從稽核觀點探討資訊系統對法令遵循之研究 —以個人資料保護法為例

張明森　　陳志誠
大同大學 資訊經營研究所
sunfloor@ms15.hinet.net　chenps@ttu.edu.tw

摘要

以往研究組織內部之資訊系統管理，大都著重在資安防護與管理制度方面，對於組織內部的資訊系統在法令遵循的方面，則較少有人以此角度加以探討。為確保組織不會發生違反法規的事件，最好的方法就是預先找出在法律與行業規範中必須要遵守的事項，然後藉以檢查現行的資訊系統與管理規範是否符合法規方面的要求並加以檢討與改善。因此本研究期能以組織內部的稽核觀點，建構一套對於資訊系統在法令遵循方面的查核機制，藉以協助組織能有效的查核內部資訊系統對於法令遵循的情形，俾使組織能降低不小心違反法律的風險，並善盡資料管理的責任。

本研究將採用「Gowin's Vee Model」作為研究策略，並以「個人資料保護法」為研究對象，從「個人資料生命週期」之各階段為研究構面，結合個人資料保護法的法律條文，透過德爾菲法(Delphi Method)之研究方法，制定「資訊系統對個人資料保護法法令遵循之內部稽核」的查核項目建構模型，以作為組織內部在稽核資訊系統對「個人資料保護法」法令遵循時之參考。

關鍵詞： 個人資料保護法、內部稽核、個人資料生命週期。

Abstract

In the past, the studies of the information system management within the organization, mostly focus on the information security protection and internal management perspective. The legal compliance of the information system within the organization was less to be discussed. To ensure the violations do not occur, the best way is to identify the legislations that must be complied with in advance, and in order to check the existing information systems and management practices compliance with regulatory requirements and to review and improvement. This study will construct a checking mechanism about the legal compliance aspects for an information system from the organize internal audit perspective, to help organizations effectively checking the internal information system for legal compliance situation, and organizations can reduce careless violation legal risks and fulfill data management responsibilities.

This study will apply the Gowin's Vee Model, explore the various stages of the "Personal Data Life Cycle". combine with the legislative provisions of "Personal Information Protection Act", through the "Delphi Method" research method, to construct a set of "information system on Personal Information Protection Act compliance audit" internal audit checking projects model for organizations.

Keywords: Personal Information Protection Act, Internal Audit, Personal Data Life Cycle.

1. 前言

在 ISO 27001 附錄 A.15 中提到，法規遵循與安全政策必須能夠有效地實施，其中「A.15.1 遵循適法性要求」的控制目標，即是讓組織避免違反任何法律、法規、合約、應盡義務及任何與安全有關的要求，也就是要降低組織不小心違反法律的風險。為確保組織不會發生違反法規的事件，最好的方法就是預先找出在法律和行業規範中必須要遵守的事項，然後藉以檢查現行的資訊系統與管理規範是否符合法規方面的要求並加以檢討與改善。有鑑於此，針對組織內部之資訊系統對法令遵循的情形，訂定一套內部稽核的查核項目，更顯出其重要性。

隨著「個人資料保護法」(以下簡稱個資法)以及「個人資料保護法施行細則」(以下簡稱施行細則)於 101 年 10 月 1 日公布施行，無論是公務機關或非公務機關，無不對於機關組織內部產生莫大的衝擊。有別於舊版的「電腦處理個人資料保護法」，新的個資法所保護的主體範圍，並不侷限於以電腦處理之個人資料檔案，更擴大到涵蓋以任何形式存在的個人資料，且適用的主體也包括所有的公務機關以及任何自然人、法人、團體。除此之外，機關組織無論是直接蒐集或是間接蒐集個人資料，均負有告知之義務。另外，新增了團體訴訟機制以及當產生個資訴訟事件時負有舉證責任等多項變革，更讓機關組織不得不重新檢視企業內部對於個人資料保護的適法性。

探究組織內部之資訊系統是否對「個人資料保護法」已達其法令遵循之要求，以往機關組織大都針對「個人資料電腦檔案」，並從資安防護與內部管理之觀點切入。然而「個人資料之風險評估」並不等於資安風險評估；「事件之預防、通報及應變機制」也不等於資安事件通報機制[1]，資安風險管

理已不足以因應個人資料保護法的要求。

基於前述的研究背景與動機，本研究將以「個人資料生命週期」的四個階段為研究構面，結合個資法與施行細則的法律條文，以及研究個案之專家意見，透過德爾菲法(Delphi Method)專家問卷調查方式，訂定檢查資訊系統對個資法之適法性的稽核項目，並以國內 T 銀行旗下「保險經紀人股份有限公司」之「保險經紀管理系統」進行系統驗證。本研究目的有三：

(1) 從「個人資料保護法」的法律層面及稽核觀點，提供建置中的資訊系統在建構時應注意到的控制項目。

(2) 對於已建置的資訊系統，檢視其現有控制項目是否符合「個人資料保護法」的法令遵循。

(3) 提供資訊系統對「個人資料保護法」法令遵循情形稽核項目的設計模式，以作為其他資訊系統在建置時設計控制項目所參考。

2. 文獻回顧與探討

本研究以「個人資料保護法」、「個人資料生命週期」、「個人資料管理制度」等三大議題來探討相關文獻，藉以明確訂定研究的方向。

2.1 個人資料保護法

依據個資法的立法精神，該法主要在於規範個人資料之蒐集、處理及利用，以避免人格權受侵害，並促進個人資料之合理利用。除消極的保護個人私生活之不受干擾與任意公開，也積極的尊重當事人自主控制之「資訊隱私權」。[2]

所謂「資訊隱私權」，乃保障人民決定是否揭露其個人資料、及在何種範圍內、於何時、以何種方式、向何人揭露之決定權，並保障人民對其個人資料之使用有知悉與控制權及資料記載錯誤之更正權。[3]

個資法也同時導入「亞洲太平洋經濟合作會議」（Asia-Pacific Economic Cooperation， APEC）於 2005 年「APEC 隱私權保護綱領(APEC Privacy Framework)」中所提出的 9 大隱私權保護原則[4]：

—「預防損害」(Preventing Harm)
—「告知」(Notice)
—「蒐集限制」(Collection Limitation)
—「個人資料之利用」(Use of Personal Information)
—「當事人自主」(Choice)
—「個人資料之完整性」(Integrity of Personal Information)
—「安全管理」(Security Safeguards)
—「查閱和更正」(Access and Correction)
—「責任」(Accountability)。

表 1 APEC 隱私權保護綱領與個資法條文對應表

APEC 隱私權保護綱領	對應法條
1.預防損害	§12,18,27~40
2.告知	§7~9
3.蒐集限制	§6、15、19、53
4.個人資料之利用	§5、16、20
5.當事人自主	§3、10、11、13
6.個人資料之完整性	§11
7.安全管理	§27
8.查閱及更正	§3、10、11、13、17
9.責任	§21

資料來源：[5]、本研究整理

新版個資法除對於「適用主體」、「保護客體」、「資料保護」有更詳盡的規範外，亦增加了須取得當事人的「書面同意」、「國際傳輸」的限制，以及負有「告知」及「通知」義務。另就違反個資法要求之行為，課予行為人相當之義務，包括對於當事人之民事損害賠償責任、國家對於行為人之刑事訴追、以及主管機關立於行政監督之立場，課予行為人之行政罰等。然而，更為重要的是，由於新增了「團體訴訟」以及「舉證責任」之倒置，對非公務機關而言，更加重了刑罰和損害賠償責任，因此，「證據留存」將變成是相當重要的課題，機關組織內部應該加以重視。茲就與稽核作業相關的個資法條文整理如下：

表 2 公務機關與非公務機關均須遵守之條文

條　文	說　明
第二條	(個人資料的定義) 個資查核時，必須要確認所查核的資料是否符合第二條所列有關個資的定義。
第六條	(特種個資的定義) 特種個資只有在特定的情況下才可以加以蒐集。
第八條	直接蒐集個人資料時所應告知的事項。
第九條	間接蒐集個人資料後於處理、利用前所應告知的事項。
第十條	當事人應有的權利。
第十一條	個人資料的刪除。
第十二條	發生個資事件時需通知當事人。
第十三條	當事人請求查詢、刪除個人資料的處理時限。
第五十一條	個資法的除外規定。

資料來源：本研究整理

表 3 公務機關須遵守之條文

條　文	說　　明
第十五條	蒐集、處理個人資料的規定
第十六條	利用個人資料的規定
第十七條	公開於電腦網站的事項
第十八條	專人維護個人資料的規定

資料來源：本研究整理

表 4 非公務機關須遵守之條文

條　文	說　　明
第十九條	蒐集、處理個人資料的規定
第二十條	利用個人資料及利用個人資料行銷時的規定
第二十一條	個人資料國際傳輸的規定
第二十七條	安全措施及個人資料安全維護計畫或業務終止後個人資料處理的規定

資料來源：本研究整理

2.2 個人資料生命週期

個人資料保護法第 1 條明定個資法的立法目的：「為規範個人資料之蒐集、處理及利用，以避免人格權受侵害，並促進個人資料之合理利用，特制定本法。」因此，關於個人資料之保護，應始於資料之「蒐集或產生」，中間歷經「儲存、使用、傳輸」(處理及利用)，至最後的「刪除或銷毀」，均須有適當的個人資料保護措施並留下足以證明已盡保護責任之證據。

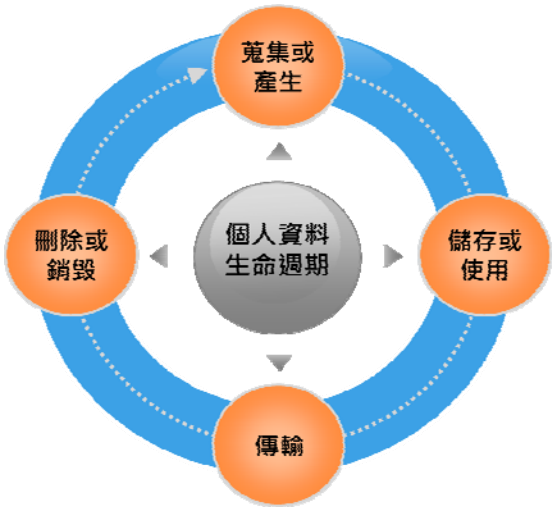

圖 1 個人資料生命週期[6]

新版個資法舉證責任的倒置原則，組織必須證明自身無故意或過失行為，才有可能不必擔負損害賠償責任。由於現今許多資料大多是透過資訊系統來處理，因此系統的 Log 是最容易保存與取得的證據，然而證據留存的完整性是否足夠，則是一項難有定論的議題。雖然目前資訊系統或資安設備大都可以留存 Log，但這些 Log 資料保存期間有限，且多是單點資料，如要證明組織沒有過失，尚必須串連其他的系統或設備，方能完整描繪事件的經過。

證據留存必須結合個人資料生命週期，保留個人資料從蒐集、處理、利用到銷毀的所有記錄，甚至可以讓稽核人員用來驗證有沒有做好改善事項。藉由系統記錄可確認變更個人資料的行為時，是否經過當事人本人之要求，確保資料異動是在當事人提出要求的情況下進行，透過系統監測與記錄，以降低企業的違法風險。[7]

因此，就資訊系統而言，內部稽核人員應從個人資料在系統中的流程進行個資盤點，並從「適法性」的角度檢視各項流程中是否均符合個資法的要求，同時就每一項流程做到「風險評估」及「權限清查」。藉由對個人資料流程進行盤點，才能確認保存地的相關證據是否足夠，以降低蒐集機關違法之風險。

2.3 個人資料管理制度

由於 ISO 27001:2005 對於個資保護的焦點，著重在處理階段，且在其控制項目中，針對個人資料保護部分僅有一條。顯見 ISO 27001 對於個資的保護部分尚有不足之處。[8]

有鑑於個人資訊保護的重要性愈來愈重要，全球各國政府均立法規範確保個人資料受到適當保護與運用。日本早於 2003 年即積極規畫資訊安全管理系統 ISMS 認證基準，並成功導入 JISQ 15001 隱私標誌制度。2005 年獲得日本內閣認可，發行日本隱私權證照，配合日本個人資料保護法全面實施，協助政府推動隱私權。

BSI 英國標準協會於 2009 年正式發佈 BS 10012:2009 個人資訊管理系統 Personal Information Management System (PIMS) 標準。此標準應用了「計畫－執行－檢查－行動」(Plan-Do-Check-Act, PDCA)循環，為個人資訊管理系統提供了一個架構，讓組織能維持和改善對資料保護法律及優良實務的遵循[9]。

2009 年 8 月行政院在「塑造資安文化、推升資安產值」產業科技策略會議，決議推動電子商務個人資料管理暨資訊安全行動方案，並委由資策會科技法律研究所在經濟部計畫支應下，建立之針對個人資料之管理制度臺灣個人資料保護與管理制度（Taiwan Personal Information Protection and Administration System, 簡稱 TPIPAS）。其適用範圍係針對蒐集、處理、利用及國際傳輸個人資料之事業，訂定相關規範事項，以建立個人資料管理制度，確保個人資料之安全。此一管理制度旨在提供一套系統化的標準，如事業的個人資料保護與管理制度符合該標準之規定，即可向該制度之授證機構提出驗證申請，如驗證通過，即可獲得「資料隱私保護標章」(DP Mark) [10]、[11]。

往昔蒐集機關對於個人資料保護的內部控管與稽核，多只著重在「管理層面」和「技術層面」，但現在可能要改正這個觀念，因為若不從「法律層面」著手，就算內控制度再完善，資安設備再昂貴，如果對於個人資料的蒐集、處理、利用等行為本身就已經違法，即便對於個人資料的控管持續有效的做到 PDCA（計畫－執行－檢查－行動），反而只是在確保蒐集機關的違法狀態持續而有效。

儘管蒐集機關針對個人資料的保護措施已全力投入，不論是建立防火牆、修補系統漏洞、弱點掃描、檔案雙重加密，甚至通過諸如 ISO27001、BS10012 等資安與個資管理認證，但相關作為其實都只能做到「降低風險」，而無法檢視蒐集機關在蒐集、處理或利用當事人個人資料的每項流程是否均合於個資法的要求。[1]

因此，本研究遂採從法律層面，並以內部稽核的觀點，針對資訊系統探討對個資法方面的遵循程度，以確保蒐集機關是在無違法的情況下，持續而有效地施行個人資料管理制度。

3. 研究方法與設計

3.1 Gowin's Vee Model

本研究主要目的在於建構一套檢查「資訊系統對個人資料保護法法令遵循之內部稽核」的查核項目訂定機制。因此，本研究採用「Gowin's Vee Model」作為研究策略，在 V 型左側的概念端，透過對個資法的解讀、參考專家學者對個資法的文獻探討，並藉由深度訪談法及德爾菲法與學者專家們做深入的討論，來彌補文獻資料的不足，進而彙整出關於資訊系統中較為具體的查核問項，以建構出查核項目訂定機制。而在 V 型右側的方法端，則以前面彙整出的查核問項，以個案研究方法進行實務面的驗證，並藉以測試本研究的可用性及有效性。最終目的在使本研究結果不僅是適用於本研究個案，亦可以運用於其他資訊系統。

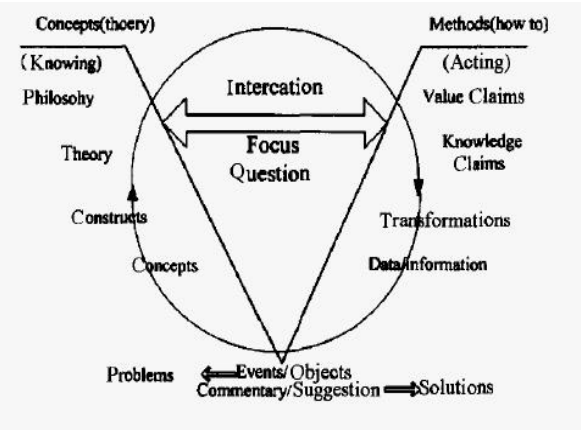

圖 2 Novak and Gowin's Vee Model, 1984

3.2 深度訪談法 (In-Depth Interview)

深度訪談法(In-Depth Interview)是一種無結構的、直接的、個人的訪問，透過自由的交談，調查人員對被調查者做深入性的訪談，以揭示對某一問題的潛在動機、信念、態度和感情。深度訪談法主要是用於獲取對問題的理解和深層瞭解的探索性研究[12]。

本研究除先以文獻探討方式彙整部分查核問項外，另為補足文獻方面的不足，並配合實務上的運作，第一階段採用深度訪談法(In-Depth Interview)為起點，依據「個人資料生命週期」四個階段以及「國際傳輸」、「團體訴訟」、「舉證責任」等個資法的重大變革，設計針對資訊系統的訪談大綱，並就資訊從業人員層面、研究個案從業人員層面、稽核人員層面等各種不同的構面，選定適當的受訪者進行訪談，以探求在個人資料保護法施行後，各受訪者對於本身業務上所接觸到的資訊系統與個人資料保護法適法性之間的初步看法與建議，進而整理出較為完整控制項目，並在第二階段以德爾菲法方式進行專家問卷調查。

表 5 深度訪談大綱

訪談項目	大綱內容
背景	1. 請問，您目前職位名稱為何？所從事的工作性質內容為何？
對個資法的認知	2. 就您的認知，個人資料保護法於 101.10.1 施行後，對於您目前所從事的業務範圍內，最大的衝擊是什麼？
	3. 就您的認知，在您業務範圍內所接觸到的資訊系統，是否符合個人資料保護法相關法規的規範？有哪些是符合的？哪些是尚待加強的？(試舉例說明)
個資蒐集	4. 就您目前業務上所接觸到的資訊系統，有關個人資料的蒐集，您覺得在資訊系統上應該要做那些查檢項目，以符合個資法的規範？
個資儲存與使用	5. 就您目前業務上所接觸到的資訊系統，有關個人資料的儲存和使用，您覺得應該要做那些查檢項目，以符合個資法的規範？
個資傳輸	6. 就您目前業務上所接觸到的資訊系統，有關個人資料的對外傳輸(含國際傳輸)，您覺得在資訊系統上應該要做那些查檢項目，以符合個資法的規範？
個資刪除與銷毀	7. 就您目前業務上所接觸到的資訊系統，有關個人資料的刪除或銷毀，您覺得在資訊系統上應該要做那些查檢項目，以符合個資法的規範？

證據保全	8. 就您目前業務上所接觸到的資訊系統，有關個人資料的異動日誌(Log)，您覺得在資訊系統上應該要做那些查檢項目，以符合個資法的規範？

資料來源：本研究整理

表 6 深度訪談受訪人員背景資料表

代號	服務單位職稱	專業領域	工作資歷
A	銀行資訊處 副處長	銀行系統	25 年
B	銀行資訊處 資訊安全科科長	資訊安全	8 年
C	保經公司 業務部經理	保險經紀	5 年
D	銀行稽核處 副處長	內部控制	10 年
E	銀行稽核處 電腦稽核科科長	電腦稽核	15 年

資料來源：本研究整理

3.3 德爾菲法 (Delphi Method)

德爾菲法（Delphi method）是一種結構化的決策支持技術，它的目的是在信息收集過程中，通過多位專家的獨立的反覆主觀判斷，獲得相對客觀的信息、意見和見解。調查者通過匿名方式對選定專家組進行多輪式意見徵詢。調查者對每一輪的專家意見進行彙總整理，並將整理過的材料再寄給每位專家，供專家們分析判斷，專家在整理後材料的基礎上提出新的論證意見。如此多次反覆，意見逐步趨於一致，得到一個比較一致的並且可靠性較大的結論或方案。其要點是：被徵詢意見的專家採用匿名發表意見，專家之間不可互相討論，不發生橫向聯繫，從而避免專家意見向少數影響大的專家意見趨同[13]。

本研究第二階段採用德爾菲法專家問卷調查方式，專家挑選原則包含：(1)業務從業人員、(2)內部稽核人員、(3)資訊部門人員、(4)系統廠商人員、(5)專家學者人員、(6)法律執業人員。

德爾菲法問卷針對第一階段彙整出來的控制項目進行問卷調查，每道問項包含了結構性問題，包括將「適用與否」用來決定該控制項目是否適用於檢查資訊系統對個資法的適法性，答案分為「適合」與「不適合」；以及詢問各控制項目在檢查適法性的「重要性程度」，並以五等尺度李克特氏量表（Likert Scale）做為呈現個別專家意見之指標。

本研究德爾菲問卷總計發放兩回合，透過兩回合的專家問卷來取得專家意見的一致性。本研究於兩回合問卷回收後利用 SPSS 統計軟體進行分析以瞭解並確定各控制項目在對於檢查資訊系統對個資法之法令遵循方面，是否具有重要性與有效性，進而確定有效的查核項目，俾利進行未來對研究個案的系統驗證。

表 7 德爾菲法專家背景資料表

代號	服務單位職稱	工作資歷
A	保險經紀公司業務部經理	5 年
B	保險經紀公司壽險科科長	5 年
C	保險經紀公司產險科科長	5 年
D	保險經紀公司企劃科科長	5 年
E	銀行稽核處副處長	10 年
F	銀行稽核處副處長	5 年
G	銀行稽核處電腦稽核	15 年
H	銀行稽核處電腦稽核	15 年
I	銀行資訊處資安科科長	8 年
J	銀行資訊處程式科科長	9 年
K	銀行資訊處制度科科長	13 年
L	保經資訊系統廠商總經理	10 年
M	大學教授	10 年
N	大學教授	20 年
O	執業律師	12 年

資料來源：本研究整理

4. 資料分析與整理

本研究於兩回合問卷回收後，將利用 SPSS 統計軟體進行分析，而問卷分析的依循準則有下列三點：

1. 效度分析：
   採用 Lawshe 所提出的內容效度比率（Content-Validity Ratio，CVR）[14]來評估問卷題項的「專家效度」，所計算出來的 CVR 值通常介於-1.0 至 1.0 之間，CVR 值愈高，表示專家們認為此題項的「適合性」程度愈高。當專家人數在 15 人時，CVR 值必須在 0.49 以上才符合內容效度比。
2. 一致性分析：
   以標準差及四分位差的值來評定問項的「一致性程度」，當專家對某項目的意見分佈四分位差小於或等於 0.6 時，即專家群對該項目的意見達到高度一致性，四分位差介於 0.6 與 1 之間則為中度一致性，而當四分位差大於 1 時，則為未達一致性。若以標準差作分析，專家意見的標準差大於 1 時，表示未達成一定的專家共識[15]、[16]。
3. 重要性分析：
   以平均數資料來評定問項的「重要性程度」，「重要性程度」是以五等尺度李克特氏量表（Likert Scale）做為呈現個別專家意見之指標，因此平均數越高的題項代表越受全體專家的重視。

5. 個案說明與實證

T 保險經紀人股份有限公司(以下稱保經公司)成立於 102 年 2 月 6 日，為其母公司 T 銀行百分之百轉投資設立之保險經紀人公司。

保經公司係為綜合保險經紀人公司，設立目的係以顧客導向引進多元化保險商品，並結合母公司 T 銀行的整體資源，整合行銷銀行保險業務，提供客戶多樣化選擇與全方位金融服務。其營業範圍包括人身保險經紀及財產保險經紀業務。

所擁有之「保險經紀管理系統」採雲端化設計，主要功能包括：「佣金計算」、「行政管理」、「訊息中心」、「業務管理」、「人事管理」、「網站管理」、「平台管理」、「系統管理」、以及「銷售管理」等九大類。其中「人事管理」含有保經公司內部員工之個人資料；「業務管理」與「銷售管理」則儲存大量保戶及保單等外部個人資料。其個人資料流向，係由 T 銀行之保險專員承接要保戶的保單後，經過保經公司統一審核、管理，並經由保險經紀人簽署文件後，轉給上游各保險公司進行核保。

本研究於獲得專家問卷分析結果後，將所得之重要性及有效性的題項，針對研究個案之資訊系統進行實證稽核，除藉以驗證本研究結果的可用性外，並提出對個案資訊系統在對於個資法法令遵循方面的建議。

6. 研究結論與建議

隨著政府推動個資法所帶來的連鎖效應，使得個資安全與稽核相關工作成為時下非常熱門的課題。本研究以稽核角度探討個資安全與稽核實務，除了可以讓 IT 資訊人員了解個資安全保護在實際環境中的計劃、實作與稽核方法外，更讓個資法可以藉由 IT 人員的協助以及稽核人員的查核工作，進一步地落實並培養出技術面與流程面的管理系統互補能力。

6.1 研究結論

經由本研究針對個案資訊系統的探討得到以下結論：

(1) 以目前個人資料保護法之內容，對資訊單位之最大衝擊，在於未來如有發生訴訟案件時，如何進行數位鑑識，以及如何提供具有證據能力之紀錄、軌跡資料，俾利提供企業組織在當事人提出損害賠償時，能證明資料之流向，據以協助企業組織提出無故意或過失之證明。

(2) 以往資訊系統在設計上，因考量記憶體與儲存設備的成本昂貴與資訊系統復原之所需，多數僅留有更新紀錄之軌跡，而不留存查詢紀錄之軌跡，此部分係需要加強的地方。

(3) 在資料交換的過程，如採用人工方式進行時，由於需要將資料下載，其中間可能有暫時性資料落地之情況，而該資料所暫時儲存的資訊設備在資料完成交換後，因需要人為介入，往往疏忽而忘記將資料刪除。

(4) 在傳輸過程方面，是否採取安全措施(如加密措施)，以及是否產生資料落地的情況，相對應的保護措施亦有不足之虞。

(5) 對於銷毀資料之作業紀錄再被銷毀，很難判定究竟是原先銷毀的資料不曾存在過，還是曾經存在但已經被銷毀。故對於銷毀資料之作業紀錄應予永久保留，以利釐清該資料是否曾經存在過。

(6) 有關個人資料之日誌資料(Log File)，系統之最高權限管理者或是具有該檔案修改權限者，亦應另於系統日誌中留存對日誌資料之修改與刪除軌跡資料。

6.2 研究貢獻

關於研究資訊系統對於法令遵循情形，除了本研究範疇所探討的「個人資料保護法」外，隨著各行業的性質不同，其適用的相關法規亦不盡相同。因此，本研究期能以內部稽核觀點，建構一針對資訊系統在法令遵循查核機制的方法論，藉以協助組織能有效的查核內部資訊系統對於法令遵循的情形，俾使組織能降低不小心違反法律的風險，並善盡資料管理的責任。最終目的在使本研究結果不僅是適用於本研究個案的資訊系統上，亦可以運用於其他資訊系統。其主要貢獻為：

(1) 對於尚在建置中的資訊系統，可即時加入法規面應注意到的控制項目設計。

(2) 對於已建置的資訊系統，可檢視其現有控制項目是否符合相關的法令規範。

(3) 研究方法可提供其他資訊系統對於法令遵循情形之稽核項目的設計模式，以作為在設計稽核項目上的方法論。

6.3 研究限制與建議

個人資料保護法的涵蓋範圍相當廣泛，要討論的議題也非常多，並非僅靠資訊系統的適法性一環即可保證完全符合個資法之法令規範。此外，本研究的對象僅針對個案公司的資訊系統，並未做全面性的研究，因此對於未來的研究方向，則有下列幾項建議：

(1) 本研究範圍僅限於個案資訊系統的管理層面，對於非資訊系統方面的作業流程則未加以探討，未來可擴大研究範圍，俾使組織在法令遵循方面更加周全。

(2) 資訊系統在提供數位證據的廣度與深度方面，究竟要達到何種程度，方足以滿足個資法上的要求，亦是未來可研究的方向。

參考文獻

[1] 葉奇鑫、王慕民, "內部稽核應納入個資適法性查檢," *內部稽核*, pp. 22-25, 2012.

[2] 邱映曦、劉敏慧、何寶中, "我國個人資料保護法與個人資料管理制度," *資訊安全通訊*, vol. 19, pp. 45-62, 2013.

[3] 司法院—大法官解釋第 603 號. (2005). *資訊隱私權*. Available: http://www.judicial.gov.tw/constitutionalcourt/p03_01.asp?expno=603

[4] 法務部. (2007). *APEC 隱私保護綱領中英文對照*. Available: http://www.moj.gov.tw/ct.asp?xItem=79529&ctNode=28156&mp=001

[5] 楊期荔, "鑑識會計用於銀行業資通安全之研究 -以新版個人資料保護法為例," 碩士, 科技管理學程碩士在職專班, 輔仁大學, 新北市, 2011.

[6] 呂錦峯、謝持恆, *個人資料保護法教戰守則*. 台北市: 永然文化出版股份有限公司, 2012.

[7] 廖珮君. (2012). *證據留存範圍應涵蓋個人資料生命週期*. Available: http://www.informationsecurity.com.tw/article/article_detail.aspx?aid=6652#ixzz2aYH8Vbp3

[8] 張碩毅、黃迺康、陳央庭、蘇仲杰, "企業個人資料保護管理機制之建構與實證," *電腦稽核*, pp. 89-111, 2012.

[9] 蒲樹盛, "全球風險下的個人資訊保護方案 BS 10012:2009 個人資訊管理系統," *品質月刊*, vol. 46, pp. 28-29, 2010.

[10] 維基百科. (2012). *臺灣個人資料保護與管理制度*. Available: http://zh.wikipedia.org/wiki/%E8%87%BA%E7%81%A3%E5%80%8B%E4%BA%BA%E8%B3%87%E6%96%99%E4%BF%9D%E8%AD%B7%E8%88%87%E7%AE%A1%E7%90%86%E5%88%B6%E5%BA%A6

[11] 經濟部. (2012). *臺灣個人資料保護與管理制度（Taiwan Personal Information Protection and Administration System, TPIPAS）*. Available: http://www.tpipas.org.tw/model.aspx?no=159

[12] M. 智庫百科. *深層訪談法(In-Depth Interviews)* Available: http://wiki.mbalib.com/zh-tw/%E6%B7%B1%E5%B1%82%E8%AE%BF%E8%B0%88%E6%B3%95

[13] H. A. Linstone and M. Turoff, *The Delphi Method : Techniques and Applications*: Addison-Wesley Pub. Co., Advanced Book Program, 2002.

[14] C. H. Lawshe, "A Quantitative Approach To Content Validity," vol. 28, 1975.

[15] 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, pp. 5-24, 1993.

[16] 顏志宏, "網際網路為基礎之德爾菲法," 資訊管理研究所, 成功大學, 2004.