規要求，因此比起從零開始建立制度，已通過第三方資安驗證的學校早有相關基礎[9]，加上電算中心人數規模大的學校人力充足，所以能在制度的導入上較規模小的學校好。

表 4-29：電算中心專任職員人數與通過資安驗證交叉表

電算中心專任職員人數		通過第三方資安驗證				總計
		ISO27001	教育體系資通安全管理規範	進行中	否	
10人以下	樣本數	8	12	10	12	41
	百分比	12.3%	18.5%	15.4%	18.5%	63.1%
10人以上	樣本數	10	13	2	0	24
	百分比	15.4%	20.0%	3.1%	0.0%	36.9%
總計	樣本數	18	25	12	12	65

表 4-30：電算中心人數規模與資安訓練的交叉表

電算中心專任職員人數		舉辦職員資安訓練			總計
		是	否	考慮中	
10人以下	樣本數	14	4	23	41
	百分比	34.1%	9.8%	56.1%	100%
10人以上	樣本數	15	0	9	24
	百分比	62.5%	0.0%	37.5%	100%
總計	樣本數	29	4	32	65
	百分比	44.6%	6.2%	49.2%	100%

在「貴校將舉辦教育訓練與意識提升，確保所有職員都能夠按照適當程序處理個人資料。」與「貴校將能確保個人資訊管理制度在蒐集和處理個人資料的適當性、相關性和不過度。」此2問項的平均值可知，電算中心人數規模大的學校完成度較佳。且電算中心專任職員人數規模與舉辦職員教育訓練交叉分析有顯著相關（P-value=0.047），電算中心專任職員人數在「10人以上」的學校，62.5%已舉辦職員教育訓練；「10人以下」的學校，多處於56.1%尚在考慮是否舉辦教育訓練，9.8%並不考慮舉行（表4-29）。由此可知，電算中心人數規模大的學校，對職員是否具備個人資訊管理認知相當重視，也意會到唯有推廣校內個人資料保護意識，讓職員了解其重要性，培養職員的資安技能，使職員能遵循校內規定之程序處理個人資料，才可降低個人資料外洩風險，因此能較「10人以下」的學校表現較好。

在「貴校的個人資訊管理制度將隨時保持在最新的更新狀態。」、「貴校的個人資訊管理制度將有觸發通知的程序和確保能得到最新且準確的通知。」，與「貴校的個人資訊管理制度將能確保個人資料的完整性與正確性」此 3 題問項的平均值可知，電算中心職員人數規模大的學校完成度較佳，且此 3 問項皆選填「部份完成」與「完成達成」時，電算中心專任職員人數在「10 人以上」的學校，已預計好經費的比例多於「10 人以下」的學校。綜合上述結果，顯示已預計好所需經費的學校，能提供個人資訊管理制度及相關系統進行維護，或是升級時所需的資源，因此能定期提醒校內人員更新個人資訊，以維護個人資訊的正確性。此外，因規模大的學校人力資源充足，因此能派遣職員或成立小組，專門負責個人資訊管理制度，以確保校內個人資訊管理制度能反映法規及資料維護之需求。

- 監督與審查構面分析（表 4-26）：此構面 4 題問項皆達顯著水準。此結果顯示不同電算中心專任職員人數規模，對於舉行內部稽核、挑選稽核員、定期審查個人資訊管理制度與提供管理層稽核報，皆有差異存在。透過比較平均值發現，電算中心專任職員人數在「10 人以上」的學校，在「監督與審查」構面的平均值皆高於「10 人以下」的學校，由此可知「10 人以上」的學校在此構面發展較佳。

深入探討具顯著差異的問項，發現未通過 ISO 27001 與教育體系資通安全管理規範的學校，在「監督與審查」構面的發展較為緩慢，此 4 題問項多填答「構思中」或「尚未考慮」，且皆為電算中心專任職員人數在「10 人以下」的學校。而在「貴校將有舉行內部稽核來監控及審查個人資訊管理制度的有效性及效率。」與「貴校將定期或週期性審查個人資料管理制度，確保可用性、充分性和有效性。」此 2 問項中，電算中心專任職員人數在「10 人以上」的學校完成度較高，顯示規模大的學校已

有相關的監督基礎。

另外在「貴校對個人資訊管理制度進行內部稽核時，將能為客觀及公正的稽核工作計挑選適當的監督員。」，與「貴校的個人資訊管理制度將定期進行內部稽核且將稽核報告提供給管理層。」此 2 問項中，電算中心專任職員人數在「10 人以上」的學校完成度較佳。此是由於通過第三方資安驗證，已讓校內有相關監督與審查的基礎，如稽核員的挑選方式和稽核報告的提供等，因此可在原有的基礎上，再納入個人資訊管理制度稽核部份。

- 改善構面分析（表 4-27）：本構面 3 題問項皆達顯著水準。此結果顯示不同電算中心專任職員人數規模，對個人資訊管理制度定期進行風險評估、透過預防和矯正持續進行改善，具有差異存在。以下深入探討具顯著差異之問項。電算中心專任職員人數在「10 人以上」的學校，在此 3 題問項平均值皆大於「10 人以下」的學校。推估此是由於在確認不符合事項後，需由權責單位負責提出預防與矯正措施，因電算中心人數規模大的學校人力充足，甚至有專門小組負責個人資訊管理制度的相關事宜，所以在制定改善措施的進度較快。

4.8 研究發現

1. 69.2%受訪者認為「校譽受損」對學校的衝擊最大（表 4-6）。且受訪者職位與對學校造成的衝擊交叉分析具有顯著相關（P-value=0.000），其中 64.6%為電算中心管理層皆認為，「校譽受損」對學校衝擊最大（表 4-7）。顯示受訪者尤其是電算中心主管，普遍認為一旦個人資料外洩，將造成學校形象受損、招生率下降，影響學校永續發展。其次對學校衝擊最大的為 18.5%「賠償金額」，因個資法將罰鍰提高為二億元，對擁有成千上萬筆個人資訊的學校而言，所承擔的風險不容小覷（表 4-6）。
2. 56.9%受訪者所屬學校，考慮採取防止個人資料外洩方式為「加強內部稽核」（表 4-8）。且防止個人資料外洩方式與電算中心專任職員人數交叉分析具顯著相關（P-value=0.048），不論學校規模大小，多數都考慮採取「加強內部稽核」（表 4-9），因其能在合理管理成本下加強控制，所以考慮採用比例最高。其次，27.7%考慮採取「再購買資安設備，加強系統(含資料庫)之稽核與監督」，因個資法通過後，主要是防止從資料庫外洩資料，因此部分學校考慮購買現成資安設備，加強監控資料的流向及其使用行為（表 4-8）。
3. 44.6%受訪者所屬學校仍在評估因應個資法所需經費，30.8%受訪者所屬學「尚未評估」（表 4-10），由於個資法施行細則尚未公布，為確保能完全符合法規，部份學校選擇等個資法施行細則公布後，再進行經費評估。且預計所需經費與防止個人資料外洩方式交叉分析具有顯著相關（P-value=0.029），選擇「加強內部稽核」作為防止個人資料外洩的學校，多數還在評估需投入多少經費（表4-11），推估因採取內部稽核的學校，需對職員進行稽核的相關訓練，將花費較多成本及人力，因此多數學校尚在評估能提供多少經費。而已預計好所需經費的學校，多選擇「再購買資安設備，加強系統(含資料庫)之稽核與監督」，以加強電腦應用系統，達到防止個人資料外洩的目的（表4-10）。
3. 44.6%受訪者所屬學校有舉辦職員的教育訓練（表 4-13），因多數學校已了解個資法帶來的影響，因此透過教育訓練推廣個人資料保護意識。且舉辦職員教育訓練與對個人資訊管理制度了解程度交叉分析具有顯著相關（P-value=0.031），可見有舉行職員個資法訓練的學校，多能達到其訓練目的，受訪者對個人資訊管理制度已「了解」或「非常了解」（表 4-14）。僅 6.2%的受訪者所屬學校未舉辦職員的教育訓練或說明會（表 4-13）。
4. 此次全國大專校院主任研討會參與者，40.0%為「北部」的學校（表 4-15）。且學校所在區域與職員教育訓練交叉分析具有顯著相關（P-value=0.034），已舉辦職員個資訓練或說明會者，27.4%為北區學校（表 4-16），顯示北區學校相當重視職員是否具備個資法的認知，以及是否了解校內個人資訊管理制度，因此較其他地區優先舉行職員訓練活

動。而位於其他地區的學校，對於是否舉行職員教育訓練或相關活動，多處於在「考慮中」，發展較為緩慢。而此項調查中有 4.6%受訪者未填選學所在區域（表 4-15）。再者，本研究結果顯示，學校所在區域與個人資訊管理制度了解程度交叉分析具有顯著相關（P-value=0.015），顯示北區因優先舉辦職員的訓練活動，所以 29.1%的北區學校對個人資訊管理制度了解程度較其他地區學校好。

4. 目前大專校院在個人資訊管理制度中四個構面的發展，以「實行與運作」構面發展最佳，其問項整體統計，在 19.6%「部份完成」與 18.7%「規劃中」此兩答項佔全體比例較高。顯示目前大專校院有在因應個資法，也有施行部份管控措施，降低個人資訊外洩風險，但由於個資法施行細則未公布，國內也未有相關可依循的標準，因此發展也並未完善。而「監督與審查」和「改善」構面的整體比例較低，多處於「規劃中」，顯示此兩構面發展較為落後，目前大專校院較缺乏此兩構面的控管，還有待加強（表 4-19）。

5. 分析目前大專校院在個人資訊管理制度「規劃」構面（表 4-20），僅「貴校將定義個人資訊管理制度的範圍和規定個人資料管理的目標。」處於「規劃中」，其餘問項皆處於「部份完成」。顯示因個資法提高更多個人資料管理方面的責任與義務，所以多數學校還在規劃保護範圍與管理目標。而深入分析在「完全達成」的問項，發現「貴校由高階主管負責維護個人資訊管理政策，並表態支持。」與「貴校個人資訊管理政策有說明需承諾遵守國內個資法。」此兩問項比例皆超過 10%。推估因在一般資訊安全環境的建設中，需由高階主管帶領組織，所以高階主管的支持與較高的資訊安全意識，能為學校在資訊安全活動帶來正面影響。

6. 分析目前大專校院在個人資訊管理制度「實行與運作」構面（表 4-21），在 15.4%「貴校與第三方合作時，能確保個人資料揭漏處於被管制的狀態。」、12.3%「貴校有具體指明處理個人資料之目的，且不用於目的外用途。」，以及 10.8%「貴校的個人資訊管理制度有銷毀過期（或是不在保存範圍內）之個人資料。」中，「完全達成」比例皆超過 10%。推估因學校以往在電腦處理個人資料保護法中，是被規範的對象，因此個人資訊管理制度中已有相關規定，且教育部規定學校需通過第三方資安驗證，所以校內也已有資訊安全的框架，因此在此三問項能表現得較好。

7. 分析目前大專校院在個人資訊管理制度「監督與審查」構面中的問項（表 4-22），皆處於「規劃中」比例最高，推估雖以往在相關法規中已有規範，但卻未見有再詳細的規定，可知部份學校原先不見得存在相關監督規範，但因個資法的規範較詳細，因此需重新規劃對於個人資訊監督的目標與範圍。

8. 分析目前大專校院在個人資訊管理制度「改善」構面（表 4-23），僅 10.8%「貴校有持續透過預防和矯正措施來改善個人資訊管理制度。」，遠比其餘問項在「完全達成」比例高，超過 10%。且本研究發現，若此問項選填「完全達成」，則受訪者所屬學校內，四個構面整體達成度相較其他單位好，推估是因這些學校已有實施個人資訊管理制度，為要確保所施行的內部控制能達到預期的目標，因此須透過內部稽核，持續改進個人資訊管理制度，幫助學校符合法律規範，因此完成度較高。

9. 本研究將學校所在區域劃分為北、中、南、東和離島，與 33 題問項進行單因子變異數分析，其結果證明不同區域的學校，目前在個人資訊管理制度的導入上，並無顯著差異。

10. 電算中心職員人數規模與「規劃」構面進行單因子變異數分析（表 4-24），僅 4 題問項達顯著水準，電算中心專任職員人數在「10 人以上」的學校平均值皆高於「10 人以下」的學校。且兩群體與預計所需之經費交叉分析具有顯著相關（P-value=0.003），電算中心專任職員人數在「10 人以上」的學校，58.3%已在評估所需經費，37.5%已預計好經費；「10 人以下」的學校，46.3%還未評估（表 4-28）。綜合上述結果，顯示因個資法已勢在必行，為符合法規要求以降低營運風險，不論學校規模大小，電算中心主管皆有表態

支持，但因為規模大的學校，資源較為充足，因此在「規劃」構面表現佳。

11. 電算中心職員人數規模和「實行與運作」構面進行單因子變異數分析（表 4-25），共 13 題問項達顯著水準，電算中心專任職員人數在「10 人以上」的學校平均值皆高於「10 人以下」的學校。歸結研究結果發現，因規模大的學校因人力充足，能指派較多的職員或是成立小組負責個人資訊管理政策之相關事宜。再者，電算中心人數規模大的學校幾乎都有通過資安驗證（表 4-29），比起從零開始建立制度，已存在相關的資安規範。第三，電算中心專任職員人數規模與舉辦職員教育訓練交叉分析有顯著相關（P-value=0.047），電算中心專任職員人數在「10 人以上」的學校，62.5%已舉辦職員資安訓練；而「10 人以下」的學校，56.1%尚在考慮是否舉辦教育訓練，9.8%並不舉行（表 4-30）。顯示規模大的學校對於職員是否具備個人資訊保護管理技能與認知相當重，因此較快舉辦訓練活動，推廣個資保護意識。最後，因規模大的學校能提供經費，讓個人資訊管理制度及相關系統進行維護，或是升級時所需的資源，所以能確保制度或系統維持在最新狀態，因此電算中心人數規模大的學校在「實行與運作」構面表現較佳。

12. 電算中心職員人數規模與「監督與審查」構面進行單因子變異數分析（表 4-26），4 題問項皆達顯著水準，且電算中心專任職員人數在「10 人以上」的學校平均值皆高於「10 人以下」的學校。且未通過 ISO 27001 與教育體系資通安全管理規範的學校，發展較緩慢，在此 4 題問項多填答「構思中」與「尚未考慮」（表 4-29）。顯示電算中心人數規模大的學校較快導入個人資料的內部稽核，且因通過第三方資安驗證，讓校內已有相關資料保護的基礎，因此可在原有的基礎上，納入個人資訊管理制度的稽核，因此在「監督與審查」構面發展較快。

13. 將電算中心職員人數規模與「改善」構面進行單因子變異數分析（表 4-27），3 題問項皆達顯著水準，電算中心專任職員人數在「10 人以上」的學校平均值皆高於「10 人以下」的學校。此是由於在確認不符合事項後，需由權責單位負責提出預防與矯正措施，因電算中心人數規模大的學校人力充足，甚至有專門小組負責個人資訊管理制度的相關事宜，所以在制定改善措施的進度較快。

5. 結論與建議

5.1 結論

本研究有下列主要結果如下：

1. 在個資法通過後，當學校不慎洩漏校內個人資料時，64.6%的電算中心管理層，認為「校譽受損」對學校造成的衝擊最大，其次為 18.5%「賠償金額」（表 4-7），顯示電算中心主管重視學校形象更勝於賠償金額。因校譽是靠長久累積而來，若受到衝擊，將導致招生率下降，影響學校永續發展。而為防止個人資料外洩事件發生，不論學校規模大小，多數學校選擇採取「加強內部稽核」（表 4-8），以能在合理管理成本下加強控制作為考量，因此考慮採用比例最高。

2. 個資法通過後，為防止個人資料外洩，學校對於電算中心專任職員是否具備個資意識也開始重視，因此已有 44.6%的學校舉辦職員教育訓練（表 4-13），而有舉行職員資安訓練的學校，37%能達到對個人資訊管理制度「了解」或「非常了解」（表 4-14），而在已舉辦職員教育訓練的學校中，29.1%為北區的學校（表 4-17），顯示北區因優先舉辦職員教育訓練，所以在個資保護制度的了解較其他地區來的佳。

3. 目前個資法通過將近一年的時間，大專校院也已有發展個人資訊管理制度。而現階段的發展多處於「規劃」與「實行與運作」當中，深入了解此兩構面可發現，目前的發展以「實行與運作」構面最佳，在 19.6%「部份完成」與 18.7%「規劃中」此兩答項佔全體比例較高（表 4-19），推估是因為教育部有規定學校必須通過第三方資安驗證，所以多數學校原先已有存在資安相關的保護制度，如：電腦處理個人

資料保護法、ISO27001、教育體系資通安全管理規範…等制度,由此可知目前大專校院不僅有在因應個資法，也有施行部份管控措施，但由於目前政府尚未公布個資法施行細則，國內也未有針對學校的標準可以依循，加上個資法通過時間不到一年，因此在大專校院在「實行與運作」構面的發展也並未完善。至於目前大專校院在「監督與審查」和「改善」構面的發展則多處於「規劃中」，對此兩構面較缺乏控管。但若要確保校內所施行的管控措施是有效的、是否真能達到當初所預計的效果，則必須施行監督與改善措施進行評估，透過評估內部的控制缺失及衡量營運的效率，提供改進建議,讓個人資訊管理制度能符合法規要求。

4. 本研究將學校所在區域劃分為北、中、南、東和離島進行單因子變異數分析。而研究結果發現，雖然大專校院已有發展個人資訊管理制度，但在深入了解不同區域的發展進度上，卻無顯著差異存在。但由表 4-16「學校所在區域與職員教育訓練交叉表」，與表 4-17「學校所在區域與個人資訊管理制度了解程度交叉表」可知，北區較其他地區學校快舉行個資法的教育訓練，電算中心專任職員對個資法也有較深入的了解，但卻在個人資訊管理制度的發展未有較佳的表現，可能與學校未能針對不同的職位進行不同的訓練需求，或是職員所學的技能未能轉移到實際的工作中，又或者是因職員尚未作好準備…等因素有關[6]，亦或與本研究對象於東區與離島的學校樣本過少，所以造成無法推估各區學校差異，因此建議可增加此兩區域的樣本。

5. 本研究將電算中心專任職員人數劃分成為「10 人以下」與「10 人以上」兩群體進行單因子變異數分析。深入了解兩群體的差異發現，目前在「規劃」和「實行與運作」構面，規模大的學校導入較快、表現較佳，是因能提供較多資源進行支援，如：人力、經費或其他資源，且十分重視校內電算中心職員的教育訓練，促使學校在此兩構面中部份項目發展較良好；規模小的學校則在各方面的資源較少，往往要一人身兼數職，因此在執行進度上較為緩慢。再者，在「監督與審查」和「改善」構面，依舊以規模大的學校導入較快、表現較佳，規模小的學校發在此兩構面的導入較為落後，尚有待加強，由於目前大專校院多採取 ISO 27001 與教育體系資通安全規範兩種制度，而規模小的學校未通過比例達 29.3%（表 4-27），所以部分學校在資料保護基礎已較落後，此兩構面發展也較差，因此必須從重新規劃保護措施。

6. 大專校院個人資訊管理制度加強建議如下：

表 5-1:電算中心專任職員人數在 10 人以上的加強建議

規劃	研究結果：在「規劃」構面最重要的是制訂管理範圍與目標。而「10 人以上」的學校目前在範圍與目標制定上較為落後，離「完全達成」仍有段距離。且規劃到落實仍有段時間，須加速規劃，降低這段期間個資外洩之風險。 建議：可由各部門推派職員，成立跨部門的專責小組，能了解電算中心各部門的作業流程，因此對於範圍與目標規劃上會更為快速。
實行與運作	研究結果:「10 人以上」的學校資源與人力都較充裕，但多數問項介於「規劃中」與「部份完成」，可能資源與人力分配不理想有關。 建議:1.在資源方面，需重新檢視校內資源的配置以及人力的分派。2.在流程上可以透過個人資料的盤點，了解內部擁有哪些重要的個人資料檔案，而這些個人檔案會流經哪些單位，再指派各單位負起不同職責，以分頭進行資料的控管，加速落實個人資訊管理制度。
監督與審查	研究結果：在「監督與審查」構面必須做到定期舉辦內部稽核，確保制度的可用性、充分性和有效性，而目前「10 人以上」的學校在此項完成度並不高。 建議：1.持續推廣校內職員的個人資訊保護意識，加強職員的資安技能。2.能定期舉行內部稽核，發現缺失，作為持續改善，或作為個資法施行細則通過後之調整建議。
改善	研究結果:「10 人以上」的學校，在改善構面仍多介於「規劃中」與「部份完成」。 建議：1. 可以透過現有的稽核報告，制定改善方案。2. 將以往發生過有關資料的安全事件，以及系統異常事件納入分析，再針對這些風險或是流程的缺陷，制定改善措施，填補其制度上的缺失，持續改進個人資訊保護制度。

表 5-2：電算中心專任職員人數在 10 人以下的加強建議

規劃	研究結果：在「規劃」構面的管理範圍與目標制定上，「10 人以下」的學校多處於「構思中」與「規劃中」，而此又是在發展個人資訊管理制度最主要的部份，必須趕快建立。而在文件化發展不足，將影響制度的傳遞。 建議：1.考量「10 人以下」的學校人力較不足，建議可將人力投入在個資保護範圍的制定上，加強範圍與目標制定的完成度。2.加速制度的文件化，至少如 BS 10012 標準所列，包含個人資訊管理制度的範圍與目標、政策、職員所負的責任、可提供的資源和如何發展成為組織文化，或是依照法規的規定作為文件化的基本要求。
實行與運作	研究結果：「10 人以下」的學校，目前在指派職員負起個人資料相關事宜上因人力、資源缺乏，職員身兼多職，無法專注於個人資訊管理制度的執行，如：定義與識別高風險個資、風險評估等…等，因此在「實行與運作」構面發展落後。 建議：1.能舉辦職員的資安訓練，讓職員在資料處理與蒐集的流程能符合規範外。2.因人力較少，可先將人力集中於個人資料的盤點，從中挑出高風險資料或流程，進行控管，再慢慢擴及其他中低風險的資料上。
監督與審查	研究結果：「10 人以下」的學校，目前在是否有定期舉行內部稽核的部份，明顯較為落後，皆處於「規劃中」與「構思中」的階段，此兩者在「監督與審查」構面皆佔了相當大的比例。 建議：1.對個人資料施行的內部控制措施，先進行稽核，確保能控制措施是有效的。2.持續加強校內職員的個人資訊保護意識，與資安技能。
改善	研究結果：「10 人以下」的學校，目前「改善」構面皆介於「構思中」與「規劃中」，顯示「10 人以下」的學校在個人資訊管理制度「改善」構面才起步不久。 建議：加快落實速度，透過風險評估或是了解資料流程，以了解哪些流程是個人資訊管理制度的關鍵環節，能從關鍵部分開始構思，能針對關鍵部分優先規劃預防措施，並再沿伸到其他資料環節。

5.2 建議

對未來研究有以下建議：

- 本論文只有針對電算中心職員及主管作研究，後續研究可以擴大學效樣本，即包含學校各單位之調查，而問卷調查的回收率愈高，其所得的研結果也將愈詳盡。
- 本論文只有針對學校所在區域及電算中心專任職員人數作研究，後續研究可調查不同學校之類型，即包含技術學院、科技大學、公私立大學和專科，比較不同學校類型對於個人資訊管理政策的差異性。

致謝

本研究問卷得以順利完成，十分地感謝元智大學范書愷資訊長同意作者於「99 年全國大專校院電算中心主任研討會」上發放問卷，使本研究有良好的樣本資料，能得以順利進行研究。由衷感謝!

參考文獻

[1] 元智大學，〈99 學年度大專校院電算中心主任研討會〉，網址：http://ccds2010.yzu.edu.tw/index.php?page=info，上網日期：2010 年 12 月。

[2] 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。

[3] 行政院法務部，〈電腦處理個人資料保護法〉，http://law.moj.gov.tw/LawClass/LawOldVer_Vaild.aspx?PCODE=I0050021，上網日期：2010 年 12 月。

[4] 行政院法務部，〈私立學校及學術研究機構電腦處理個人資料管理辦法〉，網址：http://law.moj.gov.tw/LawClass/LawAll.aspx?Pcode=I0050024，上網日期：2010 年 01 月。

[5] 林家輝，〈我國中小學階段學生個人資料保護之研究〉，碩士論文，臺灣師範大學政治學系，2009 年。

[6] 胡雯雯，〈臺、日、英、德企業教育訓練制度與組織績效關係之比較研究〉，碩士論文，中央大學人力資源管理學系，2002 年。

[7] 教育部電子計算機中心，〈教育體系資通安全管理規範〉，網址：http://www.edu.tw/moecc/content.aspx?site_content_sn=5194，上網日期：2010 年 12 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：2011 年 3 月。
[9] 黃彥棻，〈因應個資法，可以先做的 8 件事〉，網址：http://www.ithome.com.tw/itadm/article.php?c=65133，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 年。
[11] 楊國樞等編，社會及行為科學研究法，東華書局出版，1989 年。
[12] 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。
[13] 趨勢科技，〈2010 上半年檔案威脅趨勢〉，網址：http://www.overclocker.com.tw/readvarticlen.asp?id=20751，上網日期：2010 年 11 月。
[14] BS 10012, “Data Protection - Specification for a Personal Information Management System, British Standards Institution,” 2009.
[15] Gounaris, Anastasios and Theodoulidis, Babis, “Data Base Management Systems (DBMSs): Meeting the Requirements of the EU Data Protection Legislation,” International Journal of Information Management, Vol. 23, Jun. 2003, pp. 185-199.
[16] Greenleaf, Graham, “Five Years of the APEC Privacy Framework: Failure or Promise?,” Computer Law & Security Report, Vol. 25, 2009, pp.28-43.
[17] Henderson, Sandra C. and Snyder, Charles A., “Personal Information Privacy: Implications for MIS managers,” Information and Management, Vol. 36, Oct. 1999, pp. 213-220.
[18] Hilton, Jeremy, “Improving The Secure Management of Personal Data: Privacy On-line IS Important, But It's Not Easy,” Information Security Technical Report, Vol. 14, Aug. 2009, pp. 124–130.
[19] ISO/IEC 27001, “Information Technology – Security Techniques – Information Security Management Systems – Requirements,” 2005.
[20] Ku, Cheng-Yuan, Chang, Yi-Wen and Yen, David C., “National Information Security Policy And Its Implementation：A Case Study in Taiwan.” Telecommunications Policy, Vol. 33, Aug. 2009, pp. 371–384.
[21] Kennedy, Gabriela, Doyle, Sarah, Lui, Brendand and Contributors, “Data Protection in the Asia-Pacific Region,” Computer Law & Security Report, Vol. 25, Jun. 2009, pp. 59–68.
[22] 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.
[23] Rezgui, Yacine and Marks, Adam, “Information security awareness in higher education: An exploratory study,” computers & security, Vol. 27, Dec. 2008, pp. 241–253.