## 壹、前言

此次奉派至美國地區研習該國金融監理機構對電腦作業之檢查，為期三週，期間拜會聯邦準備理事會、財政部金融局、聯邦存款保險公司、聯邦準備銀行紐約分行、紐約州政府銀行局等金融監理機關，及中國國際商銀、第一銀行及彰化銀行等本國銀行之紐約分行，並隨台灣金融研訓院之海外參訪團拜訪花旗銀行總行(citi corp.)，另與本行謝人俊專員拜訪紐約銀行總行(Bank of New York)，對瞭解該國電腦稽核現況與未來發展，以及擴大國際金融視野，獲益良多。

近年來，該國一直強調以風險為基礎(Risk-based focus)的監理方式，對一般財務業務稽核(Safety and Soundness Examination)如此，對電腦稽核(BIS, Bank Information Systems Examinations)亦復如是。該國各監理單位間之協調合作機制、電腦稽核人員之培訓、檢查程序及其內容、均有可供我國借鏡之處。尤其近年來隨著科技的快速發展，透過開放式公共網路辦理網路銀行業務如雨後春筍般紛至沓來，對其發展的現況以及未來的趨勢，均可參考他國經驗，作為我國制訂相關法令規章之參考。

## 貳、金融監理機構檢查分工情形

美國聯邦金融監理機構計有四個，州政府銀行局亦有核發營業執照及檢查之權力，各監理單位負責監理的金融機構類別分述如下：

榮聯邦準備理事會(FRB, Board of Governors of the Federal Reserve System)，除設有檢查科之外，其檢查業務係由轄下之聯邦準備銀行十二家分行辦理，檢查單位包括屬聯邦會員之州註冊銀行(State-Chartered Bank)、銀行控股公司(Bank Holding Company)以及其非銀行之子公司（如保險公司、經紀商）、艾奇法公司(Edge Act and agreement corporations)、外國銀行在美國之分行或代表處以及其母行。

㠯財政部金融局(OCC, Office of the Comptroller of the Currency )檢查單位包括國家銀行（National banks, 即聯邦註冊銀行）、外國銀行聯邦註冊分行及代表處(Federal branches and agencies of foreign banks)以及銀行關聯機構(IAPs, Institution-affiliated parties)。

㠰聯邦存款保險公司(FDIC, Federal Deposit Insurance Corporate) 檢查單位包括非聯邦會員之州註冊銀行以及參加聯邦存款保險之外國銀行在美國之分行。

㠱儲貸協會監理局(OTS, Office of Thrift Supervision)檢查單位為儲貸機構（Thrift institutions）

㠲州銀行局(State Banking Department)檢查單位為州註冊之銀行、信託公司(trust company)、儲蓄銀行(savings bank)、投資公司(Investment company)及外商銀行(Foreign Banking Institution)。

為因應近年來監理政策的改變，如改以風險為基礎的檢查方式與持續監理程序，聯邦準備銀行紐約分行與紐約州銀行局不約而同在 2000 年 7 月變更其金融監理部門組織架構。以聯邦準備銀行紐約分行為例，變更後的組織，在金融監理群(Bank Supervision Group)之下，設立政策運用(Policy and Application)、風險管理(Risk Manage-ment)、公共關係(Relationship Management)與人事總務(Resource and Logistics Management)等部門，其中風險管理部門職司檢查業務，又分為市場與流動性風險、作業風險、信用風險、銀行營運趨勢、法律風險、及保險風險等六個小組；對於資訊科技發展之現況（如金融機構採用之套裝軟體、作業系統、新種技術…等），則由政策運用部門之下的政策分析小組負責研究分析，並不定期提出報告供資訊作業檢查人員參考，如有必要，亦會召集檢查人員進一步說明在檢查該系統（或軟體）時之檢查技巧及應注意之潛在風險。

## 參、檢查頻率、人力

在檢查頻率方面，依據 OCC 之檢查手冊(Bank Supervision

Process Comptroller's Handbook)，以國家銀行為例，原則上電腦作業檢查頻率與一般財務業務檢查相同且同時進行，亦即每 12 個月或 18 個月檢查一次。對屬於複合區域資料處理服務者(MDPS, Multiregional Data Processing Servicers)之獨立資料中心，其檢查頻率則依聯邦金融機構檢查委員會(FFIEC, Federal Financial Institution Exami-nation Council)之評等系統評定結果而定，通常為每 12 個月、18 個月或 24 個月檢查一次，非屬 MDPS 之資料中心則每 12 個月檢查一次。

在檢查人力方面，在走訪之五個監理機構中，電腦稽核人員普遍不足，且多由財務業務稽核人員轉任或兼任，以電腦稽核人員比例最高的聯邦準備銀行為例，全部約 450 名檢查人員中，電腦稽核人員約有 60 名。電腦稽核人員在正式執行電腦作業檢查之前，會給予相當的訓練，也鼓勵其取得電腦稽核協會(ISACA)核發之電腦稽核師執照(CISA)，其後並不定期選送參加相關訓練課程。

## 肆、檢查程序及內容

㈠檢查前會發送受檢單位準備資料清單(First day Letter)，以聯邦銀行紐約分行資料為例，清單內容包括：

㈡內部及外部稽核(Internal and External Audit)：

本年度及下一年度內部稽核計畫及內部稽核作業手冊；自上次檢查結束後，截至目前為止與資訊作業有關之內部稽核報告與會計師報告書影本；電腦稽核人員及主管人數、簡歷清單；若採用電腦稽核軟體，請提供軟體計畫名稱、作者、目的、使用頻率、申請紀錄等。

㈢組織架構(Organization)：

全公司之組織圖，包括董事會、高階經營管理部門及資深技術管理部門監控與技術相關業務單位；自上次檢查結束後任何計畫或技術之改變，如應用系統、資料庫管理系統、

全球資料中心、網路架構、資訊安全、緊急應變計畫等，及技術顧問曾經對任何與科技有關業務之審視紀錄或報告；技術策略與長、短期計畫；較常變動之政策、程序、準則以及變動較頻繁的日期等之清單；提供技術服務之金融機構清單。

㈡基礎設備(Infrastructure)：

提供全球資料中心清單，註明：㈠每一單位目前使用的中央處理器(CPU)名稱（包括製造廠商、機型、磁碟容量等），係租用或自購、作業系統版本、重要系統軟體（如網路、資料安全軟體）等；㈡主要簽約廠商名稱及聯絡電話；㈢佈線方式（Topology Diagram）係屬當地、區域或全球網路；㈣現有或計畫中的區域網路(LAN)或廣域網路(WAN)說明（包括每一位網路管理員的聯絡電話）以及網路的作業系統、採用之通訊協定與網路管理工具，並描述其認證、授權、存取控制架構以及對敏感性較高資料之保護方式；㈤網路政策與程序，包括邏輯與實體安全、系統管理與操作、應變計畫與災變復原、通訊安全、使用者教育與訓練、遠端連線、變更管理等；㈥處理重要應用程式之獨立（Stand-alone）微電腦清單，並記載應用系統名稱與使用之軟體；㈦提供政策、程序與標準涵蓋微電腦之採購、程式撰寫、安全以及應變計畫。

㈢完整性(Integrity)：

提供自動化資訊系統架構圖（包括全部軟硬體設備），自行開發或委外開發之應用系統清單，並描述每一系統使用之作業平台與程式語言，以及負責維護單位名稱；委外開發軟體的廠商名稱、地址、聯絡人與目前維護情形；敘明所有作業平台之程式修改程序，若為委外修改，則描述其修改步驟；每一作業平台程式變更控制準則之名稱；涵蓋系統開發方式與程式變更控制的系統與程式功能作業準

則，並說明如何確保遵守法規；概述各資料庫管理系統狀況及各系統間之關係，提供每一個資料庫系統的管理員姓名與聯絡電話、系統管理方式及未來計畫，並說明其安全架構；自上次檢查結束後迄今，曾經設計系統或撰寫程式之軟體公司與簽約程式員清單；說明外部資源的評估方法及費用支出情形及內、外部資源的比率；出售給其他金融機構的軟體清單，簡單描述軟體名稱、用途，及保管客戶清單的負責人姓名及電話。

艹可行性(Availability)：

資訊技術部門之應變計畫影本，資料中心與應用程式發生當機時之資料處理替代地點、其作業主機之製造廠商、中心容量、作業系統名稱、版本、重要系統軟體、與資料中心之距離、以及自上次檢查結束後迄今進行測試的紀錄與結果；資料處理替代設施之協議書（假如有的話）；異地儲存程式、文件以及資料檔案備份地點之名稱與地址，並提供異地儲存計畫（包括記錄之型態、頻率與保存期限）。

弟安全性(Secrity)：

資訊安全計畫影本（包括資料、實體設備、通訊、網路、作業系統、網際網路與最終使用者安全以及書面政策、準則、指導原則及程序）；資訊安全部門之組織圖，註明資料安全管理單位、名稱及所在地以及管理員姓名、該部門有權人員及職員人數；每一硬體平台，涵蓋安全監督、違規及入侵偵測（包括網路系統）、存取重驗證(Access Recertification)等項目之資源、頻率及分配報告清單；外部會計師或顧問對資訊安全環境（如強度測試）的審查報告影本；執行每一硬體平台之建置或移除權限等管理程序時所需文件樣例。

茎網際網路/先進技術：

描述目前維護網際網路或內部網路或外部網路連結之情

形，提供防火牆架構系統圖並予說明；涵蓋網際網路存取權限、使用、內容、變更控制、安全性與開發等項目之政策、程序與標準作業手冊；對現行諸如電子商務、智慧卡、資料倉儲(Data Warehousing)等技術使用情形之說明；條列與網際網路、電子商務等有關外界廠商資料；描述採用新科技之動機與實際使用的過程；督導網際網路活動的委員會及其成員名單；與網際網路有關之外界服務提供者及顧問名單；對於關切網際網路及先進技術的高階管理階層及董事會所提簡報內容。

查開始檢查時，檢查程序及內容多依據聯邦金融機構檢查委員會(FFIEC, Federal Financial Institution Examination Council)於1996 年頒佈之資訊系統檢查手冊(Information System Examination Handbook,分為上、下二冊)，至於近年因科技發展快速而產生的「虛擬」銀行業務，如透過公用網路系統連結客戶與銀行主機的電子銀行或網路銀行業務，則以財政部金融局於 1999 年 10 月訂定之「網路銀行檢查手冊」（Internet Banking Comptroller's Handbook）為主，本文段將先敘述 FFIEC 檢查手冊主要內容：

並第一部分概論及管理，共有七章，第一章為簡介；第二章主要介紹以風險為主的資訊系統監理計劃及風險定義、分析與監理策略；第三章敘述檢查規劃，包括檢查型式、頻率、時間、資料蒐集、檢查範圍、工作協調及通知；第四章論述檢查技術，包括實地檢查程序、時間與預算、工作底稿之格式與覆核、檢查結果備忘記錄與彙總、檢討會、檢查報告及服務提供者報告之發送及改善通知;第五章介紹資訊系統檢查評等作業;第六章介紹多區域資料處理服務者(MDPS, Multiregional Data Processing Servicer)計畫；第七章討論共用應用軟體覆核 (SASR, Shared Application Software Review) 計畫。

芓第二部分--監理工具自第八章至第二十三章，第八章係論述內部、外部稽核之政策、角色、程序及功能；第九章敘述受檢機構資訊單位在組織、計劃、控制、財務分析、保險、管理評估、管理資訊系統、資料處理外包、系統轉換、先進技術、網際網路、主從架構(client/server)系統、電子影像(electronic image)系統、電子資料交換(EDI, electronic data interchange)等方面之管理情形；第十章說明緊急應變計劃之責任、組織計劃準則、備援與緊急應變計劃之關係、資訊系統緊急應變計劃、對抗實體災害與其他災害之維護措施、以及包括硬體、程式、軟體、資料檔案及通訊設備之備份、保險；第十一章探討管理資訊系統之覆核、與 MIS 有關之風險、評估 MIS 風險之弱點及重新檢視 MIS 之內容；第十二章敘述系統發展與程式撰寫，說明專案管理、系統發展標準、軟體購買、程式撰寫標準、測試標準、系統執行、軟體維護、軟體系統整合、作業系統、程式安全、文件標準、應用軟體文件、文件維護、使用者操作手冊、購買軟體文件、資料庫管理系統及電腦輔助軟體工程(Computer-Aided Software Engineering)；第十三章說明與操作有關之責任劃分與輪調、設備維護與操作及控制、備份作業、操作員控管、程式館控管、資料檔案媒體控管、環境整潔、緊急程序、交易處理、交易資料輸入、批次作業結果驗對與借(貸)方餘額控管(Batch Proof and Balancing Control)、終端機輸入（輸出）資料分送與控制、輸出資料之覆核與彙整；第十四章敘述實體與資料安全，包括安全管理與帳戶權限管理(accountability)、安全規劃、使用者教育、實體設備與建物及金庫（櫃）的安全性、個人電腦及資訊系統環境安全、人員與資料檔案媒體及電腦操作安全性、軟硬體存貨、資料安全性、邏輯存取安全與控制、程式安全、資料完整性、通訊安全與存取控制、傳輸控制、

電腦病毒；第十五章論述與主從架構網路系統有關之網路架構（設備）、邏輯模型、其他通訊協定及標準、資料傳輸、主機設備、外界連接、通訊媒體與傳送單位(carriers)、網路結構(configurations)、網路管理、商業網路服務、其他通訊、政策與程序、網路安全、災變回復、法規標準(Legally Enforceable Standard)、風險與控制、主從架構之簡介與背景、高階管理階層的角色、主從架構網路系統定義、主從架構的要件與特性、意見與建議；第十六章則談到最終使用者使用之電腦設備(End-user computing)，包括使用要點及標準、軟硬體選擇、操作、災變復原或應變計畫、網路與電訊、小型系統、風險與控制考量、安全性、電腦操作、上線與維護、系統軟體、資料庫管理軟體、中介軟體(middleware)；第十七章敘述文件圖像定義、背景、控制與安全風險區域、系統元件、利基、風險、執行；第十八章整批電子資金移轉，探討整批或大額資金移轉系統、支付移轉風險控制、檢查要點、洗錢與線上移轉議題(money laundering and wire transfer issues)、銀行秘密法(BSA, Bank Secrecy Act)對資金移轉紀錄之保存規定、線上移轉控制考量、線上移轉訊息、國際性強化(International Enforcement)、外匯資產管制署(OFAC, The Office of Foreign Asset Controls)；第十九章聯邦網路電子資金移轉，包括當地安全管理人員(Local Security Administor)、各項安全設定、使用者/存取報告評估、覆核範圍(verification field)、覆核開端(verification threshold)、一般控制、災變/應變、聯邦網路線上移轉功能；第二十章消費性電子資金移轉（自動提款機與銷售點服務），包括自動提款機(ATM, Automated Teller Machine)、銷售點服務(POS, Point-of-Sale)、轉帳卡(Debit Card)及智慧卡、家庭銀行(Home Banking)、消費性電子資金移轉之內部控制、個人識別碼(PIN, Personal Identification

Number)控制準則、塑膠卡控制準則、端末分享及網路切換；第二十一章票據交換所，敘述票據交換業務之成長、操作員及風險與檢查要點；第二十二章資訊系統服務—供應者與接受者，使用單位控制、技術控制、使用單位與服務提供者之保險、記錄保護與使用機構之保存、契約、契約指導（inducement）要點、使用單位與服務者之金融資訊、服務接受者之考量、潛在服務提供者議題、潛在服務接受者議題；第二十三章社區銀行電腦稽核計畫，包括社區（銀行）工作計畫、簡介、購買比率(Rationale for Acquisition)、系統需求評估、可行性研究、軟硬體要點、資料轉換、服務契約、災害/應變計畫、後續議題與要點、檢查程序。

㈡第三部分為法律與政策，第二十四章為法律與規定之概述第二十五章至第三十章則為聯邦金融機構檢查委員會與聯邦存款保險公司、聯邦準備理事會、國家聯合信用管理協會、財政部金融局、儲貸協會監理署等各監理單位相關政策。

㈢第四部分為其他參考資料與工具

因檢查前的各項準備工作，如蒐集受檢單位相關資料、發送檢查資料清單等方式與財務業務查核之方式並無不同，本報告擬針對實地檢查程序及檢查評等內容詳述如下：

㈠實地檢查程序方面，電腦稽核領隊必須確保檢查內容與檢查目標及範圍一致，助檢人員在完成檢查後，除在檢查項目工作底稿(workprogram)填寫評註外，也要蒐集資訊以驗證其檢查結果，所有的結論必須記載與保存於工作底稿並送交領隊人員覆核。為控制檢查的水準，領隊必須採取下列措施：

㈠於檢查開始時，會見資深資訊部門人員；

㈡請助檢人員檢視受檢單位提供資料與檢查資料清單所

列項目是否相符；

㜷如有必要，調整檢查範圍；

㛹假如預期檢查範圍、檢查人力及期間會有重大改變，應通知檢查機關電腦稽核主管及財務業務稽核領隊人員；

㛺確定已收到管理部門提供之資料，並立刻分送有關人員；

㛻在整個檢查過程中，持續瞭解工作進度、缺失評註、結論與掌握預定檢查期間，以有效利用檢查時間；與助檢、檢查機關電腦稽核主管及財務業務稽核領隊人員討論所有重要項目，以期在檢討會時有正確之資料；檢查期間若有重要意見，須讓受檢單位高階與資訊部門管理者瞭解；依據檢查計畫、工作底稿、結論備註、評註草稿以及時間表，確定所有檢查工作已按照監理政策進行；覆核已經完成之檢查工作，包括檢查計畫部分、結論備忘記錄、評註草稿及報告內容；在正式檢討會之前，先與受檢單位管理部門討論溝通會議內容；

㛼參與受檢單位董事會議；

㛽如果分別檢查金融機構與資訊服務提供單位，仍須準備資料，安排與資訊作業管理部門之檢討會；

㛾通知適當人員（如金融機構與資訊服務提供單位管理部門、檢查單位主管等）召開檢討會之日期、時間與地點；

㜀如有必要，要求受檢單位總經理(CEO,Chief Executive Officer)在下一次董事會就檢查結果提出簡報；

㜁假如可行，對管理方式提出建議；

㜂以’Camera Ready’格式完成電腦稽核報告草稿，同時分送檢查機構電腦稽核部門主管與財務業務稽核領隊人

員；

㈩與覆核評註合併，並將報告分送檢查機構電腦稽核部門主管與財務業務稽核領隊人員。

㈠資訊技術統一評等系統(URSIT, Uniform Rating System of Information Technology )係由 FFIEC 於 1999 年 1 月發佈，並於 4 月 1 日啟用，該系統係以風險評估為基礎，包括稽核 (Audit)、管理 (Management)、系統發展與購置 (Development and Acquisition)及支援與傳送(Support and Delivery)等四個評等項目。適用對象為金融機構與服務提供廠商。該系統前身為 1978 年 10 月之資訊系統評等制度 (Information System Rating System)，由於近年科技快速發展以及監理政策與監理程序的改變，因此 FFIEC 乃配合此一趨勢，修訂該評等制度內容，並更改其名稱。在評等項目方面，刪除「系統發展與程式設計」(Systems Development and Programming)及「作業」(Operation)兩項，增加「系統發展與購置」及「支援與傳送」。並特別強調風險管理作業的品質，明確指出各評等項目之風險型態；其評等方式類似「統一銀行評等系統」(Uniform Interagency Bank Rating System)，各監理機關之電腦稽核人員先依據四個評估項目，分別給予評等(Component Rating)，然後將四項評等彙總產生綜合評等(Composite Rating)。評定之等級共分為五級，第一級最佳，表示資訊中心(Data Center)之運作相當健全，即使有極小缺失，亦為該銀行可予控制者，在風險管理方面，則配合組織規模、業務複雜程度及各項風險組合，訂定足以辨認及控制風險的完善計畫，管理階層可以對變動中的市場、業務及技術需求迅速採取行動，對稽核及監理單位提出的任何問題，也可以馬上瞭解並即刻改正。對服務提供者(Service Providers)而言，則意味其財務狀況良好，整體表現亦讓監理單位無話可說；若評為第二

級，表示金融機構及服務提供者的各項作業尚屬穩健，但在操作績效、監督、管理程序及系統開發方面有中等程度的弱點，各項缺失可以在不影響正常營運情形下改正，風險管理作業尚能配合組織規模、業務複雜程度及各項風險組合，辨認及控制風險，策略計畫雖予定義，但需加以適當分類、組織之協調性或內部溝通模式仍待加強。管理階層雖然參與各項決策，但對於變化中的市場、業務及技術需求無法立即採取行動，對於稽核及監理單位提出的問題尚能瞭解，並採取適當的改進措施。但是較依賴稽核及監理單位予以協助始能順利提出解決方案。在服務提供者方面，則表示其財務狀況尚可，但可能在內部控制方面存在部分弱點，惟無重大缺失，監理機關採取之行動較為溫和；若屬第三級，表示監理單位在彙總各項從中度到嚴重程度不等之缺失後，會對金融機構及服務提供者提出意見要求改善，假如缺失持續存在，可能進而損及金融機構或服務提供者之財務狀況及營業績效。風險管理作業未能配合組織規模、業務複雜程度及各項風險組合，有效辨認及控制風險，對策略計畫之定義亦欠明確，以致在利用資訊技術之初，無法提出正確方向，而管理階層則難以對於變化中的市場、業務及技術需求採取行動，自我評估實務不良造成稽核及監理單位時而採取例外的查核行動。稽核單位一再重複提出的意見顯示管理單位似乎缺乏改善的能力或意願。服務提供者之財務狀況欠佳，或營業狀況日益惡化，惟財務及營運尚不致有倒閉之虞，但是必須加強正式或非正式的監理以確保改正措施之有效；評為第四級則認為金融機構及服務提供者處於不健全之作業環境，可能損害往後的生存能力。各項作業的弱點顯示出管理上有嚴重瑕疵，而風險管理作業未能配合組織規模、業務複雜程度及各項風險組合，以辨認及控制風險，策略計畫定義不

明，且缺乏內部協調或溝通，因此管理階層與理事會無法或無力確保符合技術需求。管理階層未實施自我評估，亦缺乏改正稽核及監理單位所提問題之能力或意願，而服務提供者之財務狀況已遭嚴重損害並且正在惡化當中。除非資訊技術問題獲致解決，否則金融機構及服務提供者均將面對倒閉的危機。監理機構將會密切注意其經營狀況，在大多數情形下，並會發函糾正(Enforcement Action)；第五級為最差，金融機構及服務提供者在經營績效方面有嚴重缺失，必須立刻採取導正措施。作業問題及嚴重弱點存在於整個機構之中，而風險管理作業之嚴重瑕疵及未依據組織規模、業務複雜程度及各項風險組合提供管理階層相關風險資料，未訂定策略計畫或所訂計畫無效，管理階層與理事會無從決定採用資訊技術之方向，無法知悉或注意其決策是否符合資訊技術之需求。管理階層無意亦無法改正稽核及監理單位提出之問題，而服務提供者極度惡化之財務狀況及營運績效，使其倒閉的可能性極高，有必要對其採取持續的監理。影響評等項目之因素如下：

娮稽核(Audit)

此項評等結果可反映出該機構整體資訊技術稽核計畫的適足性，包括內部與外部稽核及時發現並向管理階層與董事會報告重大風險的能力，也顯示內部及外部稽核對提昇作業安全、穩健與有效性的能力。評估因素包括：稽核的獨立性；理事會與管理階層之監督與支援能力；用以配置稽核資源與時程規劃的風險分析方法妥適性；內部與外部稽核報告之範圍、頻率、正確性與及時性；稽核人員參與應用系統開發、購置及測試之程度，以確保內部控制及稽核軌跡之有效性；整體稽核計畫涵蓋資訊技術風險之妥適性；遵守職業道德規範之程度；稽核人員是否足以勝任工作及其培

養訓練情形；檢查意見之追蹤（Follow-Up）與管理階層對改善情形的報告；內部及外部稽核對資訊技術稽核的品質與有效性。

㚢管理（Management）

此項評等顯示董事會與管理階層對資訊技術購置、研發及作業等方面之能力，包括理事會與管理階層對資訊技術活動的監督與支援水準與品質；管理部門在現有資訊技術之下規劃及研發新產品的能力，並瞭解變動中的業務情況可能產生的風險；管理部門提供資訊報告，用以進行規劃與制訂決策之能力；針對重要業務的資訊作業與風險，其內部政策與內部控制之適足性與一致性；風險監控系統的有效性；及時的改正措施；法規瞭解程度與遵循情形；管理之延續性；管理階層監控提供服務及衡量快速有效達成既定目標的能力；適當的契約及監督外部廠商(3rd Party Servicers)之能力；策略規劃與風險管理實務之妥適性，包括管理部門自行評估的能力；管理階層針對現有資訊技術的需求與解決方案以辨認、衡量及監控風險；服務提供者的財務狀況及持續經營的能力；服務提供者的後續支援維護能力；契約條件與計畫的妥適性。

㚣系統發展與購置(Development and Acquisition)

此項評等反映出金融機構對辨認、瞭解、建置與維護合宜的資訊技術方案的能力，其執行績效與相關風險管理實務係建立在下列因素：高階管理階層與董事會的監督與支援的水準與品質；組織與管理架構之妥適性；風險暴險的數量、性質與範圍；系統開發生命週期(SDLC,System Development Life Cycle)的適當性；供研發及操作人員、執行管理階層、獨立廠商與其附屬服務單位以及最後使用者遵循之專案管理之計畫與實務

的品質；品質確認作業的獨立性及計畫內容變更控制的妥適性；系統文件的品質與完整性；網路、系統與應用軟體的完整性及安全性；資訊技術方案的發展符合使用者需求；使用者對系統開發的參與程度；服務提供者提供(release)軟體與文件；服務廠商對客戶的訓練。

㈥支援與傳送(Support and Delivery)

此項評等反映出組織在安全的環境中提供技術服務的能力，不僅顯示資訊技術作業的狀況，諸如可信賴性、安全性、完整性，都將影響資訊傳遞系統的品質。而其評等結果係以下列因素為基礎：提供符合業務需要的服務能力；安全性政策、程序與實務之適足性；資料輸入、處理、輸出等項管制的有效性；資訊中心、網路、服務提供者以及業務單位之緊急應變計畫與業務復原計畫；作業程序或計畫監控容量(Capacity)與績效之品質；監控服務廠商的能力；協助使用者處理問題的能力；營業政策、程序與作業手冊的適足性；實體與邏輯安全品質與資料的隱密性；防火牆架構之妥適性及與公用網路連結之安全性；服務提供者服務顧客的情形；服務提供者應能達到符合客戶要求的維修服務水準。

## 伍、電子銀行業務之發展

拜科技快速發展之賜，透過通訊網路進行交易之趨勢方興未艾，網路作業環境讓世人得以取得即時、全球性資訊、產品及服務，網際網路已成為一個龐大的市場，估計其使用者已超過 3 億人，金融服務業的資訊部門再度成為炙手可熱的單位，委外作業(Outsourcing)亦趨盛行。根據 Price Waterhouse Coopers 公司在 2000 年 1 月對 1,020 位公司總裁所作調查顯示，有 88%認為 Internet 對

金融業將產生重大影響甚至改變其經營型態，只有 2%認為沒有影響。而國際資料公司(IDC, International Data Corporation)預測，至西元 2003 年，美國地區金融機構從事線上銀行(Online Bnking)業務的比率將達到 86%。依據美國地區金融機構填報報表(Call Report)及非正式場外監控資料顯示，截至 2000 年 9 月，約有 4,100 個金融機構建置網站，約佔全體金融機構數之 40%，其中具有交易功能的網站有 1,423 個，約佔全體金融機構數之 14%，在 1995 年 12 月，建置網站及交易功能網站的數目分別為 130 個及 1 個，成長速度著實驚人。在已建置交易功能網站的 1,423 家金融機構中，其中由 FDIC 負責檢查的有 657 家，占 46%，由 OCC 負責檢查的有 478 家，占 34%，由 FRB 負責檢查的有 176 家，占 12%，由 OTS 負責檢查的有 112 家，占 8%，依資產規模與金融機構家數列示如下：

| 資產總值（美元） | 家數 |
|---|---|
| 1 千億美元以上 | 7 |
| 100 億至 1 千億 | 83 |
| 50 億至 100 億 | 46 |
| 10 億至 50 億 | 174 |
| 5 億至 10 億 | 166 |
| 1 億 5 千萬至 5 億 | 474 |
| 1 億 5 千萬及以下 | 473 |

若依銀行資產規模及占相同規模金融機構之比率列示如下：

| 資產總值（美元） | 占相同規模機構比率(%) |
|---|---|
| 100 億以上 | 85 |
| 30 億至 100 億 | 54 |
| 10 億至 30 億 | 46 |
| 5 億至 10 億 | 36 |
| 1 億至 5 億 | 17 |
| 1 億及以下 | 5 |

隨著電子商務(Electronic Commerce)之崛起，利用網路銀行進

行交易將更趨多元化，銀行利用超連結(Hyperlink)方式，連結至其他策略聯盟廠商網站，可增加客戶點選銀行網站之機會，進而創造更大的商機。惟其連帶產生之各項風險議題，仍待進一步探究。

對網路銀行業務的檢查，主要依據 OCC 於 1999 年 10 月訂定之「網路銀行檢查手冊」(Internet Banking Comptroller's Handbook)，另 FDIC 亦編有「電子銀行檢查程序」(Electronic Banking Examination Procudure)，而各監理機關亦不定期針對電子銀行或網路銀行業務發佈應注意事項（各監理機構之網址及發佈與電腦稽核有關之注意事項編號，請參見附錄），期能使金融機構確實瞭解相關議題的內容及其應注意之風險；OCC 檢查手冊分為概論及檢查程序二部分，概論部分對網路銀行業務加以定義，敘述網路銀行成長緣由，銀行型態，對潛在的信用、利率、流動性、價格、匯率、交易、法律、策略及聲譽等各項風險予以說明，並論及風險管理、內部控制方式，另對自行開發或委外作業技術以及網路銀行相關議題均有陳述。在檢查程序部分，則描述一般檢查程序，暴險數量，以及如何控管風險管理品質，最後談到結論及檢討會。本報告僅摘述一般檢查程序、風險管理品質控管程序及總結程序如下：

菜一般檢查程序

檢查程序係為判斷金融機構對網路銀行政策、程序及內部控制的適切性，在執行測試與程序時，檢查人員應以風險為基礎予以評估，此項評估並應涵蓋考量受檢單位內部及外部稽核工作執行情形，以及政策、程序、內部控制與管理資訊系統的有效性。檢查人員應利用 FFIEC 之資訊系統檢查手冊及 OCC 另外公布之資料及指導原則，作為檢查之參考。

全部完成所有檢查程序並不必要，在進行檢查規劃時，檢查人員需判斷銀行在網路銀行業務及其監控方面仰賴外部廠商的程度，並將委外作業之評估納入一般檢查程序。

檢查目標：訂定網路銀行風險數量與風險品質管理之範圍。

檢查程序：

芷檢視下列文件，確認先前已知與網路銀行有關且應予追蹤之項目, 如上次檢查報告（資產管理、自有資本及風險性資產、業務及法規遵循狀況等）、監理策略、領隊備忘錄、追蹤事項、上次檢查工作底稿、內部與外部稽核報告、與監理機關往來文件。（注意：若檢查人員被指派查核內部及外部稽核項目，應取得該檢查人員對該項檢查所提重大缺失的複本。如果內部與外部稽核項目不在此次檢查範圍，則要覆核並取得受檢單位最近一次內部稽核及外部稽核報告提列缺失清單）。

芧確認檢查資料清單所列資料之完整。

茎取得由內部或外部稽核、顧問或聘用之專業人員所做之審查、評估或系統認證報告，注意其提列之缺失。

苔確定是否利用外部廠商提供何種服務或產品，檢查人員應將負責系統開發、操作及維護網路銀行系統的主要廠商資料予以記錄。

花檢視文件並與管理部門作初期討論，以判斷網路銀行的安全性、管理階層監督網路銀行及委外作業之成效、政策與實務及人事或控制系統是否有重大改變、影響網路銀行的內部與外部因素。

茉檢視銀行的業務與策略計畫，以判斷管理階層的網路銀行業務計畫是否明確，並能反映受檢單位目前的經營方向。

荃判斷管理部門之緊急應變及業務回復計畫內容是否收納網路銀行業務。

苣檢視銀行網站，以瞭解受檢單位網路銀行業務及揭露情形。

茇以執行前述各項步驟為基礎，與領隊或其他適當檢查人員討論，已決定檢查範圍和目標。

茖執行檢查程序時，對受檢單位之政策或實務及內部控制程序加以測試，驗證任何不足的監督與不相稱的風險，與領隊討

論採取額外檢查程序的必要性。

茲評估銀行對法令規章遵循情形，包括判斷銀行是否受銀行服務公司法(Bank Service Corporation Act)第 1867©(2)節之限制公告必要資料(例如銀行與網路服務供應者之投資或合夥關係)；銀行是否瞭解網路銀行相關法令；檢視最近檢查缺失(資產管理、自有資本及風險性資產、商業活動及法令遵循)及內、外部稽核報告對網路銀行所提之相關問題，判斷管理階層是否已改善各項缺失；是否適當揭示聯邦存款保險公司之公告，是否明確標示未投保之商品及服務；注意是否有用以驗證與網路銀行業務有關之潛在洗錢活動之申報程序；判斷國外資產管制局(OFAC,Office of Foreign Asset Control)是否仍維持對網路銀行產品與服務之驗證及申報能力；判斷管理階層對於因安全控管之疏漏導致訴訟或調查時，是否對使用者建立警訊、宣告入侵者進入私人電腦、未經核准之存取或使用不被允許及依法構成刑責之犯罪；若銀行發覺電腦相關犯罪，確定該可疑行為是否申報歸檔；判斷銀行對與網路銀行產品有關隱私權是否予以正確揭露。

查風險管理之品質

芘政策與策略規劃

檢查目標：判斷董事會是否對網路銀行採取有效之政策，該政策與安全穩健之銀行實務一致，並適合該銀行之規模、性質與作業範圍。

娮判斷網路銀行安全政策是否包括明確界定系統安全責任、網路及資料存取控制。

姶判斷網路銀行防火牆政策是否敘明防火牆維護與監控責任、完善之存取規則、存取規則說明允許或禁止何種傳輸方式。

婓判斷是否於政策中明定亂碼作業程序，並包括亂碼化過程之控制負責人員、如何亂碼、資料分類技術、於內部及開

放網路傳輸期間，以亂碼化方式保護通行碼與訊息及資料之傳送。

娆若使用公開金鑰密碼系統，判斷私密金鑰是否由銀行控管，且政策中是否註明私密金鑰之管理，並包括由銀行或第三者產生金鑰之管理、私密金鑰儲存之安全控管、由何人存取金鑰及該環境如何控制、若私密金鑰由第三者保管如何控管、金鑰因遺失或被解碼及到期取消與重新簽發之政策與實務、儲存在伺服器或電腦中未與外界網路連結之金鑰管理。

娛判斷是否使用防毒軟體，並註明使用商品名稱。

娛確認安控政策是否定期檢視及更新，且經董事會或高階管理階層核准。

娚判斷該機構是否建立超文件連結(Hypertext Link)政策，使顧客得以清楚分辨已投保與未投保之金融商品、銀行及非銀行商品、何時離開銀行網站。

芧程序

檢查目標：判斷程序與實務（包括內部控制）是否有效。

娮透過與管理階層會談，檢視技術性規劃，評估銀行對於網路銀行產品之長短期策略。於評估銀行之規畫過程考量網路銀行是否與銀行整體政策、策略目標及操作計畫一致、董事會及高階管理階層監督之程度、管理階層對同業之了解，以確保系統相容性及共用性、業務之成本效益分析是否將啟用、運作狀況、系統升級、客戶支援服務及維護成本一併考量、管理階層對於安控風險、危機及弱點之評估、該機構對內部專業人員及訓練要求、網路銀行系統與 Y2K 相容情形、管理階層對於系統安全監控、測試及執行監控之重視程度、管理階層是否熟知聯邦政府與州政府有關網路銀行及電子商務之法規與釋義。

娰管理階層是否有適當程序，定期評估網路金融商品組合及

行銷成效？並將策略規劃程序與評估結果結合。

㜷審查銀行執行安控風險評估程序之適當性

娆評估銀行之用人過程，確保網路及資料存取控制可靠性及正確性。

娛廠商管理

㹋選擇廠商前，評估管理階層過程，是否考量策略及業務計畫與委外事項一致、高階管理階層與董事會應參與委外決策及廠商之選定、簽約前應蒐集廠商資訊並加以分析，且考慮其聲譽、財務狀況、研發與維護及支援成本、內部控制及回復程序、服務協定以及廠商與管理階層之責任

㳇判斷銀行是否審核合約，適當的釐清雙方責任。

㳄是否依據 FFIEC 資訊系統檢查手冊「合約」篇之規定。

㳀判斷銀行是否取得內部與外部稽核報告，評估廠商管理程序或與資訊系統相關之特定廠商關係。

㳂管理階層是否指派專人負責管理廠商，注意管理階層之責任及在監督上是否可信賴。

㳆若銀行係網路銀行軟體提供者，管理階層是否有適當程序指定程式原始碼維護人員。

㳈若由廠商提供軟體，銀行是否有適當程序確定供應商維護之軟體有附條件委付契約並定期更新檔案。

㳉若廠商可以維修目的連線至銀行系統，銀行是否訂定適當程序確保廠商之行為受到良好控制，以及員工忠誠保險範圍是否擴及廠商。

娔密碼

評估網路銀行密碼管理程序之妥適性及使用密碼驗證使用者身份之程序是否適當。

娉防火牆

㹋評估管理階層決定網站型態（屬資訊性、溝通性或交易

性）之過程是否適當。

浮是否制定完善程序，確保網站與內部網路或電腦系統間之路徑均適度控制。

淯判斷程序管理是否可防範任何未經授權對內部網路及電腦系統之存取。

涋若防火牆系統自外界購入，銀行是否有適當程序釐清本身與供應商之責任。

淞確定銀行防火牆架構管理之妥適性。

浮銀行是否有程序，以建立滲透測試及認證、確認執行認證之公司或個人資格

涎對於限制存取伺服器及相關設備之防火牆，銀行是否有一套有效程序評估實體控制之妥適性。

浯是否訂定適當程序界定遠端存取，管理階層如何監控該項存取？

粂對於限制存取防火牆架構之書面文件，評估其程序妥適性。

嫚實體安全

是否訂定與網路銀行系統有關之軟、硬體及資料傳輸設備等實體安全控管之適當程序，並包括網路伺服器安全、如何防止設備有未經授權之存取、銀行是否確定廠商擁有設備、資料中心或其他放置文件及設備之場所，是否有適當的實體控管。

娮交易確認

是否訂定適當程序以驗證交易，避免客戶提出否認交易之申訴。

寇亂碼化與保密性

毡是否訂定適當程序選擇適合本身環境之亂碼化系統，且選定之亂碼程式是否建置於公開、私人或二者兼具之系統？

㵟若銀行從事跨國金融業務, 判斷銀行是否了解美國政府出口政策及出口管制、亂碼化技術之使用。

㳇判斷銀行是否有適當程序蒐集及使用客戶個人資料以保護其隱私權。

㖞病毒偵測與預防

㹋網路銀行系統是否設置偵測病毒與防範措施, 並考量使用者明瞭銀行對病毒防範之努力、最近一次風險評估或（及）稽核報告中提及有關病毒控制之缺失、更新防毒軟體之頻率。

㵟是否有病毒偵測與防範程序, 若有, 則應考量病毒偵測軟體之遞送是否透過銀行伺服器下載、銀行之軟體遞送過程是否提供偵測病毒與預防。

㚔業務復原與緊急應變計畫

㹋是否設置適當程序開發及檢視銀行業務衝擊分析, 應考量網路銀行是否被視為重要業務、若網路銀行商品及服務無法正常運作, 管理階層是否檢視此一衝擊對銀行聲譽之影響

㵟是否訂定適當程序開發並測試業務回復與緊急應變計畫, 包括應變計畫及業務重建計畫是否適當、是否於正常情形下測試該項計畫

㳇對銀行網路系統之回復是否訂定適當程序。

㳆銀行是否檢視最近之業務回復與緊急應變計畫測試結果, 管理階層是否要求每年定期測試復原過程及系統、評註定期測試所產生之缺失、將測試結果告知董事會及執行經理部門

㙆人事

目標：了解銀行之規模與架構, 確定銀行管理階層或人事部門對網路銀行業務之管理均有合理之認知與專業技

術。

娮透過與管理階層之會談，確定對專業知識之了解程度，並衡量了解程度是否涵蓋該行網路銀行業務之規模與範圍。

姶評估訓練計畫及安全控管專業技術，包含管理階層是否提供定期專業訓練機會與衡量安全之有效性、行員及網路銀行使用者是否了解安全控管之責任及銀行政策、管理階層仰賴外部供應商之專業技術的程度。

苜控制

目標：判斷管理階層是否建構符合網路銀行風險型態與水準之控制點

娮數位簽章及認證機構

毡判斷管理階層是否要求使用數位簽章以驗證銀行、使用者及交易

浮判斷數位簽章是否由外部供應商發給、管理、認證。

淯如果銀行本身為認證機構，應注意數位簽章系統係採開放式或封閉式、認證之啟用與更新及廢除是否有書面政策與程序、銀行如何建立及確認使用者憑證、管理性報告系統是否適當提供查閱目錄與稽核、憑證機構設備及範圍是否安全，並涵蓋適當之控制以保護存放憑證機構資料及指引之伺服器、若因系統失效或遭受損害，應變計畫應符合客戶需要、對於提供憑證機構之功能，銀行註明其法律含意、憑證機構符合全國標準與科技研究部及網際網路工程小組等既定標準、應有適當之稽核程序、對於認證是否建立限制交易之數量、型態及有效期限、認證機構是否基於訊息或交易敏感性而建立認證等級、銀行是否於適用法規下持續運作、對該項業務作定期之成本效益分析。

姀生物辨別器設施

為達認證目的，銀行是否使用生物辨別器裝置；該裝置是否執行風險評估、稽核或成本效益分析；是否建立容量限度及政策，以驗證被執行之交易；是否取得並檢視生物辨別器運作結果之管理報告。

婓監控

毆與管理階層討論監控網路銀行系統安全所使用之專業技術，取得並檢視各項抽樣報告，包括滲透測試(Penetration Test)範圍及結果、違反安全之訊息、即時入侵偵查報告、敘述安全漏隙及侵入系統之報告

浮是否使用安全控管分析軟體，並敘明其功能。

淯由管理階層或由供應商主導滲透測試，並評估是否由客觀的一方執行、對執行人員是否有適當之約束、執行次數是否至少每年一次，或在管理階層基於風險分析及風險容忍限度內，以可接受之次數執行滲透測試、並嚴格控管測試資料及文件

涋管理階層監控、查證內部或外部網路入侵方式，是否包含使用監控軟體追蹤即時網路傳輸，由合格人員負責平日網路傳輸之監控及維護並覆核工作日誌，偵測入侵技術可立即通知網路管理者及安控人員，安全控管政策對陳報事項之定義，應通知之管理階層、董事會及外部主管機關之程序

淞經檢視報告或洽詢管理階層，判定銀行若有變更網頁、由外部或內部未經核准之存取，或因入侵造成財務損失且經確定後，是否依據財政部金融局規定填報「電腦犯罪報告」(Reporting Computer-Related Crimes)等上述情形，則應於工作底稿中註明

浮管理階層是否訂定緊急回應程序，並評估處理未經核准侵入程序之有效性。討論並記錄遠端存取控制情形，是

否包含註明遠端存取安全政策、行員瞭解政策內容並監控其遵行情形、保留稽核日誌以監控遠端存取

娆執行之監控

管理階層如何監控系統之執行（如交易量、回應時間、有效性、績效報告、客戶服務紀錄及申訴案件彙總）及規劃未來系統需求之方式，以確保網路後續運作符合客戶需求。

娛支援客戶服務

毹衡量網路銀行產品中客戶服務及支援之角色與品質。

滓檢視客戶支援功能之組織與責任劃分。

淯客戶支援服務若委外辦理，應注意供應商之責任，並確定管理階層如何監督客戶有關問題、需求及申訴。

涋是否已建立客戶服務標準，若是，則管理階層如何監督，以符合該項標準。

淞管理階層如何評估客戶服務之適切性。

浮檢視客戶服務報告或問題紀錄，並與管理階層會談，了解程序是否有所缺失。

涎網路銀行發展計畫及資源規畫是否將客戶服務納入考量。

娛軟體之配置(distribution)

毹判斷是否有程式變更控制，該項控制且足以防止未經核准之軟體變更，而該核准程序是否位於系統開發過程中各控制點上；緊急或臨時性及新版本軟體變更程序；變更控制文件可提供適當稽核軌跡及支援各項軟體變更。

滓評估網路銀行控制及軟體配置程序,並涵蓋軟體配置之適當性（自動下載、使用者啟動下載或人工遞送）、在配置過程中設定完善之控制以防止病毒感染，並確保軟體完整性、在配置前先執行軟體測試

娚稽核

匏內部或外部稽核之範圍是否涵蓋網路銀行業務。

浮對重要管理實務是否執行風險評估或實施稽核，並檢視相關之報告。

涪內部稽核是否涵蓋網路銀行系統之規劃及建置。

涋儘量取得銀行內部或外部稽核報告，評估廠商管理程序或與特定廠商之關係。

淞取得管理報告或與管理階層會談，確定該行是否對廠商管理加以評估，且管理階層是否考量該行安全控管及報告涵蓋管理階層是否了解並評估存取控制之安全性、使用者認證及資料保密性、廠商執行即時入侵偵測及內部或外部網路滲透測試之安全監控活動、服務水準及廠商之能力符合約定水準、產品配送前由廠商測試、病毒偵測程序、應變計畫及業務重建計畫。

浮若網路銀行係委外處理，確定廠商名稱，且確認銀行是否取得並檢視主管機關對該廠商之檢查報告。

涎稽核功能是否檢視其安全、隱私標準之揭露及實務運作間之一致性。

嫞網際網路服務提供者(ISP,Internet Service Providers)

匏銀行若仰賴他人支援其網路業務，管理階層是否監督該 ISP，包含執行績效是否與約定相符、要求 ISP 監控銀行網路連線並報告有關連線當機或失效之情況、確認 ISP 應變計畫及系統復原之能力、確認 ISP 有適當之維護人力、確定銀行是否因受制於不同存取型態而減少可接受之支援、ISP 是否提供銀行界過濾系統或建置本身之防火牆過濾參數、ISP 對於銀行網址之變更是否設計健全之控制程序、評估 ISP 財務狀況之穩健性、檢視 ISP 之安控水準及實際操作情形。

浮若因系統故障或不當操作，造成 ISP 無法處理銀行網路

傳輸，銀行是否設置替代路徑。

㈥總結程序

目標：溝通檢查缺失，對違規或其他缺失採取更正行動

㈠彙總本次網路銀行之檢查結果，針對其暴險情況、風險管理品質、風險之方向及影響整體風險之風險管理實務範圍作成結論：

㈡於彙總底稿上評註策略及業務計畫、政策遵循、管理資訊系統及內部控制之妥適性，遵守法規及行政命令情形、對於政策、程序、實務運作或其他相關業務缺失事項提供改進建議、網路銀行業務之未來展望及其他重大事項；

㈢與檢查領隊討論關於檢查之發現及結論，如有需要，應作成「董事會應注意事項」(MRBA,Matters Requiring Board Attention)，內容應包括偏離穩健基本原則，可能造成財務惡化，導致違反法律或規定。MRBA 須論及問題之形成原因、不採取行動之結果、管理階層對更正行動之承諾、負責改正行動之人員及期限；

㈣與管理階層討論檢查結果，包括與風險有關之結論，如有需要，應取得其改善之承諾

㈤檢查報告中提出有關網路銀行業務之意見

㈥以備忘錄方式特別評註財政部金融局於未來監督該行網路銀行業務時應辦理事項，涵蓋監督目標、期限、所需人員及工作天數。

㈦更新電子資訊系統及任何可用之檢查行程或對照表。

㈧依據財政部金融局之指導原則，更新工作底稿。

## 陸、公元二千年之經驗

千禧年危機曾經造成全世界對電腦作業的恐慌，除部分落後國家之外，無不盡全力投入大量金錢及人力以防範全球性系統危機的產生。值得慶幸的是，迄今尚無重大災害發生，美國在這

方面一直扮演先鋒的角色，各金融監理單位自 1997 年開始，不斷針對金融機構可能發生的風險發佈多項指導原則或應注意事項，督促各機構重視這項問題並積極改進，其相關的作法，不啻為各國之參考，在此期間，我國亦不斷蒐集相關資料，做為主管機關制訂政策之參考。FFIEC 亦於 2000 年 3 月就整個計畫執行之過程及結果予以回顧，列述其所得經驗，本報告除簡述該國金融監理機構執行狀況外，亦摘述該文分享，茲分敘如下：

Y2k 計畫自 1997 年開始進行，共分四個階段。

第一階段係研訂指導原則，並開始陸續對金融機構發佈各項與 Y2K 前置作業相關之安全穩健要求，並訂定計畫之時程，1998 年 4 月以前完成系統清查分析評估作業，1998 年 9 月以前完成系統修改作業，1998 年 12 月以前完成內部系統測試及上線作業，1999 年 6 月以前完成委外部分之測試及上線作業，1999 年 7 月以後開始使用符合 Y2K 版本之系統進行作業。

第二階段在 1998 年初期，金融機構在此階段應準備周延的書面計畫，內容涵蓋系統清單、修改優先順序、人力費用及支出預算等，提供檢查人員審核，計畫內容若不符合監理單位之要求，金融機構高階經理人員應依照監理單位訂定之期限提出修正計畫。若未依規定期限提出可行計畫，監理單位將採取監理行動。

第三階段為 1999 年中期，實地評估銀行執行 Y2K 計畫之進度是否符合監理單位訂定時程。金融機構若有小缺失，高階經理人員將被監理單位召見並訂定改善期限。如果金融機構未遵守、監理單位所定時程及安全穩健要求，或不符合前述針對小缺失訂定改善期限前及時改善，監理單位也會採取監理行動。

第四階段自 1999 年中期到 1999 年底，每月拜訪主要機構(Key Players)及部分特定機構，確認所有經修改及測試之自行維護或委外系統均可順利運作；定期與其他金融機構電話聯繫，如果發現任何作業上或其他方面缺失，則立即實地追蹤訪視。

在整個專案計畫當中，以紐約州銀行局為例，檢查人力需

求最殷之時，共有 114 名檢查人員參與此項計畫之檢查工作，為其中僅有 4 人屬專業電腦稽核人員，因此在執行檢查工作之前，該局依照各階段所需人力，召集檢查人員予以訓練講習，俾能順利執行檢查工作。

FFIEC 認為 Y2K 專案帶給世人寶貴經驗，而充分準備(Best-Prepared)的金融機構具有如下特質：㈠高階管理部門及董事的重視與各部門間的合作，高階管理部門與董事會審慎監督整個計畫從規劃到執行的程序，不分銀行特別建立新的陳報機制，使高階管理部門得以明瞭執行進度以管理風險。該機制亦有利於進度的控管與資源的有效運用。並建立品質確認覆核及內部稽核制度以確保各項風險得到適當管理。而資訊與業務、法律部門之協調及企業之聯繫有助於管理風險，並藉此強調該計畫在整個組織中的優先地位。㈡綜合資訊清單，金融機構擬具資訊技術系統與應用系統清單，使機構得以整個企業為主體，合併、刪除或整合各項計畫，有效率的規劃可催化電腦系統現代化並將新、舊系統加以整合，綜合清單亦可形成較好的風險評估及決策內容，確保資訊技術系統與營運策略一致。㈢較佳的廠商管理，金融機容建立較佳的管理程序，監督那些提供重要服務項目及產品的服務提供者與軟體廠商。許多倚賴服務提供者、軟體廠商以及技術顧問的金融機構發現，有一些與廠商管理有關的風險未被適當的衡量、監控與管理，許多金融機構因而強化其對服務提供者、軟體廠商以及技術顧問的能力分析以確保能履行契約義務。㈣ Y2K 專案期間，藉由對資訊部門與業務單位間相互依存的認知，使正式的測試策略(Formalizedtesting strategies)改善整體測試程序。許多金融機構首次研究資訊技術系統的正式策略與標準，金融機構、服務提供者與軟體廠商也藉由創造更多有效的測試方式與變更管理實務，改良了測試程序與環境。㈤詳盡的緊急應變計畫，許多金融機構均提出其從發展 Y2K 緊急應變計畫及事件管理(Event Management)計畫所獲得之顯著利益，緊急應變計畫係以假

設的狀況推演出解決問題及訓練工具，有助於在遭遇作業停擺或天然災害時，立即採取因應措施。金融機構透過分析主要業務程序（如收受存款、放款、信託服務等）在系統當機時，產生的潛在風險，研擬更詳盡的緊急應變計畫，決定每一主要業務作業最低之輸出及服務標準，計畫之測試，並請獨立的第三者確認其結果。金融機構亦瞭解重新審視規劃與緊急應變有關的所有資訊與非資訊作業環境的必要性。浮良好的內部控制與安全，金融機構以較佳的保護軟體偵測內部及外部詐欺、惡意或疏忽的行為，良好的內部稽核，其控制點應包括設備、人員、政策與程序、通訊、系統軟體、應用軟體、服務提供者與軟體廠商，保護系統安全的重要預防措施包括強化資料存取限制、檢視雇用人員背景、適當的責任分工與有效的稽核軌跡。金融機構也擬具聯絡資料，作為當電腦與通訊系統遭到入侵或攻擊時，可以得到如何回應的建議。金融機構內部稽核人員對發現缺失及管理風險提供重要的控制機能，許多金融機構在 2000 年專案計畫以前，未將電腦稽核視為重要項目，或未評估稽核功能。內部稽核早對測試與緊急應變計畫程序以及獨立確認其有效性提出意見。他們也審核測試與追蹤結果之文件並再度測試。涎公開資訊分享，Y2K 計畫是一個特殊的合作示範，並且跨越業務競爭及監理界線，開啟個人與組織之間聯繫通道，金融機構史無前例的與其他金融機構、服務提供者、軟體廠商、貿易協會、監理單位及其他產業分享資訊與策略，並附和媒體報導的舉動則可能會降低大眾對金融服務業的信心。洽公共關係的改進。Y2K 計畫替銀行製造許多與客戶溝通的機會，不論新舊客戶，金融機構在確定客戶得到金融業已經完成千禧年各項準備的訊息方面往前跨了一大步，例如，金融機構按月或按季寄送有關 Y2K 資訊、在營業大廳張貼海報、在自動提款機顯示相關資訊、透過當地報章及廣播電視廣告或特別設立 Y2K 網址等。粂徹底重新審視法律，許多金融機構從專案管理小組的法律顧問諮詢中獲益良多，法律顧問重新檢視有關管理

廠商的契約，在「公元二千年資訊及準備揭露法案」(Year 2000 Information and Readiness Disclosure Act)相關規定前提下，提供管理部門許多可行的避風港。在與法律顧問重新審視契約內容初期，部分金融機構避免與服務提供者及軟體供應商談論契約問題，許多金融機構也建立保存文件與保留記錄並存的方法，作為法律防衛策略的一部份。本身的法律顧問也因與技術部門主管及資訊部門主管密切的工作關係，同時接受不同領域的訓練而獲益匪淺。

## 柒、結論與建議

### 榮結論

美國聯邦準備理事會主席 Mr.Greenspan 多次在公開場合強調以風險為基礎的監理之重要性，並指出科技之快速發展影響金融業的變革，隨著科技持續創新，金融商品不斷推陳出新，因此金融監理的方式也必須有所因應調整，不應再鉅細靡遺地檢查全部業務，應衡量銀行對業務所採用風險管理模式之妥適性。巴塞爾金融監理委員會電子金融小組在 2000 年 9 月及 10 月針對電子銀行業務頒布有關之跨國監理與風險管理等二項白皮書，受重視程度可見一般。電腦稽核的範疇也由傳統的針對受檢單位本身資訊作業管理良莠的查核，藉由資訊科技的改良，進而必須跨越國界，尋求與他國監理機關的合作。電子金融的蓬勃發展，也帶給各國監理機關更大的挑戰。而此次拜訪的監理單位均認為，電腦稽核人員現在以及未來最大的挑戰是如何與日新月異的科技保持同步，令人深有同感。另美國各監理機關指出，金融機構經營網路銀行業務尚有部分缺失待改善，如：對該業務缺乏完整的規劃與更新政策及稽核計畫；對敏感性資料未予適當控制；缺乏隱密條款；客戶授權尚有弱點；過度依賴廠商；不瞭解相關法規內容。

查建議

他山之石，可以攻錯，我國金融監理制度向亦參考他國制度、作法。值此金檢一元化制度尚未定案之際，僅就本次研習所得，研提拙見供參考，茲述如次：

艼美國各監理單位均感現有檢查人力已不足支應檢查需求，致對於一般檢查(Full Scope) 漸趨縮小其查核範圍，嘗試由資深人員擔任專案經理人(portfolio manager，類似帳戶管理員制度)，於檢查前蒐集受檢單位相關資料，研判該單位可能的風險較大之業務種類或作業方式，指定檢查人員必須查核項目，可節省檢查人力。觀之我國情況，三個監理單位之檢查人力亦顯不足，似可參酌該國作法。

芧美國監理單位如聯邦準備銀行紐約分行、財政部金融局及聯邦存款保險公司均設有專職研究最新科技及金融機構採用之相關資訊技術及軟體，分析其潛在風險，作為電腦稽核人員查核之參考。我國各監理單位則尚無此項職務編制，電腦稽核人員對電腦新知乃至作業系統、應用軟體之特性及其安全控管之弱點，所知較為片段，難有完整之瞭解，若能成立類似之諮詢單位，再加以完整的教育訓練，對查核工作應有助益。

芚美國聯邦金融機構檢查委員會自 1979 年開始實施資訊系統評等制度，該項評等結果係作為制訂檢查頻率之依據。我國監理政策及方式雖不同於美國，惟因資訊中心安全管理之重要性與日俱增，似可參酌該國作法，於檢查結束後，就檢查結論予以評等，並將評等結果納入本行報表稽核系統（CARSEL）或中央存款保險公司之全國金融預警系統（CAMEL)，使各系統產生之綜合評等（警訊）內容更具參考價值。

芣由於該國金融機構倚賴外界廠商之程度日深，據估計，在具有交易功能的 Internet 銀行中，約有 75%倚賴 10 家廠商，對監理機關而言，其中有 8 家屬新公司。有鑑於此，FFIEC 資訊小組亦正擬訂「網際網路銀行廠商監理計畫」，將具有「重

要市場佔有率」(significant market presence)之廠商納入一般檢查計畫之中，該國監理機構近年來除加強查核金融機構對委外作業廠商之管理情形，亦對資訊服務提供廠商採取監理行動，即所謂的'SASR'(Shared Application Software Review)計畫；其作法係由各監理單位互相協調，對金融機構使用之套裝軟體(Turnky software)、單機作業軟體(Stand-alone custom software)及整合軟體(Integrated package)提供廠商，由一個監理單位進行查核後，將檢查結果提供給其他監理單位參考，免除同一軟體廠商分由數個監理單位查核，浪費檢查人力之情形。我國迄今對於該等廠商尚無查核之法源依據，尚待相關主管機關研酌。

㈥美國金融監理機構對受檢單位之內部稽核獨立性及外部稽核要求頗高，稽核報告亦為每次檢查必有的項目，對於營業單位所做自行查核則較不重視，較之我國將內部自行查核每列為檢查項目並經常提列意見之情形顯不相同，自本人擔任檢查工作以來，與金融機構人員接觸的過程當中，時常得到對該項作業有效性的質疑，對營業單位而言，多將該項作業視為例行公事，草然了事，自無成效可言。以本人淺見，毋寧打破現有制度的窠臼，建立金融機構稽核部門有效之運作機制（如人事任免、人力運用、稽核軟體、營業單位評等制度、風險管理…等），提昇其稽核功能，既能提早或適時發現政策制度或作業缺失，速謀改善之道，亦可簡省營業單位作業負擔。

# 附錄

各監理機關針對資訊技術發布之參考資料主要有：

聯邦準備理事會（網址：www.federalreserve.gov)

| | |
|---|---|
| 2-00 SR Letter 00-4 | Outsourcing of Information and Transaction Processing |
| 2-00 SR Letter 00-3 | Information Technology Exami-nation Frequency |
| 10-99 FRB New York Staff | Paper：Outsourcing Financial Service Activities |
| 04-98 SR Letter 98-09 | Assessment of Information Tech-nology |
| 12-97 SR Letter 97-32 | Sound Practices Guidance for Information Security for Networks |
| 12-97 SR Letter 97-28 | Suspicious Activity Reporting-Computer Crime |

財政部金融局（網址：www.occ.treas.gov)

| | |
|---|---|
| 10-99 Advisory 99-44 | Examination Handbook on Inter-net Banking |
| 05-99 Advisory 99-06 | Guidance to National Banks on Web Site Privacy Statements |
| 05-99 Bulletin 99-20 | Certification Authority System |
| 03-99 Bulletin 99-09 | Infrastructure Threats from Cyber-Terrorists |
| 09-98 Advisory 98-11 | Pretext Phone Calling |
| 08-98 Bulletin 98-38 | Technology Risk Management: PC Banking |
| 07-98 Bulletin 98-31 | Electronic Financial Services and |

| | | |
|---|---|---|
| | | Consumer |
| 02-98 Bulletin 98-03 | | Technology Risk Management—Guidance for Bankers/Examiners |
| 12-97 Advisory 97-09 | | Suspicios Activity Reporting—Computer Crime |
| 09-96 Bulletin 96-48 | | Strored Value Card Systems—Information for Bankers/Exami -ners |

儲貸協會監理局（網址：www.ots.treas.gov)

| | | |
|---|---|---|
| 06-99 Memo | 99-109 | Guidance on Transational Web Sites |
| 11-98 Memo | 98-97 | Policy Statement On Privacy and Accuracy of Customer Informa-tion |
| 11-98 Rule | N/A | Electronic Operations--Final Rule |
| 07-98 Memo | 98-90 | Electronic Financial Services and Consumer Compliance |
| 12-97 Memo | 97-75 | Suspicious Activity Reporting -- Computer Crime |
| 10-97 Bulletin | 32-6 | Information Technology—Exa-mination Procedures |
| 06-97 Memo | 97-70 | Guidance on Online Retail PC Banking |

聯邦存款保險公司（網址：www.fdic.gov)

| | | |
|---|---|---|
| 12-99 FIL | 113-99 | Financial Institution Web Site Privacy Survey |
| 07-99 FIL | 68-99 | Risk Assessment Tools and Prac-tices for Information Security |
| 06-99 FIL | 49-99 | Bank Service Company Act |
| 09-98 FIL | 98-98 | Pretext Phone Calling |
| 08-98 FIL | 86-98 | Electronic Commerce and Consu |

| | | |
|---|---|---|
| | | mer Privacy |
| 07-98 FIL | 79-98 | Electronic Financial Services and Consumer Compliance |
| 12-97 FIL | 131-97 | Security Risks Associated with the Internet |
| 12-97 FIL | 124-97 | Suspicious Activity Reporting—Computer Crime |
| 02-97 FIL | 14-97 | Electronic Banking Examination Procedures |
| 08-96 FIL | 59-96 | Stored Value Cards and Other Electronic Payment Systems |