

# 學校機關個人資料風險評鑑與控管系統之設計與開發

李珮璇

國立中正大學

shuan1017@gmail.com

洪新原

國立中正大學

syhung@mis.ccu.edu.tw

## 摘要

2012年10月1日我國個人資料保護法正式實行，我國各公務/非公務機關皆需遵行其規範。學校內部從行政單位到教學單位都擁有眾多的個人資料，學校有責任保護這些個人資料，避免個人資料遭受侵害。由於缺乏警覺性，個人資料的侵害常讓人不易察覺。本研究目的就是採用行政院研究發展考核委員會所提供的風險評鑑與控管架構，建立學校個人資料風險評鑑與控管的流程及標準，以分析與瞭解個人資料可能的風險，進而為學校中的個人資料加上風險層級記號，讓處理人員在面對這些資料時能有所警訊，降低所有可能的傷害。而學校方面也能夠進一步制定必要的保護措施，避免違反個人資料保護法。

風險評鑑與控管流程及標準設計完後，我們使用一個案例，實際執行一遍以評估設計是否適當；同時也針對學校中個人資料可能遭遇之風險進行問卷調查，瞭解目前學校中個人資料的主要風險。評估結果顯示：風險評鑑與控管的流程及標準能夠適用於學校環境。此外，透過風險分析問卷調查，瞭解在學校的環境中，個人資料可能遭遇之十七項高風險項目，我們也分別針對這些高風險項目提出風險處理對策，提供學校在個人資料保護措施選擇之參考。

**關鍵詞：**個人資料保護、風險評鑑、風險控管、資訊系統開發

## Abstract

Personal Information Protection Act was formally introduced on October 1, 2012. In order to avoid violating the law, each university needs to formulate a plan to protect their personal information. This study aims to propose a methodology to assess and control the risk of personal information at the universities. Through the design of the procedure and the methods, we can identify risks and reduce those risks. To demonstrate the applicability, an example was also illustrated. From the example, sixty-seven risks related to personal information protection were identified. Means to assess and control those risks were also provided. Finally, the risk assessment and control system was developed to help the personal information protection work.

**Keywords:** Personal Information Protection, Risk Assessment, Risk Control, Information Systems

## Development

### 1. 緒論

在資訊時代，個人資訊隱私指的是一種能夠自我控制關於個人資訊的能力[1][2]。簡單的來說，就是一種個人能夠自行決定是否、何時、以及給誰個人的相關資訊[3]。近年來，網路與資訊系統快速的發展讓我們有足夠的能力在不同的單位間處理、儲存、傳輸大量的資料[4]。而各組織廣泛的應用資訊科技來蒐集、分享個人資料，也引發了強大的隱私問題。此外，資料分享與資料探勘等技術在各領域的應用，如：醫療、犯罪分析、借貸評估、顧客關係管理等，也讓越來越多人開始關注其個人隱私的威脅，隱私問題若處理不當，可能會嚴重的傷害組織的形象[5]。

個人資料保護法其立法的目的是「為了要避免人格權受到侵害，同時促進個人資料的合理使用，因而制定此法來規範個人資料的蒐集、處理以及利用」[6]。根據個人資料保護法的定義，所謂的個人資料指的是自然人之姓名、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、職業等可以直接或間接識別個人之資料。iThome 在 2012 年的調查，政府機關與學校在因應個人資料保護法上僅有 6.2% 完成因應措施；而政府機關與學校平均要 8.5 個月的準備才能符合個人資料保護法的規定；此外，調查也發現，要因應個人資料保護法，最困難的挑戰是目前缺乏可遵循的標準做法[7]。因此本研究將利用風險評鑑與控管的技巧，針對學校環境中的個人資料提出一套完整的風險評鑑與控管方式，以瞭解學校個人資料的風險，降低個人資料可能遭受的侵害。

### 2. 文獻探討

#### 2.1 資訊隱私

所謂的「資訊隱私」指的是有條件的限制存取個人的相關資訊[8]。隨著企業作業流程越來越依賴資訊與通訊科技，增加了個人對於資訊隱私保護的憂慮。而企業與政府大量的蒐集資料，個人資訊隱私也就很容易被這些有權存取的人侵害[9]。到了 1990 年，資訊隱私的議題成為消費者最關心的議題之一，這種關注是因為資訊科技在日常生活中的影響越來越大[8]，再加上媒體的關注，在報章雜誌、

書籍，甚至是電視節目上，有越來越多的報導、文章，而這些都造成了資訊隱私關心的提升[10]。

因此，組織必需時時刻刻的關心對於個人資訊隱私的問題以及任何他們若沒有採取適當預防措施來保護他們所蒐集的個人資料而可能會發生的問題[10]。但由過去的研究可知，大多數的企業對於隱私保護多是採取被動的方式[11]，因此由政府組織出面制定具有法律效力的規範才能使個人資訊隱私獲得較大的保障。

一般來說，一個國家對於組織資訊隱私的管理方式會被其文化價值和民眾對於隱私的關心程度所影響；此外，若是政府對於組織資訊隱私管理的介入越深廣，組織內部的管理也將會更嚴謹，因此，民眾大多趨向於希望政府能夠制定嚴格的法律來降低他們對於隱私侵犯的憂慮[11]。

## 2.2 個人資料保護

資訊科技的使用快速的在政府、業界、學術界拓展，使得個人資料能夠很容易的在世界各地蒐集、傳輸、儲存，也造成了個人資料使用與保護的挑戰與問題的提升[12]。大部分的隱私侵害其實並非是有意的，而是由於設計者當初在設計時沒有預先考慮到這些資料如何被使用、以及由誰使用[13]。

資料蒐集時應遵守以下四個原則：(1)個人資料的蒐集只為了達到合法的組織目標；(2)資料的蒐集應該適當並且與組織目標相關，不得超出組織相關目標之外；(3)以合法的方式取得相關資料；(4)必需要獲得當事人的同意才能蒐集其個人資料。而應用資料時則應遵守：(1)個人敏感資料應該在輸入資料庫前做好確認；(2)資料必需是正確無誤的，若是有必要，必需定期保持更新，以維持資料的正確性；(3)這些資料檔案應該是可得到的，才能確保資料的正確性；(4)如果當事人不同意這份資料的準確性，在任何公開的檔案中都應該包含了個人的說法。除此之外，為了要確保資料的機密性，應該：(1)電腦安全程序應該包含硬體、技術、管理的安全措施；(2)除非法律上的需求，沒有個人的許可，第三方不得存取資料；(3)應該要注意公開資料的維護；(4)當資料與原本蒐集時的企業目標不符時不應該公開[14]。

## 2.3 風險管理

一般來說，風險可以定義為：一個事件或一個活動潛在負面的結果。風險包含了兩個主要構成要素，第一，風險是一個可能存在的負面結果或損失；第二，風險發生的結果是不確定的，可以事件發生機率的方式表示之[15]。

不同的領域對於風險的認知也不同，主觀的觀點認為風險指的是未來發生的不確定性[16][17]；而客觀的觀點則認為，風險是可以衡量的[18]。風險評鑑主要目的是為了決定資訊資產的價值，識別

已存在或潛在的威脅與弱點，並且瞭解組織中已存在的控制措施和這些控制措施對風險識別的影響，判斷可能的結果，最後將風險排列優先順序[19]。

## 3. 研究方法

### 3.1 個人資料風險管理

本研究應用行政院研究發展考核委員會所訂定的風險管理架構依序執行個人資料風險評鑑與控管流程，執行流程與內容說明如表 1 所示。

表 1 個人資料風險管理執行步驟

步驟	內容
1.建立風險管理執行背景	藉由實地訪談，瞭解個人資料生命週期；同時盤點個人資料並評估個人資料價值。
2.風險識別	透過文獻探討與訪談，瞭解個人資料可能遭遇之風險。
3.風險分析	利用德爾菲法瞭解個人資料可能遭遇的風險與所帶來的衝擊影響。
4.風險評估	瞭解目前擁有的資源，決定需要優先處理的風險。
5.風險處理	針對需要處理的風險提出可能的解決措施，並決定處理的優先順序。

### 3.2 德爾菲法

德爾菲法主要是由一連串的密集的問卷往返並提供意見回饋，來獲得專家一致的意見。而藉由問卷的方式重複的詢問專家，能夠避免專家們之間直接對質[20]。同時也能夠讓分散的專家達成共識[21]。本研究採用 Murry and Hammons (1995)所提出之德爾菲法研究流程，分為四個階段[22]：1.文獻蒐集：蒐蒐集國內外相關文獻，並透過訪談來瞭解個人資料可能遭受的風險；2.設計德爾菲法問卷：參考過去相關文獻並修改，同時訪談學校各單位之人員，直接發展出問卷；3.選取並確認專家小組成員：邀請校內相關單位人員協助風險分析調查。並向各專家說明本研究的目的與施測方式；4.執行德爾菲法問卷調查：將問卷發放給專家小組成員，並且以電話、E-mail 追蹤填答進度，待問卷全部回收後進行統計分析。

在問卷分析部分，本研究採用 Holden and Wedman (1993)所提出的方法，若專家小組對於問項所回答之意見分佈四分位差小於或等於 0.6，即代表專家小組對此一問項具有高度一致性意見[23]。

## 4. 應用實例

#### 4.1 建立風險管理執行背景

在執行個人資料風險管理之前，必須先瞭解風險管理的對象：個人資料，因此在執行其他步驟之前必需先盤點個人資料，瞭解學校所擁有的個人資料以及其相關細節之後才能執行接下來的步驟。

##### 4.1.1 盤點個人資料

各單位確認其所負責管理之個人資料，並記錄於個人資料盤點表，執行範例如表 2 所示。此研究將針對學校數位學習碩士在職專班考試報名資料庫進行盤點，瞭解此筆資料所含的資料項目以及其作業流程。

表 2 個人資料盤點表

負責單位/人員：招生組				
編號	檔案名稱	檔案類型	保管人	盤點時間
012_110	數位學習碩士在職專班考試報名資料庫	系統檔案、電子檔案、紙本檔案	招生組	2013.05.20

##### 4.1.2 個人資料價值評估

個人資料價值評估是為了瞭解每一筆個人資料對於學校的重要性及影響性，讓學校在獲得個人資料風險層級之後，可依此做為參考，作為個人資料風險評估及風險處理方式選擇的參考資料。

個人資料價值評估是根據個人資料遭受損害時對於學校作業流程影響的程度與範圍來估計，將這些資料詳細記錄於個人資料價值評估表，可獲得每筆個人資料的價值。

個人資料價值評估執行範例如表 3，作業流程影響程度/範圍與個人資料價值參考標準如表 4、表 5。

表 3 個人資料價值評估表

負責單位/人員：招生組				
編號	檔案名稱	作業流程影響程度	作業流程影響範圍	個人資料價值
012_110	數位學習碩士在職專班考試報名資料庫	中	中	中

表 4 作業流程影響程度/範圍參考標準

影響程度	影響範圍	程度/範圍
作業流程無法執行	影響超過 5 個行政/教學單位之作業	大
作業流程尚能執行，但會影響執行效率	影響 2~4 個行政/教學單位之作業	中
作業流程仍能執行	影響低於 1 個行政/教學單位之作業	小

表 5 個人資料價值參考標準

個人資料價值		作業流程影響程度		
		小	中	大
作業流程影響範圍	小	極低	低	中
	中	低	中	高
	大	中	高	極高

#### 4.2 風險識別

風險識別的目的是找出需要管理的風險。此階段必須盡可能的找出所有的風險並記錄於個人資料風險識別表，無論此風險是否已在學校的控制之下，因為此階段未被發現的風險將會被排除在之後的步驟。

本研究參考過去文獻以及訪談內容，整理出個人資料可能遭遇之風險，並將風險分類為：人員、軟體、硬體、網路、傳輸、場所六大類，如表 6 所示，執行範例如表 7 所示。

表 6 個人資料風險分類說明表

分類	說明	風險數量
人員	校內負責處理個人資料的人員，或其他可能接觸個人資料人員。	20
硬體	校內負責執行個人資料蒐集、處理、利用的實體設備，包括電腦、儲存裝置、輸出/輸入裝置、行動裝置等。	7
軟體	校內資訊系統中負責執行個人資料蒐集、處理、利用的程式化指令，可控制、協調電腦硬體元件。	6
傳輸	傳送電子、系統個人資料之網路以及傳送紙本個人資料之公文交換方式。	6
管理	學校對於個人資料之處理流程，或是保護個人資料的策略。	26
場所	存放電子、系統個人資料的儲存媒體之存放地點，或是存放紙本個人資料之資料櫃。	2

表 7 個人資料風險識別表

負責單位/人員：招生組	編號：012_110	檔案名稱：數位學習碩士在職專班考試報名資料庫
風險來源	風險發生原因/情境	
缺乏人員	缺乏人員執行個人資料保護。	
不合適的人員	個人資料負責/處理人員無法勝任個人資料處理等相關工作。	

### 4.3 風險分析

本研究應用德菲法，藉由專家的實際經驗與專業知識評估學校個人資料可能遭遇的風險、風險發生的可能性以及風險所帶來衝擊的嚴重性。

本研究整理過去文獻，以及實際訪談後將風險分為六大類：人員、硬體、軟體、傳輸、管理、場所。讓每位專家依其過去的實務經驗與專業知識回答每一項風險是否可能發生，若選填「可能」再依序回答此風險發生的機率與所帶來的衝擊影響；若選填「不可能」則需回答不可能的原因。

風險發生的機率分為：極高(5)、高(4)、中(3)、低(2)、極低(1)；衝擊影響則分為：非常嚴重(5)、嚴重(4)、普通(3)、輕微(2)、非常輕微(1)。每一回合問卷結束後將統計填答各項目的累積次數、平均數、四分位差，若四分位差小於 0.6 表示達到高度一致性，在下一回合問卷中將刪除此問項。在第二回合之後的問卷中也會提供這些統計數據供各位專家再次填答時參考之用。

本研究將問卷回收後，計算每一個風險項目的發生機率與衝擊影響的平均數，視為風險之發生機率與衝擊影響。由於本研究問卷設計使用李克特五點尺度，但風險判斷基準提供之標準為三點尺度，因此本研究將五點尺度衡量後的平均數，再使用三點尺度做判斷，評斷風險發生機率與衝擊影響的高低。

風險分析結果如表 8 所示，執行範例如表 9 所示，機率與衝擊影響參考標準如表 10、表 11 所示，風險判斷基準如表 12 所示。

表 8 風險分析結果

風險項目	風險數量	九級風險	六級風險	四級風險
人員	20	8 (40.00%)	7 (35.00%)	5 (25.00%)
硬體	7	1 (14.29%)	3 (42.86%)	3 (42.86%)
軟體	6	1 (16.67%)	5 (83.33%)	--
傳輸	6	--	4 (66.67%)	2 (33.33%)
管理	26	7 (26.92%)	9 (34.62%)	10 (38.46%)
場所	2	--	--	2 (100%)
合計	67	17 (25.37%)	28 (41.79%)	22(32.84%)

表 9 個人資料風險分析表

負責單位/人員：招生組	編號：012_110	檔案名稱：數位學習碩士在職專班考試報名資料庫						
風險來源	原因/情境	風險評估		現有控制機制	殘餘風險		風險層級	
		可能性	衝擊影響		可能性	衝擊影響		
缺乏人員	缺乏人員執行個人資料保護	中	中	4	無	中	中	4

表 10 機率敘述分類表[24]

等級	可能性分類	發生機率百分比
高	幾乎確定	81-100%
中	可能	41-80%
低	幾乎不可能	0-40%

表 11 衝擊影響敘述分類表，修改自[24]

等級	可識別性	資料量	敏感程度	形象
輕微	無法識別個人或需耗費大量資源始得識別個人	20 筆以下	含個人識別資料	未有新聞媒體報導負面新聞
普通	可間接識別個人	20~100 筆	含個人活動資料	區域新聞媒體報導負面新聞
嚴重	可直接識別個人	100 筆以上	含個人特種資料	台灣/國際新聞媒體報導負面新聞

表 12 風險層級判斷基準[24]

影響(衝擊或後果)	風險分布		
嚴重	風險層級：3	風險層級：6	風險層級：9
普通	風險層級：2	風險層級：4	風險層級：6
輕微	風險層級：1	風險層級：2	風險層級：3
	幾乎不可能	可能	幾乎確定
	機率		

### 4.4 風險評估

根據風險分析的結果，會同專家與各單位人員，由於人力、時間、資源有限，無法針對每一層

級之風險個別處理，因此本研究將處理風險層級為九，即經由風險分析後，其風險發生機率與衝擊影響之平均皆在 3.34(含)以上之項目，如表 13 所示。

表 13 個人資料高風險項目

分類	項目
人員	很難取得跨部門的合作、人員的異動、新的不熟悉的事情、欠缺監視機制、工作複雜、缺乏外部顧問的支援、對於現有的資料/應用系統/IT 瞭解不足、不合適的人員
硬體	未控制之複製
軟體	不可靠的軟體
管理	欠缺資訊安全責任之適當配置、欠缺風險識別與評鑑之程序、工作說明中欠缺資訊安全責任、欠缺通報安全弱點的程序、欠缺 ISMS 記錄監督之正式程序、欠缺已定義之資訊安全事故懲處過程、欠缺資訊處理設施之授權

#### 4.5 風險處理

在獲得風險評估的結果之後，對於高風險的個人資料必需盡可能的找出可行的風險處理方式，並決定使用何種方式來降低或防止風險的發生；同時也必需準備相關的資源以確實執行風險處理。

由於時間與人力關係，無法針對每一項可能之風險提出處理對策，因此本研究針對高風險之個人資料風險提出可行之管理辦法，以提供學校參考實行。

表 14 個人資料風險處理記錄表

負責單位/人員：招生組	編號：012_110	檔案名稱：數位學習碩士在職專班考試報名資料庫
風險項目	風險對策	
很難取得跨部門的合作	成立專案小組負責部門間連絡與溝通	
人員的異動	建立工作交接標準作業流程；接辦人員更換使用者識別帳號	
新的不熟悉的事情	加強職員教育訓練	
工作複雜	建立工作執行標準作業流程；加強職員教育訓練	
欠缺監視機制	以 log 記錄個人資料存取的時間、次數等；建立個人資料使用的申請流程	
缺乏外部顧問的支援	學校成立專案小組支援	
對於現有的資料、應用系統、IT 瞭解不足	加強職員教育訓練；針對資料、應用系統、IT 建立作業手冊	

表 14 個人資料風險處理記錄表(續)

負責單位/人員：招生組	編號：012_110	檔案名稱：數位學習碩士在職專班考試報名資料庫
風險項目	風險對策	
不合適的人員	加強職員教育訓練；負責資料處理人員簽訂保密切結書	
未控制之複製	以帳號密碼管理影印、列印機；建立相關的授權、監督與記錄之機制；浮水印或次數限制	
不可靠的軟體	限制軟體之下載；安裝防火牆、防毒軟體或防間諜程式；定期檢視、更新作業系統與應用程式漏洞	
欠缺資訊安全責任之適當配置	設置資料管理統一單位；依照工作區分資料的權責單位，釐清資訊安全責任之配置，並且以文件記錄作為憑據	
欠缺風險識別與評鑑之程序	建立風險識別與評鑑程序，並請專案小組確實執行，高階主管定期稽核	
工作說明中欠缺資訊安全責任	建立工作資訊安全責任手冊	
欠缺通報安全弱點的程序	建立通報程序標準作業流程；定期檢視安全弱點	
欠缺 ISMS 記錄監督之正式程序	建立 ISMS 記錄監督程序	
欠缺已定義之資訊安全事故懲處過程	學校高階管理者制定違反個人資料保護之懲處細節	
欠缺資訊處理設施之授權	以帳號密碼控管資訊處理設施；確認資訊處理設施使用之必要，授予權限	

#### 5. 結論與建議

本研究參考行政院研究發展考核委員會所提供的風險評鑑與控管架構建立的個人資料風險評鑑與控管之流程與相關標準，經由實際的執行，證明此架構中的風險管理流程能夠協助學校識別在個人資料蒐集、處理、利用當中可能發生的風險，杜絕個人資料可能遭受的侵害，避免違反個人資料保護法。另外，由於個人資料其價值難以數字衡量，因此採用個人資料對於學校作業流程影響程度與範圍為參考依據，以獲得個人資料價值，作為後續風險處理之參考依據。而經過實際執行，也證明此衡量方式可行。

最後，根據風險處理對策的探討，學校目前當務之急即是成立一個個人資料保護的專案小組，負責處理個人資料保護的工作。專案小組成立的目的與工作內容包含：1.協助各單位執行風險評鑑與控管的流程；2.針對學校個人資料蒐集、處理、利用

的每個程序建立一套標準作業流程；3.制定緊急狀況的應變措施；4.定期稽核學校各單位個人資料保護措施執行的狀況。

在個人資料風險分析部分，分析項目共有 67 項，分析的結果中，這些風險都落在風險層級四至九級，其中九級之高風險有 17 項，占 25.37%，也就是說有四分之一的高風險項目。由此可知學校目前對於個人資料保護的措施仍然不足。而其中在人員與管理方面的高風險項目分別占 40%26.92%，可知在個人資料保護方面人員與管理是最難控管的部分。因此學校不但要制定完整的相關制度，也必需要資料處理相關人員的配合，才能夠落實個人資料保護。

## 6. 研究限制

本研究在資料蒐集、研究方法、問卷設計、訪談力求完整、可靠，但礙於時間、人力等因素，仍有以下之限制：

(1)不易掌握風險分析問卷填答對象之認知：

個人資料風險的評鑑是由資料相關負責人、專家共同討論，雖有提供相關的評鑑標準，但還是無法完全提供客觀的結果，風險評鑑的結果可能會因為不同的人而有所差異。另外，由於個人資料保護法實施未滿一年，學校內各單位對其認識不深，對其可能的風險與所帶來的衝擊可能尚在摸索階段。

(2)訪談對象限制

訪談對象個數略顯不足，對於系統設計與風險分析應要進行全校全面性之訪談，採納多方意見，才能將系統與流程的需求更完善。此外，由於問卷之發放集中在單一學校，因此概化能力略顯不足，應多採集更多學校相關意見與資訊，如此才能真正反映出本研究所設計之流程的合適性。

## 參考文獻

- [1] M.J. Culnan, "How did they get my name?: an exploratory investigation of consumer attitudes toward secondary information use," *MIS Quarterly*, vol. 17, no. 3, 1993, pp.341-363.
- [2] R.O. Mason, "Four ethical issues of the information age," *MIS Quarterly*, vol. 10, no. 1, 1986, pp.5-12.
- [3] J.H. Saltzer, and M.D. Schroeder, "The protection of information in computer systems," *Proceedings of the IEEE*, vol. 63, no. 9, 1975, pp.1278-1308.
- [4] G. Dhillon, and J. Backhouse, "Technical opinion: Information system security management in the new millennium," *Communications of the Association for Computing Machinery*, vol. 43, no. 7, 2000, pp.125-128.
- [5] X.-B. Li, and S. Sarkar, "Class-Restricted Clustering and Microperturbation for Data Privacy," *Management Science*, 2012, pp.1-17..
- [6] 個人資料保護法(民 99 年 5 月 26 日)。
- [7] iThome(民 101)。2012 年個資法大調查—因應現況。取自 <http://www.ithome.com.tw/privacylaw/article/76902>
- [8] H.J. Smith, "Privacy policies and practices: inside the organizational maze," *Communications of the Association for Computing Machinery*, vol. 36, no. 12, 1993, pp.104-122.
- [9] I.L. Auerbach, "Professional responsibility for information privacy," *Journal of Information Systems Management*, vol. 2, no. 1, 1985, pp.77-81.
- [10] S.C. Henderson, and C.A. Snyder, "Personal information privacy: implications for MIS managers," *Information & Management*, vol. 36, no. 4, 1999, pp.213-220.
- [11] S.J. Milberg, H.J. Smith, and S.J. Burke, "Information Privacy: Corporate Management and National Regulation," *Organization Science*, vol. 11, no. 1, 2000, pp. 35-57.
- [12] A. Kobsa, "Personalized hypermedia and international privacy," *Communications of the Association for Computing Machinery*, vol. 45, no. 5, 2002, pp.64-67.
- [13] A. Anne, and S. Martina Angela, *Privacy in Multimedia Communications: Protecting Users, Not Just Data*, Springer, 2001.
- [14] M.H. Agranoff, "Controlling the threat to personal privacy: Corporate policies must be created," *Journal of Information Systems Management*, vol. 8, no. 3, 1991, pp. 48-52.
- [15] W.D. Rowe, *An anatomy of risk*. Wiley,1977.
- [16] F.C. Crane, *Insurance Principles and Practices*. New York: John Wiley and Sons, 1980.
- [17] J.S. Resenbloom, *A Case Study in Risk Management*. New York: Meredith Corp, 1972.
- [18] J.C.A. Williams, and R.M. Heins, *Risk Management and Insurance*(4th ed.). New York: McGraw Hill, 1981.
- [19] ISO 27005:2008
- [20] N. Dalkey, and O. Helmer, "An Experimental Application of the Delphi Method to the Use of Experts," *Management Science*, vol. 9, no.3, 1963, pp.458-467.
- [21] M.R. Czinkota, and I.A. Ronkainen, "International Business and Trade in the Next Decade: Report from a Delphi Study," *Journal of International Business Studies*, vol. 28, no. 4, 1997, pp.827-844.
- [22] J.W. Murry Jr, and J.O. Hammons, "Delphi: A Versatile Methodology for Conducting Qualitative Research," *The Review of Higher Education*, vol. 18, no.4, 1995, pp.423-436.
- [23] M.C. Holden, and J.F. Wedman, "Future issues of computer-mediated communication: The results of a delphi study," *Educational Technology Research and Development*, vol. 41, no. 4, 1993, pp.5-24.
- [24] 行政院研究發展考核委員會(民 98)。風險管理及危機處理作業手冊。