資訊資產分類與風險評鑑之研究—以銀行業為例

陳志誠
大同大學資訊經營系所

林淑瓊
大同大學資訊經營系所

李興漢
大同大學資訊經營系所

許派立
大同大學資訊經營系所

摘要

企業的資訊安全作法繁多，但不一定能聚焦於最需要之處，以及考慮到成本與時間效益。因此，為企業資訊資產進行分類與建立風險評鑑機制，不僅可以得到資訊資產詳細的風險等級，也可使資訊安全管理決策更精確、完整及有效，避免資訊安全事件的發生。目前國內外有關資訊資產風險評鑑的研究不多，本研究對重視資訊資產管理的銀行業進行研究，以國內某知名銀行為例，由資訊安全管理之作業要點BS 7799-1：2000、資訊安全系統規範BS 7799-2：2002和資訊技術安全管理指導綱要ISO/IEC TR 13335做為問卷設計的依據，再以美國國家技術標準局（NIST）於2001年制定的「資訊科技系統風險管理指導」三項程序，進行風險管理。研究中由個案公司的資訊資產清冊中選出十一類24項較可能發生資安事件的資訊資產，使用德菲法進行資料收集分析，評估出資訊資產的相關威脅、弱點及風險等級，同時進行定性與定量的風險分析。研究結果說明個案公司資訊資產風險等級為中等者只有主路由器一項，其餘均為低等級，基於BS 7799-2：2002持續改善的原則，研究中對高風險等級的資訊資產提出建議及改進措施。由於銀行業的資訊環境具有高度雷同性——主要核心業務放在大型主機，外圍由中小型伺服器處理非帳務性系統，且研究個案之規模和資訊系統在銀行業中具有代表性，本研究獲致之成果具實務上的參考價值，可協助企業降低資訊資產風險與資安事件的發生。

關鍵字：資訊資產、資訊安全、風險評鑑

Classification of Information Assets and Risk Assessment: by Example of Banking Industry

Patrick S. Chen
Department of Information Management, Tatung University

Shu-Chiung Lin
Department of Information Management, Tatung University

Shing-Han Li
Department of Information Management, Tatung University

Perry Shi
Department of Information Management, Tatung University

Abstract

Many incidents of information systems result in imperfect protection of information assets. Since overall protection is expensive, even impossible, security measures should be made at the most needed places in terms of cost and time. By means of classification of information assets and their risk assessment, we are able to know the degree of risk of the assets and to achieve a better decision in security measures. Owing to the secrecy policy, research reports on risk assessment of information assets are rarely made public. In this research we classified the information assets of a financial institution and assessed their risks. Because the institution is one of the major banks in Taiwan, the research results should be representative. The Delphi method was adopted in this research and the questionnaires were designed based on the guidelines of information security management of BS 7799-1: 2000, BS 7799-2: 2002 and ISO/IEC TR 13335. In total, 24 information assets subject to security breaches were chosen for risk assessment, and 7 experts in information security and computer auditing were invited to answer the questionnaires concerning current value of the assets, possible threats, vulnerabilities and degree of risks. Risks are expressed in low, medium and high, ranging over 10 degrees on risk scale. The results revealed that there is one item, the core router, with medium risk while others are of low risk. We also made suggestions for enhancing security measures for all assets with risk degree greater or equal to 2. Owing to the lack of publications of researches on classification

of information assets and assessment of their risk in financial field, the results achieved in this study is of practical value.

Key words : Information Assets, Information Security, Risk Assessment

壹、導論

資訊科技使得銀行相關業務幾乎都經由電腦進行處理，並儲存其資料於資料庫。近年層出不窮的銀行資安事件，主要是有心人士的覬覦，而詐騙集團更青睞銀行所擁有的大量客戶資料（陳志誠、許派立，民95）。表1羅列2001-2007年數則國內外重大資安事件相關報導，分析外洩資料內容、管道及流向，由此可知國內有些銀行業者的客戶資料已落入詐騙集團手中，一般民眾小則收到莫名其妙的簡訊，大則信用卡被盜刷，造成業者和消費者的損失，這都顯示銀行客戶資料經常處在危險中。

由表1中呈現的各條新聞事例可以歸結說明資訊安全受損或資料外洩的發生原因，主要是組織對於重要的資訊資產未作妥善的保護與控管，以致於內部員工或外部人士有機可乘，加上電子商務犯罪已向圖利型發展（陳志誠，民92），使得詐騙集團透過各種方式取得資料，並且運用不斷翻新的詐騙手法困惑民眾，造成社會動盪與人民恐慌；可知銀行業面對日新月異的資訊科技，詐騙手法不斷翻新，對於資訊資產的保護及控管將愈形重要，因而進行銀行業者資訊資產的分類與風險評鑑是刻不容緩之事。執是之故，本研究將針對資訊安全管理中，資訊資產的分類與風險評鑑進行深入探討，接著對風險等級較高者提出建議及改進措施，以防止類似事件再度發生。為使研究能具體呈現，本研究選擇國內存放款總額已逾三兆具代表性的大型銀行為個案研究對象，並用德菲法（Delphi Method）進行資料收集和分析。研究的主軸為二：

1. 對個案公司資訊中心的資訊資產進行全面性的分類和風險評鑑，以得到詳細的風險等級。
2. 對評估結果所得之資訊資產風險等級較高者，提出具體改進與控管作法。

由於個案公司規模龐大且部門及分行頗多，研究範圍無法全面涵蓋，因而只以資訊中心的資訊資產清冊為主。此外，由於評估資訊資產的財務價值、預期損失和控制成本必須長時間的資料蒐集，在研究中定量風險分析，只能給予風險等級，而後續的計算年度預期損失等，亦不在本研究範圍之內。

本文其餘內容安排如下：第二節說明資訊資產分類及風險評鑑背景知識與文獻探討；第三節略述德菲法及其如何運用於本研究；第四節詳述銀行業資訊資產的分類及其定性與定量的風險評估；第五節結論說明本研究的貢獻、未來研究及其在管理上的意涵。

表1：2001-2007年國內外重大資訊安全事件分析表

時間	事由	國家	外洩資料內容	外洩管道	外洩資料流向	估計損失
2001-2002	財金公司資料外洩[1]	臺灣	信用卡「內碼」及金融卡資料	偽卡集團勾結財政部所屬的財金資訊公司工程師，盜取客戶信用卡及金融卡資料	偽卡集團	20-30億

[1] 自由時報91年9月21日政治新聞版。

時間	事由	國家	外洩資料內容	外洩管道	外洩資料流向	估計損失
2003/10	金融卡盜領事件[2]	臺灣	金融卡密碼及內碼	92年7-9月間在多台自動櫃員機裝置側錄器，十月十日國慶日當天集體盜領	盜刷集團	3000萬
2004/06	兩岸駭客聯手入侵台灣網路銀行[3]	臺灣	網路銀行帳號及密碼	發出植入「木馬程式」的電子郵件，入侵民眾的個人電腦，再竊取他們的網路銀行帳號及密碼	網路銀行盜領集團	上千萬
2005/07	信用卡客戶資料外洩[4]	美國	姓名、帳號及認證碼（威士卡約2200萬筆、萬士達卡約1400萬筆）	駭客利用軟體安全漏洞在Card Systems Solutions公司（付款資料處理機構）植入惡意程式	可能被用來盜刷	不明
2007/01	瑞典銀行慘遭史上最大網路詐騙[5]	瑞典	重要的帳戶資料	俄羅斯幫派份子將內含特製木馬程式的釣魚郵件假冒瑞典銀行的名義寄給若干顧客，並鼓勵收信客戶下載一個「反垃圾郵件」應用軟體。使用者若下載後，便會被植入木馬程式。當使用者試圖登入瑞典線上銀行時，使用者會被引導至假的首頁，輸入重要的帳戶資料。接著，惡徒便利用獲得的資料到真正的瑞典銀行網站取走帳戶內的錢	俄羅斯幫派份子	4000萬台幣
2007/02	中國駭客網路釣魚，警方經清查估計十萬筆個資外洩[6]	臺灣	個人基本資料、網路銀行帳號密碼及憑證、航空公司會員資料及帳號密碼等	來自中國大陸的駭客，以新型「網路釣魚」、駭客入侵等手法，密集架設假網站，有計畫的竊取台灣民眾個人基本資料	犯罪集團	不明
2007/02	大陸駭客入侵，台灣索尼通訊網路So-net網站上千客戶資料外洩[7]	臺灣	會員個人資料外洩、信用卡被盜刷，被盜刷的信用卡約1840張，國內幾乎所有發卡銀行都受害	So-net公司內，有六成以上電腦都被植入木馬程式，疑似遭大陸駭客入侵	不法集團	約有五百多萬元的信用卡被盜刷
2007/05	員警及電信公司員工將個人資料販賣給暴力討債的徵信業者[8]	臺灣	民眾之戶籍、車籍、出入境及住家、公司等基本資料	板橋地檢署發現暴力討債的徵信業者向員警、遠傳電信、富邦產物保險公司員工，以每筆二千元代價，查詢民眾管制資料，藉以對債務人進行監控，並以暴力手段討債	暴力討債的徵信業者	不明

[2] 財訊月刊92年12月261期。

[3] 東森新聞報93年6月9日社會新聞。

[4] 自由時報94年6月19日國際新聞。

[5] 科技資訊網新聞專區http：//taiwan.cnet.com/ 96年1月27日

[6] 中國時報96年2月7日。

[7] 聯合報96年2月23日。

[8] 中國時報96年5月17日

貳、背景知識及文獻探討

一、個案公司的資訊系統架構

大部份銀行業的資訊環境皆分為前台與後台二大部份，後台為封閉式的大型主機，前台是開放式PC，主要核心業務，如：存款、放款、匯款及帳務系統皆放在大型主機上，外圍由中/小型伺服器處理非帳務性次要性系統，如：外匯、基金、信用卡及網路銀行等，以分擔大型主機的負荷。圖1描繪出個案公司的資訊系統環境，主要以封閉式的區域網路（Local Area Network, LAN）為主，若要從Internet入侵到大型主機，並且取得大量資料並不容易，所以具有此種資訊環境的特性，其內部控管成為銀行業者資訊安全控管的主要工作。

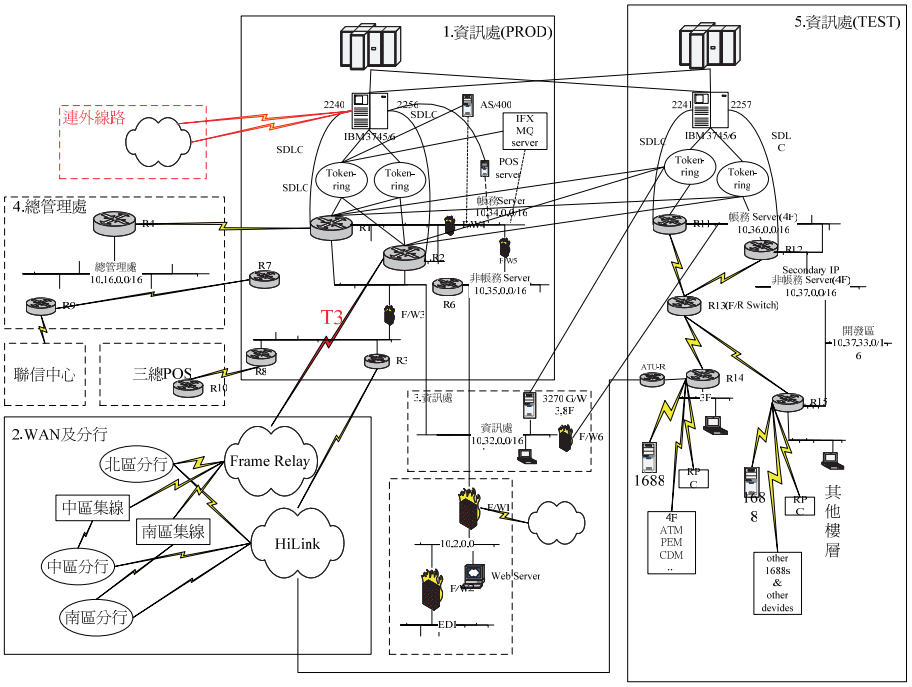

圖1：個案公司資訊系統環境

二、資訊資產分類與研究現況

銀行業是全球最重要的服務產業之一，資訊資產理當是最受到重視的，但由於銀行財務資料事涉機密，目前國內外並無專門針對銀行業資訊資產分類及風險評鑑之公開研究報告，而其它有關資訊資產的研究，主要側重於以下三方面：

1. 風險分析對企業的重要性：Budgen（1992）定義風險分析並討論風險分析的必要性及作法，強調風險分析技術將可使優質工程進行順利。Groom（2003）討論資訊技術（Information Technology, IT）安全系統在保護資訊資產上的演化，說明要

保護資訊資產就是要持續不斷提供保護措施。Perna（1995）建議企業將各種數據變成資訊資產，分析各種資訊後再轉成重要的競爭優勢。

2. 建立風險評估模式：Vorster and Les Labuschagne（2005）提出一個風險分析模式，說明企業在選擇定性、定量或其它風險分析方法前，可先利用風險分析模式，找出合適的風險分析方法。Hoqqanvik and Stolen（2005）透過調查專業人士和學生（非專業人士）對風險的看法，得到風險概念模型結果。王秀文（民94）建立兩階段的資訊資產評估模型系統，以找出關鍵性的資訊資產。瞿鴻斌（民93）建構一個資訊安全風險評估驗證系統，並模擬訂單主機遭到攻擊後，進行定量風險分析，產生資產所遭受到的實際威脅和計算出預期損失。
3. 對各種產業資訊資產進行風險分析：蕭吉宏（民94）對機敏軍事單位資訊部門進行風險定性分析，發現資訊設備如隨身碟、筆記型電腦等之管理有需要加強之處。張芳珍（民94）以國際標準BS 7799為基礎，配合個案航空公司對資訊資產的現行保護作法，歸納出資訊資產分類與管理的建議方法。Harris（1996）建議以預先服務之管理方式，將電信業者的資訊資產轉變成競爭上的優勢。鄭年華（民93）以電信公司為例建立風險評鑑五大步驟，實地驗證模式之應用，並歸結有助於企業資訊安全之管理。

由以上先前學者的研究分析得知，資訊資產安全探討的面象極為廣泛，但專門針對銀行業資訊資產分類與風險分析之研究非常稀少，由於銀行業對資訊系統的高度倚重，愈發突顯銀行業資訊資產分類及風險分析的重要性，而對於目前相關研究闕如之部份，也說明此研究進行時資料蒐集的困難度，所以能將個案公司的資訊資產逐一檢視，並依BS 7799的分類依據進行風險評估，再由其中挑選較具高風險的資訊資產進行分析，更增加此開創性研究對於學術界與實務界之重要性。所以在本研究中主要參考資訊安全管理之作業要點BS 7799-1：2000、資訊安全系統規範BS 7799-2：2002和資訊技術安全管理指導綱要ISO/IEC TR 13335。雖然學界尚無一致性定義的「資訊資產」，由於BS 7799已被國際標準組織（International Organization for Standardization, ISO）明訂為重要的安全規範，也成為實務界進行資訊安全維護遵循的重要標準。因此在本研究中對於資訊資產的分類就以BS 7799-1：2000定義的四類為主，分述說明如下：

1. 資料資產：包括資料庫、資料檔案、系統文件、使用手冊、教育訓練教材、 操作或支援程序、企業持續經營計畫、緊急應變計畫、備份資訊等。
2. 軟體資產：包括應用軟體、系統軟體、開發工具、套裝軟體及公用程式等。
3. 實體資產：包括電腦設備（伺服器、主機、筆記型電腦、個人電腦）、通訊設備（橋接器、集線器、路由器、網路交換器、數據機、電話自動交換機、傳真機、答錄機）、儲存媒體（磁帶機、磁帶櫃、磁帶、磁碟、光碟、光碟機），以及其他技術設備（不斷電系統、發電機、電源供應器、空調設備）等。
4. 服務資產：包括網路及語音通訊服務、一般公共設施（冷暖氣、照明、電力 、空調）等。

三、資訊資產的風險管理

美國國家技術標準局（National Institute of Standards and Technology, NIST）於2001年制定「資訊科技系統風險管理指導」（Risk Management Guide for Information Technology Systems NIST SP 800-30），包括風險評鑑（Risk Assessment）、風險降低（Risk Mitigation）以及評估與評鑑（Evaluation and Assessment）三項程序，茲分說明如下：

1. 風險評鑑

風險是事件發生的可能性及其後果的結合，是由一項特定威脅來源運用特定潛在可能性的弱點，對組織造成的負面衝擊。資訊安全風險的構成要件可分為資產（Asset）、弱點（Vulnerability）、威脅（Threat）、可能性或機率（Likelihood/Probability）與衝擊或後果（Impact/Consequence）。NIST將風險評鑑設定為九項步驟：

步驟1—系統特性描述（System Characterization）：界定資訊資產風險評估的範圍，應用群組區分其價值與重要性。

步驟2—威脅識別（Threat Identification）：威脅是指威脅來源利用弱點的機率造成負面的影響。威脅識別分別從威脅來源、動機與行動三構面進行釐清與分析，常見的威脅來源分為天然（如水災、地震）、人為（如未經授權的存取）及環境（如電力不足、污染）等。

步驟3—弱點識別（Vulnerability Identification）：識別並編列有可能成為潛在威脅來源利用的弱點，以NIST I-CAT弱點資料庫之弱點清單作為風險評估之參考[9]。

步驟4—控制分析（Control Analysis）：目的在於分析組織已執行或規劃實施的控制方法，能否將威脅利用弱點的可能性最小化或排除，控制的方法分為技術性（如電腦軟硬體設置）與非技術性（如管理及作業性控制），控制的類別分為預防性控制（如安全政策、加密）及偵測性控制（如稽核）。

步驟5—可能性判斷（Likelihood Determination）：判別潛在弱點發生危害的可能性，必須考量三項管理因素，分別為威脅來源的動機與能力、弱點的本質和現行控制的存在與有效性。

步驟6—衝擊分析（Impact Analysis）：判別威脅來源運用弱點造成的負面衝擊，以便評量風險的等級。

步驟7—風險判斷（Risk Determination）：特定威脅與弱點的風險判斷，確定那些是可以被運用的威脅或被利用的特定弱點，藉此可以確定發生負面的衝擊程度，降低或排除風險的存在，規劃適當的控制，判別風險的等級。

步驟8—控制建議（Control Recommendation）：控制方法是以降低或排除確定風險並適合組織運作為條件，控制建議是降低風險等級以達到某一可接受的程度，而接受控制建議的前提是必須進行成本效益分析，以選擇判斷其必要性與適當性。

步驟9—成果文件（Results Documentation）：完成風險評鑑（識別威脅來源及弱點、評

[9] 弱點清單可參照（http：//icat.nist.gov）。

估風險、提供建議控制），必須將成果書面化並向高階管理者簡報，以協助高階管理者依據政策、程序、預算、營運及管理，調整或變更其決策。

2. 風險降低

排除所有風險通常是不切實際且不可能的，以有系統的方法減少對組織產生的負面衝擊，並將危害程度降至最低的可接受程度，是較具體可行的方式。風險降低可經由以下的選擇達成：

（1）風險承擔（Risk Assumption）：接受潛在的風險，即持續監控在某一可接受的等級，亦可稱為風險接受（Risk Acceptance）。

（2）風險規避（Risk Avoidance）：規避風險是經由移除風險原因或結果以降低風險。

（3）風險限制（Risk Limitation）：限制風險是透過執行控制的方法（如預防、偵測）減少威脅，以及利用弱點所造成的負面衝擊。

（4）風險計畫（Risk Planning）：管理風險是經由排序、實施與維持的控制方法發展風險降低的計畫。

（5）研究與確認（Research and Acknowledgment）：降低風險的損失可經由確認弱點及研究控制方法進行弱點矯正。

（6）風險轉移（Risk Transference）：轉移風險可經由其他選擇方式進行損失補償，例如購買保險。

3. 評估與評鑑

主要強調有效的風險管理實施是組織必須持續的工作，並且需要持續進行風險評估與評鑑的功能，以營造一個完善的風險管理程序，風險之產生與發生原因均會依時間與環境的需要而有所不同，所以不斷的利用稽核評估機制是風險管理中不可缺少的一環。同時也由於對管理模式循環不斷的操作，才能有效控制、降低或避免風險的發生（劉智敏，民93）。評估或排列風險優先順序的方法，大致可分為定量風險分析（Quantitative Risk Analysis）和定性風險分析（Qualitative Risk Analysis），或者是兩者的組合。

（1）定量風險分析：運用數學模式計算，提出「事件發生的機率」及「可能造成的損失」，最常用到的方法即為對風險來源所發生之機率與所受之衝擊的分級制度（Ward 1999）。因而當企業要進行風險分析時，有六個步驟要逐一達成：

步驟1：資產鑑定，包含硬體、軟體、資料、人員、文件與週邊設備的鑑定。

步驟2：決定弱點，透過問卷調查的方式判定企業內所有可能的弱點來源。

步驟3：估計弱點會被利用的可能性，主觀決定步驟2所訂出之弱點會被利用的可能性。

步驟4：計算年度預期損失，透過簡單的機率計算，將資產價值（步驟1）乘以弱點可能被利用的機率值（步驟3），估算出整個企業之年預期損失金額。

步驟5：審視可用的控制以及控制的成本，選擇可用的控制機制降低弱點被利用的可能性，並評估每一項控制機制的成本是否符合效益。

步驟6：專案可節省年度損失，採用新的資訊安全控制機制，明確計算新控制專案為企業省下的損失金額。

（2）定性風險分析：依據管理者的判斷、直覺、經驗與業界的案例，利用德菲法、檢核表（Checklists）與訪談等方式，仔細觀察與分析描述風險發生的情形，再根據不同風險機率、威脅的嚴重性及資產的敏感性情境進行分析（Iheagwara 2003）。可知定性風險分析是利用嚴謹的程序作為評量資產價值及威脅的可能性，再以專家的知識與經驗描述進行風險分類，如高度、中度及低度等。定性風險分析的優點在於給予具有不確定本質的風險一個衡量準則，提供重大衝擊的測量，使其可運用在建議控制的成本效益分析作業；缺點是主觀判斷，對於層次的差距無法做一致性的界定。

參、研究方法

許多探討社會現象或政策制訂相關的研究，都採用質化方法進行質化資料的蒐集，原因在於許多現象或政策的考量是眾多因素共同影響，並且是自然發生、不能分割、無法重複、亦無法以實驗設計求證或推論，若採用不適當的方法分析質化資料，研究結果常會偏離現實，得到錯誤結論（Jones 1995）。為了維持事件原貌，以質化分析方法系統性的徵詢專家學者意見，以解釋現象、凝聚共識或形成假說，是社會科學常用的研究方法（Hoddinott and Pill 1997）。目前常採用的質化研究方法有深度訪談法（In-depth Interview Method）（Chapple and Rogers 1998）、焦點群體法（Focus Group Method）（Powell and Single 1996）、專家名義團體法（Nominal Group Method）（Malterud 2001）及德菲法（Gupta and Clarke 1996）等。其中深度訪談法是以面對面的方式進行探索性研究之資料蒐集，並非以預設問題進行探究，是要將研究主題更具體化的描述（Greenhalgh and Taylor 1997）。Goldman and McDonald（1987）指出焦點群體法主要是利用參與者間的互動討論激盪出豐富的討論內容，並且再利用所得的資料進行分析以萃取出研究者欲觀察的現象；Gallagher et al.（1993）指出專家名義團體法是針對非結構化的問題彙集專家群體，並以小組方式進行互動討論；而德菲法是利用專家團體意見推測不確定性事件的發生，透過特有的嚴謹研究程序整合與收斂專家們的意見，以得出更合宜的研究資料和結果（Rowe and Wright 1999）。因而本研究依研究目的和主題特性，採用德菲法進行資料收集和分析。

一、德菲法的定義與特徵

德菲法是運用於團體溝通的一種技術，允許專家能夠有系統地應付一項複雜的問題或任務，將一系列的問卷寄送給預先選定的專家小組成員，並向專家們諮詢意見（Kuo and Yu 1999; Mendoza and Prabhu 2000），在彼此匿名的情況下，進行數次的個別問卷調查。每次問卷調查後，再將分析結果與新的問卷分送給參與研究的專家學者，經過反覆實施，直到專家學者的意見差異降到最低為止。德菲法的進行具有三項主要的特徵（Rodriguez-Diaz 2000）：

（1）匿名（Anonymity）：因為專家學者的意見受到保密，可以無所顧忌表達自己的觀點，調查結果也較能反應真正的看法。

（2）反覆（Iteration）：由於問卷多次往返，具有相互激盪與啟發的效果，得到的結論也較為完善；並且在第二次以後的問卷，均提供專家學者上一回問卷的統計結果，參與者可以從中瞭解別人的想法，能啟發自己，並對自己原先的意見提出修正。

（3）回饋（Feedback）：每次問卷回收，即做簡單統計結果，讓專家學者獲知別人意見的訊息，讓所得到的結論更為接近問題的核心。

德菲法以匿名、反饋控制和統計回應描繪報告中之發現，對於探討與知識管理相關之議題是非常有幫助的工具（Saunders and Jones 1992; Liebowitz 1999; Dhaliwal and Tung 2000; Munier and Ronde 2001）；而在研究進行中一個良好的工具應要有足夠的信度與效度，在德菲法研究過程當中，因採重覆施行測驗並予以回饋控制，可以避免部分誤差變異的發生，所以在一連串反覆嚴謹程序中可說明德菲法具有穩定性（Stability）和一致性（Consistency）的信度，而反覆的步驟主要在凝聚與收斂專家團體們的意見，經由此測量工具的實行可以真正測出研究主題，所以在研究中運用德菲法，可具體說明其信度與效度可達相當水準（Grant and Kinney 2008; 林耀垣 民93）。

二、德菲法進行步驟

以德菲法進行資料分析與蒐集，主要的關鍵元素在於資訊流程建立、回饋給參加者與參加者一律匿名，所以德菲法主要經由十個步驟完成（Fowles 1976）：

步驟1：在指定的主題上組成一組團隊，以進行德菲法的流程。

步驟2：在研究領域中選定一組或更多組專家小組，而專家小組成員通常是此研究領域的專家。

步驟3：發展第一回的德菲法問卷。

步驟4：查看問卷的措辭是否恰當（例如去除模稜兩可或含糊的字眼）。

步驟5：將第一回的問卷發給專家小組參加者。

步驟6：對第一回的專家小組意見進行歸納綜合、分析。

步驟7：準備下一回的問卷（如果可能，可進行預測）。

步驟8：將下一回的問卷發給專家小組參加者。

步驟9：對下一回的專家小組意見進行歸納綜合、分析（重複步驟7到9，直到結果達到要求或必要的穩定性）。

步驟10：由統計分析的團隊準備一份結論報告書（吳俊儀，民94）。

三、德菲法受訪專家、共識指標與項目分數

本研究依據德菲法的定義與進行步驟選擇七位熟悉資訊安全標準與電腦稽核實務的專家學者，背景資料描述於表2。七位學者專家們的資訊安全標準實務經驗平均年資約為8.5年，電腦稽核經驗平均年資約為6.5年。

德菲法專家訪談過程中，通常使用統計與主觀認定兩種方式決定訪談專家在某一研究項目是否達成一致性之共識（de Meyrick 2003），統計方法常在決定每一回合訪談過程是否達成共識之收斂指標的標準差值（Fink 1995）；而主觀認定法則是以有三分之二（含）以上訪談專家於某一研究項目達成一致性之共識（Pasukeviciute and Roe 2001）。本研究的研究項目特質適合採用主觀認定法。因此，本研究定義達成一致性共識之指標有二項：第一，每一回合訪談過程中有三分之二（含）以上訪談專家接受該風險項目，則此風險項目不去除。第二，在每一回合訪談後該風險項目有三分之二（含）以上訪談專家分數相同，則認定此風險項目已達成一致性共識，不再列入下一回問卷中。最後，定性風險分析在第三回合達成一致性共識，定量風險分析在第五回合達成一致性共識。

表2：受訪專家學者背景描述（單位：年）

受訪人員	資訊安全標準經驗	電腦稽核經驗
銀行資訊安全科科長	11	7
銀行資訊安全科副科長	10	7
銀行稽核處電腦稽核員A君	10	10
銀行稽核處電腦稽核員B君	6	6
會計師事務所稽核員	5	5
資訊管理研究所教授C君	12	5
資訊管理研究所教授D君	6	6

四、定量風險分析之計算模式

資訊資產定量風險分析問卷建置是依據BS 7799-1：2000的四類定義進行，而風險分析步驟則依據ISO/IEC TR 13335-3：1998附錄E之風險分析方法型式計算。其中ISO/IEC TR 13335-3：1998附錄E之各項值是藉由德菲法整合學者專家的意見，對個案公司資訊資產提出風險項目和將資訊資產的重要性、弱點、可能遭受的攻擊和遭受攻擊後的影響給予量化，再達成一致性共識後，接者導出資訊資產的風險等級。而定量風險分析的風險估計值共有五大部份構成，計算值包含的項目以A～G表示，相關說明如本文之附錄所示。五大部份及其包含的項目描述如下：

（1）資訊資產重要性：分為機密性（以A表示）、完整性（以B表示）、可用性（以C表示）與依賴程度（以D表示）等四個重要特質表示。

（2）資訊資產威脅：說明威脅事件發生的來源與可能性（以E表示）。

（3）資訊資產弱點調查：說明脆弱性與等級（以F表示）。

（4）衝擊影響：威脅發生後的影響嚴重程度與嚴重程度（以G表示）。

（5）風險估計值與風險等級：風險估計值是依據前四項的乘積而得，在將乘積值依據風險等級對照標準表（以H表示），給予風險等級。計算公式為

Value＝MAX{A，B，C} × D × E × F × G，

而A～G則分別表示前四項經過德菲法分析後專家學者共識所得的值。

五、定性與定量風險分析之問卷項目選定

研究中問卷項目來源分別是以BS 7799-2：2002附錄A控制目標與控制措施A3到A12的十項控制領域作為定性風險分析的問卷標準，而由於各項目之子項目非常之多，受限於時間以及資料取得問題，本研究則無進行十項控制領域之子項目分析，且由於BS 7799已被國際標準組織明訂為重要的安全規範，因而在本研究中定性風險分析的控制措施A3到A12之十項控制領域就僅用BS7799-1：2002附錄A的控制目標為主，並且以此規範中的專有名詞為問卷之內容與文字編碼，以符合研究過程中資料分析的一致性且符合共通之標準。而BS 7799-1：2000對資訊資產的定義和ISO/IEC TR 13335-3：1998附錄E風險分析方法的型式，則作為定量風險分析的問卷標準，並且自個案公司資訊資產清冊中選取較易發生資安事件的資訊資產共有99項，但完成後的定量風險分析問卷浩繁，並且重要等級差異頗大，因而再與進行德菲法中的兩位專家進行多次討論，分別再由資訊資產清冊中選取具有代表性的十一類共24項資訊資產進行風險分析。其中十一類資訊資產的選取是依據BS 7799-1：2000的分類標準，包含有資料資產、軟體資產、實體資產與服務資產等，而24項的資訊資產主要是以銀行業日常運作過程中最主要也常使用到的資訊項目為主，同時也是銀行業資訊安全維護最重要的項目，包含應收帳款伺服器、網路銀行伺服器、信用卡系統伺服器、主路由器、大型主機、磁帶館與備份磁帶、系統文件、人員安全、個人電腦、軟體、安全管理設備等。在選取的過程中同時需要顧及資訊資產使用的重要性與調查的廣度；而兩位參與資訊資產十一類24項選定的專家，一位選自實務界資訊安全部門的資深主管，另一位則是來自學術界且於資訊安全耕耘多年研究卓越的學者。

肆、資訊資產的分類與風險評鑑分析

典型的風險分析方法分為定量風險分析與定性風險分析二種，前者適合公司規模較大者；反之，後者適合公司規模較小者。本研究為了將銀行業資訊資產風險評鑑系統化，使分析的過程與結果更具實用價值，此兩個模式皆採用，並以BS 7799-2：2002和ISO/IEC TR 13335-3：1998，做為定性與定量風險分析的問卷標準，再以美國國家技術標準局制定「資訊科技系統風險管理指導」之風險評鑑、風險降低以及評估與評鑑三項程序進行分析與描述，以使資訊資產具有明確分類後，可依據不同類別進行風險管理。藉由德菲法整合學者專家的意見後，進行資訊資產的風險等級說明，並對風險等級較高的項目提出建議改進措施。

一、定性風險分析調查結果

根據個案公司的資訊安全管理政策，研究中定性風險分析問卷依照BS 7799-2：2002之十項標題項目進行問卷設計後，再由學者專家對照BS 7799-1：2000要求的各項控制目標進行定性風險分析調查，並以美國國家技術標準局制定「資訊科技系統風險管理指

導」之風險評鑑及評估與評鑑步驟進行分析與描述。發現個案公司雖有明白宣示之安全政策，但其指標無法量化，以致於成效難以評估，且該公司規模龐大，但安全稽核人員不足，是為弱點；另外，門禁管制不確實，人員進出紊亂，應立即改善。可知，由定性風險分析發現的風險以組織管理層面居多，宜藉由改進資訊安全管理系統進行調整，研究中並由BS 7799-1：2000、BS 7799-2：2002和ISO/IEC TR 13335提出建議及改進措施，如表3中說明。

表3：定性風險分析調查結果說明與建議改進措施

風險說明	建議改進措施
項次：A.3/類別：安全政策。 威脅：安全政策有效性無法確認。 弱點：無可量化之安全目標。 說明：個案公司的資訊安全管理政策並無可量化之安全管理目標，難以評估資訊安全管理之有效性。	安全政策加入可量化目標，例如：每年執行緊急應變演練之次數，每年病毒事件最高次數限制等等。
項次：A.4 /類別：安全組織。 威脅：安全組織尚未建立完善。 弱點：資訊安全稽核人員不足。 說明：個案公司的安全組織尚在建立中，且缺乏相關資訊安全專業稽核人員。	導入更完整的資訊安全管理組織。
項次：A.5 /類別：資產分類與控制。 威脅：非實體性資產管理不良。 弱點：對非實體性資產沒有指定管理人員。 說明：對非實體性資產，如人員資產，目前沒有適當之管理方式。	指派專人負責保管所有資訊資產，包括軟硬體等實體資產，以及資訊文件、人員等項目。
項次：A.6 /類別：人員安全。 威脅：跨單位之系統或管理整合不良。 弱點：部分跨單位管理機制無專職人員。 說明：部分跨單位系統未指派專人負責，以致管理機制不佳，例如應收帳款系統。	建議增設以下工作執掌，並指派人員負責跨單位協調及管理工作。 1. 網路系統總管理員：負責整體網路設定和規劃，各網路安全設備（路由器、Switch、防火牆等）需更改設定時，各設備管理員須和網路系統總管理員充分討論和確認設定變更是否違反安全原則。 2. 文件管理員：負責保管資訊室所有資訊安全管理文件，包括各項程序書、標準作業流程等。 3. 程式原始碼管理人員：設計科應指派專人負責原始碼之保管。
項次：A.7 /類別：實體與環境安全。 威脅：人員進出混亂。 弱點：無單一出入門禁或專人管控管。 說明：資訊中心辦公區域為開放式空間，無門禁管制和專人控管，委外廠商和外部人員進出難以控管。	1. 改善委外廠商進出問題，修改廠商管理辦法及《委外服務管理程序書》。 2. 指派專人負責廠商初進入時登記、通知承辦人員及控管廠商在定點等候等工作。
項次：A.8 /類別：通訊與作業管理。 威脅：網路安全設備設定不一致，恐有漏洞產生。 弱點：無規劃整體網路系統人員。 說明：各種網路系統多已建置，各設備管理員對各自設備能確實管理，惟缺少負責規劃整體網路系統人員。	如A.6項建議：指派專人擔任網路系統總管理員，負責整體網路設定和規劃，各網路安全設備（路由器、Core Switch、防火牆等）要更改設定時，該設備管理員應知會網路系統總管理員，並充分討論和確認設定變更是否違反安全原則。

風險說明	建議改進措施
項次：A.9 /類別：存取控制 威脅：最高權限管理人員之人為錯誤或弊端。 弱點：缺乏對系統特權人員的監控機制。 說明：特權管理的機制較薄弱，管理人員均擁有最高權限，但無適當之監督管理機制。	1. 各系統主機之最高權限Administrator（或Root）應由系統管理員之主管控管，密碼不得提供給他人。另新增等同於最高權限之帳號給系統管理員和其代理人使用。 2. 系統主機管理員及代理人不可共享同一帳號。 3. 應用系統承辦人員不得擁有主機之管理權限。
項次：A.10 /類別：系統開發及維護。 威脅：原始碼遺失或版本錯誤。 弱點：原始碼集中管理機制。 說明：原始碼由各系統承辦人員負責管理，缺乏版本管制措施。	1. 在尚未使用原始碼進出管理系統之前，建議使用人工方式統一管理原始碼。 2. 設計科應指派專人擔任所有原始碼之管理工作，各承辦人員應將定版之程式原始碼及編譯後的執行碼交由該員管理。 3. 當應用系統需修改程式時，承辦人員應要求程式碼管理員取出正確程式碼，提供給程式開發人員修改。
項次：A.11 /類別：營運持續管理 威脅：安全事故發生時，營運中斷時間長。 弱點：跨單位應變協調機制和演練不足。 說明：缺乏營運持續性之計劃和演練。	1. 建立緊急應變及災害復原計畫，並定時演練。 2. 訂定年度計畫演練時程。
項次：A.12 /類別：符合性 威脅：資訊安全管理效果無法確認。 弱點：未明確執行內部稽核作業 說明：未明確規定執行內部稽核作業的時間週期與作法。	建立定期內部稽核制度，並按規定實施。

二、定量風險分析調查結果

定量風險分析問卷以BS 7799-1：2000定義作為資訊資產的分類標準，在風險分析方面則以ISO/IEC TR 13335-3：1998作為評估標準，並以美國國家技術標準局制定「資訊科技系統風險管理指導」原則之風險評鑑及評估與評鑑步驟，進行分析與描述，本研究由資訊資產清冊中選取具有代表性的十一類共24項資訊資產進行風險分析，分析資料分別以表4～14說明個別的風險等級，而各表中各子項目之威脅來源與脆弱性風險項目的內容訂定，則是依據七位專家經過五回合的德菲法問卷調查之共識形成後，所共同提出。如下分別描述十一類24項的資訊資產風險分析：

（1）應收帳款伺服器：屬於實體資產，系統包括軟/硬體及資料，是銀行業務中很重要的設備，安全威脅除了硬體故障外，主要是廠商及內部維護人員竊取客戶資料，應加強內部人員的管控。所以缺少技術純熟的技術備援人力，是該資訊資產最脆弱的地方，風險值估計為96；總體評之，其風險仍屬最低的第一級，如表4。至於風險等級之計算，請參照附錄之表H風險等級對照標準表。

（2）網路銀行伺服器：主要的威脅來自使用者身分認證，通行碼應經常更新以確保安全，防範未授權之資料存取與異動，總體資產風險等級為1，表示情形尚佳，如表5。

表4：應收帳款伺服器定量風險分析表

資訊資產相關資料	資訊資產重要性				威脅來源		脆弱性		衝擊影響	風險		資產風險等級
資產名額/資產類別	機密性	完整性	可用性	依賴程度	威脅	可能性	脆弱性	等級	嚴重程度	風險估計值	等級	
應收帳款伺服器/實體資產	2	2	2	2	委外廠商未遵守約定	1	機密性資料遭竊	2	2	16	1	1
	2	2	2	2	使用者操作失誤	1	不充足的資訊安全訓練	3	2	24	1	
	2	2	2	2	硬體設備損壞	1	維護及人力不足	2	2	16	1	
	2	2	2	2	人員短缺	3	缺少技術人力備授機制（技術純熟者）	4	2	96	1	
	2	2	2	2	系統紀錄損毀	1	缺少稽核程序	1	2	8	1	

表5：網路銀行伺服器定量風險分析表

資訊資產相關資料	資訊資產重要性				威脅來源		脆弱性		衝擊影響	風險		資產風險等級
資產名額/資產類別	機密性	完整性	可用性	依賴程度	威脅	可能性	脆弱性	等級	嚴重程度	風險估計值	等級	
網路銀行伺服器/實體資產	2	4	4	4	委外廠商未遵守約定	1	機密性資料遭竊	2	2	64	1	1
	2	4	4	4	使用者操作失誤	1	不充足的資訊安全訓練	2	2	64	1	
	2	4	4	4	硬體設備損壞	1	維護及人力不足	2	2	64	1	
	2	4	4	4	人員短缺	1	缺少技術人力備授機制（技術純熟者）	2	2	64	1	
	2	4	4	4	權限未做定期修正	1	未經授權的更改環境或資料	2	2	64	1	

（3）信用卡系統伺服器：主要的威脅是委外廠商竊取客戶資料、主機系統老舊和服務超載，如表6。

表6：信用卡系統伺服器定量風險分析表

資訊資產相關資料	資訊資產重要性				威脅來源		脆弱性		衝擊影響	風險		資產風險等級
資產名額/資產類別	機密性	完整性	可用性	依賴程度	威脅	可能性	脆弱性	等級	嚴重程度	風險估計值	等級	
信用卡系統伺服器/實體資產	2	4	4	4	委外廠商未遵守約定	1	機密性資料遭竊	2	2	64	1	1
	2	4	4	4	使用者操作失誤	1	不充足的資訊安全訓練	2	2	64	1	
	2	4	4	4	硬體設備損壞	1	維護及人力不足	2	2	64	1	
	2	4	4	4	人員短缺	2	缺少技術人力備援機制（技術純熟者）	2	2	128	2	
	2	2	2	2	服務超載	1	系統老舊	1	2	8	1	

（4）主路由器：含有防火牆與入侵偵測系統(Intrusion Detection System, IDS)皆屬於實體資產，是資訊中心連接銀行T3骨幹網路的通道，單一點的故障將使所有單位對資訊中心聯絡全部中斷，因此補救措施與路由器的設定特別重要，此風險等級被認定為第4級，如表7。

表7：主路由器定量風險分析表

資訊資產相關資料	資訊資產重要性				威脅來源		脆弱性		衝擊影響	風險		資產風險等級
資產名額資產類別管理者	機密性	完整性	可用性	依賴程度	威脅	可能性	脆弱性	等級	嚴重程度	風險估計值	等級	
主路由器CORE ROUTER/實體資產	3	3	5	5	網路安全設備失效	1	不充足的補救程序	3	2	150	2	4
	3	3	5	5	通訊網路服務中斷	2	單一點故障	2	3	300	4	
	3	3	5	5	設定錯誤	3	錯誤的規則	1	2	150	2	
防火牆/實體資產	2	2	2	2	備援機制失效	1	缺少永續計劃、程序與管理	2	2	16	1	1
	2	2	2	2	設定錯誤	1	錯誤的規則	2	2	16	1	
	2	2	2	2	硬體設備損壞	1	維護及人力不足	2	2	16	1	
	2	2	2	2	人員短缺	1	缺少技術人力備援機制（技術純熟者）	2	2	16	1	
IDS入侵偵測系統/實體資產	2	2	2	2	使用者操作失誤	1	不充足的資訊安全訓練	2	2	16	1	1
	2	2	2	2	設定錯誤	1	錯誤的規則	2	2	16	1	

（5）大型主機、磁碟陣列及不斷電系統：前兩者是銀行的核心系統，大型主機是用來保持存放款系統的正常運行，磁碟陣列則是儲存許多重要資料之處所，都是銀行高度依賴的設備，所幸都受到良好的保護，遭受威脅的可能性低，兩者共同的威脅是資料的保護不週延及技術人才的培養不足，大型主機尚須考慮系統負載的問題，至於該行的不斷電系統則屬可靠，如表8。

表8：大型主機、磁碟陣列及不斷電系統定量風險分析表

資訊資產相關資料	資訊資產重要性				威脅來源		脆弱性		衝擊影響	風險		資產風險等級
資產名額資產類別管理者	機密性	完整性	可用性	依賴程度	威脅	可能性	脆弱性	等級	嚴重程度	風險估計值	等級	
大型主機/實體資產	4	4	4	5	委外廠商未遵守約定	1	機密性資料遭竊	2	4	160	2	2
	4	4	4	5	使用者操作失誤	1	不充足的資訊安全訓練	2	4	160	2	
	4	4	4	5	人員短缺	1	缺少技術人力備援機制（技術純熟者）	2	4	160	2	
	4	4	4	5	系統容量超載	1	不充足的系統測試	2	4	160	2	
磁碟陣列/實體資產	4	4	4	5	資料未受保護	1	沒有加密保護	2	4	160	2	2
	4	4	4	5	使用者操作失誤	1	不充足的資訊安全訓練	2	4	160	2	
	4	4	4	5	人員短缺	1	缺少技術人力備援機制（技術純熟者）	2	4	160	2	
不斷電系統/實體資產	2	2	2	4	電力供應故障	2	不穩定的電力輸送模式	1	2	32	1	1

（6）磁帶館與備份磁帶：前者屬於實體資產，後者屬於資訊資產，磁帶館的硬體可靠性如果很好的話，風險較低；但備份磁帶的盜賣防護則特別重要，如表9。

表9：備份磁帶定量風險分析表

資訊資產相關資料	資訊資產重要性				威脅來源		脆弱性		衝擊影響	風險		資產風險等級
資產名額/資產類別	機密性	完整性	可用性	依賴程度	威脅	可能性	脆弱性	等級	嚴重程度	風險估計值	等級	
磁帶館(主要備份)/實體資產	2	2	2	2	硬體設備損壞	1	維護及人力不足	2	2	16	1	1
備份磁帶(台中備援中心)/資訊資產	4	5	1	2	資料外洩	1	管理者盜賣	5	4	200	3	3
	4	5	1	2	設備損壞	1	缺少週期性更新計劃	1	1	10	1	

（7）系統文件：含ZS-390操作手冊與設計一科系統文件皆屬於資訊資產，且以紙本呈現，有良好的儲存環境，因此風險等級不高，如表10。

表10：系統文件定量風險分析表

資訊資產相關資料	資訊資產重要性				威脅來源		脆弱性		衝擊影響	風險		資產風險等級
資產名額/資產類別	機密性	完整性	可用性	依賴程度	威脅	可能性	脆弱性	等級	嚴重程度	風險估計值	等級	
ZS-390操作手冊/資訊資產	2	2	2	2	無	1	無	1	1	4	1	1
設計一科系統文件/資訊資產	2	2	2	2	無	1	無	1	1	4	1	1

（8）人員安全：含有大型主機系統人員、大型主機程式人員與機房人員皆屬於資訊資產。主機系統管理人員及應用系統的開發人員盜賣風險是值得注意的，如表11。

（9）個人電腦：含有印表機與影印機屬於實體資產，其中印表機有資料被列印後外洩的風險，如表12。

（10）軟體：含有Windows XP、DB2、Symantec AntiVirus等皆屬於軟體資產，並且大都存在於光碟片中，只要本身程式無漏洞，風險不高，如表13。

表11：人員安全定量風險分析表

資訊資產相關資料	資訊資產重要性				威脅來源		脆弱性		衝擊影響	風險		資產風險等級
資產名額資產類別管理者	機密性	完整性	可用性	依賴程度	威脅	可能性	脆弱性	等級	嚴重程度	風險估計值	等級	
大型主機系統人員/資訊資產	4	3	3	3	資料外洩	1	使用者盜賣	5	4	240	3	3
	4	3	3	3	人員短缺	1	缺少技術人力備授機制（技術純熟者）	2	2	24	1	
大型主機程式人員/資訊資產	4	3	3	3	資料外洩	1	使用者盜賣	5	4	240	3	3
	4	3	3	3	人員短缺	1	缺少技術人力備授機制（技術純熟者）	2	2	24	1	
機房人員/資訊資產	2	2	2	2	使用者操作失誤	1	不充足的資訊安全訓練	3	2	24	1	1

表12：個人電腦定量風險分析表

資訊資產相關資料	資訊資產重要性				威脅來源		脆弱性		衝擊影響	風險		資產風險等級
資產名額資產類別管理者	機密性	完整性	可用性	依賴程度	威脅	可能性	脆弱性	等級	嚴重程度	風險估計值	等級	
個人電腦/實體資產	2	2	2	2	儲存媒體失效	1	未做備份	2	2	16	1	1
	2	2	2	2	使用者操作失誤	1	不充足的資訊安全訓練	3	2	24	1	
	2	2	2	2	惡意程式碼攻擊	1	系統程式漏洞	2	2	16	1	
印表機/實體資產	2	2	3	2	資料外洩	2	列印無限制	5	4	240	3	3
影印機/實體資產	2	2	3	2	資料外洩	1	列印無限制	5	4	120	2	2

表13：軟體定量風險分析表

資訊資產相關資料	資訊資產重要性				威脅來源		脆弱性		衝擊影響	風險		資產風險等級
資產名額資產類別管理者	機密性	完整性	可用性	依賴程度	威脅	可能性	脆弱性	等級	嚴重程度	風險估計值	等級	
Windows XP/軟體資產	2	2	2	2	惡意程式碼攻擊	1	系統程式漏洞	2	2	16	1	1
	2	2	2	2	使用者操作失誤	1	不充足的資訊安全訓練	2	2	16	1	
	2	2	2	2	硬體設備損壞	1	維護及人力不足	2	2	16	1	
DB2/軟體資產	2	2	2	2	使用者操作失誤	1	不充足的資訊安全訓練	2	2	16	1	1
	2	2	2	2	硬體設備損壞	1	維護及人力不足	2	2	16	1	
	2	2	2	2	人員短缺	2	缺少技術人力備授機制（技術純熟者）	2	2	16	1	
Symantec AntiVirus/軟體資產	2	2	2	2	軟體故障	1	不充足的系統劒試	2	2	16	1	1
	2	2	2	2	使用者操作失誤	1	不充足的資訊安全訓練	2	2	16	1	
	2	2	2	2	硬體設備損壞	1	維護及人力不足	2	2	16	1	
	2	2	2	2	人員短缺	2	缺少技術人力備授機制（技術純熟者）	2	2	16	1	

（11）安全管理設備：含有刷卡門禁系統與數位監視錄影系統是屬於服務資產，主要必須維持其功能的正常運作，以保護環境安全，可能的威脅是使用者操作失誤，脆弱之處在於督導與獎懲機制是否落實，如表14。

表14：安全管理設備定量風險分析表

資訊資產相關資料	資訊資產重要性				威脅來源		脆弱性		衝擊影響	風險		資產風險等級
資產名額/資產類別	機密性	完整性	可用性	依賴程度	威脅	可能性	脆弱性	等級	嚴重程度	風險估計值	等級	
刷卡門禁系統/服務資產	2	3	2	1	使用者操作失誤	2	缺少安全督導及獎懲機制	2	1	12	1	1
數位監視錄影系統/服務資產	2	2	2	1	使用者操作失誤	2	缺少安全督導及獎懲機制	2	1	8	1	1

三、定量風險分析建議及改進措施

經由學者專家仔細針對24項銀行業資訊資產進行風險評估，得到風險估計值與風險等級，如表4～14所示，研究中再將風險等級量化標準規定之級距1到9，依平均比例區分為低（1-3）、中（4-6）、高（7-9）風險，而24項資訊資產中風險等級為4的有主路由器1項，屬於中等風險，為3者有4項，為2者共4項，其餘的風險等級皆為1，皆屬於低風險，接著再以美國國家技術標準局制定「資訊科技系統風險管理指導」之風險降低原則，進行風險降低之建議與改進說明。

由以上的分析可以得知，目前個案公司資訊中心僅有主路由器之資訊資產受到較高風險的威脅，其可能遭受的問題為通訊網路中斷可能使整個銀行業務陷於停頓。學者專家對此風險提出建議與解決方案是增加主路由器之數量，並進行流量分析。而此個案公司中目前尚未有受到高風險威脅的資訊資產，研究中認為其原因在於資訊中心有設置資訊安全科，全職負責資訊安全的管理，使得資訊資產的風險值皆不高。雖然整體風險值不高，不過基於BS 7799-2：2002持續改善的原則，本研究認為還是應將風險值較高之項目轉移風險或降低，因此對風險值大於2之項目提出以下之改進措施，如表15所示，而其中除了主路由器外，其餘資產主要受到的威脅為資料外洩，原因皆出自於使用者的使用道德問題，受到外部不當的誘因將資料進行非法的轉售，成為安全管理的死角，因而增加對資料使用的管理與稽核，將可有效扼止不當使用與被盜用的問題。

表15：定量風險分析建議改進措施表

資產名稱	資產類別	威脅	弱點	風險估計值	資產風險等級	建議及改進措施
主路由器	實體資產	通訊網路服務中斷	單一點故障	300	4	增加路由器數量
大型主機系統人員	資訊資產	資料外洩	使用者盜賣	240	3	資料轉換為非原始資料
大型主機程式人員	資訊資產	資料外洩	使用者盜賣	240	3	資料轉換為非原始資料
備份磁帶	資訊資產	資料外洩	使用者盜賣	200	3	資料加密
印表機	實體資產	資料外洩	列印無限制	240	3	機密性資料無法列印

伍、結論

國際標準組織明定的資訊安全管理規範BS 7799-1：2000、7799-2：2002和ISO/IEC TR 13335為企業的資訊安全管理提供一份完整的參考指標，其目的就是要協助組織保護企業的資訊資產，但此一規範僅僅是提供一些原則性的建議，而不同的公司和產業會有不同的作法，才能有效的管理與稽核企業資訊資產的安全。截至目前能真正提出有效作法及持續落實的組織是少數，且執行的困難相當高。就以銀行業而言，因涉及太多個人的敏感資料與隱私問題，若要確實執行會有許多的障礙需克服。為了讓銀行業的資訊安全作法更具有成本及時間效益，減少因資料外洩造成無法彌補的損失，進行資訊資產的分類和風險評鑑是勢在必行。我們以美國國家技術標準局制定之「資訊科技系統風險管理指導」的風險降低原則，對資訊資產風險等級較高者提出控管與改進建議，有效提出解決因資料外洩而引發的種種問題與現象。因而在本研究中，建立了一套銀行業資訊資產分類與風險評鑑模式，此模式可提供給其他銀行業者參考，以及其他倚重資訊資產之產業一個遵循的依據，也是本研究對學術研究與實務影響最深之處。

在本研究中，我們首先將銀行業資訊資產依BS 7799-1：2000四大資產類型建立99項清冊，並分析銀行資訊安全管理政策，清楚說明威脅與弱點來源，提出建議改進措施；接著再分別針對資訊資產清冊中24項高風險群的設備評估其風險等級，同時提出改善方案，如此逐層抽絲剝繭的進行銀行業資訊資產分類與評鑑，得到以下三項的重要結果：

1. 資訊安全的評估方式很多，但同時以定性與定量的雙管道衡量方式進行資訊資產之風險分析則較為稀少。本研究以質與量並重方式進行分析是較能將無形之資訊資產轉換成易於控制與衡量的模式：量化之分析資料可使管理者較明確掌握風險等級與實際的影響程度，質化之分析資料則將風險發生的緣由清楚描繪，如此可以提供給管理者一個明確的判斷準則。
2. 依據本研究建立的分析步驟與過程，可以提供銀行業者一套嚴謹的遵循模式並且實際實行，不僅容易將資訊資產遭受的風險量化，同時對風險等級較高者提出控管與改進措施，以降低風險發生的機率與危害，對於重要性及機密性高的資訊資產提供一個更好的保護方式。所以此模式可具體化成為一般資訊資產分類與風險

分析和評鑑模式，協助各種產業進行資訊資產的風險管理。

3. 各種類型的資訊資產對銀行業者而言都是一種極其重要的資產，平日須持續做好妥善保護與管理，不讓資訊資產受到任何外界可以威脅與干擾的機會，確保組織營運的有效性，以及得到穩定的投資報酬率和商機。因而研究中將各項資訊資產易遭受到的威脅與弱點等說明，是提供管理者一個容易管理與降低風險的機制。

現實世界所發生的資訊安全的漏洞往往不是技術性上的問題，大部份是由內部使用者違反規定導致資訊安全的漏洞；所以加強人員管理及資料加密以保護資訊資產，成為銀行業者刻不容緩的工作。而資訊安全問題是備受各國關注的議題，本研究以國際標準的資訊安全管理規範分析國內大型銀行的資訊資產風險，對實務上的運作具有下列三點重要的意涵：

1. 透過資訊資產分類及風險等級評鑑量化表，讓資訊資產的威脅、弱點及風險能夠有更精確的呈現，並且此一等級評鑑量化表可以廣泛被使用在各行各業，以強化組織資訊資產之安全控管。
2. 並非所有資訊資產都具有相同價值，而保護資訊資產亦是需要投入相當大的時間、金錢、人力與物力等，所以企業透過評鑑資訊資產風險等級的高低，給予不同等級與適當性處理和管理，可以節省開銷，增加管理與維護上的效益。
3. 在競爭激烈的環境中，公司可使用的資源是非常的有限，當企業考量在資訊安全的投資時，可先從風險等級的角度著眼，以分析決定投資的方向及目標，可使公司的資源獲得更合理的分配。

由於銀行業資訊資產的研究闕如，本研究鉅細靡遺的呈現分析資料，是為了使業者能更清楚瞭解資訊資產的風險來源與重要性，以使銀行業者更能加以掌控風險問題與防範風險的發生。我們並且在完成分析後，請專家學者提出改善建議，這些具體的作法期望能對實務界可以產生參考之價值，以及未來可繼續耕耘的研究方向，有如下三點：

1. 由於研究中僅針對一家具代表性的銀行業者進行個案研究，無法進行個案間的綜合分析。因而本研究認為可於此研究之後，依據此研究得到的結果以及相關文獻的整理，再進行多家銀行業者之個案研究，並且藉由跨個案研究分析之精神與多重資料之驗證，將可再提出銀行業資訊資產管理機制及研究命題的具體結果，對於實務界將具有資訊資產管理與避險的實際幫助和實證參考之價值。
2. 由於在銀行產業少有研究進行資訊資產的分類與風險評鑑分析，所以本研究建立之模式可提供給其他業者導入組織中實際實行，並且將可在後續研究中進行實行此一模式的經驗分析，據此進行更深入的研究與探討實行的效益與價值評估。
3. 由於研究中以BS7799-2：2002附錄A控制目標與控制措施A3～A12十項控制領域的標題項目作為定性風險分析的問卷標準，而無進行各標題項目之子項目的調查，而此部份將可為後續進行更深入與詳細之研究的討論，以更臻獲得資訊資產之廣度與深度的研究。

最後，由於本研究的研究對象僅限於個案銀行之資訊中心，並未擴及到其總公司、國外分公司和國內300多家的營業單位。但資安事件不只在資訊中心發生，其它單位也會有發生的機會，因此未來研究可將範圍擴大到全公司，為組織各單位與部門進行總體檢，以便得到更完整的結果。另外，本研究只提供資訊資產分類及風險等級評鑑量化，許多有關於資安技術方面的資訊，礙於保密規定，並未能提供相關之資料；若未來研究可不必針對特定對象，可針對不同的資安技術進行風險評鑑之比較，將可獲得更廣範性研究結果。

誌謝

作者感謝二位匿名審查學者給予本論文諸多寶貴意見，使本論文內容更臻完善；本研究承蒙行政院國家科學委員會的經費支持，計畫編號：NSC 96-2416-H-036 -003 -MY2，謹致謝忱。

參考文獻

1. 王秀文，民94，一個針對共通作業環境中資訊資產風險評估模式，國立交通大學資訊管理研究所碩士論文。
2. 吳俊儀，民94，ISO9000知識創造模式之探討，國立成功大學工業與資訊管理研究所博士論文。
3. 林耀垣，民93，應用德菲法及資料包絡分析法於我國地方政府施政績效評估之研究，國立東華大學企業管理學系碩士論文。
4. 張芳珍，民94，以BS7799落實資訊安全管理－管理類資訊資產分類與控管，國立中央大學資訊管理研究所碩士論文。
5. 陳志誠，民92，『電子商務犯罪與偵防』，收錄於電子商務安全，吳宗成（編），168～189，台北：國科會科資中心。
6. 陳志誠、許派立，民95，『資訊資產分類管理與控制之研究-以金融業者為例』，資訊管理暨電子商務經營管理研討會，中華大學主辦，第22頁。
7. 劉智敏，民93，運用BS 7799 建構資訊安全風險管理指標，國立臺北大學企業管理學系碩士論文。
8. 鄭年華，民93，企業資訊安全風險評鑑模式之研究，輔仁大學資訊管理研究所碩士論文。
9. 蕭吉宏，民94，機敏軍事單位資訊安全風險分析之研究，元智大學資訊管理研究所碩士論文。
10. 瞿鴻斌，民93，資訊安全風險評估驗證系統，世新大學資訊管理研究所碩士論文。
11. BS 7799-1. *Code of Practice for Information Security Management*, British Standards Institution, 2000.

12. BS 7799-2. *Specification for Information Security Management Systems*, British Standards Institution, 2002.
13. Budgen, P.J. "Why Risk Analysis? Risk Analysis Methods and Tools," *Colloquium on IEEE* 1992, pp:2/1-2/4.
14. Chapple, A. and Rogers, A. "Explicit Guidelines for Qualitative Research: A Step in the Right Direction, a Defence of the Soft Option, or a Form of Sociological Imperialism?" *Family Practice* 1998, pp:556-561.
15. de Meyrick, J. "The Delphi Method and Health Research," *Health Education* (103:1), 2003, pp:7-16.
16. Dhaliwal, J.S. and Tung, L.L. "Using Group Support Systems for Developing Knowledge-Based Explanation Facility," *International Journal of Information Management* (20:2), 2000, pp:131-149.
17. Fink, D. "IS Security Issues for the 1990s: Implications for Management," *Journal of Systems Management* (46:2), 1995, pp:46-49.
18. Fowles, J. "An Overview of Social Forecasting Procedures," *Journal of the American Institute of Planners* (42:3), 1976, pp:253-263.
19. Gallagher, M., Hares, T., Spencer, J., Bradshaw, C. and Webb, I., "The Nominal Group Technique: A Research Tool for General Practice?" *Family Practice* (10:1), 1993, pp:76-81.
20. Goldman, A.E. and McDonald, S.S. *The Group Depth Interview: Principles & Practice*, Englewood Cliffs, NJ: Prentice Hall, 1987.
21. Grant, J.S. DSN, RN, CS and Kinney, M.R. DNSc, RN, FAAN "Using the Delphi Technique to Examine the Content Validity of Nursing Diagnoses," *International Journal of Nursing Terminologies and Classifications* (3:1), 2008, pp:12-22.
22. Greenhalgh, T. and Taylor, R. "Papers that go beyond numbers (qualitative research)," *British Medical Journal* (315:7110), 1997, pp:740-743.
23. Groom, P.D. "The IT Security Model," *Potentials IEEE* (22:4), 2003, pp:6-8.
24. Gupta, U.G. and Clarke, R.E. "Theory and Applications of the Delphi Technique: a Bibliography (1975-1994)," *Technological Forecasting and Social Change* 1996, pp:185-211.
25. Harris, S. J. "Proactive service management: Leveraging Telecom Information Assets for Competitive Advantage," *IEEE Network operations and management symposium* (3:15-19), 1996, pp:700-710.
26. Hoddinott, P. and Pill, R. "A Review of Recently Published Qualitative Research in General Practice: More Methodological Questions than Answers?" *Family Practice* 1997, pp:313-319.
27. Hoqqanvik, I. and Stolen, K. "Risk Analysis Terminology for IT-systems: Does it Match Intuition?" *Empirical Software Engineering 2005. 2005 International Symposium on*, pp:1-10.
28. Iheagwara, C. "More Effective Risk Assessment：Using Cascading Threat Multipliers for

Assessing Intrusion Detection Systems in Complex Infrastructures," *Computer Security Journal* (19:2), 2003, pp:8-20.

29. ISO/IEC TR 13335-1. *Information Technology-Guidelines for the Management of IT Security-Part 1：Concepts and Models for IT Security*, 1996.
30. ISO/IEC TR 13335-2. *Information Technology-Guidelines for the Management of IT Security-Part 2：Managing and Planning IT Security*, 1997.
31. ISO/IEC TR 13335-3. *Information Technology-Guidelines for the Management of IT Security-Part 3：Techniques for the Management of IT Security*, 1998.
32. ISO/IEC TR 13335-4. *Information Technology-Guidelines for the Management of IT Security-Part 4：Selection of Safeguards*, 2000.
33. ISO/IEC TR 13335-5. *Information Technology-Guidelines for the Management of IT Security-Part 5：Management Guidance on Network Security*, 2001.
34. ISO/IEC TR 17944. *Banking—Security and other Financial Services—Framework for Security in Financial Systems*, 2002.
35. Jones, R. "Why do Qualitative?" *British Medical Journal* (311:6996), 1995, p:2.
36. Kuo, N.W. and Yu, Y.H. "Policy and Practice: An Evaluation System for National Park Selection in Taiwan," *Journal of Environmental Planning and Management* (42:5), 1999, pp:735-745.
37. Liebowitz, J. "Key Ingredients to the Success of an Organization's Knowledge Management Strategy," *Knowledge and Process Management* (6:1), 1999, pp:37-40.
38. Malterud, Q.K. "Qualitative Research: Standards, Challenges, and Guidelines," *The Lancet* (358:9280), 2001, pp:483-488.
39. Mendoza, G.A. and Prabhu, R. "Development of a Methodology for Selecting Criteria and Indicators of Sustainable Forest Management: A Case Study of Participatory Assessment," *Environmental Management* (26:6), 2000, pp:659-673.
40. Munier, F. and Ronde, P. "The Role of Knowledge Codification in the Emergence of Consensus under Uncertainty: Empirical Analysis and Policy Implications," *Research Policy* (30:9), 2001, pp:1537-1551.
41. NIST. "National Institute of Standards and Technology, Risk Management Guide for Information Technology Systems," *Special Publication* (800:30), 2001.
42. Pasukeviciute, I. and Roe, M. "The Politics of Oil in Lithuania: Strategies after Transition," *Energy Policy* (26:3), 2001, pp:383-397.
43. Perna, J. "Leveraging the Information Asset," *Proceedings of the 1995 ACM SIGMOD international conference on Management of data* 1995, pp:451-452.
44. Powell, R., and Single, H. "Methodology Matters—V, Focus Group," *International Journal for Quality in Health Care* (8:5), 1996, pp:499-504.
45. Rodriguez-Diaz, A. J. "Globalisation and Technology Management in the Mexican Food Industry," *Industrial Management and Data Systems* (100:9), 2000, pp:430-435.

46. Rowe, G. and Wright G. "The Delphi Technique as a Forecasting Tool: Issues and Analysis," *International Journal of Forecasting* (15:4), 1999, pp:353-375.
47. Saunders, C.S. and Jones, J.W. "Measuring Performance of the Information System Function," *Journal of Management Information System* (8:4), 1992, pp:63-82.
48. Vorster, A. and Labuschagne, L. "A Framework for Comparing Different Information Security Risk Analysis Methodologies," *Proceedings of the 2005 Annual Research Conference of the South African Institute of Computer Scientists and Information Technologists on IT Research in Developing Countries* 2005, pp:95-103.
49. Ward, S.C. "Assessing and Managing Important Risks," *International Journal of Project Management* (17:6), 1999, pp:331-336.

附錄　德菲法（Delphi Method）問卷

一、研究目的：

這是一份以資訊安全管理之作業要點BS 7799-1：2000、資訊安全系統規範BS 7799-2：2002和資訊技術安全管理指導綱要ISO/IEC TR 13335為標準的問卷，目的是將資訊資產的重要性、弱點與可能遭受的攻擊和遭受攻擊後的影響給予量化，並導出資訊資產的風險等級，期望此一研究能幫助業者減少資安事件的發生。研究中並採用「德菲法」進行評估，主要是藉由此種介於問卷調查法與會議法之研究方法特質，由專家學者們進行幾回合的集思廣益與腦力激盪之重要資訊彙總。

二、填答方式：

定性風險分析表請您以自身所知（Knowledge）、經驗（Experience）及印象（Imagine）進行主觀判斷，分別填入風險威脅、弱點和說明；在定量風險分析表部份，本研究自個案公司資訊資產清冊中選取較易發生資安事件的資訊資產共99項，風險評鑑評估項目分為四類（資訊資產重要性、資訊資產威脅、資訊資產弱點調查和衝擊影響），共九個項目，並請參考說明一、說明二、說明三和說明四的數值為填答標準，進行主觀判斷，再針對每一項資訊資產寫入風險評估的九個項目，而每個資訊資產可寫入多筆風險事件。

說明一、資訊資產重要性：由各面向評估資訊資產對個案公司的重要性

1. 機密性（表A）：資訊資產之機密程度。
2. 完整性（表B）：資訊資產完整性要求等級。
3. 可用性（表C）：資訊資產可允許之停用時間。
4. 依賴程度（表D）：資訊資產對整體營運之依賴程度。

表A：機密性量化標準表

標準	等級	量化值
具機密性之資訊，未經核定洩露後，足以使個案公司受到最嚴重損害者，僅個案公司管理階層人員可閱覽。	極機密	5
具機密性之資訊，非業務需求不得隨意閱覽。	機密	4
不具機密性之資訊，但非業務需求不得隨意閱覽。	敏感	3
資訊限個案公司內部人員使用，不得隨意公開與外人者。	內閱	2
無特殊要求，且內容可公開出示他人者。	普通	1

表B：完整性量化標準表

標準	等級	量化值
該設備資訊需完整一致不允許誤差存在；或資訊或設備內容稍微不完整時，會使作業完全停頓，足使個案公司受到最嚴重損害者，並使個案公司存續產生問題者。	極高	5
可允許設備資訊不一致但只允許較小的誤差值；資訊或設備內容不完整時，會使作業停頓，並產生客訴事件，足以使個案公司受到嚴重損害者。	高	4
可允許設備資訊不一致具有較大的誤差；或資訊或設備內容不完整時，會造成工作上的不便，會產生部分人員的抱怨或造成損害者。	中	3
可單機作業；或資訊或設備內容不完整時，僅會造成工作上的困擾，不至造成損害者。	低	2
無特殊要求，資訊或設備內容不完整時，對作業無任何影響。	無	1

表C：可用性量化標準表

標準	等級	量化值
凡某種文件、書籍、資料、圖表、照相或器材，僅容許極短暫時間（30分鐘）無法使用，否則會使公司受到最嚴重損害者。	極高	5
凡某種文件、書籍、資料、圖表、照相或器材，僅容許短時間（4小時）無法使用，作業停頓期間，極易產生客訴事件。	高	4
凡某種文件、書籍、資料、圖表、照相或器材，容許較長時間（1日內）無法使用，會造成部份人員抱怨。	中	3
凡某種文件、書籍、資料、圖表、照相或器材，容許長時間（1週內）無法使用，作業停頓間可利用其他替代方案，不至造成公司之損失。	低	2
無特殊要求，容許超過1週以上之修復時間。	無	1

表D：依賴程度量化標準表

標準	等級	量化值
當該資產損害時，會致使個案公司業務立即停止營運，影響使用者甚鉅，是維持公司存續之主要項目。	超高	5
當資產損害時，會致使公司大部分業務無法營運，影響使用者，且會有嚴重抱怨。	極高	4
當資產損害時，會致使公司部分業務無法營運，使用者會產生抱怨。	高	3
當資產損害時，雖不會影響到公司營運，但會產生管理困擾，但不會影響使用者。	中	2
當資產管理損害時，不會影響到公司營運，僅會產生輕微管理困擾，但不會影響使用者。	低	1

說明二、資訊資產威脅：威脅事件發生機率

1. 威脅：資訊資產威脅來源。
2. 可能性（表E）：威脅事件發生機率。

表E：威脅事件發生可能性量化標準表

標準	威脅可能發生的機率	等級	量化值
每週發生一次以上	90%以上	非常高	5
每月發生三次以下	75%	高	4
每季發生兩次以下	50%	中	3
每年發生三次以下	25%	低	2
三年發生兩次以下	10%	非常低	1

說明三、資訊資產弱點調查：現行管制方法下，弱點發生的可能性

1. 脆弱性：資訊資產弱點所在。
2. 等級（表F）：現行管制方法下，弱點發生的可能性。

表F：弱點發生可能性量化標準表

標準	弱點可能發生的機率	等級	量化值
無管制措施	90%以上	非常高	5
管控效果不彰	75%	高	4
管控差強人意	50%	中	3
管控措施可接受	25%	低	2
管控措施良好	10%	非常低	1

說明四、衝擊影響：威脅發生後所造成的影響嚴重程度

1. 嚴重程度（表G）：威脅發生後對整體營運造成之衝擊程度。

表G：威脅影響程度量化標準表

嚴重程度	等級	量化值
造成生命損失或影響個案公司存續	非常高	5
單位主要業務窒礙難行	高	4
單位業務運行困難	中	3
部門業務遭受阻礙	低	2
個人工作受到干擾	非常低	1

說明五、評估完成後，吾人會依據以下公式算出風險估計值，並給予風險等級

1. 風險估計值＝MAX{A，B，C} × D × E × F × G。
2. 風險估計值依據風險等級對照標準（表H），給予每項資訊資產1個評估後的風險等級。

表H：風險等級對照標準表

風險估計值	等級
0~99	1
100~199	2
200~299	3
300~399	4
400~499	5
500~599	6
600~699	7
700~799	8
800以上	9

說明六、定性風險分析表範例

項次	類別	風險說明
A.3	安全政策	威脅：沒有具體的安全政策。 弱點：沒有資訊安全管理目標。 說明：個案公司沒有資訊安全管理政策，也沒有資訊安全管理目標，無法評估資訊安全管理。

說明七、定量風險分析表範例

資訊資產相關資料	資訊資產重要性				威脅來源		脆弱性		衝擊影響	風險		資產風險等級
資產名額/資產類別	機密性	完整性	可用性	依賴程度	威脅	可能性	脆弱性	等級	嚴重程度	風險估計值	等級	
大型主機/實體資產	4	5	1	2	系統超載	1	設備損壞	5	4			
	4	5	4	4	無定期更新計劃	1	無人維護	4	4			