第一章、前言

壹、研究專案簡述

我國電子銀行業務發展及風險控管之研究

—以美國與台灣為例

貳、研究主旨說明

一、研究主題

本專案旨在將美國、英國等國家之電子銀行(e-banking)業務（本專案所稱之電子銀行業務範圍界定為經由網路銀行提供之金融服務）發展及風險控管制度作分析比較，引進新觀念與做法，作為國內推動電子銀行業務發展及風險控管機制之參考。

風險監控制度，係電子銀行業務發展最重要的一環，巴塞爾銀行監理委員會為協助銀行監控風險，業依風險的基本特徵與挑戰性，以較精確方式對 e-banking 的風險管理作處理，訂定 e-banking 風險管理原則。該委員會所訂定之十四項原則，將作為檢視我國 e-banking 風險管理之依據。

另鑒於電子銀行業務的普及化及消費者保護意識的提升，消費者個人資料及權益的保障，以營造一個安全有效率之電子化環境，亦是本次研究主題的重點之一。

二、本案緣起

本專案係行政院金融監督管理委員會銀行局之「我國電子銀行業務發展及風險控管」委託金財通商務科技服務股份有限公司(以下簡稱為本公司)之研究專案。本專案為提昇我國金融業對電子銀行的經營能力、風險控管及國際競爭力，並確保電子化效能及符合市場需求，以美國與台灣在電子銀行業務發展及風險控管之現況及制度為出發，進行系統化研究探討，並提出分析比較及建議，作為我國推動電子銀行發展之參考。

鑒於電子銀行涉及金融知識、資訊技術、稽核安全及使用者需求等領域，因而除本公司積極參與之外，並聯合政治大學商學院楊建民、季延平、謝明華等三位教授，以多年來浸於金融與資訊之研究及推廣經驗，共同探討國內外電子銀行之業務發展及風險控管。藉由國內外相關資訊之彙整，並加以系統化之研究及腦力激盪，合力予以剖析現況及提出建議，期望能為我國金融經營及競爭力有所益處。

三、研究範圍

本專案之電子銀行界定為經由網路銀行提供之金融服務。首先針對美國在電子銀行相關法規及主要銀行(Benchmark)電子銀行業務發展現況進行探討，進而以巴塞爾銀行監理委員會對 e-banking 風險控管原則，探討電子銀行之風險監控制度，作為檢視我國電子銀行風險

控管之議題。

彙集國內電子銀行相關法令規範、業務辦法、作業安全規定、電腦稽核實作或市場運作實況等相關資料，並比較美國等國家與我國之差異，進而提出建議，期盼為我國電子銀行發展豎立新的里程碑。茲將本專案之範圍概述如下：

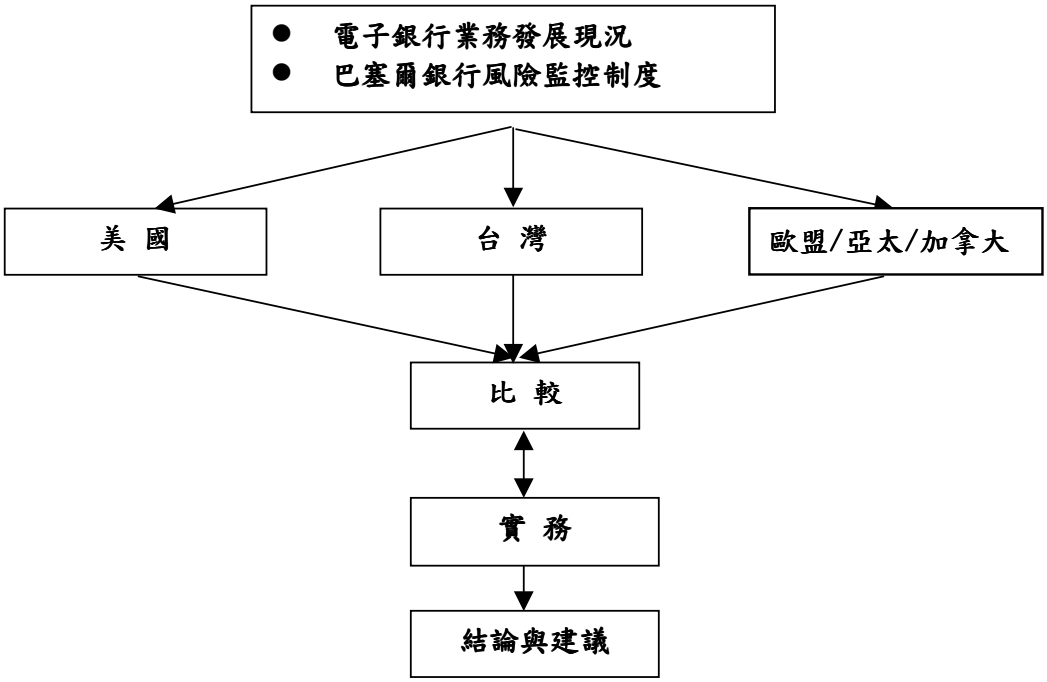
(一)、美國等國家與國內電子銀行業務之相關規範

(二)、美國與國內電子銀行業務發展現況

(三)、巴塞爾銀行監理委員會之電子銀行風險控管原則

(四)、國內銀行對電子銀行業務控管之實務面

四、研究架構



五、主要研究項目

(一)、美國與國內電子銀行發展現況

1.美國電子銀行發展現況

2.國內電子銀行發展現況

3.美國與國內電子銀行比較

(1).業務發展

(2).業務面臨之實務作業風險

(3).未來發展趨勢

(二)、巴塞爾銀行監理委員會之電子銀行風險控管原則

1.交易面銀行董事會與高階管理階層之監督管理

2.資訊安全機制以確保安全控管之落實執行

3.客戶資料保護、權益保障及客戶教育

4.電子銀行業務之內部控制

5.委外作業之管理及監督

六、專案目標

(一)、系統化蒐集及整理美國與國內電子銀行業務發展現況。

(二)、彙編美國電子銀行業務控管、監理政策及實務作業風險。

(三)、探討主管機關及金融機構對巴塞爾銀行監理委員會相關原則

之因應。

(四)、比較分析美國與台灣電子銀行業務發展與風險控管政策。

(五)、綜合分析並提出建議，供主管機關或銀行業於研訂金融法規、政策、業務方向或風險控管之參考。

(六)、配合主管機關需求，進行資訊分享或應用推廣。

參、團隊背景分析

由於網際網路的興起，帶動銀行服務通路大變革，也打破傳統業務的疆界與服務地域性的限制，造成速度與成本競賽。因而，電子銀行業務及風險控管，已成為主管機關及銀行經營上最重要議題之一。

我國電子銀行業務發展或風險控管之研究，除了應借鏡先進國家電子銀行相關之發展歷程及現況外，並應就國內相關法令、政策、資訊環境、業者實務面、消費者需求(B2C)、企業戶需求(B2B)及技術可行性等因素加以探討，並進而從顧客需求、市場趨勢、作業安全、資訊技術、風險控管及經營管理等多方面思維，研擬我國電子銀行業務及風險控管可能的最佳方向。

本公司主要產品在於提供我國電子銀行整合解決方案，除了持續引進國外先進銀行之相關應用外，並配合國內環境以推廣及建置至國內各銀行上線使用中，為我國銀行服務之效能及國際競爭力而努力。本研究專案與公司經營核心具有相輔相成之效果，將聯合產官學專家一起深入探討，共同研究我國電子銀行發展方向及風險控管問題所在，以提供主管機關、銀行界、學界或服務業等人士作業參考。

肆、研究方法與步驟

一、研究方法

(一)、對美國與台灣於電子銀行業務發展現況及國際性銀行對電子銀行業務控管等進行系統化蒐集及分析。

(二)、對巴塞爾銀行監理委員會對電子銀行作業之安控要求及新巴塞爾資本協定相關原則等相關性資料，進行蒐集及探討。

(三)、透過網際網路及產業關聯資料庫，進行市場相關資料或情報之彙整及分析，並釐定待查問題。

(四)、邀集國內外電子銀行專家或學者，共同探討電子銀行業務發展及風險控管議題。

(五)、召開會議討論、座談或報告，進行意見交流及討論，並於後續會議中進行資料修改及確認。

二、研究步驟

(一)、成立研究工作小組，蒐集美國與我國在電子銀行相關法規制定、業務辦法、風險監控或市場相關研究情報等資訊。

(二)、工作小組進行相關資料情報之分析、研討及彙編，並定期召開會議討論，就電子銀行相關議題交換意見及研判電子銀行風險監控制度及業務可能發展方向。

(三)、召集我國電子銀行產官學專家，研討電子銀行發展及風險控管等運作情況及未來展望，確保資料情報之客觀性及完整性。

(四)、選定國內外電子銀行業界標竿，並實地參訪或資料蒐集電子銀行發展及風險控管等運作及管理情況。

(五)、提出美國與我國電子銀行發展及風險控管之比較分析及初步建議等報告。

(六)、與主管機構或審查委員等意見交換或正式報告，並依照會議決議進行資料修改，而且於後續會議中進行確認。

(七)、提出正式報告及建議。

伍、參考資料來源

一、國外電子銀行業務監理或相關研究單位

1. 巴塞爾銀行監理委員會電子銀行監理之研究
2. The Office of the Comptroller of the Currency (OCC)
3. Federal Deposit Insurance Corporation (FDIC)
4. Bank for International Settlements(BITS)
5. Information Systems Audit and Control Association(ISACA)
6. 美國監理機構、支付體系或銀行等相關網站
7. Harvard Business School Press
8. Cornell Law School, Legal Information Institute
9. International Data Group/Gartner/Data monitor/The Tower Group 等公司之研究報導
10. 各國監理單位及電子銀行之相關網站或資料庫

二、國內電子銀行業務相關規範及政策

金管會銀行局網站、監理單位規定、資訊安全相關法規、資訊作業安控基準、資訊安全準則、風險控管自律規範、定型化契約及銀行電子銀行業務處理辦法、銀行相關網站及資訊安全相關網站等相關研究及報導。

三、國內外電子銀行相關產業資料庫

中華民國銀行公會、金融研訓院、中央存保、各銀行季刊、台大/政大國際學術互聯網、資訊工業策進會、學術期刊、資訊科技或顧問管理公司(IBM/CA/Microsoft/Unisys/KMPG)、專家論述及新聞網站等相關研究及報導。

第二章、國內外電子銀行之業務現況與趨勢

壹、國外電子支付系統現況與發展趨勢

網路世界改變了人類溝通及生活的方式，帶動了多元化跨業態的新交易模式，而良好的電子支付工具有加速線上交易之功效。反之，若無法有效解決支付需求，電子商務是沒有未來的，因為不便利或無信任的商場，消費者是不會喜歡的，生意自然就較不容易發生，當然供給與需求終究需要找到合適交點的。

依美國全國零售業協會(National Retail Federation)研究顯示建立一個好而有效率的電子支付體系，除可提供消費者有更多的選擇及商家享有支付便利外，在銀行及政府之推動之下，可帶動 GDP 百分比之一的經濟成長。

一、電子支付取代紙張貨幣的時代

電子支付工具可分為以卡片為基礎的金融卡 (Debit Card)、信用卡(Credit Card)、禮物卡(Gift Card)、預付卡(Prepaid Card)等，及以虛擬帳戶為基礎的電子錢包(e-Cash)、電子支票(e-Check)、行動錢包(Mobile Cash)等數位貨幣。如以發行單位可分為銀行業與非銀行業，非銀行業例如電信業、網路業者、零售業及提供金流服務第三方業者

如資訊服務公司或發卡/收單公司等。

美國 2004 年網上採購人口為 1 億人，網上營業額佔整體零售業 5%，超過 3,600 億美元。依 IDG 之 Financial Insights 報導指出，未來幾年亞太區網路銀行業務前景看好，網路銀行活躍用戶數將從 2003 年的 3,680 萬增至 2007 年的 1.09 億。電子支付發展，正悄悄地改變並促進了經濟成長。

據有關統計，2004 年全美國相關支付收入市場總量為 2800 億美元,其中由銀行收取的有 1/2，其餘部分由非銀行機構收取。美國相關支付收入市場總量在 2004 年佔全球支付收入總量 7,800 億美元的 1/3。美國的支付收入市場將按每年 8%的增長率增長，預計於 2008 年達到 4,110 億美元。

二、美國支付體系概述

1. 票據交換中心（Automated Clearing House，ACH）

ACH 提供銀行間匯款、電子支付、清算等處理交換中心服務。ACH 支援的交易包括:工資發放、社會福利發放、各種貸款的自動還款、B2B 支付、電子支付、聯邦及各州的所徵稅款支付。在 2004 年全年，ACH 處理的總交易量數為 100 億筆，總交易量為 20 萬億美元。其中商業交易佔 90%以上，其他為政府交易。

2. VISA 和 MasterCard 組織機構以會員形式，為金融及非金融機構發放信用卡。VISA 和 MasterCard 組織獨立建設支付標準、清算系統、POS 或網路 ATM 及風險控管系統。

3. 第三方獨立發卡和清算機構，例如美國運通（American Express）。美國運通在 2004 年底的發卡量為 6,500 萬張，全年交易量為 4,200 億美元。此類支付卡的清算是在本機構內實現的。

4. 支付服務提供商，如美國的第一資料公司(First Data Co.)。獨立建設 POS、ATM 系統及網路，並提供將最終用戶與發卡銀行直接連接的服務和收單業務，因此與 Visa 和 MasterCard 組織有一定競爭。同時其旗下的西聯匯款(Western Union)提供即時線上現金匯款業務，它是全球覆蓋最大的現金匯款網路。

5. 電匯業務提供者，如 CHIPS(Clearing House Interbank Payments System)、Fedwire(by Federal Reserve Financial Services)及 SWIFT (Society for Worldwide Interbank Financial Telecommunication)，主要建設並聯結銀行之間的帳戶電匯業務。在跨境的電匯業務中，SWIFT 的使用率是非常高的。

6. 提供收單業務的銀行，如美國 Wells Fargo 銀行。

三、電子支付快速成長的時代

依據美國聯邦準備 2003 年資料，全美非現金支付交易所佔比例分別為支票(36.7%)、信用卡(19%)、金融卡(15.6%)、電子支票(9.1%)等，其中以金融卡及電子支票透過網路支付各式各樣帳單或繳費成長最為快速。另依美國銀行家(American Bankers)調查顯示：金融卡在 2005 年佔全美零售業消費的 33%。又銀行藉由提供存款戶收付服務，而帶動的營收佔全部收入的 40%至 60%。由此觀之，支付工具的演變為銀行營運與生存命脈所在。

由於電子商務需求，帶動企業儲值卡及數位貨幣等小額支付體系之興起。依美國聯邦準備預估美國成人世界中有 24%沒有信用卡(全美約一億人口沒有信用卡)及 13%家計單位沒有銀行戶頭(約 3,700 萬人口)，這群人口對金流服務便捷化的需求，逐漸被新創的小額支付方式加以填補。如企業儲值卡、Western Union 匯款服務、 PayPal、Bill Me Later 、MoneyGram and Yahoo Direct 等。

近來零售業發行的儲值卡取代禮券相關盛行，依 National Retail Federation 統計 2005 年美國企業儲值卡約售出 200 億美元，佔線上(On-line)購貨比例為 39%。而銀行 ATM 及零售業 Kiosk 已開始提供企業儲值卡或預付卡之加值、提現、售卡、繳費或買票等客戶基本需求

服務，以增加收益。另銀行結合儲值卡功能，轉化為企業薪資卡(Payroll Card)代替支票發薪。

四、美國市面上著名虛擬貨幣機制簡介

1. PayPal

PayPal 小額付款系統，於 1998 年被設計出來，目前應用於美國及全球其他 20 個國家，同時是拍賣網站 eBay 最受歡迎的付款方式，也是公認最佳 C2C 付費服務與市場 C2C 付款機制的主流。該公司目前已擴展至 B2B 及 B2C 的付款服務。用戶已經能在 ATM 自動取款機上從 PayPal 帳戶中提款了。

PayPal 是世界上第一個提供以 e-mail 帳號付款的服務，亦即透過 e-mail 移轉金錢，商家及消費者不需要裝設任何軟體，其亦允許使用者透過 PDA 與上網手機等無線設備來移轉錢。付款者只要在 Paypal 網站上註冊開立戶頭，登錄姓名、電子郵件帳號、信用卡或銀行帳戶號碼、帳單地址等，付款時輸入收款者 e-mail 帳號及款項，對方即可收款，付款金額自動於線上帳戶扣除或進入信用卡帳單上，即付款者可以用信用卡或 PayPal 帳戶裡的錢付款，你可以寄錢給任何人，只要他有 e-mail 帳號，收款人收款方式包括 ATM 提款、支票、轉入銀行帳戶。

2. BitPass

2003.12 發表其小額收付款作業平台，主要服務對象為小型、獨立的數位內容提供者，爲其提供線上小額付款機制。採預付制，使用者開立一個 BitPass 帳號，將錢存入該帳號內，即可在 BitPass 的網站進行各項數位內容的消費。目前有超過 300 個數位內容業者加入該網站，較知名的有微軟(用 MSN 送 SMS 訊息至個人手機)與 Disney (以 Disney 各個卡通人物為主的網路遊戲)。

3. Peppercoin

成立於 2002 年，不同於一般的預付制小額消費，該公司產品的核心技術是可將多筆小額消費累積成一筆大額消費，如此消費者的信用卡只會被收取一次的手續費。主要經營市場是網路小額的實體物品販賣業者、數位內容業者與行動電信業者。

Peppercoin 可讓使用者調整其消費金額累積的方式，其產品也提供網路商家多種彈性的商業模式設定。

4. Qpass

成立於 1997 年，該業者在處理電信業者的數位內容產品與服務的付款上處於領先地位，其著名之客戶有 Cingular Wireless, T-Mobile International, Vodafone, Sprint, SunCom, Alltel, US Cellular, One and Skype 等。

QPass 適用於『點選付費』（Pay-per-Click）、『使用付費』（Pay-per-Use）的下載產品、訂閱制的產品、限制時間的網站連結等，其系統強調提供包括交易、認證、售後服務的完整解決方案。

目前在美國小額付款市場方面是百家爭鳴，沒有一套共同標準。均以強調簡單、快速、安全、便宜，讓使用者與商家容易上手或安裝，而且所需費用遠小於傳統的支付工具。

貳、國內外電子銀行之業務發展與安全防護

一、國外網路銀行業務現況概述

網路銀行為銀行及顧客帶來的效益與便利日漸顯著，並已漸漸形成銀行的主要通路(eChannel)之一，以 2005 年為例英國、德國網路銀行使用者線上戶數已超過 50%。而美國和日本已使用網路銀行比率分別為 38%及 30%，其中美國的 Bank of America、Wells Fargo 及 Citibank 等三大網路銀行戶數皆超過全部戶數的 50%。

中國大陸網路銀行發展迅速，依中國互聯網路資訊中心(Chain Internet Net Information Center, CNNIC) 所調查報告，在 2006 年 1 月用戶數已達 1.1 億萬戶，目前在十大經濟發達城市中，已有近 20%的個人用戶和超過 10%的企業用戶正在使用網路銀行服務。其中中國工商銀行 2005 年 11 月，個人網路銀行客戶已經突破 1,540 萬戶，交易額達到 5,237 億元；企業網路銀行客戶突破 30 萬戶，交易額突破 38 萬億元，居大陸網路銀行之首。而電子銀行的交易量已經佔到全行總交易量的四分之一以上。

二、我國晶片金融卡應用與安全防護

我國晶片金融卡在銀行局及財金資訊公司全力推動之下，已成功發行 3,600 多萬張卡，並不斷創新如網路 ATM、全國繳費平台、電子錢包、購物消費等應用，將磁條卡快速全面轉化為晶片卡，成功典範已廣受國外關注。

該晶片安全標準係依照國際標準組織 ISO 7816 的規範，採元件化概念設計，晶片本身具有極為嚴密的實體安全能力，能有效防止斷電密碼攻擊、斷電重新開機攻擊、EEPROM 破壞竊取等攻擊，而晶片安全等級亦符合歐規 ITSEC E4 (Trusted Computer System Evalution Criteria Evaluation 4)及美規 EAL5 (Evaluation Assurance 5)等標準，以確保交易資料的安全性與完整性。

目前藉由晶片在實體上及邏輯上所具有的安全特性，使得經由它所進行的交易，具有身分的認證及交易的不可否認性，使用更擴充至電話、手機、寬頻、網際網路等通路，因而金融服務功能亦不斷被延伸。

三、國內電子錢包逐漸萌芽茁壯

目前國內小額支付工具，除銀行晶片金融卡、VISAwave、Paypass 等金融機構發行的電子錢包外，民間企業為配合客戶需要有交通業

發行的悠遊卡、台中 e卡通、高速公路卡(FETC) 、南部交通卡(Taiwan Money)；連鎖體系發行的企業儲值卡如統一超商 iCASH、星巴客隨行卡、丹堤 e 卡及網路業者發行得點數卡、EZpay 等電子支付逐漸醞釀中。

四、我國網路銀行相關應用發展

我國電子銀行在政府機構推動及業界競爭之下，自 83 年陸續推出金融 EDI 稅費支付系統、銀行網站、金融 EDI 跨行付款系統、網路銀行、PC Banking/EDI 服務 (TurnKey)、網路繳稅、網路下單、網路轉帳、行動銀行、隨身銀行 (PDA Banking)、金融 XML 支付款系統、企業銀行、C 計畫金流服務及銀行公會 FXML 訊息格式等業務，在功能方面不斷創新，並與時代科技不斷演進，惟因顧客使用上有安全疑慮、方便性不足及銀行欠缺行銷策略等因素下，用戶數或使用率一直未有明顯的增加。

目前國內隨著網路普及與電子商務的到來，銀行也陸續推出電子金融商品如企業電子金融整合服務平台(EAI)、金融電子資料交換(FEDI/FXML)、企業財務自動化管理、企業統收/統支帳款管理(e-Billing)、學生線上繳費/貸款、電子支票(e-Check)、線上融資(e-Loan)、電子押標金帳務處理、FXML 全球收付款整合作業管理、全

球線上信用查核(Coface)、企業貨款支付及現金股利發放、企業整合性託收、媒體交換及資料回饋等創新性附加服務，為企業或個人提供嶄新的金流服務，銀行亦因作業流程自動化及服務模式的改變而不斷提昇效能。

五、網路銀行安全與防護

網路銀行業務除了銀行業務風險，如信用風險、市場風險、流動性風險、交易風險、法律風險、外匯風險、戰略風險、信譽風險等之外，又產生了一些新的電子作業風險，如網上交易的網路安全風險、資金轉移中可能涉及嚴重的操作風險、潛在債務和消費者權益保護的問題等。

目前網路銀行安全防範措施：

1. 交易網路的安全性與可靠性

客戶信任程度的大小決定網路銀行的成敗。交易網路的安全性、可靠性是提高客戶信任度的關鍵。防火牆通常被用來保護網路銀行的電子資訊安全，將預防、偵測和糾正控制功能有效地結合在一起，防止未經授權者或駭客侵入銀行的網路系統。網路銀行通常使用私鑰(Private Key)與公鑰(Public Key)雙重加密系統來保護客戶

資訊和核實真偽。電子審計跟蹤系統也被用來保護交易網路的安全性和可靠性。

2. 消費者權益保護

網路銀行帳戶的資訊可能被金融機構的其他部門濫用，造成對消費者權益的侵害。相應的防範措施有電子審計跟蹤系統，監管機構要求網路銀行增加資訊披露與透明度，制定更好的保密性和安全性監管標準，優化網路銀行軟體系統，提供幫助消費者識別、防範欺騙與盜竊的知識等等。此外，許多機構提供代理人幫助消費者尋找或比較相關產品或服務，另網上交易的信用風險可由數位簽名或預先鎖定等方法來防範。

3. 監管的國際合作

網路銀行不需要有形設施便可以提供跨境國際業務，這對各國監管的有效性提出了挑戰。跨境的電子銀行業務產生了一些特殊的風險因素。比如，跨境履約問題、資料庫共用問題；從事跨境網路銀行業務及其相關聯的非銀行業務，可能出現不受任何國家金融管理機構監管的「真空地帶」；各國監管者對本國居民進入其他司法管轄區的電子銀行網址的業務活動進行監控存在困難等。因此，監管的國際合作日顯重要。

針對電子銀行業務風險管理作業，依巴賽爾銀行「金融業進行

電子銀行與電子貨幣活動之風險管理」之建議，強調規劃重點應著重於減輕開放電子銀行業務對金融機構及一般民眾所承受風險，及保護消費者兩大原則。

參、美國網路銀行個案探討—富國銀行(Wells Fargo Bank)

一、全力發展電子銀行的銀行

依 Tower Group 統計報導：2004 年富國銀行在網路銀行客戶已超過 500 萬戶以上，使用網路交易比率超過全部戶數 50%以上，僅次於美國商業銀行(Bank of America) 排名全美第二；其中往來企業戶中有 70%使用該行商業電子金融平台(Commercial Electronic Office Portal)與銀行進行相關業務往來，於 2004 年該平臺處理線上支付金額達 4.1 兆美元。

該網站是首家與線上購物結合的銀行網站，並勇於採用各種新式電子支付工具(晶片卡、數位現金)及依企業規模大小提供多元化電子金融服務(超過 45 種線上金融服務項目)，被全球金融雜誌(Global Finance Magazine) 2005 世界最好的網路銀行競爭評比中，列為美國最佳企業/機構網路銀行、網站最佳設計及最好資訊安全創始者(採 128 位元加密認證)等美譽。

該行有鑑於家庭使用電腦的比例急速上升，及越來越多的顧客使用網際網路及電話語音服務。因而，加速使用新科技，提供全天候全方位的便利服務。於 2005 年該行發現支票客戶中有 51%已使用連線交易，建置「企業全球財富管理平台」，全力拓展企業網路銀行，並進行

虛擬通路系統整合(如網路、電話、ATM、Kiosk 等)，並作為業務經營中心，經評估除可節省 10%-25%的各別 IT 投資及作業的成本外，尚可提高客戶自助性 (ATM/Kiosk)及帳單繳費等自主性服務。進而，提供企業整合性支付、資金管理及貿易外匯等金融服務。目前，有 50 萬中小企業戶及 10 萬商業公司戶接受網路銀行服務，並帶來大量新客戶。

二、以行銷策略主導的網路銀行

富國銀行為首先提供網路上運營的銀行之一，初期使用各種方法鼓勵顧客申請網路銀行的服務。如顧客直接線上登記並選擇密碼，即可進行網路銀行的各項交易。接著，當微軟推出探險家瀏覽器(Internet Explorer)時，富國銀行與微軟共同合作以確保顧客的隱私權和安全性，同時採取解決顧客網路銀行安全性問題之一系列措施。接著提供顧客可在不同的帳戶間轉帳，也可以線上支付信用卡帳單。此後，又開放可以讓不同類型的顧客利用網路銀行處理更多服務。

富國銀行於 1997 年中宣佈使用網路電視(WebTV)以及諾基亞(Nokia9000)行動電話的顧客，也可以進行網路銀行的交易活動。和這兩家公司緊密合作，以測試安全資料傳輸 (SSL) 計畫執行狀況。接著，提供線上申請貸款的服務、推出策略性的武器－帳單整合，顧客在網路上可以查出全部的帳單及其他的相關資訊。並且，可以選擇一

次付清或分期付款、安排付款的時間，如顧客對某一項帳單明細項目有疑問的時候，可以直接線上提出疑問。

持續提供個人化服務功能如「我的開支報告」 (My Spending Report)，將客戶的支票卡、信用卡、支票帳戶和帳單付款等開支往來簡便地綜合在一起，透過安全的銀行網路頁面讀取，而且每日自動更新。使用簡單，好處很明顯。客戶不必自己輸入資料，便可獲得多功能個人理財軟體的優點，可節省時間和資金。將消息散佈到市場、發展新客戶群電子和帳單支付交易按客戶熟悉的方式分類，如汽油/汽車、雜貨、ATM 提款等。Wells Fargo 客戶亦可儲存該資訊或列印該報告。

建立財務管理網路社群，提供顧客一些關於理財規劃、財務管理以及投資等資訊和服務，建立與顧客互信關係，並提供顧客感興趣的資訊和服務，進而建立顧客彼此互動、互相諮詢和協助，以便分享共同關注的問題。

三、提供線上銀行安全的承諾

富國銀行為確保網路交易安全，除系統採取密碼及訊息加密認證和程式安全保護外，在與客戶連線契約書(Online Access Agreement)明確說明電子銀行業務規範及與客戶雙方的權利與義務。保證客戶 100%

無須擔心因正確使用安全的線上服務而遭受任何金錢損失，惟客戶對於帳號、密碼被竊、未被授權轉移、資料輸入錯誤或者錯用等部分應由客戶自負責任。

美國存款保險公司(FDIC)提供線上交易保險，富國銀行針對每一個支票帳戶每筆交易 50,000 美元以內的投保，如銀行方面錯誤，銀行同意支付合理承擔的任何費用或財務費。另對客戶損失之權利義務亦有所規範，如客戶帳戶金額未被授權的轉移(EFT)之責任，在兩營業日內通知銀行，在獲悉密碼的損失或者偷竊之後，客戶責任將不超過 50 美元或者在客戶察覺之前發生的未被授權的轉移之金額中較少者。如果客戶不能在兩營業日內通知銀行，在獲悉密碼的損失或者偷竊之後，客戶責任將不超過 500 美元或者總數中的較少者，並應在一定期限內陳述事由。富國銀行並提供一天 24 小時，一周 7 天任何時候，可能以電話、電子郵件或者以書面形式通知。

線上使用費方面：前兩個月免費外，個人支票帳戶餘額至少保持 5,000 美元可免費，否則，帳戶管理費每個月收 6.95 美元；企業商務戶收 9.95 美元帳戶管理費，尚不包括每筆額外 0.40 美元的處理費。

富國銀行允諾保證客戶的隱私，除法律允許外，不透露給不附屬於富國銀行的任何第三者。另有關任何與客戶爭端的解決，以美國仲裁協會的商業仲裁規章裁決為準則。

四、依目標顧客群進行系統設計及推展

依顧客群不同需求提供整合性金融服務如顧客資訊、帳戶內容、服務記錄等，並以使用者容易存取資料的形式呈現，以主動行銷方式把資訊傳遞給公司內部所有與顧客接觸的員工以及顧客本身，這也是網路銀行普及成功因素之一。主要功能說明如下：

1. 不同的客戶群劃分的很清楚，會有不同的登入方式及資訊情報。
2. 可切換不同語言。
3. 資訊內容豐富，並提供站內搜尋及網網相連服務。
4. 提供快速客服連絡方式(電話、e-mail、當地公司、郵件)，登入後可提供即時的線上問答。
5. 提供線上教學服務及導覽展示功能。
6. 一站購足(One Stop Shop)的經營模式。
7. 不斷創新其金融服務，以達個人化之目的，如推出 My Spending Report 服務。
8. 提供經濟、外匯或貿易等金融情報。

為了提供顧客更高價值的服務，Wells Fargo 整合所有的顧客資訊以及應用程式，讓業務及服務人員能夠提供一站購足的服務與交易，並整合後台系統，滿足顧客在網路上亦可一站購足的需求。

五、結論

富國銀行網路銀行業務之成功，有其獨特之處，而網路銀行設置的目的，並不在於取代實體銀行，更重要的是拓展更多實體銀行所達不到的業務。因而，如何站在顧客的需求出發，除了確保交易安全及操作簡便之外，應以有效的行銷手法來達成所預期的目標將是業務規劃重點，這或許是我國網路銀行可借鏡之處。

第三章、主管機關電子銀行業務之監理規範

壹、美國監理單位與網路銀行風險控管

美國通貨監理局（Office of the Comptroller of the Currency, OCC）於 2001 年 7 月 16 日公佈「聯邦立案銀行經營電子銀行業務規範」草案暨相關規定，該項草案提供全國銀行就目前已許可電子銀行業務之相關指導原則。並依據美國金融服務業現代化法〔The Gramm-Leach-Bliley Act，簡稱 GLB Act〕第 729 條規定，聯邦政府銀行主管機關應主導一項有關金融服務方式之銀行法規研究，包括假定金融性交易過程會有直接接觸諸多規定，及配合現行連線銀行業務及放款建議；故 OCC 與其他聯邦銀行機構對線上金融服務傳遞以及線上銀行業務與放款等相關規定與法令提出建議。

為確保電子銀行服務能兼顧銀行穩健發展，OCC 亦提出與銀行使用技術相關之監理指導原則，指示各銀行資訊安全標準需配合 GLB Act 規定並據以執行。另出版網路銀行相關指導手冊，探討銀行透過網際網路提供商品與服務相關議題、經營此類業務之風險以及 OCC 對網路相關的檢查程序等。該項規範著重三項議題：〔一〕OCC 採用的規範與監理政策如何指導全國銀行使用電子化技術且兼顧銀行安全與穩健；〔二〕OCC 於何種情況下可用較為彈性的解釋以適應新的技術；

〔三〕OCC如何加強從事電子銀行業務之銀行營運上之彈性且兼顧銀行安全與穩健。

由於新技術的迅速發展，使得銀行業者必須能夠立即且有效回應不斷改變的顧客需求，因此該案明確規範電子銀行業務係屬銀行業務。當銀行經營業務之界限重新劃分並提供新的金融商品以服務顧客時，即需不斷地評估從事電子銀行業務之權限是否合宜。其中對於聯邦立案銀行與關係機構以及第三團體等共享聯名網站或電子交易時，必須採取適當步驟使其顧客可明確分辨何種產品與服務為銀行所提供，何種產品與服務為非銀行者所提供等部分有相關規定。

美國 OCC 為檢查人員便於查核或瞭解網路銀行之業務風險重點及應管控之關鍵要素，分別於檢查手冊中，就網路銀行與信用、利率、流動性、價格、外匯、交易、法律、策略和信譽等可能潛在風險，逐一詳加說明，並就銀行立場對電子銀行業務相關之內部管控、安全作法或應注意事項等，也提示其重點所在，可供國內監理單位或銀行在執行電子銀行查核或管控之參考。

一、各類風險與網路銀行關聯性

1.信用風險

信用風險是指債務人未能履行合約而對銀行收益或資本所造成的風險。在動作的成功性依賴於對方、放款人或借款人行為的情況下，所有這些動作中都存在著信用風險。當提供、調撥、投資或透過真實的或隱含的契約協議而給銀行資金造成暴露時(不管在銀行資產負債表之內，還是在銀行資產負債表之外)，都會產生信用風險。

網路銀行業務為銀行提供了擴展地域範圍的機會。顧客可以在任何地方與特定的銀行進行連結。當透過網際網路與顧客進行交易時，由於缺乏人與人之間的接觸，在如何驗證顧客的誠意方面為銀行機構帶來了挑戰。而這是作為貸款決定的一個要素。對於外地借款人，在驗證抵押品和完善安全協議方面也極具挑戰性。如果不能實施合理的管理，網路銀行業務就可能導致外地貸款的集中或貸款集中於單一產業。另外，對於哪一國的法律將適用於管理網際網路關係，這一問題仍在爭論之中。

對於透過網際網路獲得貸款，其有效管理必然要求董事會和管理部門瞭解並控制銀行的貸款風險情況和信用文化背景。他們必須保證，有效的策略、程序和實務在實施之中，以控制與這類貸款相關的風險。

2.利率風險

利率風險是指利率的變化為銀行收益或資本所造成的風險。以下幾種情況會造成利率風險：利率變動時點和現金流動時點之間的時間差(重新定價風險)；影響銀行運作的不同利益曲線中利率關係的變化(標竿風險)；跨越到期日範圍的利率關係的變化(收益曲線風險)；銀行產品中所包含的、與利率相關的選擇權(選擇權風險)。對利率風險的評估必須考慮複合的、非現金的套利策略或產品的影響，也必須考慮利率變動對收費的潛在影響。

與其他的行銷形式相比，網路銀行業務可以從更多的潛在顧客吸收存款、貸款和建立其他關係。接近顧客(他們主要尋求最優的利率或條件)的機會越多，銀行管理人員就越有必要維持恰當的資產、債務管理系統，包括對市場狀況的變化進行快速回應的能力。

3.流動性風險

流動性風險是指銀行無力清償到期債務(並沒有造成不可接受的損失)而對銀行收益或資本所造成的風險。流動性風險包括銀行無法管理融資來源的計劃之外的變化。市場狀況影響著銀行以最低限度損失而快速變現資產的能力，而銀行並沒能識別市場狀況的變化，這時也會造成流動性風險。

網路銀行業務將加大存款的波動性，因為顧客只根據利率或條款來開設帳戶。資產、債務和貸款組合管理系統應該適用於透過網路銀行提供的產品。根據網際網路帳戶活動的交易量的特徵，應加強流動性和存貸款變化的監控。

4.價格風險

價格風險是指所交易的金融工具組合的價值變化對銀行收益或資本所造成的風險。這種風險來自於市場發展、利率市場、外匯市場、權益市場。

作為網路銀行業務流動的結果，如果銀行創立或擴展存款經紀服務、貸款銷售或證券化計劃，這些都將帶銀行給價格風險。如果銀行資產被頻繁交易的話，應該保持恰當的管理系統來監控、衡量和管理價格風險。

5.外匯風險

當貸款或貸款組合為外幣或以外幣借款進行融資時，就會出現外匯風險。在某些情況下，銀行承擔了多幣別貸款的義務，從而允許借款人在每個轉換期選擇他們喜歡使用的幣種。政治、社會、經濟發展等因素可能會加劇外匯風險。如果所涉及的一種貨幣受到嚴格的外匯管制或受到大範圍匯率波動的影響，那麼可能會造成不利銀行的結果。

如果銀行接受非本國居民的存款或創立外幣帳戶，這將帶給銀行外匯風險。如果銀行參與了這些活動，應該開發恰當的系統來管理相關的風險。

6.操作風險

操作風險是指由於欺詐、錯誤和無力傳送產品或服務、無力維持競爭地位、無力管理資訊而對收益和資本所造成的當前風險和預期風險。在所提供的產品和服務中，操作風險都是顯而易見的，其中圍繞著產品開發和傳送、交易處理、系統開發、電腦系統、產品和服務的複雜性以及內部控制環境等都有可能發生這類風險。

網路銀行業務的產品伴隨著很高的操作風險，特別是銀行未能恰當地規劃、實施和監控業務品質的情況下，透過網際網路提供金融產品和服務的銀行必須能夠迎合顧客的期望。銀行也必須確保具有正確的產品種類，有能力傳送準確的、即時的、可靠的服務，從而建立起顧客對其品牌的高度信任。如果金融機構不具備完善的內部控制來管理網路銀行業務，那麼透過網際網路展開業務的顧客可能無法容忍該金融機構的錯誤或疏忽。

對銀行電腦和網路系統的攻擊或嘗試入侵是一個重要問題。有關研究表明，與外部攻擊相比，系統更易受到內部的攻擊，因為內部系

統用戶更瞭解該系統及其存取方法。銀行應該具有合理的預防和監測控制，以保護網路銀行系統免受內部或外部的攻擊。

銀行必須確保在不利事件發生的情況上能夠提供產品和服務，因此，緊急應變和業務恢復計劃是十分必要的。當金融機構制定緊急應變和業務恢復計劃時，應該考慮到安全性方面的問題。在這種情況下，備份中心的安全性和內部控制應該與主處理中心的安全性和內部控制同樣完善。系統的高可用性將是顧客的主要願望，是區分網際網路上的金融機構成功程序的重要指標。

提供帳單呈送和支付服務的銀行應該具有恰當的程序來結算銀行、顧客和外方之間的交易。除了操作風險外，結算失敗也將造成信譽風險、流動性風險和信用風險之損害。

7.法律風險

法律風險是指違反或不遵從法律、法規、規章、慣例或倫理標準而對銀行收益或資本所造成的風險。在管理銀行產品或顧客行為的法律或法規不明確或未檢驗的情況下，也會引起法律風險。法律風險使金融機構面臨著罰款、民事罰款、賠償損害和契約失效的風險。法律風險將導致貶低信譽、降低免賠限額、限制業務機會、降低拓展潛力以及缺乏契約的可實施性等等。

大多數的網路銀行顧客將繼續使用其他的銀行傳送通路。因此，銀行必須保證，網路銀行通路(包括 Web 網站)上的資訊披露與其他傳送通路上的資訊披露保持一致，從而保證向顧客提供一致的、準確的資訊。

廣告和記錄保存要求也適用於銀行網站以及所提供的產品和服務。廣告應該明確、顯著地列出保險通告(在適用的地方)，從而顧客可以很容易地確定某產品和服務是否保險。對銀行網站的例行監控將有助於遵從適用的法律、法規和規章。

打算允許顧客透過網際網路設立新帳戶的銀行應該制定嚴格的帳戶開設標準。此外，銀行應該建立控制系統以識別非例行的或可疑的行為，並且在適當的時候編寫可疑行為報告。

8.策略風險

策略風險是指由於不利的業務決策、決策的不恰當實施或對行業變化缺乏回應而對銀行收益或資本所造成的當前影響和預期影響。該機構的策略目標、為實現這些目標而制定的業務策略、針對這些目標所使用的資源、實施的品質等之間的一致性將對策略風險產生影響。完成業務策略所需的資源包括有形資源和無形資源，其中包括通信通路、作業系統、傳送網路、管理才能和潛在能力等。必須對照經濟、

技術、競爭、立法和其他環境變化的影響來評估該機構的內部特徵。

在決定開發特定的業務種類之前，管理部門必須瞭解與網路銀行業務相關的風險。在某些情況下，銀行可以透過網際網路來提供新的產品和服務。管理部門瞭解風險和決定的結果是十分重要的。業務風險必須依賴於技術和管理資訊系統(MIS)的支援。由於很多銀行將在現有業務領域之外與金融機構進行競爭，所以展開網路銀行業務的銀行必須把所採用的技術和策略規劃過程密切連結起來。

銀行在導入網路銀行產品之前，管理部門應該考慮該產品和技術是否與銀行策略規劃中的、明確的業務目標相一致。銀行也應該考慮是否具有足夠的專門知識和資源來識別、監控和管理網路銀行業務中的風險。計劃和決策過程應該注重考慮網路銀行產品是如何滿足特定的業務需求，而不是把該產品作為一個獨立的個體去關注。銀行技術專家應該在決策和規劃過程中發揮作用，他們應該保證該計劃與銀行的整體業務目標相一致，並且在銀行的風險承受能力之內。新的技術(特別是網際網路)將引起競爭力的快速變化，因此，策略上的遠見應該確定網路銀行產品的設計、實施和監控方式。

9.信譽風險

信譽風險是指負面的公眾輿論給銀行收益和資本所造成的當前

影響和預期影響。信譽風險影響了該機構建立新關係或提供新服務的能力，或繼續為現有關係提供服務的能力。信譽風險使金融機構面臨著訴訟、金融損失或顧客減少的危險。信譽風險存在於整個機構之中。在應付顧客和公眾時，該機構有責任倍加小心。

如果銀行沒能應付市場要求提供產品或沒能提供準確的、即時的服務，那麼其信譽將受到損害。這包括沒能充分地滿足顧客的貸款需求、提供不可靠的或無效率的資訊系統、沒能對顧客的要求即時地作出回應、侵犯顧客隱私等。

如果銀行沒能很好地實施網路銀行服務或疏遠了顧客和公眾，那麼這將損害銀行的信譽。計劃周密的市場行銷(包括資訊披露)是教育潛在顧客的一種方式，這將有助於限制信譽風險。顧客必須瞭解，他們能夠從產品或服務中合理地期望什麼，以及使用該系統將帶來什麼樣的特定風險和效益。因此，行銷觀念必須與恰當的披露聲明密切協調。銀行不應該基於網路銀行系統所不具有的特徵或特點進行銷售；行銷方案必須公正地、準確地展開其產品。

銀行必須確保其業務連續性計劃包含了網路銀行業務。銀行應該對業務連續性計劃進行例行測試(包括與新聞界和公眾的溝通策略)，從而確保對不利的顧客反應或媒體反應作出有效的、迅速的回應。

二、網路銀行業務風險管理

金融機構應該具有技術風險管理程序，從而能夠識別、衡量、監視和控制技術風險暴露。新型技術的風險管理具有三個基本要素

- 技術應用的規劃過程。
- 技術的實施。
- 用於衡量和監控風險的措施。

監理單位確定銀行是否以安全、合理的方式展開網路銀行業務。銀行是否使用嚴格的分析過程中來識別、衡量、監視和控制風險。審查人員需要確定風險級別是否與該銀行的總體風險承受能相一致，是否處於銀行的管理和控制能力之內。

1.規劃過程：風險規劃過程是董事會和高階管理部門的職責。

他們需要具備一定的知識和技能，以管理網路銀行技術的應用以及與技術相關的風險。董事會應該審查、批准和監控與網路銀行技術相關的、可能對銀行風險帶來重大影響的專案。他們應該確定該項技術和產品是否與銀行的策略目標相一致，是否滿足了市場需求。高階管理部門應該具備一定的技能，以評估所採用的技術以及所承擔的風險。稽核人員或顧問人員應對網路銀行技術和產品定期進行獨立評

估，這將有助於董事會和高階管理部門履行其職責。

2.技術的實施：技術的實施是管理部門的職責。

管理部門應該具備一定的技能，以有效地評估網路銀行技術和產品，為銀行作出正確的選擇並核查是否得到了正確的安裝。如果銀行並不具備專門的知識來履行其職責，那麼它應該考慮與專門的資訊服務廠商簽訂契約，或與具備互補性技術或專門知識的另一供應商建立聯盟。

3.衡量和監控風險：衡量和監控風險是管理部門的職責。

管理部門應該具備一定的技能，以有效地識別、衡量、監視和控制與網路銀行業務相關的風險。對於所採用的技術、所承擔的風險以及如何管理這些風險，董事會應當定期吸取有關的報告。監控系統性能是一個關鍵的成功因素。作為設計過程的一部分，銀行在網路銀行系統中應當包含有效的品質保證和稽核過程。銀行應當定期對系統進行檢查，以確定該系統是否符合性能標準。

三、網路銀行業務內部控制

對網路銀行系統的內部控制應該與該機構的風險級別相當。如同

其他的銀行業務領域一樣，針對網路銀行技術和產品，管理部門具有責任來開發並實施合理的內部控制系統。

對控制系統的例行稽核將有助於確保這些控制方法是恰當的，並且良好地發揮著功能。例如，對於個別銀行的網路銀行技術和產品來說，控制目標可能為：

1.技術規範與策略目標的一致性，其中包括運行效率與節約措施，並且遵從了公司策略和法律要求。

2.資料可用性，其中包括業務恢復計劃。

3.資料完整性，其中規定了資產防護措施、正確的交易授權、處理和輸出的可靠性等。

4.數據機密性和隱私權保護措施。

5.管理資訊系統(MIS)的可靠性。

一旦制定了控制目標，管理部門就有責任來設定必要的內部控制，以實現這些目標。管理部門也有責任在成本及效益分析的基礎上評估這些控制方法的恰當性。這種分析可能考慮了某過程中各種控制的成效、該過程中流動的資金量、控制的成本等。

在上面所討論的基本內容控制中，可以發現三種控制類型。

1.預防性的控制：用來防止某種事情(通常為錯誤或非法行為)的發生。邏輯存取控制軟體就是這種控制類型的一個例子，該軟體只允許經授權的人員使用帳號和密碼來存取網路。

2.檢測性的控制：用來識別已經發生的行為。入侵檢測軟體就是其中的一個例子，該軟體具有報警功能。

3.更正性的控制：一經發現，立即更正。軟體備份(用來恢復被毀壞的軟體或資料庫)是其中的一個例子。

提供交易型網路銀行產品的服務，供應商必須具備較高級別的控制，以有助於管理銀行的交易風險。這些控制包括：

1.監控交易行為，以發現交易類型、交易量、交易額中的異常。

2.監控登錄入侵或嘗試，以識別可疑行為(包括異常請求、異常計時或異常格式)的模式。

3.使用誘騙和追蹤技巧來識別請求的來源，並與已知的顧客相對照。

而例行報告和異常交易審查將有助於識別：

1.未經授權的入侵。

2.顧客輸入錯誤。

3.進行顧客教育的良機。

四、網路銀行業務技術開發管控

與安全性、運行、規劃和監控等特定領域相關的不同程度的複雜性，迫使許多銀行的網路銀行產品全部或部分委外開發或處理。因而，銀行應該定期地重新評估技術支援的來源，以確定既定的解決方案能否繼續適合業務計劃，能否彈性地滿足預期的未來需求。不管由銀行本身還是由第三方服務商提供技術服務，銀行都必須把技術提供廠商與銀行的策略規劃過程密切連結起來。這使得該銀行能夠把新的產品和服務與現有的技術和產品種類連結在一起。

銀行自己開發必要的應用軟體，可彈性地提供訂製的產品。然而，這些銀行必須特別留意，以保證其安全性沒有受到損害。

在選擇資訊服務廠商來提供網路銀行服務之前，銀行仍需作出一定的努力。它們應該與資訊服務廠商簽訂正式的服務協議，以明確地規定所涉及各方的義務和責任。銀行應該監視資訊服務廠商的運行績效、財務狀況、與不斷發展中的技術保持同步的能力等等。通常，銀行透過獲得內部稽核報告或第三方稽核報告來履行職責，以確保資訊服務廠商具有合理的內部控制。

五、網路銀行業務中的問題

為了保持公眾對單一銀行及其品牌以及對整個金融系統的高度信任,對銀行產品和服務(尤其是透過網際網路提供的產品和服務)的有效管理是至關重要的。在開放的網路環境中，以下幾個方面將有助於保持公眾的高度信任：安全性、認證、信任、不可否認性、隱私和可用性。

1.安全性

安全性是網路銀行系統中存在的一個問題。銀行要能夠提供與資訊敏感性、銀行的風險承受能力相當的邏輯安全和實體安全。

由於網際網路通常缺乏安全性。因此，銀行必須具有合理的內部控制系統，以防止對任何形式電子存取的安全性的破壞。有效的控制(預防性的控制、檢測性的控制、更正性的控制)系統將有助於確保網路和資訊的完整性。

在網路銀行系統中經常使用防火牆，以作為一種完全措施來保護內部的系統。對於與外部網路相連的任何系統，都應該考慮使用防火牆。防火牆提供了電子閘門的功能，用來阻止未經授權的個人進入銀行的網路。

防火牆的簡單存在並不能確保邏輯安全，防火牆也不是不可穿透

的。必須對防火牆進行配置，以滿足特定運行環境的需要。也必須定期評估和維護防火牆，以確保其成效和要求一系列的安全控制。

2.認證

認證是網路銀行系統中存在的另一個問題。網際網路或其他通信網路上的交易必須是安全的，以實現高度的公眾信任。在網路環境中，如同在實體的世界中一樣，顧客、銀行和商戶需要確信他們將收到所預訂的服務或所請求的商品，並且他們知道交易對方的身份。

通常，銀行使用對稱加密技術來保證資訊的安全，使用非對稱(公鑰／私鑰)加密體制來鑑別各方的身份。非對稱加密體制使用兩個密鑰。即公鑰和私鑰。在數學上，這兩個密鑰是連在一起的，但是卻不能從一個密鑰推導出另一個密鑰。例如，為了確定某條資訊來自發送方，發送方使用其私鑰加密此條資訊。只有發送方自己知道該私鑰。但是，該資訊一經發出，只能使用發送方的公鑰進行讀取。由於能夠使用發送方的公鑰讀出該資訊，所以接收方就能知道該資訊的確來自預期的發放方。

網路銀行系統應該採用與系統中風險等級相適應的加密方式。較強的安控會降低系統的性能，而管理部門必須在安全性需求、性能和成本問題之間作出均衡。因此，銀行在確定恰當的加密等級時，應該

進行風險評估，審查不同加密系統的成本和效益，並作為一種業務決策來確定恰當的加密機制。管理部門並應為其決策進行支援性的分析。

RSA 是一種常見的非對稱加密系統，它所作用的密鑰的長度多達 1024 位。透過混合使用這兩種加密機制(即使用對稱加密來保護資訊、使用非對稱加密來鑑別所涉各方的身份)，銀行就能夠保證資訊的安全，並對所涉各方的身份具備了高度的信任。

生物測定法是一種先進的鑑別形式。這種方法可能採用視網膜掃描、指紋掃描、面部掃描或聲音掃描的方法。儘管目前仍然未把生物測定法應用作為一種主流，但是，一些銀行仍嘗試使用生物測定學方法進行認證鑑別。

3.信任

信任是網路銀行系統中存在的另一個問題。如前所述，在網路環境中，可以使用公鑰／私鑰加密機制來保證資訊的安全性，並鑑別交易各方的身份。可信的第三方是該過程的一個必要部分。該第三方被稱為“認證機構”(RA/CA)。

認證機構是一個可信的第三方，它在網路環境中驗證所涉及各方的身份。一些人把認證機構的功能解釋為線上公證人。基本的觀念就是，銀行或其他的第三方利用其好的名聲來驗證交易中的各方。這類

似於銀行在信用狀中已扮演過的歷史角色，此時，買賣雙方互不認識，但是銀行瞭解這兩方。因此，銀行利用其好品牌來促使交易的完成，並從中收取一定的費用。

4.不可否認性

不可否認性是指交易發送方和接收方參與了該筆交易的不可拒絕的證據。這就是建立公鑰加密體制的原因，也即用來鑑別電子的資訊，防止發送方或接收方對交易的拒絕或否認。

5.隱私

隱私是一個消費者問題，其重要性正在不斷地增加。隨著電子商務和網際網路的不斷發展，公眾對個人資訊的收集和使用是否恰當這一問題將可能給予更多的關注。

6.可用性

在網路環境中，可用性是保持公眾高度信任的另一要素。對於顧客來說，如果網路不可使用或不方便，那麼前面的幾個要素就毫無價值。網路用戶希望每天 24 小時、每週 7 天之中，隨時都可以對系統進行存取，因此系統的高可用性是必須的。與系統可用性相關的考慮包括能力、效能監控、重複和業務恢復。提供網路銀行服務之銀行和服務供應商必須確信他們在硬體和軟體方面具有足夠之能力，能夠始

終如一地提供高品質的服務。

另外，效能監控技巧為管理部門提供了諸如通信量、交易期間、顧客等待服務的時間等資訊。管理部門應該定期地對能力、停機和效能進行監控，以確保網路銀行系統的高可用性。

參考文獻

1. OCC - Office of the Comptroller of the Currency, Administrator of National Banks, http://www.occ.treas.gov/
2. OCC Electronic Banking, http://www.occ.treas.gov/netbank/netbank.htm
3. Internet Banking Comptroller's Handbook，Comptroller of the Currency Administrator of National Banks
4. Legal Information Institute, Cornell Law School, Title 12—Banks and Banking, http://www.law.cornell.edu/uscode/html/uscode12

貳、香港金融管理局對網路銀行之監理制度

香港的銀行機構數目名列於全球之前茅，其中 71 家為全球 100 家最大型的銀行。在 2005 年 9 月底認可機構，有 131 家持牌銀行、36 家有限制牌照銀行及 35 家接受存款公司，共 202 機構合共經營 1,311 家分行，組成龐大的金融服務網。

香港金融管理局(以下簡稱金管局)，對於電子銀行監理的目的及用意，特別強調在於建立及維持銀行安全與穩健成長的環境，以促進電子銀行業務能夠在香港有良好的發展，而不會受到阻礙。

為此，該局在電子銀行監理方面，在原本「銀行業條例」法規及參考 BASEL 風險控管原則之下，依序訂有「風險為本監管制度」強調公司治理、董事會及高階管理階層應負最終責任，並持續推行了「風險管理的一般措施」、「電子銀行的監管」、「科技風險管理的一般原則」及「持續業務運作規劃」等監管制度、措施、原則、指引、通告或建議手冊等，並預期銀行會達到的最低標準，以及應達到的最佳經營手法。

有監管制度但可彈性運用

香港金融管理局對電子銀行所訂定各監管制度或原則等係以建議

文件形式發出的非法定指引，做為電子銀行業務之指引，本身保持中立角色，使認可機構(銀行)能靈活選擇及運用其電子銀行服務，以配合的科技不斷的演進。

該局認為就電子銀行訂下絕對的風險管理要求或一成不變的科技標準，是不切實際及會帶來反效果。大原則在於認可機構應實施「適合」的風險管理措施，即能配合個別認可機構許可的交易類型及金額所涉及的風險、採用的電子傳遞通路及風險管理系統。

由該局相關法規或手冊中，我們可初步得知香港金融管理局對電子銀行的監理態度，具有「寬鬆中帶緊」的監理功效。「帶緊」的是強調董事會及高階管理階層應負最終的責任，並應制定有效的風險管理架構及執行檢討制度，其後至少每年進行一次正式風險評估(可委託外部專家)；另銀行須在有條件下，對客戶直接損失的負責等等。「寬鬆」的是以原則性建議規範或商討方式，協助銀行辦理電子銀行業務，如推出電子銀行服務前無須取得正式批准，但應事先與金管局商討其計劃、准予申設虛擬銀行或准許儲值卡跨業等等。以彈性及務實的態度面對多元多變電子商務環境需求，而可機動調整其監理方式，且不至於因受到法規限制而阻礙銀行發展電子銀行業務。特將其重點說明如下：

一、電子銀行及科技風險

該局所擬訂電子銀行監管政策與指引，主要在於強調協助銀行業制定政策與指引、推廣客戶的保障與教育及安全意識、持續監察與審查及在國際層面的合作等四大目標。

該局自 1997 年起已向認可機構發出一系列通告，表明對電子銀行服務的監管方式，並就有關的風險管理提供建議予認可機構參考。儘管認可機構在推出電子銀行服務前無須取得金管局的正式批准，但仍要事先與金管局商討有關計劃及其風險管理措施。

該局認為儘管資訊的絕對安全並不存在，但期望銀行應採取切合服務需要的資訊安全措施，亦即是按照交易的類別與金額涉及的風險、使用的電子傳送通路，以及機構的風險管理系統而制定相對應的安全措施，金管局發出「電子銀行服務保安風險管理的建議文件」，向認可機構之高級管理階層進一步提供資訊安全的建議。

此外，金管局要求認可機構委託專家對電子銀行服務的資訊安全措施進行定期獨立評估，並於推出服務前先由可信賴的獨立專家進行這類評估，其後最少每年再進行一次，或當有關服務的風險評估出現重大改變或安全系統不能防禦入侵時再作評估。為此，金管局發出「電子銀行交易服務保安事宜獨立評估的建議文件」。

虛擬銀行的認可資格

虛擬銀行是指主要透過網路或其他電子傳送道路提供銀行服務的機構，但不包括現有實體銀行所提供的網路服務。金管局於 2002 年 9 月發出「認可指引」，向有意根據「銀行業條例」申請認可資格的機構提供指引。該指引其中一章為「虛擬銀行的認可」，列出金管局決定是否給予虛擬銀行申請人認可資格時所考慮的原則。只要有關機構能符合適用於傳統銀行的認可標準，金管局不會拒絕認可在香港開設虛擬銀行服務的申請人。

網路上的存款廣告

規定任何有關存放在香港以外地區的存款廣告、邀請及文件（廣告材料）均須遵守資料披露規定。有關的宣傳資料須載明警告，表明接受存款機構本身並未根據「銀行業條例」獲得認可，因此不受金管局監管。該廣告亦須載明有關該境外機構及存款計劃的若干具體資料。此舉是要確保有意在該機構存款的公眾人士可獲知有關事實，以便自行判斷是否將存款存入該機構。並發佈「藉互聯網發出徵求存款的廣告材料的規管指引」。

持續業務應變計劃

金管局為處理大型災難事故及銀行應變能力，曾先後發出有關持續業務應變計劃的通告及「持續業務應變計劃建議文件」，供銀行作為參考。並繼續修訂有關指引，以提出更全面的電子銀行及科技風險管理的建議。

客戶的保障與教育及安全意識

電子銀行與其他銀行服務一樣，應遵守「銀行營運守則」，應有足夠的透明度，讓客戶更能了解他們對有關服務可以有何合理期望，以及他們為保障有關服務的資訊安全而應採取的防範措施。並應於服務章則與條款內清楚列明認可機構與客戶各自的權利與義務。有關章則與條款對認可機構與客戶都必須公平及適當。認可機構必須提醒客戶他們在使用電子銀行服務時有責任維護資訊安全，以及他們因未能履行此責任而可能會承擔的後果。此外，章則與條款應特別指出認可機構與客戶之間會如何分擔因安全事故、系統故障或人為錯誤而引致的損失。就此而言，金管局認為除非客戶作出欺詐或嚴重疏忽行為，如未能妥善保管電子銀行服務的設備或密碼，否則客戶無須對因經其帳戶進行的任何未授權交易引致而蒙受的直接損失負責。認可機構應通知客戶向認可機構通報或投訴安全事故的方法，以便能及早察覺、報告、回應及解決潛在安全事故或投訴。

此外，金管局已與業內公會、資訊科技署、香港警務處的科技罪案組及其他有關組織建立聯繫，以提高公眾對電子銀行安全的意識、為銀行業建立共同的事故通報及回應機制，並增強公眾對電子銀行的信心。

持續監察及審查

金管局除了發出有關電子銀行的監管政策與指引外，在 2002 年推行以認可機構的電子銀行、科技風險管理及持續業務應變計劃為重點的現場審查程序。金管局在制定這個程序時曾參考先進地區銀行監管機構的類似程序，以及巴塞爾銀行監管委員會有關電子銀行風險管理的建議，並按照該程序對香港的主要銀行進行有關的現場審查。為了更有效決定監管工作的優先次序，金管局建立了銀行科技風險的資料檔案，同時亦推行認可機構的科技管控自我評估程序。

在國際層面的合作

在國際層面的合作方面，金管局參與了巴塞爾銀行監管委員會之下的電子銀行小組。該小組研究電子銀行涉及的監管問題，包括電子銀行服務的跨境問題及風險管理原則。金管局亦就監管電子銀行業務積極與亞太區及中國內地的銀行監管機構交流經驗。

強調公司治理方面

金管局預期銀行在公司治理方面應遵守的最低標準。就銀行業而言，公司治理是關於個別銀行的董事會及高階管理階層如何指導及管理銀行的業務及事務。此外，公司治理也提供一套制度，讓銀行確立目標、制定達成目標的策略，以及監察銀行的表現。

企業經營環境快速變化，增加了銀行業所面對的風險。這些變化包括全球化趨勢、金融市場開放、金融產品推陳出新，以及科技發展。因此，金管局應確保銀行維持有效的公司治理。

風險管理程序董事會應確保銀行已制定適當的政策、程序及管控制度，以管理銀行承受的各類風險，包括銀行局就風險為本監管模式所指明的風險。

金管局每年都與各銀行全體董事會成員會面，原因是與銀行董事會溝通的正式及直接的管道是非常重要的。並評估風險管理及內部管控的品質，並表達監管方面的主要關注事項。

二、風險管理的一般措施

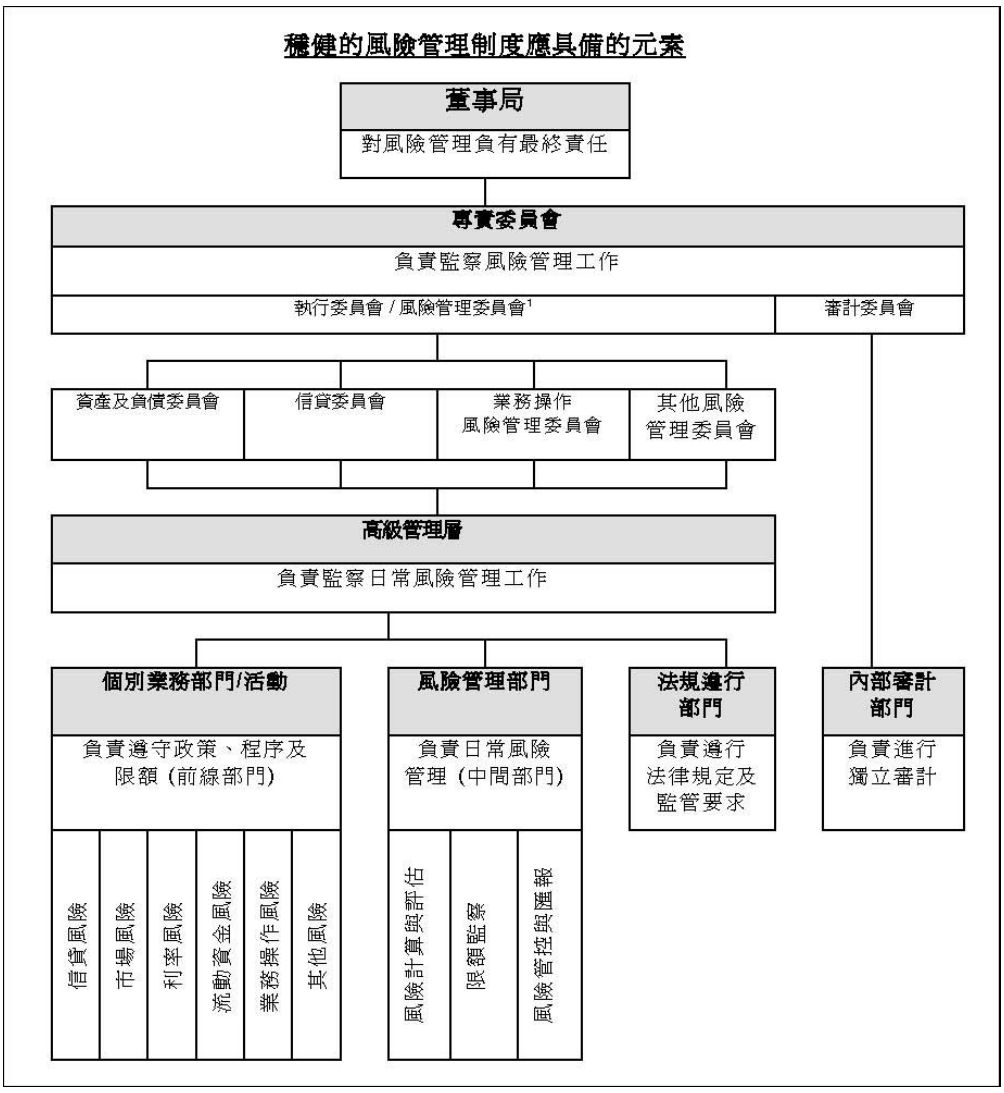
該局提供「風險管理的一般措施手冊指引」，預期銀行的風險管理

制度應具備的一般措施。根據巴塞爾委員會的「有效監管銀行業的主要原則」第 8 至 13 項原則，銀行業監管機構須要確定銀行備有全面的風險管理程序，以鑑別、計算、監察及管控貸款風險（包括過度集中及國家風險）、市場風險及其他主要風險，例如流動資金風險、利率風險、業務操作風險及信譽風險。

設立有效的風險管理制度

銀行建立穩健風險管理制度及運作架構，成立風險管理委員會以利風險管理有確實被執行之需要，其具備的元素及架構如下圖：

高階管理階層應負責根據董事會所定的風險管理策略，制定詳細的政策、程序及限額，以管理銀行的業務活動所引起的不同範疇的風險。高階管理階層亦有責任設計及實施經董事會核准的風險管理制度。有關制度應在整個機構實施，而各層面的職員都應了解其在風險管理方面的責任。風險管理政策與程序應能配合不斷轉變的經營環境。風險管理程序及有關的內部管控措施應定期作出審查及測試。



註：在說明部分情況下，成立風險管理委員會是專門為了承擔總管各個範疇的風險管理工作。董事會負有最終責任，了解銀行所承擔的風險及確保妥善管理有關風險。

網路銀行的監管

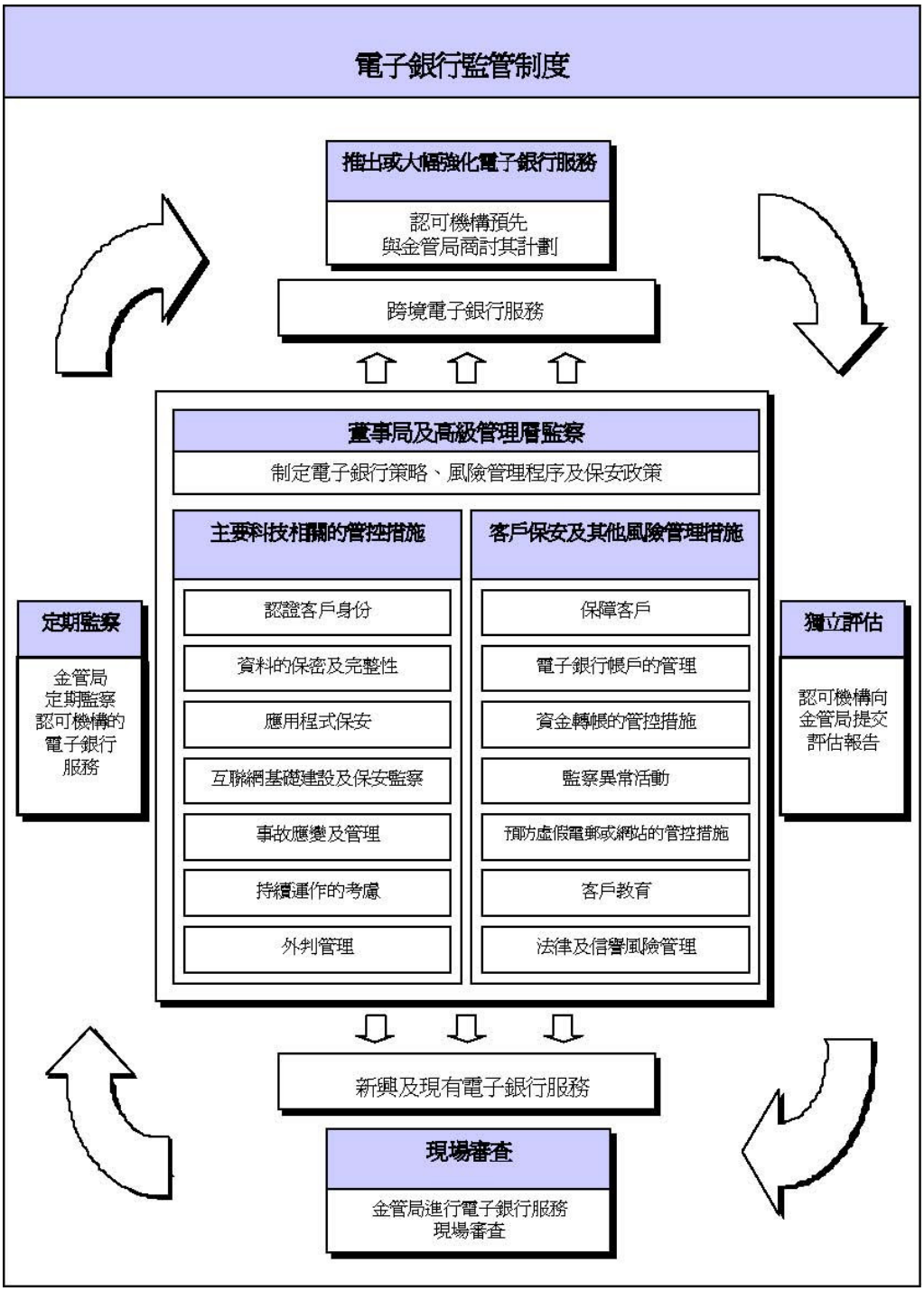
列載金管局對銀行的網路銀行服務的監管模式，以及向銀行提供有關網路銀行風險管理一般原則的指引。金管局監管目的是要建立及維持安全與穩健的環境，以促進網路銀行的發展，但同時又不會構成

阻礙。

銀行應實施「適合」的風險管理措施，即能配合個別銀行許可的交易類型及金額所涉及的風險、採用的電子傳遞通路及風險管理系統。

該網路銀行監管制度依巴塞爾銀行監管委員會於 2003 年 7 月發出的「電子銀行風險管理原則」及 2003 年 7 月發出的「跨境網路銀行業務的管理與監管」有關網路銀行的文件而訂定。

有關電子銀行監管制度及運作架構如下圖：


電子銀行監管制度
推出或大幅強化電子銀行服務
認可機構預先
與金管局商討其計劃
跨境電子銀行服務
董事局及高級管理層監察
制定電子銀行策略、風險管理程序及保安政策
主要科技相關的管控措施
認證客戶身份
資料的保密及完整性
應用程式保安
互聯網基礎建設及保安監察
事故應變及管理
持續運作的考慮
外判管理
客戶保安及其他風險管理措施
保障客戶
電子銀行帳戶的管理
資金轉帳的管控措施
監察異常活動
預防虛假電郵或網站的管控措施
客戶教育
法律及信譽風險管理
定期監察
金管局
定期監察
認可機構的
電子銀行
服務
獨立評估
認可機構向
金管局提交
評估報告
新興及現有電子銀行服務
現場審查
金管局進行電子銀行服務
現場審查

獨立評估

銀行在推出新的網路銀行服務或大幅強化現有服務前，其高階管理階層須委任可靠的獨立專家（評估人員）進行獨立評估，評估報告應提交金管局作為參考。銀行應於其後至少每年進行一次正式風險評估，以確定是否需要再進行任何獨立評估，如有需要，則亦要確定獨立評估的次數及範疇。

跨境網路銀行服務的監管

一般而言，本地註冊銀行如計劃在其沒有實體辦事處的另一個地區推出跨境網路銀行服務，應預先與金管局商討。銀行須要令主管機關相信其已進行充份的嚴格調查（例如銀行已諮詢適當的當地監管機構），以確定有關的海外地區的法令、規章及監管標準的適用情況。此外，銀行應具備有效及持續的風險管理程序，以管理其跨境網路銀行業務的風險。

風險管理程序

董事會或其指定委員會應確保網路銀行風險管理是銀行的風險管理制度不可分割的部分。因此，銀行應按其銀行服務的需要實施及推行適當的風險管理政策及程序，以及其風險管理制度規定的相關內部管控措施及審核程序。

制定資訊安全政策

高階管理階層應確保銀行定期制定及更新與其網路銀行服務有關的全面資訊安全政策。有關政策應由高階管理階層批准及發出。政策文件應明列有關的政策、程序及措施，以保障銀行的業務運作免受安全及入侵事故影響。政策文件亦應界定個別人員的責任，以及說明執行方法及針對不遵守有關政策、程序及措施情況下的紀律處分。除外，高階管理階層亦應傳達這項訊息，從而在機構內培養安全文化。

事故應變及管理

銀行應備有正式的事故應變及管理程序，以便即時舉報及處理懷疑或證實的安全事故、騙案或網路銀行服務中斷的情況（包括在辦公時間以內或以外）。並應設立事故應變小組（可由來自科技風險管理部門或其他有關部門的人員組成），以按照上述程序管理事故及作出回應。

持續運作的考慮

銀行應持續提供網路銀行服務，其系統並有合理的回應時間，符合機構的章則及條款以及預計的客戶期望。

銀行應制定每項關鍵網路銀行服務的表現準則，並應根據有關準則評估服務水準。銀行應採取適當措施，確保網路銀行系統及與內部

系統的界面能應付網路銀行的預計交易量及日後的增長。

委外管理

由於網際網路的技術相當複雜，加上其全球化性質，部分銀行可能會倚賴銀行集團內的另一個單位或外聘服務供應商，操作及維持與其網路銀行服務有關的資訊科技系統或業務程序。在這些情況下，銀行應明訂有關科技委外管理的管控措施；及定期進行嚴格調查，評估外聘服務供應商的財政穩健情況及能力，以維持適當的安全水準及趕上快速轉變的科技。

保障客戶

銀行必須在其章則與條款內清楚列明機構與客戶之間各自的權利與義務。有關的章則與條款對機構與客戶雙方都應該公正中肯。除非客戶作出欺詐或嚴重疏忽行為，否則客戶無須對因經其帳戶進行的任何未經授權交易引致而蒙受的直接損失負責。

網路銀行帳戶的管理

若銀行容許其現有客戶在網上開設網路銀行帳戶，機構便應確保備有足夠管控措施，以減低不法之徒在真正客戶不知情的情況下，開設網路銀行帳戶的風險。

監察異常活動

銀行應具備有效的監察機制，以即時察覺可疑的網上交易及異常活動。若出現可疑網上資金轉帳及異常活動，銀行的監察機制應迅速通知其監察人員。

法律及信譽風險管理

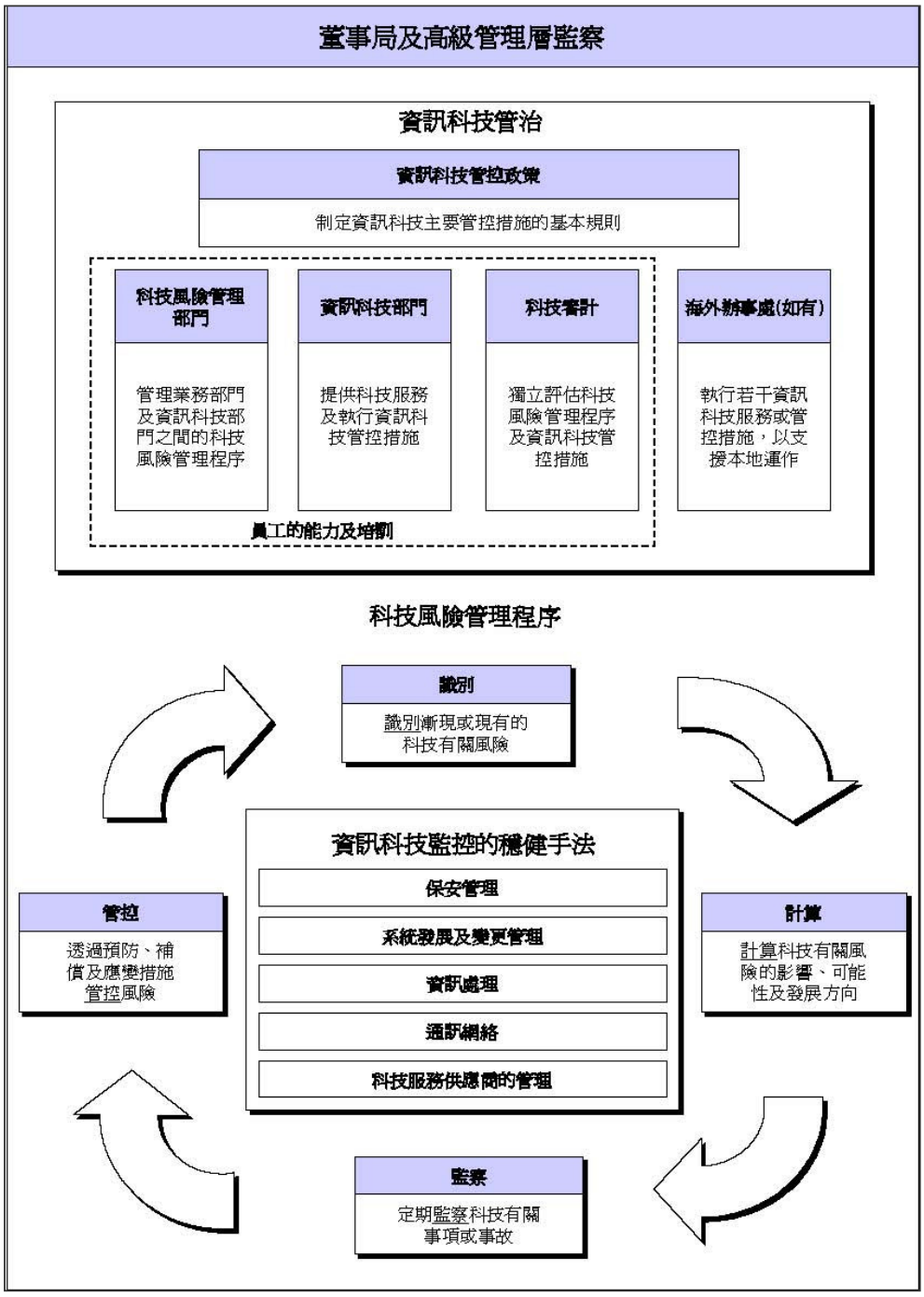
銀行應適當地評估其網路銀行服務涉及的法律及信譽風險。若網路銀行服務是提供予另一個地區或可能被視作以另一個地區為目標，這個評估便特別重要。

三、科技風險管理的一般原則

本指引文件目的在於金管局要求銀行的科技風險管理應考慮的一般原則。由於銀行愈來愈依賴利用科技來提供銀行服務，銀行使用科技資源不當可能會構成重大風險。

董事會負有最終責任，了解銀行所承擔的風險及確保妥善管理有關風險；高階管理階層則有責任設計及實施經董事會或其指定委員會核准的風險管理制度。為達到這個目的，高階管理階層應制定有效的

科技風險管理架構。一般而言，這個架構包含資訊科技治理、持續科技風險管理程序及就資訊科技管控執行穩健的實務手法。以下概覽科技風險管理的一種穩健架構：



資訊科技管控政策

若要在整個銀行內，就資訊科技管控的穩健手法維持貫徹標準，便須得到董事會及高階管理階層的明確指示及承擔。

高階管理階層應確保查核是否遵守資訊科技管控政策的程序，以及要求核准豁免遵守資訊科技管控政策的程序。高階管理階層亦應訂定未依從這些程序會帶來的後果。整體而言，個別業務部門及資訊科技部門應在科技風險管理部門的協助下，負責確保本身遵守資訊科技管控政策及要求核准豁免遵守這些政策的程序。

資訊科技部門的監察及組織架構

高階管理階層應為資訊科技部門制定有效的組織架構，以便為業務部門提供科技服務及日常的科技支援。銀行應以明文記錄清晰的資訊科技組織架構及個別資訊科技部門的職責，並由高階管理階層核准。

銀行宜設立資訊科技規劃或督導委員會，負責監察銀行本身是否有效利用資訊科技資源，以支持業務策略。

科技稽核

部分銀行的內部稽核部門可能較難累積內部的科技稽核專業水準。在這些情況下，科技稽核支援工作可由外聘專家或同一銀行集團

其他辦事處的內部科技稽核人員提供支援。

員工的能力及培訓

鑑於科技發展迅速，高階管理職應確保資訊科技、科技風險管理及內部科技稽核部門的員工均具備適當能力，並持續符合所需的專業及經驗水準。此外，確保員工編制足以應付現有及預期的工作量，並能合理地應付員工流失亦很重要。銀行可鼓勵員工（如負責安全管理、科技風險管理及科技稽核的員工）考取有關的專業資格，如有需要更應作出適當配合。

科技委外的管理

科技服務供應商應具備足夠資源及專業知識，以遵守銀行資訊科技管控政策的實質內容。委外協議應清楚載明科技服務供應商的表現標準及其他責任，以及軟體與硬體擁有權的事項等。除定期監察外，銀行亦應進行年度評估，以確保關鍵的科技服務供應商有足夠的資訊科技管控環境。

持續業務運作規劃

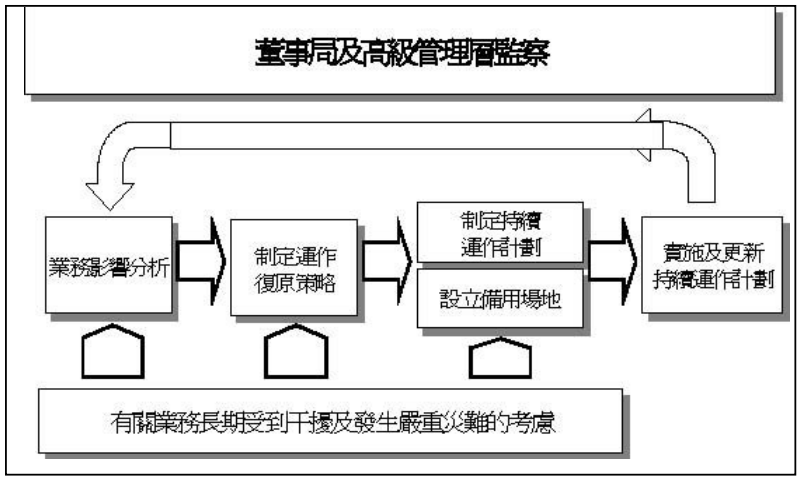
目的說明金管局對持續業務運作規劃的監管方式，以及主管機關期望銀行在持續業務運作規劃時會考慮的穩健做法。在於事先進行的計劃及準備，以識別因緊急或災難事故引起的潛在損失的影響。制定

及推行可行的運作復原策略。制定運作復原計劃，以確保在該等情況下銀行仍能繼續提供服務以及實施全面的測試及更新計劃。

董事會及高階管理階層監察

銀行的董事會及高階管理階層對持續業務運作規劃及持續運作計劃的成效負有最終的責任。高階管理階層應訂立持續業務運作規劃的政策、標準及程序，並應得到董事會的贊同。高階管理階層應確保各級員工都對持續業務運作規劃採取認真及嚴謹的態度，並要為實施有關計劃投入足夠資源。

持續業務運作規劃建議採納的程序包含以下幾個主要項目（如下圖所示）：



高階管理階層應清楚確立機構內負責管理整個持續業務運作規劃過程的部門。

四、 香港多用途儲值卡的監管

香港「銀行業條例」賦予金融管理專員監管多用途儲值卡發行的權力。監管制度的目的，是確保多用途儲值卡計劃及發卡人符合穩健標準。

該條例規定：

- 持牌銀行被視為已獲准發行或促進發行多用途儲值卡；
- 如屬特別目的公司，而其主要業務是或將會是發行或促進發行多用途儲值卡，則可申請認可為接受存款公司，以便獲批准經營該主要業務；
- 金融管理專員可宣布某儲值卡或某類儲值卡就本條例而言，不屬於「多用途儲值卡」，以豁免這些儲值卡需要符合批准條件；
- 發行單一用途儲值卡無須根據該條例取得批准。

在制定這套監管制度時，金融管理專員力求在維持支付系統（以至整個金融體系）的穩定避免窒礙。

為了達到上述目標，並且鑑於只有持牌銀行才可直接使用香港的支付系統，因此條例規定只有持牌銀行才可發行用途不受限制，可用

以購買任何貨品和服務的多用途儲值卡。這類儲值卡具有「被廣泛接納的購買力」，因此與貨幣非常近似。另一方面，根據目標，非銀行發卡人亦應該有機會申請批准發行用途受到限制的多用途儲值卡。

香港金管局已發出「申請成為認可機構的指引」，說明金管局在行使該條例下有關認可多用途儲值卡計劃的權力時所依循的原則及標準。

金管局在監察零售支付系統運作的安全與效率時，一直鼓勵業界透過發出及遵守相關的實務守則，進行自我監管。八達通卡的系統營運商—八達通卡有限公司—已發出「多用途儲值卡營運實務守則」。該守則是自願發布的非法定守則，金管局認可該守則，並會不時檢討守則內容及監察遵行守則的情況。該守則透過列出多用途儲值卡發卡機構、系統供應商及收單機構在日常運作中應遵循的指導原則，以促進多用途儲值卡營運的安全及效率，從而提高公眾對多用途儲值卡營運的信心。

倘以八達通卡多用途儲值卡為境界，我國如擬在交通卡或企業儲值卡突破跨業限制問題，可能需調整現有相關法規之障礙或在有條件之下，准予非金融業發行多用途儲值卡。

參考文獻

1. http://www.info.gov.hk/hkma, The Hong Kong Monetary Authority (HKMA) 香港金融管理局網站

2. Basel Committee on Banking Supervision, Risk Management Principles for Electronic Banking, July 2003, Bank for International Settlements

3. 香港金融管理局所頒布的電子銀行相關監理法規或指引

   - 銀行業條例，1997 年第 4 號第 2 條修訂
   - SA-1 風險為本監管制度 11.10.2001
   - CG-1 本地註冊認可機構的企業管治 21.09.2001
   - IC-1 風險管理的一般措施 25.04.2003
   - TM-G-1 科技風險管理的一般原則 24.06.2003
   - TM-G-2 持續業務運作規劃 02.12.2002
   - TM-E-1 電子銀行的監管 17.02.2004
   - TM-E-2 在互聯網發出有關存款的廣告資料的規管 24.05.2002

參、我國電子銀行業務相關監理規範

一、國內電子銀行相關管理及作法

目前國內銀行界參考巴塞爾銀行監督委員會（Basel Committee on Banking Supervision, BCBS）電子銀行風險管理，已有訂定相關風險自律原則及資訊作業安控基準。並分為管理監督；外部資源和第三方的管理；體制、資料庫和運營上實行職責分離；在網路銀行業務體制、資料庫和運營上有經過授權的合適措施和控制系統；對所有電子交易明確的審計跟蹤系統；客戶身份和資料的真實有效性的證實；電子交易的不可撤銷性；高級的安全控制；保證交易、檔案、資訊的真實完整性；合適的資訊披露；保護顧客資訊的私密性；保證體制與服務的連續可用性；高效的針對意外事件的應急反應系統；監管者對網路銀行業務的管理結構、運營、內部控制和應急計劃的外部監管評估等項目皆有詳加說明，可供銀行資訊作業安控之參考。

另銀行公會訂定「金融機構辦理電子銀行業務安全控管作業基準」，為銀行線上系統或交易在設計或業務控管之原則，可供銀行實際執行相關安全之參考。

其次「保障消費者權益」方面，金融業在廣泛運用 ATM 自動櫃員機、銷售點端末機、電話交易、個人電腦銀行及網路銀行等電子資訊處理設備，處理銀行與客戶間支付交易，難免會發生各種交易糾紛，

目前完成「個人電腦銀行業務及網路銀行業務服務契約範本」，以資遵循。其特點大致為，金融業務包括查詢、授權轉帳、電子交易、一般通信及金融資訊服務等。當客戶與銀行間電子交易往來之一般性共通約定，就網路交易之特殊風險，明訂雙方責任分際，對網路駭客入侵所造成的損害，依民法危險負擔法理，由銀行負擔。

二、國內電子銀行業務相關法規

目前國內有關消費者保護、資料安全、資訊作業安控或電子銀行等風險管理，係由行政院、法院、財政部、金管會、消保會及公會組織等單位皆配合時空演變及需求，陸續有頒布相關的法令、準則、規範、辦法、要點或契約範本等，提供銀行業界之遵循或參考。

1. 電子簽章法 (http://www.moea.gov.tw/~meco/doc)
2. 電腦處理個人資料保護法 (http://www.cmvttc.gov.tw/law)
3. 金融機構電子銀行業務安全控管作業基準

   (銀行公會 2006/01/16 修訂版)
4. 行政院及所屬各機關資訊安全管理要點

   (http://www.rdec.gov.tw/lp.asp)
5. 行政院及所屬各機關資訊安全管理規範

(http://www.rdec.gov.tw/lp.asp)

6. 財政部及所屬機關機密資料維護準則

7. 銀行發行現金儲值卡許可及管理辦法(銀行公會)

8. 電子銀行（e-banking）十四項風險管理原則(金融研訓院)

9. 電子銀行風險管理自律規範(銀行公會金融業務電子化委員會資安小組九十三年九月編修版)

10.Basel II 銀行自有資本之計算與自有資本標準之國際通則：修正版架構 (金管會銀行局/銀行公會/台灣金融研訓院)

11.銀行間資金移轉帳務清算之金融資訊服務事業許可及管理辦法

12.個人電腦銀行業務及網路銀行業務定型化契約範本

—簡稱「網路銀行服務契約範本」(銀行公會)

13.網路交易定型化契約應記載及不得記載事項指導原則

(行政院消費者保護委員會 94.03.31)

14.銀行申請轉投資之資訊服務業屬金融相關事業之認定標準

15.金融機構作業委託他人處理應注意事項

16.公開發行公司內部控制實施要點

三、電子銀行業務相關處理辦法

各銀行為辦理電子銀行業務之需要，各別訂定內部相關業務處理手冊、安全控管作業要點及約定書等規範，以供作業辦理之準則。

- 電子金融業務處理手冊
- 企業網路銀行安全控管作業要點
- 電子銀行服務申請書及約定書（個人戶專用）
- 晶片金融卡服務申請書或服務約定書
- 企業財務管理系統及金融電子資料交換作業系統服務申請書及約定書
- 金融 XML 資金管理(自行憑證)業務申請書及約定書

四、金額受限以降低網路交易風險

國內銀行為配合實際作業環境的需求及防止詐騙集團，依交易安全等級，設定每日轉帳交易最高的限額，以降低網路交易的風險。各交易安全等級及轉帳限額彙編如下表。

<table>
<tr><td rowspan="8">個人轉帳限額</td><td rowspan="6">密碼方式</td><td rowspan="3">一般</td><td>固定密碼（SSL 機制）</td><td>限轉入已約定帳戶</td><td>每日累計最高金額為新台幣 300 萬元。</td></tr>
<tr><td rowspan="2">動態密碼（OTP機制）</td><td>轉入已約定帳戶</td><td>每日累計最高金額為新台幣 300 萬元。</td></tr>
<tr><td>轉入未約定帳戶</td><td>每日累計最高金額為新台幣 10 萬元。</td></tr>
<tr><td rowspan="3">大額（專案申請）</td><td>固定密碼（SSL 機制）</td><td>限轉入已約定帳戶</td><td>每日累計最高金額由客戶自訂，惟不得超過新台幣 2000 萬元。</td></tr>
<tr><td rowspan="2">動態密碼（OTP機制）</td><td>轉入已約定帳戶</td><td>每日累計最高金額由客戶自訂，惟不得超過新台幣 2000 萬元。</td></tr>
<tr><td>轉入未約定帳戶</td><td>每日累計最高金額由客戶自訂，惟不得超過新台幣 300 萬元。</td></tr>
<tr><td colspan="4">SSL、OTP 機制之轉帳限額合併計算。</td></tr>
<tr><td rowspan="2">電子憑證方式</td><td colspan="2" rowspan="2">NON-SET 機制</td><td>轉入已約定帳戶</td><td>客戶自訂</td></tr>
<tr><td>轉入未約定帳戶</td><td>客戶自訂</td></tr>
<tr><td rowspan="3">企業轉帳限額</td><td>密碼方式</td><td colspan="2">固定密碼（SSL 機制）</td><td>限轉入已約定帳戶</td><td>每日累計最高金額由客戶自訂，惟不得超過新台幣 2000 萬元。</td></tr>
<tr><td rowspan="2">電子憑證方式</td><td colspan="2" rowspan="2">FXML 機制</td><td>轉入已約定帳戶</td><td>客戶自訂</td></tr>
<tr><td>轉入未約定帳戶</td><td>客戶自訂</td></tr>
<tr><td colspan="6">累計金額之相關規定
1.存戶利用網路轉帳繳納各項公共事業費用、罰款、學雜費等款項，每筆金額在新台幣 10 萬元以下者，得免約定轉入帳戶。
2.存戶辦理綜合存款項下活期性存款轉存定期性存款、以存戶名義購買基金、繳納存戶華銀信用卡帳款等款項時，免申請即視為「已約定轉入帳戶」，其轉出金額應受本契約「轉入已約定帳戶」之最高金額限制，但稅費無最高金額限制。
3.存戶自香港分行存款帳戶辦理單筆轉帳交易者，限轉入已約定帳戶。
4.跨行轉帳每次金額不得超過新台幣 2000 萬元。</td></tr>
</table>

肆、國外電子銀行業務相關監理法規說明

一、美國通貨監理局(簡稱 OCC)相關法規說明

Comptroller of the Currency Administrator of National Banks

1. 美國個人資料保護法，以保護個人資訊之隱私。其相關法規包括:
   - 1974 Privacy Act
   - 1980 Privacy Protection Act
   - 1986 Electronic Communications Privacy Act (電子通訊隱私權法)
   - 1986 Computer Fraud and Abuse Act
   - 1987 Computer Security Act (電腦安全法)
   - 1988 Computer Matching and Privacy Protection Act
   - 1989 Computer Matching and Privacy Protection Amendments Act
   - 1990 Computer Matching and Privacy Protection Amendments Act
   - 1994 Computer Abuse Amendments Act
2. Law: Gramm–Leach–Bliley Act (USC 6801)
3. 10/12/2005　OCC Authentication in an Internet Banking Environment
4. 10/28/2003　" Check 21 Act " , Check Clearing for the 21st Century Act, Public Law 108–100
5. 02/05/2003　FFIEC Information Security Booklet: Information Security Guidance FFIEC Press Release

   (FFIEC：Federal Financial Institutions Examination Council)
6. 5/16/2002　OCC Issues Final Rule on Electronic Banking　Release

7. 05/15/2002 OCC Issues Risk Management Guidance for Banks that Use Foreign-Based Third-Party Service Providers Release 2002-43
8. 09/07/2001 Electronic Fund Transfer Act and Regulation E (EFTA)
9. 07/02/2001 OCC Issues Proposed Rule on Electronic Banking Release 2001-60
10. 05/03/2001 OCC Basel Committee Report Outlines Risk Management Principles for Electronic Banking Release 2001-42
11. 11/28/2000 Risk Management of Outsourcing Technology Advisory Letter 2000-12
12. 02/03/2000 OCC Proposes Rules to Implement Gramm-Leach-Bliley Act Privacy Provisions Release 2000-5
13. 10/14/99 OCC Issues Examination Handbook On Internet Banking Release 99-94
14. 05/06/99 OCC Issues Guidance on a National Bank Acting as a Certification Authority for Digital Signatures Release 99-42

二、香港金融管理局（簡稱金管局）相關法規說明

Hong Kong Monetary Authority (HKMA)

(一)、監理特色：

1. 強調促進電子銀行在香港的發展，但不會構成阻礙，並認為在科技方面保持中立，使銀行能靈活選擇及運用與其電子銀行服務配合的科技。就電子銀行定下絕對的風險管理要求或一成不變的科技標準，是不切實際及會帶來反效果。一般以建議文件形式發出的非法定指引。
2. 指明參考國際監管機構,特別是巴塞爾銀行監管委員會建議的監管模式及指引而編製。
3. 推出新的電子銀行服務前不須取得金管局的正式批准,但認可機構應事先與金管局商討其計劃。
4. 強調公司治理董事會應負有最終責任,及強調資訊科技治理高級管理層應制定有效的科技風險管理架構,並定期外聘專家評估及強調員工訓練及專業資格的取得。

(二)、香港電子銀行相關監理建議文件及法定指引

編號	標題	類別 1	狀況 2	發出日期
SA-1	風險為本監管制度	GN	F	11.10.01
CG-1	本地註冊認可機構的企業管治	SG	F	21.09.01
CG-2	委任經理的管控制度	SG	F	24.05.02
CG-3	行為守則	SG	F	21.06.02
IC-1	風險管理的一般措施	SG	F	25.04.03
TM-G-1	科技風險管理的一般原則	GN	F	24.06.03
TM-G-2	持續業務運作規劃	GN	F	02.12.02
TM-E-1	電子銀行的監管	GN	F	17.02.04
TM-E-2	在互聯網發出有關存款的廣告資料的規管	SG	F	24.05.02

更新日期：2006 年 2 月 14 日

附註：1 GN = 建議文件, SG =法定指引

2 F = 已完成

三、新加坡金融管理局相關法規說明

Monetary Authority of Singapore (MAS)

1. 消費者保護局及商務部：「電子簽章法」

(Electronic Signatures In Global And National Commerce Act)

June 2001

2. **MAS**：網路銀行風險管理原則

(Internet Banking Technology Risk Management Guidelines)

June 2003

3. **MAS**：新加坡Basel II建置之建議書

(Proposals for the Implementation of Basel II in Singapore)

August 2005

四、中國大陸：銀行業監督管理委員會相關法規說明(簡稱銀監會)

China Banking Regulatory Commission (CBRC)

(一)、「電子簽名法」2005.04.01 頒布

(二)、中國銀行業監督管理委員會(銀監會) 2006.03.01 施行

- 「電子銀行業務管理辦法」
- 電子銀行安全評估指引」

- 「電子銀行安全評估機構業務資格認定工作規程」
- 「銀監會行政許可實施程式規定」
- 「中資商業銀行行政許可事項實施辦法」
- 「非銀行金融機構行政許可事項實施辦法」

(三)、中國人民銀行

- 「網路銀行業務管理暫行辦法」2001 年制定頒布
- 「電子支付指引(第一號)」2005.10.26 公佈

參考文獻

1. http://www.occ.treas.gov

   美國通貨監理局(Comptroller of the Currency/Administrator of National Banks 簡稱 OCC)

2. http://www.info.gov.hk/

   香港金融管理局（Hong Kong Monetary Authority 簡稱 HKMA）

3. http://www.mas.gov.sg/

   新加坡金融管理局(Monetary Authority of Singapore 簡稱 MAS)

4. http://www.cbrc.gov.cn/

   大陸：中國銀行業監督管理委員會(China Banking Regulatory Commission 簡稱銀監會/CBRC)

第四章、銀行資訊作業風險控管實務

壹、資訊風險控管與委外監理

隨著技術的演進，創新的金融商品應用日益廣泛，各式新種網路銀行服務亦不斷推陳出新，如何使得金融機構強化電子銀行資訊安全與風險控管機制，並提升金融機構相關人員對於電子銀行安全管理與稽核專業能力，以提高資訊安全水準與消費者的信心為金融機構的首要課題。

我國銀行體系對於銀行之資訊安全治理程度相較於國外領先的銀行體系仍有許多可以進步的空間，如能採用一套完整且有效的資訊安全管理標準，將可提昇整體運作的效能。目前國際企業為資訊作業達到上述目標，陸續推行資訊風險控管之認證及技術管理例如 BS7799 與 Information Technical Service Management (ITSM)等，藉由系統化管理標準促使資訊安全管理更趨於完善。銀行如能取得此類資訊安全管理認證，不僅可以強化整體資訊風險的控管機制，同時也是對客戶電子銀行交易安全保證的決心。

此外，資訊委外的趨勢漸漸成型，委外的比重日益增多，因此委外管理亦是風險控管中重要的一環。委外管理制度包括訂定必要的職責、角色、目標和控制方法，以因應未來的變化，並管理委外服務的

推動、維護、績效、成本與控制。這是企業組織和服務供應商必須主動採取的一種流程，才能以共同的、一貫的和有效的作法來安排委外事務及監理。

貳、銀行資訊風險科技管理體系

一、 BS7799 資安管理體系

BS7799 認證為由英國標準協會（BSI）制定之資訊安全管理系統（Information Security Management System，簡稱 ISMS），作為企業或銀行建置資訊安全體系之管理標準，係運用一套有系統之方法，對敏感或機密資訊資產進行管理，以維護資訊安全。

國內銀行業為確保資訊作業及電子交易安全，特於 2004 年 6 月 21 日成立金融業務電子化委員會資安小組，作為政府主管機關與會員銀行之間、會員銀行相互之間、以及會員銀行與民眾之間的橋樑，負責執行資訊作業安全管理規劃與維護等事項，目前除已訂定「金融機構電子銀行業務安全控管作業基準」外，也積極推動 BS7799 認證。

(一)、金融業及相關服務之資訊安全管理系統標準 ：

(1) ISO 17799-1:2000／BS 7799-1:2002 資訊安全管理作業要點

Code of practice for information security management－分為 10 章節，共有 36 個控制目標及 127 個控制措施。

(2) BS7799-2:2002 資訊安全管理系統要求

Specification for information security management systems

(3) ISO/TR13569 :1997 銀行及相關金融服務業－資訊安全指引

Banking and related financial services – Information security guidelines（該指引，由 ISO 技術委員會「ISO/TC68 銀行、債券及他項金融服務」及下屬委員會「SC2 資訊安全防護管理及一般銀行運作」編製而成）。

台灣的國家標準 CNS 17799、CNS 17800，就是參考 BS7799 的 Part 1 和 Part 2 且加以中文化。目前資安管理在國際趨勢上，以 BS7799 為主流的管理系統標準，亞太地區由於起步較晚，所以每年增加的驗證張數最多，而金融業為強化資訊管理及確保整體作業安全爭取導入意願較高。

據調查，無論國內或全球，一百件安全事件中，第一名是病毒之外，人為的事件（不當存取控制等）就佔了三成，駭客等問題其實只有個位數百分比，而 BS7799 資安管理導入可將人為的因素減到最低。

目前全球獲得 BS 7799 驗證的企業組織約有四百多家，在台灣，目前獲得 BS 7799 的單位共有十餘家，分別是：國家資通安全會報技術服務中心、宏瞻科技、立駭科技（SOC）、ING 安泰人壽、建華銀行、財金中心、宏泰人壽、宏碁（eDC）、檔案管理局、台灣證券交易所以及台灣網路資訊中心（TWNIC）等。主要是在金融、銀行、壽險等產業，因為金融業有明顯而迫切的需求，並且金融事件直接影響企業聲譽與經營，因此導入意願強烈。金融業則著重在風險管理之要求，資訊安全控管的檢視及規劃有其需求。

由於金融活動相關之資訊犯罪案例及手法不斷增加翻新。而金融服務產業與國家安全、發展及社會安定息息相關，與人民生活更是密不可分。為保護資訊相關資產，確保營運持續，金融機構及其高層主管負有實施有效控制資訊安全之系統的責任。而絕大部份造成資訊安全事件的原因都不是專業技術的層面，而是在管理面上出現的漏洞所導致。有鑑於此，我們必需有一套能在組織中展開的資訊安全管理機制，

藉由組織內人員的知識及警覺來形成資訊安全的防護體系，使有心人士不易得逞，適度提高犯罪的成本或難度。

目前電子金融交易資安機制如：

(1). SSL（Secure Socket Layer）：對交易中的資訊進行加密及認證，以防止封包竊聽。

(2). SET（Secure Electronic Transaction）：處理有關否認性、認證、授權、以及確認以 MASTER 及 VISA Card 等銀行信用卡付款的問題。惟因作業較繁瑣使用者接受度較低，目前國內認證公司有意停止發放 SET 憑證。

(3). 金鑰管理系統基礎建設(PKI)：金鑰管理系統提供一個安全可靠的環境以進行電子交易，其主要組成部分包括金鑰密碼保護、憑證的管理和提供密碼服務的外部供應商。

(二)、國內銀行業推動 BS7799 現況

銀行公會在這方面，除了已參照 BS7799 訂定金融機構資訊安全基準外，並鼓勵各銀行取得資安驗證，也不斷地與會員分享資安經驗，且不斷加強單位內部的資安意識，以下分別說明：

1. 取得 BS7799 提升銀行公信力

在 BS7799 導入過程必須經過驗證的程序，由公證的第三者來評斷單位內部執行的過程是否符合要求，銀行公會的立場，為提升銀行在資訊安全方面的公信力及讓民眾安心，鼓勵銀行取得驗證。

因為銀行是以對客戶的信用及安全服務，維持永續的經營，其為便民的公器，所以特別需要大眾的認同，而驗證目的是在取得一般公眾的信任，最重要的是將資安工作落實。

2. 教育每個人使其了解在資安中扮演的角色

由於金融界本身對安全問題就很重視，所以從備援中心、災害復原、演練、亂碼機制、安全載具、委外延伸都已考量到，但整體對資訊安全管理之意識是較微弱的一環，透過不斷地教育訓練使用者，喚起他們的資安意識。

3. 金融機構資訊系統安全基準供各單位參考

銀行公會的金融機構資訊系統安全基準，從政策面著手做到準則，至實際的處理流程，與電腦工具結合，融合巴塞爾條約中的電子銀行風險管理之原則與 BS7799 之做法，方便內控人員及稽核人員執行。

4. 以案例分享提高警覺性

銀行公會舉辦的資安會議，最常討論的內容即是案例檢討，最近銀行單位推動晶片金融卡，就會將近期發生的案例與會員分享，提醒各行庫注意並提高警覺性。

二、資訊技術服務管理機制—ITSM

企業為確保資訊作業品質及穩定，以「資訊技術服務管理」（IT Service Management, ITSM）及「資訊技術服務規範」(Information Technical Infrastructure Library, ITIL）為架構，建構企業資訊整體服務或運作之機制，目的在於利用流程管理將現有資訊相關資源或服務做到最佳化，俾發揮投資或管理最大效能。

銀行導入ITSM可以達到降低成本、增加生產力、提升服務品質的目標，並使IT部門與其客戶間能有更好的關係。根據IDC機構進行統計的結果，企業導入ITIL流程後，平均可讓企業IT人員生產力提昇53%、效率提昇26%，資訊系統Downtime縮減31%，整體ROI更高達1296%，成效相當顯著，因此目前許多著名的跨國公司如IBM、HP、Microsoft、P&G、HSBC、CA等，都是ITIL的積極實踐者。

另根據MetaGroup 的預測，2007年以前美國將有約40%的企業會導入ITSM，而企業是否導也將被視為是檢視供應商、委外服務承包商是否具備投標資格的關鍵指標，甚至部分政府部門規定：IT相關人員如果沒有ITSM Certificate則不予聘用！因此ITSM認證對歐美的專業IT人員而言，已成為不可不具備的認證。目前台灣市場尚處於起步階段。

ITSM各種服務管理的目標、範圍及主要的活動：

- 服務櫃檯 (Service Desk)
- 意外管理 (Incident Management)
- 問題管理 (Problem Management)
- 組態管理 (Configuration Management)
- 異動管理 (Change Management)
- 上線管理 (Release Management)
- 服務層管理 (Service Level Management)
- IT服務連續管理 (IT Service Continuity Management)
- IT服務的財務管理 (Financial Management for IT Services)
- 可用性管理 (Availability Management)
- 容量管理 (Capacity Management)
- 安全管理 (Security Management)

總之，藉由導入嚴謹管理的機制，可將日常繁雜的資訊作業，以標準化及系統化方式納入管理，自然出錯或發生弊端的機率就會減少。

參、金融資訊委外及風險管理之探討

一、資訊委外之發展與策略

根據 Gartner 的統計報導，2008 年全球資訊服務市場規模預計可達 7,550 億美元，全球資訊委外服務將占整體市場的 41%，且其中硬體維護等委外比例逐步降低，代之而起的是商業流程委外(BPO)、資訊科技委外以及系統開發與整合委外等。

資訊作業委外之演變

銀行為確保投資效能及降低成本，並配合資訊產業快速變遷需求，委外模式已逐漸改變由硬體維護委外→系統開發委外→商業流程營運外包(BPO)→知識處理外包(KPO)。而**委外地點**也由公司內部→延伸到公司外部→國內較低成本區→境外低成本區。而委外**監控模式**與對廠商要求也更加嚴謹，由系統品質要求→委外公司安全檢查→委外公司流程或製程之監理。而**委外供應商**擔任角色，除了提供更好服務

品質(CMMI)外，也要提供創新的服務，與客戶的關係轉為策略聯盟的伙伴。

資訊服務海外工作委外模式（Offshore Outsoucing）

資訊服務海外工作委外模式在印度創造成功案例後，開始成為全球專業分工的應用典範，其在軟體製程開發或專案服務的執行上，需有共同的標準，以使雙方在流程上合作無間。由於軟體能力成熟度整合模式(CMM/CMMI)旨在改善軟體發展機構的內部管理流程，建立一套工程化的標準指引，讓個人和企業在軟體開發上能有改進的依據，並著重架構的指引，隨著整體資訊委外服務中 Offshore 模式的發展，CMM/CMMI 逐漸成為主要的評鑑指標。為爭取資訊委外市場大餅，全球導入 CMM/CMMI 制度者陸續增加。先就全球 Offshore 的發展現況與趨勢說明，並分析 CMM/CMMI 應用發展的現況。

Offshore 模式發展可以概分為三大階段，分別為醞釀期、擴張期、整合期，自 1998 年至 Y2K 時期屬於醞釀期，人力與成本節省之考量帶來 Offshore 模式的發展機會；2002 年印度成功的軟體代工使 Offshore 進入擴張期；目前處於整合期初期，全球資訊服務產業分工的商業模式已建立，未來將繼續朝向跨國性分工合作與整併同類業者的方向發展，其發展的主要驅動力如下所述。

Offshore 模式帶來的效益主要有四大項，分別為降低成本、增加生產力、縮短產品上市的時間、提高品質。其中，根據 NASSCOM 調查機構指出，降低成本是 Offshore 模式最顯著的效益，以企業營運總成本來看，Offshore 模式可以減少 50%至 90%的人力成本，即使增加額外的管理支出，最終仍可降低企業 30%至 70%的營運成本。先進國家人力薪資成本的高漲，帶動 Offshore 模式起飛，以各國人力的薪資水準來看，美國的薪資成本是印度的 10 倍之多。

以各產業利用 Offshore 模式可以降低的成本來看，發現以保險業最多，達 15%，其次為銀行業，約有 12%，人力需求越高的產業，資訊委外可節省成本越高。專業分工可提高產品品質水準，為促使 Offshore 模式發展的另一驅動因素，根據 PWCC 公司於 2003 年針對 Offshore 需求端所作調查中，認為透過資訊委外可提高品質程度者高達 68%。降低成本且能提高品質的雙重效益造成 Offshore 市場快速成長。

以全球 IT 人力需求來看，北美需求程度最高，達 55.4 萬人，歐洲次之，由於 IT 人力的成本過高，企業開始在人力成本較低的區域設置分公司，或將部分業務委外至人力成本低的區域，目前印度仍為提供 IT 人力最多的地區，但以 2001 至 2005 年全球 IT 人力需求平均複合成

長率達 65%來看，印度人力供給平均複合成長率僅達 11%，未來仍供不應求，因此大陸、以色列及俄羅斯各地區正積極增加 IT 人力，搶進 Offshore 市場。

Offshore 市場處於高度成長期，全球各地委外現象熱況不減。在美國排名財富雜誌前 100 大的企業如 HSCB、MICROSOFT、IBM 等分別於印度建立發展中心；西歐地區企業如德意志銀行、霸菱則以地緣考量逐漸將資訊委外至東歐地區，印度的資訊委外服務產業領導者為應付快速成長的需求，也開始於大陸建立支援服務中心，如 Wipro。

以 Offshore 主要市場美國來看，其 Offshore 的支出自 2000 年至 2005 年複合年平均成長率達 26.4%。而 Offshore 佔 IT 費用的比例亦逐年升高，至 2005 年達 5.3%，根據 Foresster 預估，第二大 Offshore 市場西歐，至 2005 年亦將有 26 百萬美元的市場規模。

早期 Offshore 模式嶄露頭角後，陸續有企業採用此方式，2002 年與 2003 年經濟景氣趨緩，企業為降低成本，使用資訊委外的企業數量大幅增加，並廣及各類型產業，包含醫療、零售等公司。至 2004 年後，Offshore 運作模式已漸趨成熟，並成為普遍的商業模式，二線企業也將相繼採用此運作方式。

根據 ODG 調查，北美約佔 70%的全球 Offshore 市場需求，歐洲與日本則佔其餘 30%的市場需求。以企業端觀察，北美地區已有 16%的企業使用 Offshore 服務，並且有 29%的企業表示有興趣或評估中，且根據北美企業 IT 預算分配的調查中，發現高達 60.6%的企業在 IT 預算中會分配 5%至 20%至 Offshore 服務。此外，由最大資訊委外供應地區印度觀之，其資訊服務出口地區別中，美國佔最高比例，達 62%，歐洲為 24%，日本為 10%。

委外的觀念興起後，其範圍已從單純的資料處理，轉至軟體服務，未來將擴及知識服務，委外的項目已不再只是單純的系統維修及程式再造，也朝向軟體應用開發與整合，包括所有可以支援資訊科技的流程皆可以委外服務處理。

根據 NASSCOM 機構於 2003 年所作的調查，目前財富雜誌公布的 1,000 大企業中有超過 300 家的企業資訊委外至印度，全球資訊委外市場約 80%皆為印度佔有，就 2002 年至 2008 年在資訊服務出口的部分，印度遙遙領先大陸與俄羅斯，出口金額約有俄羅斯的七倍之多。

國內即便資訊委外議題已經過各方討論多時，然實際發酵程度仍屬有限，放眼各行各業，金融業堪稱走在前端者，惟僅侷限於軟體開發與維護。

二、資訊委外管理因素探討

由於資訊系統的開發、維運或服務流程等委外，涉及公司的業務、作業、法律、信用與商譽等潛在風險。因而，除了慎選合作的廠商外，並應就可能風險加以分析及進行管理。

資訊委外可能的風險：

1. 成本、時效及問題解決等較不易掌控。

2. 廠商技能或轉包問題，服務品質不如預期。

3. 公司機密資訊或資料外洩的問題。

4. 廠商文化或運作模式不同，造成溝通成本及衝突的問題。

5. 若廠商產生變化，可能產生的衝擊及對應機制。

銀行在資訊委外之前應就委外策略分析如決策考量因素、資訊委外之發展現況與未來趨勢、全球委外模式 Global Sourcing Model 從資訊科技委外 (ITO)到商業流程委外(BPO)等方面進行效益與風險評量；在管理方面可分為財務評估、技術評估、品質評估、風險評估等項目評估；在委外流程管控方面可分為規劃分析、委外的內容與需求、供應商評選、契約協商與簽訂、契約執行與管理等項目。

專案管理是否成功往往為委外成敗關鍵主要因素，如廠商是否符合國際標準如 BS7799、CMMI 或人員具有 PMP(專業專案管理師)等認證

或資歷，在委外風險管理規劃方面可分為委外風險辯識、風險分析、風險回應規劃及委外風險監控等項目。

三、美國銀行業資訊委外之監理

美國銀行監理單位(OCC)為確保銀行資訊委外風險，於 2000.11.28 公佈 Risk Management of Outsourcing Technology Advisory Letter，供銀行之參考。另外，金檢單位(FFIEC: Federal Financial Institution Examination Council) 曾先後於 2003.03 提出「資訊服務廠商之監理檢查手冊」(Supervision of Technology Service Providers/IT Examination Handbook) 及 2004.06 提出「資訊委外服務檢查」手冊(Outsourcing Technology Services/IT Examination Handbook)，作為檢查基準。

手冊上強調資訊委外為必然的發展趨勢，除了對銀行資訊委外時應考量的因素及監理程序等原則性詳加說明外，分別提出管理者主要的風險評量及需求項目，並依序分聲譽風險、策略風險、法律風險及市場風險等風險因素加以提醒及建議。另對董事會及管理階層責任、供應商選擇、合約的問題、持續監視的問題、緊急復原計畫及資訊安全等皆有所敘述，可作為我國未來相關作業之參考。

四、我國資訊委外現況及監理

依行政院主計處調查我國 93 年資訊作業委外服務全年委外經費為新台幣 166 億元，其中金融業約佔 28 億元(17%)，其中以軟體開發與維護佔經費的 70%為最大，未來如何仿傚國外 Offshore 服務模式，擴大銀行資訊委外的範圍及深度，並強化委外管理的技能，應可加速我國整體銀行的競爭力及服務能量。

行政院為加速推動所屬各機關之資訊作業，擴大委外服務及提昇效能，於民國八十三年二月公佈「**各機關資訊作業委外服務實施要點**」。該資訊作業委外服務項目共有整體規劃、系統整合、系統管理、網路管理、軟體驗證、系統稽核、硬體操作、軟體開發、軟體維護、顧問諮詢、機房設施管理、備援服務、網路服務、資料庫建置、硬體維護、資料處理、資料登錄、訓練推廣等十八項，及其他適合辦理委外服務之資訊作業項目，本手冊亦可供業界辦理資訊作業委外時之參考。

中華民國銀行公會金融業務電子化委員會資安小組所訂「**電子銀行風險管理自律規範**」及「**電子銀行資安實務參考資料**」之文件中，對於銀行資訊委外作業廠商之風險管理也提供許多務實作法，可供業界執行之參考。

總之，資訊作業外包已成為必然趨勢，銀行除了應強化資訊委外運作效能外，亦應加速選擇策略合作夥伴，並透過提昇自我管理技能，以確保風險降到最低及效益最大。

參考文獻

1. BS7799，何珮琪，「資安人」雜誌第六期

2. BS7799 不等於資訊安全？，陳瑞祥 9/5/2003「資安人」雜誌

3. 從金融資安事件談 BS7799 之應用，蒲樹盛 2/9/2004

4. 銀行業分享資安經驗，陳佳溶 11/4/2005「資安人」雜誌

5. ISMS 稽核訓練課程芻議，樊國楨 2/3/2005「資安人」雜誌

6. 美國通貨監理局(簡稱 OCC) http://www.occ.treas.gov/網站

- Supervision of Technology Service Providers/IT Examination Handbook 03/2003
- Outsourcing Technology Services/IT Examination Handbook 06/2004

7. 2001/06/04 FDIC, Technology Outsourcing Information Documents

8.國內資料來源：部份文字轉載自行政院研考會、資安人科技網及聯合報報導

9. 2005/03/09資訊服務委外 資策會MIC 作者：鍾依萍

10. 2003/11/12重要資訊系統外包風險高 聯合報報導，記者李若松

11. 2003/11/18國政評論，『資訊系統外包的隱憂』，作者：黃朝盟、王慶龍

12. 2005/11/18 資安人科技網，聚焦核心業務、金融業資訊委外方興未艾，記者明雲青

13.『Information Security 資安人科技網 』網站

第五章、巴塞爾銀行監理委員會與電子銀行監理

壹、新巴塞爾協定與全球監理概況

一、巴塞爾協定銀行監理委員會簡介

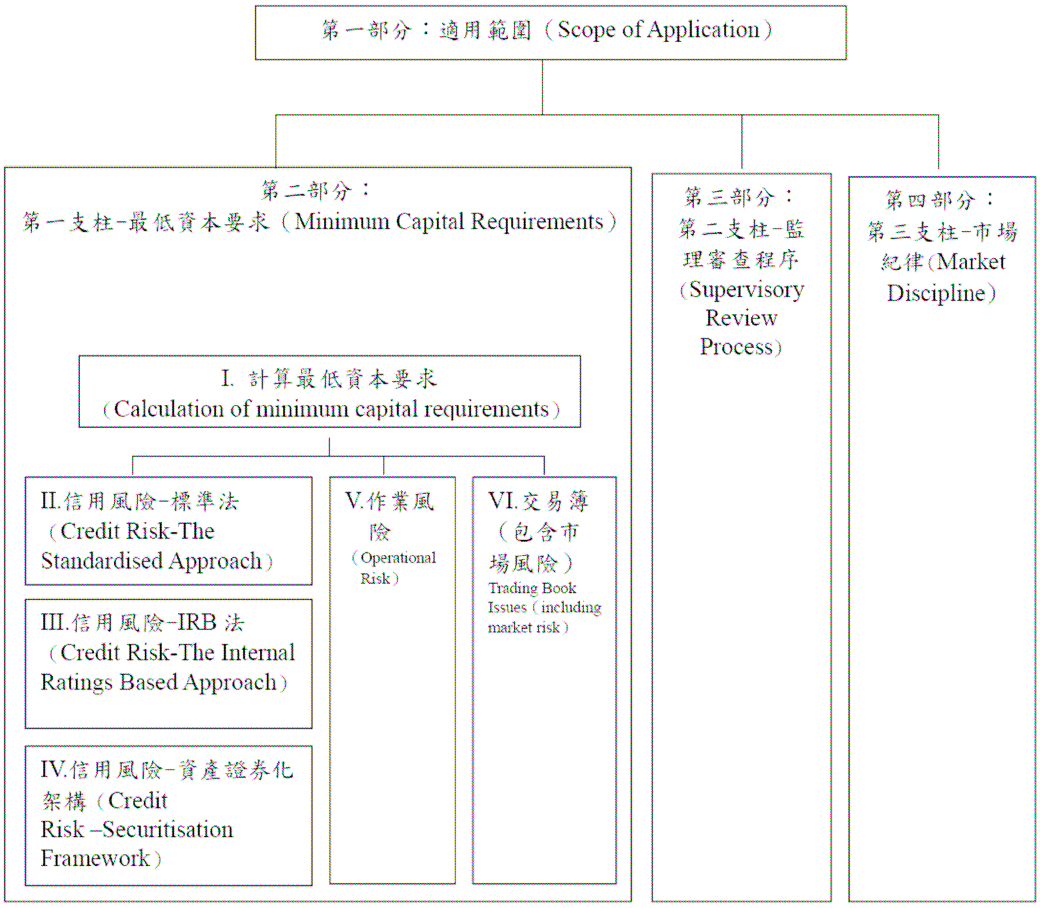
巴塞爾銀行監理委員會 (Basel Committee on Bank Supervision) 是一國際性銀行業務監理機關，於 1975 年正式成立於瑞士之巴塞爾，宗旨是促進國際在銀行監管事宜上的合作，係由十大工業國家組成（G10）組成，成員國包含比利時、加拿大、法國、德國、義大利、日本、盧森堡、荷蘭、西班牙、瑞典、瑞士、英國及美國共 13 個國家，並由各國之監理機關及央行資深代表共同執行事務，委會員通常在其常設秘書處舉行會議。

1988 年以前，國際間尚未有資本適足率的統一標準，國際銀行間形成不公平競爭現象。1988 年 7 月巴塞爾銀行監理委員會的「資本衡量及資本標準國際統合」報告，成為資本適足率的國際性統一標準。此資本標準協定，要求銀行針對其信用資產依規定權數計算「風險性資產總額」後，計提 8%之最低適足資本。1997 年 12 月實施資本協定涵蓋市場風險修正案，用以支撐銀行信用風險及市場風險的各類資本至少須達該銀行風險性資產總額的 8%以上。

在金融創新及科技進步下，銀行除傳統業務外，也積極開發包括衍生性金融商品在內之各項新種業務，以增闢收益來源，現行協定已

無法滿足金融監理及銀行風險管理的需求，故巴塞爾銀行監理委員會研擬大幅度修正現行協定。巴塞爾銀行監理委員會在研擬新資本協定架構時，亦保留現行資本協定關鍵部分，如最低適足資本仍維持在加權後之風險性資產 8%；1996 年修改之市場風險處理方式；及對合格資本之定義。

新巴塞爾資本協定架構，可由下圖簡略說明。



現行資本協定 (Basel I) 與新巴塞爾資本協定 (Basel II) 最大差異在於將作業風險 (Operational Risk) 納入計算最低資本適足率的風險加權資產總額中。另外，估算信用風險加權資產時，允許銀行使用內部評等法 (Internal Ratings-Based Approach, IRB)。銀行可依內部自行建置的風險評估模型所預測的風險大小來計提適足資本，希望所計提之資本更能真實反映銀行承擔風險，以落實銀行的風險管理，並藉由監理檢視及公開揭露兩大支柱防止使用內建模型銀行的敷衍及誤用。

二、巴塞爾銀行監理委員會對電子銀行監理的看法

多年來，銀行已經一直提供電子化服務給遠端的消費者和企業。例如電子匯款（包括小額支付和公司現金管理系統）以及自動提款機（已是全球普遍的固定設備）。而廣被接受的網際網路已成為銀行提供金融產品和服務的新通路。網際網路為銀行帶來新商機並提供銀行用戶新的好處。

雖然技術創新有顯著的好處，但電子銀行業務的迅速發展同時帶來了風險。金融機構應以謹慎的態度來瞭解並管理這些風險。由於這些現況，巴塞爾銀行監理委員會在 1998 年，針對電子銀行和電子錢的風險管理進行初步的研究。這初步的研究清楚顯示在電子銀行風險管理的領域裡仍需要更多的工作。這個任務被委任給電子銀行小組

(Electronic Banking Group；EBG)。電子銀行小組在 1998 年成立。它的成員包括銀行監理單位和中央銀行。

巴塞爾銀行監理委員會在 2000 年發表電子銀行小組有關電子銀行風險管理與監理的報告。這份報告詳列與電子銀行相關主要風險的清單，即策略風險，信譽風險，作業風險(包括安控風險和法律風險)，以及信用，市場和流動性風險。電子銀行小組論定電子銀行業務並未產生新型態的風險。不過，報告指出電子銀行業務會增加或改變部份的傳統風險，因此影響銀行的總體風險。尤其，策略風險，信譽風險和作業風險顯然會因為電子銀行業務的快速引進和支撐電子銀行業務技術的複雜性而增加。

電子銀行小組注意到電子銀行的基本特性會造成**風險管理的挑戰**：

在電子銀行業務方面，與技術和顧客服務創新有關的變化速度是空前的。在過去，新的金融應用程式在相當長的期間開發完成，並只在詳細的測試之後上線。今天，銀行可因競爭壓力在非常壓縮的時間裡推出新的商業應用程式—從概念到生產只要幾個月。

交易性質的電子銀行網站和相關的零售和批發企業應用程式通常盡可能與既有電腦系統結合，以便直通式(STP)的處理電子交易。直通

式自動化的處理過程可以降低過去人為錯誤和欺詐的機會，但是它也增加健全系統設計以及系統互通的相關性。

電子銀行增加銀行對資訊技術的依賴，因此增加很多作業和安全議題的技術複雜程度。電子銀行更促進合夥公司關係 (Partnership)，公司聯盟和與第三公司外包業務的機會。這其中許多組織未受金融監理。這種發展產生包含銀行和非銀行實體的新商業模式。這些非銀行實體包含網際網路服務供應商 (ISP)，電信公司和其他技術公司。

網際網路具有全球適用及無所不在的特性。它是一個開放式網路，不知名的使用者可以在任何地方使用它，傳遞的訊息會經過不知名的地點。而且現在還能透過日益方便的無線裝置來使用。因此，網際網路顯著的增加下列項目的重要性：安全控制，用戶驗證技術，資料保護的重要性，審計和用戶隱私標準。

為了促進這些發展，巴塞爾銀行監理委員會要求電子銀行小組定出關鍵風險管理原則，以便協助金融機構擴大現有風險監督政策與流程以涵蓋電子銀行業務。

這些風險管理原則不是嚴格的監理需求，也不能算是業界最佳實務典範 (Best Practice)，它只是為了提升電子銀行業務安全性的指導方針。巴塞爾銀行監理委員會深信，在電子銀行領域訂定風控需求的細節，可能會阻礙生產力。因為這些風控需求的細節很可能在改變快速

的技術和產品創新中，迅速的不合時宜。巴塞爾銀行監理委員會的整體監理目的是為了確保金融系統 (Financial System)的健全。這些原則表達的是巴塞爾銀行監理委員會為達成這個目的所提出的監理期望，而非嚴格的監理法條。

巴塞爾銀行監理委員會認為這些監理期望應適度修改以適用到電子銀行的通路，但是不可以在本質上與其他通路業務的風控原則不同。因為這些準則大度份都已經在 Basel II 中提及。在一些特定的領域，像是外包關係的管理、安控、法律與名譽風險、網際網路上通路的特性等，都需要有比目前所列原則更詳盡的準則。

巴塞爾銀行監理委員會認為，銀行必須針對自身的風險概況、營運架構以及公司的管理文化，去制定出一套既符合銀行業主管機關的風險管理要求，又適合銀行自身需求的風險管理流程。由於許多安控及風險管理的技術仍隨著技術與商業應用的快速成長而持續發展中，因此，本文中所提出的一些具代表性的企業風險管理個案，不應被視為最完整或最可靠的範例。

這份報告不試圖提出明確的技術方案來解決特定風險問題或者設定電子銀行的相關技術標準。當技術逐步發展時，技術議題需由金融機構和各個標準設定的機構在一個持續的基礎上處理。再者，由於業界持續在處理電子銀行的議題，像是安全性的挑戰，各種創新與低成

本的風控技術可能將有共識。這些解決方案同時可能可以解決下列的有關議題：銀行的規模與組織的複雜度、風控文化、法律與監理法規的不同。

基於這些理由，巴塞爾銀行監理委員會不相信「單一尺寸適合所有人」的作法適用於電子銀行的風險管理。巴塞爾銀行監理委員會並鼓勵大家交換好的電子銀行風控的實務與標準。基於這樣的監理哲理，巴塞爾銀行監理委員會期望這些風控原則是各國監理主管用來提升電子銀行安全的工具。各國監理主管應視各國特殊需求，經修改後再行採用。

巴塞爾銀行監理委員會認為，由於各銀行的風險概況互異，因此須在考量各自的電子銀行業務規模、現有風險的重要性以及銀行控管風險的意願與能力之後，選定適當的風險抵減技術 (Risk Mitigation Approach)。鑒於銀行間存在著前述的差異，本文所提及的風險管理原則主要目的在於提供一個具備充分彈性的指導方針，供各國的銀行參考採用。各國的主管機關當針對其所轄銀行之電子銀行業務相關風險的重要性進行評估，並進一步了解各銀行的風險管理架構是否符合本文的風險管理原則。

三、全球電子銀行監理概況

本節內容摘錄自 The Committee on Payment and Settlement Systems (CPSS) 在 2004 年 3 月發表的文件 "Survey of developments in electronic money and internet and mobile payments". CPSS 與巴塞爾銀行監理委員會同為國際清算銀行 (Bank for International Settlements) 之主要委員會。

部分國家已為網路及行動支付（Internet and Mobile Payments）制定了相關的法律規範。近年來，針對現行法規進行修正而得之新的法律條文，已為許多國家所採用，其中包含：澳洲、玻利維亞，保加利亞，捷克共和國，希臘，印度，日本，立陶宛，菲律賓，南非，台灣和委內瑞拉等國。歐盟對於網路、行動支付及一般通稱的電子商務 (e-Commerce) 的立法架構係由下列幾項指導方針所組成：電子商務指導方針(The E-commerce Directive；法規 2000/31/EC，主要針對網路市場中電子商務部份的法律面議題提供規範)，電子貨幣指導方針（The E-money Directive；法規 2000/46/EC，規範電子貨幣業務之執行及監督原則) 及電子簽章指導方針（The E-signatures Directive；法規 1999/93/EC，規範電子簽章的一致性架構)。法律架構一般適用於處理用戶與發行者 (Issuer) 間權利義務的相關問題，而有關顧客保護及數位簽章認定的相關法規，一般會對詐欺行為制定應有的罰則。

在僅考量網路繳款及行動支付的低交易量及低交易總值的前提下，各國之中央銀行對此項業務的監理應與其他業務無異。然而在付款安全性及效率性的考量之下，各國央行必須持續留意該領域的發展狀況，以期能盡到完善的監督責任。

1. 歐元體系國家對網路及行動支付的政策

2002 年秋天，歐洲央行 (ECB) 發表了一篇文件：電子支付在歐洲之歐元體系觀點 (E-payments in Europe – the Euro System's Perspective)，並舉辦一場研討會以討論電子支付的特性及歐元體系 (Euro System) 在該領域中所扮演的角色。根據市場參與者的討論，歐元體系歸納出自身的兩大主要角色：市場的催化劑及監督者。在確保安全性及效率性的前提之下，歐元體系的重點若在於維持市場的持續發展，就必須適當的扮演其作為催化劑的角色。

藉由支付過程中眾多參與者的充份合作，使得一般大眾得以利用電子支付獲得最大的利益。身為促進該領域發展的推手角色，歐元體系應致力於促成各利益團體(Stakeholders) 間的合作，並提供有利於整合的相關分析及資料。

2. 德國

在德國，經營透過電話或者網際網路來進行支付的系統，並不需要經過事先的許可。然而，鑒於支付的安全性及效率性對此類系統的重要性，德意志銀行將網路及行動支付亦納入其監理範疇之內。惟德意志銀行並未採取特別的措施去影響網路及行動支付技術的設計與運作，因為只有透過市場參與者之間的相互競爭，方能發展及提供最符合消費者需求的產品。

金融監理法規並未針對電子支付系統 (e-Payment System)提供者訂定明確的法律條文，以管理其風險。然而，銀行法 25a 的部分提到：機構應當訂出一套符合法律規範精神之原則，以管理、監督及控制該業務衍生的風險。根據銀行法 25a 的部份，聯邦金融監督局 (the Federal Supervisory Authority) 已針對委外 (Outsourcing) 業務的部份，發文一份一般管理準則供業者參考。

當技術處於持續發展的階段時，過於詳細的法規反而會產生反效果，且可能很快就流於過時而不敷採用。提供一個一般性原則的方式，較能為未來的發展保留適當的監理上的彈性。

3. 加拿大

對電子貨幣或網路支付技術並無直接的監理機制。

4. 日本

作為日本支付系統的監督者，日本銀行 (The Bank of Japan) 對私人部門零售支付系統的發展，包含電子貨幣及網路支付，採取了嚴密的監控，並適切的評估這些發展所衍生之風險面及效率面的影響。此刻，日本銀行並不希望這些措施會對日本整體支付系統的交易量、交易總值及本質造成系統性的影響。所以，制定相關法規對日本銀行而言，並非當務之急。

5. 瑞士

聯邦金融委員會 (the Federal Banking Commission) 並未採取任何具體的法律規章。

6. 美國

目前，聯邦銀行當局正不斷更新、改進現行的銀行檢視程序，以納入考量電子金融的發展及其相關之風險。然而，在處理電子貨幣產品的經驗相當有限，以及美國當地提供此類產品之機構家數稀少的前提之下，具體的監理方針將視需求而逐漸發展。

貳、 巴塞爾銀行監理委員會電子銀行風險管理原則

原則一：董事會及高階管理階層應對電子銀行業務所帶來的風險，建立有效的監督管理制度，包括各類風險的說明、風險管理政策及風險控管程序，以有效管理電子銀行業務風險。

一、在進入新的電子銀行業務之前，董事會及高階管理階層應針對該新開業務對銀行現階段之風險架構、經營策略的影響及成本/效益進行分析,並確定銀行具備充分的專業能力以管理此新開業務所帶來之風險。

二、高階管理階層應持續監督可能發生的電子銀行系統問題或是安全漏洞。

三、建立電子銀行業務風險管理之主要授權及通報機制,定期或於必要時將風險管理系統之執行狀況及任何會影響銀行經營及聲譽之緊急突發事件（例如駭客入侵、客戶資料外洩）向董事會及高階管理階層報告。

四、在辦理跨國界(Cross-Border)電子銀行業務之前，應先對該相關國之金融相關法規及國家風險，進行嚴謹的分析，並確實的遵守法規及有效的控管風險。

管理階層在從事管理監測時應注意事項：

1. 銀行的風險偏好應與電子銀行業務相契合。
2. 應建立關鍵時刻的人員配置及通報機制，以因應突發事件對銀行可能的影響。
3. 找出與電子銀行業務安全性、整體性及效益等攸關的風險因子，並要求合作的第三者廠商亦應採取同一標準來衡量風險。
4. 確認在進行跨國電子銀行業務前，銀行已完成相關之實地調查及風險分析作業。

原則二：銀行的關鍵性安全控管機制須經董事會及高階管理階層的檢視及認可。

一、建立適當之授權管理、簽入和實體存取安全控制及合適之安全控管設備，以提供內、外部使用者適當之安全介面及限制。

二、有效之安全控管機制應包含：

1. 設置專責人員負責監督銀行安全控管政策的建立及維持。
2. 確實執行簽入及實體安全管制措施，以防止未經授權者對銀行資訊安全所造成的威脅。
3. 定期檢測安全管制措施，包含：持續注意現階段金融業安控機

制的最新發展、安控軟體的安裝與升級等。

原則三：董事會及高階管理階層應建立完善且持續嚴謹之監督程序，以管理委外作業廠商及其他第三者所提供之支援電子銀行業務服務。

一、銀行對於其電子銀行系統、運用程式之委外處理者及其他合夥處理者，應該完全瞭解其所帶來之風險。並就其對於銀行的風險結構與風險控管能力所造成的影響，進行持續且完整的評估。

二、在委外及合夥契約簽定之前應詳細審核評估委外作業廠商之專業、信譽及財務能力。

三、合約上應詳細載明委外廠商、合夥廠商、提供服務之第三者之委外或合夥權利義務。

四、對於電子銀行業務委外事項之風險管理、安控機制及資料保密機制，均須符合銀行本身的標準。

五、對於電子銀行業務委外事項要定期實施內部及外部稽核

六、對於電子銀行業務委外事項應建立一套適當之緊急應變計畫。

原則四:銀行應針對透過網際網路進行業務交易的客戶，建立適當的認證措施、身份辨識及授權機制。

一、顧客原始帳戶之確認是重要的步驟，若未能有適當的認證措施，可能導致非法個人存取電子銀行帳戶，最後導致銀行財物損失及信譽受損。

二、銀行可以採用下列認證措施：PINs、Passwords、Smart Cards、Biometrics、Digital Certificates。同時採用多種的認證措施，通常能提供較佳的效果。

三、銀行宜採行相關認證及安控措施，以確保下列事項：

1. 運用於存取電子銀行客戶帳號或敏感性系統之認證資料庫，應確保避免被竄改或破壞；而對於企圖竄改或破壞資料之行為，系統應能偵測及留存稽核追蹤紀錄。
2. 凡是新增、刪除或變更個人、代理者、系統之認證資料，均需經過認證辨識及授權。
3. 銀行應有適當措施，保護電子銀行系統之連結，以防不明或不法之第三者取代正常客戶，而使客戶權益受損。
4. 經認證之電子銀行系統連線應全程保持安全性，當發生安全事件時，此類連線應重新認證客戶身份及權限。

四、 銀行在決定驗證方式時應考量下列事項：

1. 業務性質

2. 資料儲存的敏感性及價值

3. 客戶操作的難易度

五、 跨國交易的客戶身份確認工作，困難度較高。

原則五:銀行應採行交易認證方法，以加強電子銀行交易的不可否認性及建立電子銀行交易的可信度。

一、不可否認性，係為證實原始資訊的傳送者/接收者確曾傳送/接收該訊息， 以避免另一方否認。業者或可採用PKI（公開金鑰架構）；或數位認證、數位簽章等技術來確保電子銀行交易之不可否認性。

二、銀行應依交易類別及交易風險高低建立交易面安全設計，以確保下列事項：

1.降低有權使用者進行無意的交易之可能性，並讓客戶充分了解交易所伴隨的可能風險。

2.所有的交易攸關者均應透過認證系統被確認無誤。財務交易資料應確保無法被更改，且任何更改動作均可被偵測到。

原則六：對於電子銀行系統、資料庫及運用程式，銀行應確信已採行適當的分工牽制機制。

一、 職務分工，不只可減少作業流程或系統發生詐欺的機會，亦可減少發生個人詐欺的機會。網路交易，發生交易者身分被偽冒的機會較一般情形大，此時，職務分工尤其重要。如果疏於防範，有心者將利用網路安全的漏洞竊取資料，因此，經營電子銀行業務應強調：嚴格的授權及身分識別機制、安全的一貫化交易流程處理（Straight-Through Process）架構、及適當的稽核追蹤。

二、 實務上對於分工牽制機制之建立與維持，有以下的做法：

1. 對於交易處理程序及系統，單一員工或委外作業廠商無法單獨輸入、授權及完成任何交易。
2. 原始靜態資料（包含網頁內容）的建立及後續資料完整性檢核之間，必須符合分工牽制原則。
3. 電子銀行必須經過反覆的測試，以確保系統符合且無法規避分工牽制機制。
4. 電子銀行系統的開發及使用管理之間，必須符合分工牽制原則。

原則七：銀行對於電子銀行系統、資料庫及應用程式，應採行適當的授權控管及存取管理機制。

一、 分工牽制機制的維持，有賴於銀行嚴格控管授權及存取的權限。

二、 電子銀行系統對於授權和存取權限之管理可採集中管理或分散管理方式。

原則八：銀行應採取適當的措施，以確保電子銀行交易、紀錄與資訊的資料完整性。

一、 資料完整性係指保證資訊於傳輸或儲存時，非經正常授權不能被更動。資料完整性若未能被確實維持，將導致銀行的財物損失及信譽受損。

二、 一貫化交易流程處理有其本質上的缺失，銀行如採用該法，應特別重視資料的安全性、有效性及完整性，俾能即時修正程式設計上的缺失。

三、 銀行應採取適當之措施，以保護電子銀行業務交易、紀錄及資訊的正 確性、完整性與可靠性，不論資料是在網際網路傳輸或是存在銀行內部資料庫或者傳輸/儲存於第三服務提供者處。

四、 確保資料完整性的策略：

（1） 採用確保交易過程中資料不會被竄改的方式。

（2） 嚴格規範資料存取及修改的原則。

（3） 設計資料存取流程，應嚴格防範未經授權者入侵。

（4） 確保原始資料的可靠性，不會因系統控管政策（含監測流程）改變而受破壞。

（5） 採用具有可偵測資料遭破壞的機制。

原則九：銀行應對所有的電子銀行交易，留有詳細的稽查追蹤紀錄。

一、 下列型態的電子銀行交易，必須要有清楚的稽核追蹤紀錄：

1. 客戶帳戶之開戶、變更及結清資料。
2. 任何與帳務有關之交易。
3. 客戶超出授權限額的交易。
4. 系統存取權之異動。

原則十：針對傳輸中或儲存於資料庫中之電子銀行關鍵資訊，銀行應依資訊的敏感性採取適當的措施，以維持資料的機密性。

一、 只有被適當授權及經過認證之後的個人、代理者或系統管理者才可存取銀行機密性資料及紀錄。

二、 所有銀行機密性資料在透過網際網路或內部網路傳輸時必須要有加密的安控機制，以防止被未經授權者瀏覽及修改。

三、 委外廠商及提供服務的第三者對銀行機密性資料所進行的存取、運用及保護，必須符合銀行所定的標準。

四、 存取限閱資料必須留存紀錄，且確保該紀錄不會受到損害。

原則十一：銀行應於其電子網頁中，就銀行本身提供之服務內容及相關規章制度，提供充分的資訊，以供客戶進行交易前之參考。

一、 爲降低電子銀行業務所可能產生的適法性及信譽風險，銀行應在電子銀行網頁上提供足夠的資訊，例如: 銀行名稱、營業據點及總行所在地；客戶申訴管道及電話；顧客服務中心；客戶存款保險理賠; 針對特定法律管轄區，客戶所應知悉之訊息等資訊，以供客戶進行交易前之參考。

原則十二：銀行在提供電子銀行產品及服務時，應採取適當措施以保護客戶資料的隱私權。

一、 保護客戶資料隱私權是銀行之基本責任。為避免因誤用或揭露未經客戶授權之機密資料所導致的適法性及信譽風險，銀行應採取下列措施:

1. 電子銀行服務對保護客戶資料隱私權之政策及標準，應遵守相

關法令規定。

2. 明確告知客戶，銀行在提供的電子銀行產品及服務時，所採取的客戶資料隱私權政策及標準。

3. 銀行使用客戶資料不得超越客戶授權的範圍。

4. 委外作業廠商對客戶資料的使用，應符合銀行的客戶資料隱私權政策及標準。

原則十三：銀行應建立一套有效的業務復原及災變應變計畫，以維持電子銀行系統服務的持續性。

一、 為避免營運、法律或聲譽風險，銀行經營電子銀行業務應在一致的、即時的基礎上提供客戶所期待的服務項目。為達成前述目標，銀行應確保有能力將服務順利送達終端使用者；同時有能力處理駭客入侵的問題。如何在尖峰/離峰期間提供一致的服務品質，對銀行而言是一項考驗。

二、 應依電子商務市場動態及客戶對電子銀行產品及服務的接受程度，來分析規劃電子銀行系統所需容量及將來規模。

三、 經由壓力測試及定期的檢核，估計電子銀行交易處理之容量。

四、 對於重要之電子銀行業務處理程序及傳輸系統，建立災變備援及業務復原計畫並定期測試。

原則十四：銀行應建立適當的緊急應變計畫，處理突發及未預期事件(包含內部及外部攻擊)，以維持電子銀行系統及服務的正常運作。

一、 電子銀行系統及服務之緊急應變計畫，須因應在不同緊急情境下，對不同業務、地理位置等，皆能適時恢復正常運作。且應評估風險發生時對銀行之衝擊，評估範圍亦應包含委外作業廠商所提供之服務。

二、 緊急事件一旦發生，應有明確之評估及認定機制(包括事件之重要性及事件發生所帶來之危機)，進而控制因任何服務中斷所導致的信譽風險。

三、 對於市場及大眾傳播媒體所關心之安控漏洞、線上攻擊及網路銀行系統失敗之情事，要建立適當之溝通及聯絡策略。

四、 重要的安控缺失或服務中斷事件應建立緊急通報程序，通報主管機關。

五、 要設置緊急事件處理小組，小組人員須經過充分專業訓練，以分析、解釋、處理相關結果的意義及重要性。

六、 要有明確之指揮體系，處理內部或委外業務之緊急事件，並適時通報董事會。

七、 對於重要電子銀行業務中斷及業務復原，應即時對外公告。

八、　應蒐集及保留法律證據紀錄，以協助電子銀行緊急事件之追蹤檢討及提供法律訴訟之佐證。

參、巴塞爾委員會第三版諮詢文件監理審查程序重點摘要

茲參考銀行公會監理審查分組第二階段研究工作報告，按主管機關基本監理準則、銀行內控、內稽與風險管理基本原則及電子銀行業務風險管理基本原則等重點摘錄如下：

一、主管機關基本監理準則

（一）、有效的銀行監理體系，包括銀行核准設立及持續監理，督促銀行遵守法令及安全穩健經營原則，及對監理人員之法律保障，均應立法明訂，各監理機關間資訊分享及資訊保密，亦應妥適規範（有效銀行監理之基本原則）。

（二）、法律或監理法規應提供銀行遵守之最低穩健標準的架構，監理機關並應確保所管轄銀行之財務強度及績效資訊對外公開揭露（有效銀行監理原則實施方法）。

（三）、監理機關和外部稽核對於其個別角色與職責之共識，以及在適當情況下相互溝通，有助於提高銀行財務報表之稽核和銀行監理之有效性。外部稽核人員執行查核須恪守相關的道德規範和稽核準則，包括：具有專業素養、以獨立超然、公正客觀的審慎態度,妥適的規劃與監督(監理機關與銀行外部稽核的關係)。

（四）、銀行監理機關的工作是要及早發現問題，立即採取充分適當的

糾正行動，如預防性的糾正行動及處理失敗銀行的機制，另注意處理速度、考量成本效率、透明化、合作及彈性、避免道德危險等（處理弱質銀行監理準則）。

二、銀行內控、內稽與風險管理基本原則

（一）、內部控制係銀行董事會、高階管理階層及全體員工應持續有效執行的程序，以確保銀行有效率、有效果的使用其資產，並保護銀行資產免遭致損失；並提供可靠、完整、並具即時性之資訊供決策者製作決策參考；及使所有銀行業務之執行均遵照相關之法律及規章、監理機關之要求、及銀行本身之政策與程序（內部控制評估原則）。

（二）、銀行內部稽核設置目的在於協助金融機構提昇營運績效，利用有系統的專業方法，獨立客觀評估風險管理、內部控制制度及權責劃分是否有效運作，並提供改進建議，以確保組織達成預期目標。故有效之內部稽核功能可使銀行管理階層及銀行監理機關，為達成內部控制制度品質，提供有用之資訊來源（銀行內部稽核準則暨監理機關與稽核人員關係）。

（三）、有效的董事會應清晰定義其本身與高階管理人員的權力與關鍵責任；董事會成員應能執行判斷並獨立於管理階層、大股東、

或政府的看法，並有效運用內外部稽核人員提供之重要控制功能，以透明方式從事公司治理；並確保報酬制度與銀行的價值、目標、策略、及控制環境一致（強化公司治理）。

三、電子銀行業務風險管理基本原則

（一）、電子銀行業務之安全控管機制包括適當的授權機制、邏輯層及實體層的存取控管機制、妥善的安全架構，可有效的區隔銀行內、外部的使用者（電子銀行業務風險管理原則）。

（二）、在進行跨國性電子銀行業務前，銀行應進行風險評估及實地調查作業，並建立有效的風險管理計畫（跨國性電子銀行業務之管理與監督）。

（三）、健全之銀行作業風險管理應發展適當之作業風險管理環境及辨識、評估、監督及控制/沖抵等作業程序（作業風險管理與監督原則）。

肆、巴塞爾銀行監理委員會跨界電子銀行業務的監督與管理

本文係由巴塞爾銀行監理委員會的電子銀行小組(Electronic Banking Group; EBG)所制定，主要目的在闡述對於進行跨界(Cross-Border)電子銀行業務之銀行業者、其註冊母國(Home Country)及當地國家(Local Country)之主管機關，在相關業務之監督管理上的期待與準則。

本文的兩大重點如下:

一、確認銀行對其跨界電子銀行業務之風險管理責任。

本文件係 2003 年 7 月巴塞爾銀行監理委員會所發表之「電子銀行風險管理原則」的補充文件，重點在強調銀行須將跨界電子銀行業務的風險納入銀行的整體風險管理架構之中。此外，銀行在提供跨界電子業務服務之前,應針對可能產生的風險進行審慎的評估及揭露，並建立適當的風險持續監管程序。

二、強調銀行註冊母國之主管機關應對銀行之跨界電子銀行業務採取有效的監管，且持續與該業務之其他相關國家的主管單位維持合作的關係。

本文件的另一項重點在於對銀行註冊母國之主管機關及當地國家之主管機關的角色及責任進行認定。銀行註冊母國主管機關應

確認所轄銀行已就其跨界電子銀行業務採取適當的風險管理及揭露政策。而當地國家之主管機關在執行監督責任之前，應先考慮母國對所轄銀行的監理情況與效率，以及當地居民所使用之電子銀行業務內容及環境，再決定所應採取的監理措施。

1.前言

(1). 銀行業者透過電子途徑(Electronic Channel)與國內外的企業客戶進行交易已行之有年。隨著網際網路的普及與網路技術的發展，銀行利用電子途徑提供產品及服務給顧客的比例，有了大幅度的增加。這類型的銀行業務一般通稱為電子銀行業務(e-banking)或者網路銀行業務，儘管各銀行所提供之產品、服務的內容及複雜程度並不盡相同。

(2). 銀行的經營策略及商業模式一直不斷的在演進，以期能充分運用網際網路所帶來的優勢。網際網路的開放及無遠弗屆的特性，使得時間及地點均不再構成銀行與其電子銀行客戶之間的阻礙。因此，當大多數的銀行只針對其所屬國家的市場(Home Market)及設有具備合格執照之營業據點的國外市場(Foreign Market)提供電子銀行產品及服務的同時，部份銀行已開始著手進行跨界電子銀行業務(Cross-Border e-banking)；也就是：銀行透過網際網路提供電子銀

行產品及服務給國外的客戶，但該銀行於客戶所在之國家並未設有具備合格執照之營業據點。

(3). 迄今，大多數國家之跨界電子銀行業務的發展並未如其國內電子銀行業務發展之迅速。究其原因有二：其一在於消費者對於與外國機構進行電子銀行交易時可能產生的安全性問題有所疑慮；其二，銀行業者在進行跨界電子銀行業務時，客戶所在國之法律適用問題及顧客保護之相關規定所伴隨而來的不確定性(Uncertainty)，亦是阻礙跨界電子銀行業務發展的主要因素。

(4). 然而，業者及銀行監管機關仍相當看好跨界電子銀行業務在未來幾年內的發展潛力。理由如下：首先，隨著各國對電子銀行業務接受度的持續增加，消費者亦較願意透過網際網路去取得符合自身需求的銀行產品；其次，網路科技的持續創新，使得銀行透過電子途徑即能擴展其現有市場及開發新市場的目標客群，降低銀行對實體營業據點的依賴性及其伴隨產生之大量投資。

(5). 市場的高度潛力以及企業間的競爭壓力，提供銀行擴展跨界電子銀行業務規模的動機。銀行在進行此項業務時，須仔細評估並妥善管理該業務可能導致的風險，例如：策略風險 (Strategic Risk)、聲譽風險 (Reputational Risk)、作業風險 (Operational Risk)及國家風險 (Country Risk)等。

(6). 此外，由於與跨界電子商務(Cross-Border e-commerce)相關的法規仍在不斷的演進及發展，參與跨界電子銀行業務之銀行所面臨的法律風險勢必與日俱增。除非銀行能採取適當的監督及管理，否則將面臨不同國家間潛在的法令遵循風險(Non-Compliance Risk)，其中包括：消費者保護法、廣告與揭露相關法規、紀錄保存及報告之要求、隱私權保護法及洗錢防制法等。各國對於跨界電子銀行業務所訂定的法規不盡相同、銀行註冊母國及顧客所在當地國家之主管單位於該業務中所扮演的角色及應負的責任因國而異，在在都使得法令遵循的挑戰愈形複雜。儘管前述的問題在傳統的跨界銀行業務中已經存在，但電子途徑的使用，除了便利銀行提供其跨界銀行服務給客戶，亦提高了銀行法令遵循風險的挑戰性。

(7). 巴塞爾委員會認為，銀行註冊母國主管機關與客戶所在當地國家之主管機關間的合作，是有效管理跨界電子銀行業務中相當重要的一環。此外，隨著銀行組織日趨複雜、金融活動多元整合及分支機構遍佈全球之際，銀行註冊母國對電子銀行業務的監理角色便越形重要。

(8). 所以，銀行註冊母國之主管機機關必須能確定已將跨界電子銀行業務納入其監管範疇之內，且適當的評估銀行是否履行應盡之風險管理責任，其中包括風險的評估及揭露等。銀行註冊母國之主管機關

有效的監督管理並與當地主管機關進行適切的合作,將促進對跨界電子銀行業務的監理能力。

(9). 本份文件闡述的內容主要分成兩大方向：

(a) 確認銀行在進行跨界電子銀行業務時所應盡的風險管理責任。強調銀行必須將跨界電子銀行業務的風險整合至銀行的整體風險管理架構之中，且銀行有責任在跨界電子銀行業務的推行之前採取適當的風險評估並適切的將訊息對潛在的消費者進行揭露，以及提出更進一步的風險管理原則。

(b) 強調銀行註冊母國主管機關有效監理的需要，以及跨國主管機機關間的持續合作對於跨界電子銀行業務風險控管的重要性。

2. 跨界電子銀行業務的定義

本份文件定義之跨界電子銀行業務係：一國之銀行提供交易性的線上(On-line)銀行產品及服務予其他國家之當地居民，

(10). 上述的定義並不尋求去解決有關電子銀行取得當地主管機關營業執照許可的相關法律議題,也非試圖處理國際間對「銀行服務」定義上的差異,或者是去決定允許一家外國銀行提供服務給當地居

民時，應取得當地營業許可的規範與標準。

(11). 許多國家之法規規定：外國銀行在本國取得營業許可之後，須在本國設立實體營業據點，方能透過該營業據點與本國之居民進行交易(如儲貸業務)。然而，部分國家的主管機關亦允許外國銀行在取得營業許可之後，不須於當地設立實體營業據點，即能提供電子銀行產品及服務予當地居民。巴塞爾委員會認為：隨著各國電子商務(包括電子銀行)相關法規的不斷演進，以及透過國際間的協定，應能使各國對營業許可的相關規定產生較多的共識。

(12). 因此，為了能涵蓋國際上的法律規範，而又能為本文所述的跨界電子銀行風險管理準則提出實用的定義，跨界電子銀行業務被定義為透過網路線上交易的方式，提供金融商品及服務給另一國家的當地居民之活動稱之。

(13). 委員會相信，銀行採行適當措施、風險評估與持續性風險控管責任的需要程度，以及主管機關重視的範疇，應取決於銀行的電子銀行商品服務直接涉入當地國居民的多寡而定。

(14). 銀行及主管機關可採用某些有用的定性或定量指標，來決定是否視某特定國家之居民為目標客戶，進而提供電子銀行產品及服務。

3. 跨界電子銀行業務之風險管理

(15). 交易性電子銀行業務所伴隨產生的風險主要有：策略風險、聲譽風險、作業風險(包括安全性及法律風險)以及信用、市場和流動性風險。

(16). 電子銀行業務之主要風險管理原則可分為三大方向:

(a)董事會及管理階層的監督；

(b)安全性及作業風險的控管；

(c)法律及聲譽風險的管理。

適當的風險評估、監督控管以及持續的風險管理，是董事會及管理階層達到有效監理的關鍵。此外，基於銀行業者及各國監理機關的回應，電子銀行小組針對跨界電子銀行業務出兩項額外的風險管理原則，來加強前述風險評估、監督控管以及持續的風險管理措施。

原則一：在從事跨界電子銀行業務之前，銀行須先進行適當的風險評估、監督控管，並針對該業務建立一套有效的風險管理流程。

(17). 在開始提供跨界電子銀行產品及服務之前，銀行的管理階層必須先進行適當的風險評估及監督，以確保銀行具備管理相關風險的能力。此外，銀行必須遵循該項業務相關國家之法規及要求，並針對該項業務進行有效且持續的風險管理。

(18). 銀行風險評估、監督以及持續風險管理的範疇，至少需包含：國家風險、法令遵循風險、法規要求、會計準則以及提供線上產品及服務予國外客戶時，所衍生之作業性、安全性、隱私權與顧客服務方面的挑戰。

(19). 銀行進行跨界營運的主要風險之一，在於未能遵循國外的法規以及對如何選擇適用於電子商務領域的法律無所適從。由於不同國家對於營業許可、監管程序以及顧客保護要求的相關規定可能存在相當大的差異，使得銀行進行風險監控的複雜度及成本均大幅提高。

(20). 銀行可以藉由在網站上的明顯處，聲明其提供的線上商品及服務係僅針對某特定國家之居民，以減輕銀行應負的相關責任。然而，銀行應瞭解這些聲明的法律效用可能具有不確定性且其成效會因國而異。

(21). 有意從事跨界電子銀行業務的銀行，應與銀行註冊母國之主管機關諮詢相關之規定以及實務上的運作狀況。透過諮詢的過程，主管機關可以針對銀行的風險監督程序以及風險管理能力，進行其應盡之監管責任。此外，對於目標客戶所在的當地國家，銀行若能事先與當地之主管機關諮詢相關之規定，將能降低未來業務實際推行時的法律遵循風險。

原則二：銀行應於其電子網頁中，就銀行本身提供之服務內容、銀行所在國家及相關規章制度，提供充分的資訊，以供潛在客戶進行交易前之參考。

(22). 銀行於電子網頁中充分揭露服務內容、銀行所在國家及相關規章制度等資訊,將有助於提升透明度並降低跨界電子銀行業務可能伴隨產生之法律及聲譽風險。

(23). 銀行應於電子網頁中揭露的訊息，隨著客戶所在國家之法規、商業習慣的不同，而有所差異。除了電子銀行風險管理準則中所規定的項目（銀行名稱、營業據點及總行所在地)；客戶申訴管道及電話；顧客服務中心；

(24). 若銀行由於某些因素或限制，而無法對某些特定國家之居民提供跨界電子銀行產品及服務,則銀行應於其電子網頁中對該特定國家進行此項訊息之充分揭露。

4. 跨界電子銀行業務的監督與管理

(25). 巴塞爾委員會認為：各國銀行主管機關之間的合作以及資訊的分享，將有助於跨界電子銀行業務的有效監管。

(26). 電子銀行業務可視為傳統銀行業務的延伸，差異在於電子銀行

業務係採電子途徑作為其產品及服務的傳送管道。因此，大部分的國家現行的傳統銀行法規均能延伸使用至電子銀行業務上，且巴塞爾協定中對於銀行註冊母國以及顧客所在當地國家主管機關之責任與合作關係的規範亦能適用。然而，欲將前述協定中的原則套用於未設有實體營業據點的跨界電子銀行業務上時，實際操作上可能會面臨一些問題。

(27). 不同國家對於提供電子銀行服務予當地居民，且未設有實體營業據點的外國銀行，在營業許可及其他相關要求上有著不同的規範。例如：在某些國家，當地的主管機關無權要求提供跨界電子銀行業務的國外銀行接受其執照方面的相關規定。

(28). 即便不受到營業執照相關規定的約束，客戶所在當地國家之主關機關亦有責任要求提供跨界電子銀行業務的外國銀行確實遵循當地之消費者保護條例等規範。

(29). 銀行註冊母國之主管機關的有效監管，能確保銀行已針對跨界電子銀行業務相關的風險採取適當的風險管理系統以進行控管，進而降低客戶所在當地國家主管機關的疑慮。

(30). 當提供跨界電子銀行業務服務的外國銀行與客戶所在國家之當地主管機關進行聯繫時，當地主管機關應先考量銀行註冊母國之主管機關是否已針對該業務採取有效的監督管理之後，再決定自身

於該業務中所應扮演的監理角色。

A. 提供跨界電子銀行業務之銀行其註冊母國主管機關所應盡的責任及扮演的角色

(31). 跨界電子銀行業務的引進，並不會改變銀行主管機關對銀行之整體風險架構、風險管理能力及資本適足性等進行有效監管的基本責任。主管機關應針對銀行對於跨界電子銀行業務的挑戰及相關風險之瞭解程度，進行經常性的評估。

(32). 主管機關應明確的將其監督原則及期望傳達給銀行，此舉有助於銀行對於跨界電子銀行業務風險控管，並使與該業務相關之外國銀行主管機關相信該項業務已受到銀行所在國家主管機關適當的管理與監督。

(33). 主管機關應確定銀行已針對跨界電子銀行業務相關風險之認定與管理採取適當的程序，其中應包括本國及與該業務相關之外國銀行主管機關的監督原則，以及適用法規的認定。

(34). 跨國主管機關間的協調亦是跨界電子銀行業務監督管理中的重要一環。當外國監理機關洽詢母國有關在當地從事跨界電子銀行業務的監理事宜時，母國應依其法律規章，給予適當的配合。

(35). 當銀行之電子銀行業務相關資料及訊息，係委由國外之第三人

進行管理或處理時,銀行註冊母國之主管機關應確認該銀行有能力存取及控管與電子銀行業務風險管理相關之重要資料與訊息。此外,母國之主管機關也應確保可以充分的取得這類的資訊,以符合監理機制並盡到作為銀行主要監督者的責任。

B. 客戶所在國家主管機關(當地主管機關)應有的考量

(36). 由於網際網路開放的特性,使得電子銀行產品及服務相關訊息的取得相當容易。然而,資訊易取得的特性並不足以構成跨界電子銀行業務。

(37). 當提供跨界電子銀行業務予本國居民之外國銀行與當地主管機關進行聯繫時,當地主管機關應在考量下列因素後,決定是否針對該項業務履行監督管理責任:

(a) 提供該項業務之銀行其註冊母國之主管機關(外國主管機關)是否對該項業務進行有效的監管;

(b) 當地主管機關與外國主管機關之間,是否存在適當的溝通程序及管道;

(c) 外國銀行對於該項業務的計畫。亦可與外國主管機關就該業務相關的風險及考量,討論出適當的協調及合作架構;

(d) 告知提供該項業務之國外銀行關於本國銀行相關法規及要

求的適用範圍；

(e) 確認提供該項業務之國外銀行已確實遵循當地之銀行相關法規及要求。

(38). 當地主管機關若發現提供該項業務之國外銀行有任何違反當地法規之情事，可採取下列措施因應之：

(a) 就該銀行未遵循之法規及要求，對銀行進行告知；

(b) 就該銀行未遵循之法規及要求，對外國主管機關進行告知；

(c) 公開告知當地居民，該國外銀行所提供之跨界電子銀行產品及服務違反當地之法規及要求；

(d) 採取任何適當的強制性行動。

(39). 當提供跨界電子銀行產品及服務之國外銀行並未受到其所在國家主管機關之有效監管時，當地主管機關就必須承擔起較大的監督責任及風險。當地主管機關得對此類銀行所提供的產品及服務進行限制。

參考文獻

1. 中華民國行政院金融監督管理委員會銀行局之網站 http://www.fscey.gov.tw/mp.asp
2. 美國通貨監理局(簡稱 OCC) http://www.occ.treas.gov/之網站
3. Basel Committee on Banking Supervision, “Risk Management Principle for Electronic Banking”, 2003.07
4. 電子銀行風險管理自律規範，中華民國銀行商業公會全國聯合會金融業務電子化資安小組，九十三年九月編修
5. 金融機構電子銀行業務安全控管作業基準，銀行公會金融業務電子化委員會 2006/01/16 修訂版
6. 電子銀行(e-banking)十四項風險管理原則，銀行公會金融業務電子化委員會
7. 銀行公會監理審查分組第二階段研究工作報告—附錄十六：電子銀行業務風險管理原則，譯者：合作金庫銀行 蔡禎燿
8. Basel II 銀行自有資本之計算與自有資本標準之國際通則：修正版架構 (金管會銀行局/銀行公會/台灣金融研訓院)

第六章、國內外電子銀行業務發展與風險監理之比較

壹、業務發展方面

一、電子支付(e-payment)

以美國為例，對支付電子化係採取市場競爭及監理並存的經濟法則，除了銀行發行的金融卡、信用卡外，連鎖體系或網路業者各自發行的虛擬電子貨幣或儲值卡(Gift Card)等蓬勃發展中，其中金融卡消費佔比為 1/3、信用卡為 19%、電子支票為 9%、企業儲值卡為 4%等，電子化工具逐漸取代傳統現金及支票。即零售業或網路業者為滿足業務交易便利需要，紛紛提供企業體系內支付收付電子化或線上服務。因而，新式電子支付工具的引進及推廣如電子錢包或虛擬貨幣等，可帶動整體電子商務及商業活動之消費能量。並進一步拓展為全球性的支付工具如 PayPal 或 Western Union。

我國 2005 年信用卡佔消費比 20.5%(即約 80%為使用現金交易)，目前已成為國內唯一的主要消費電子支付工具，相對於美國金融卡或企業儲值卡等市場運用，國內應有相對發展空間。如全體銀行集中以信用卡為主要業務主軸，除了無法滿足消費者、零售業及市場多元化的需求外，也間接提高銀行在信用、利率、價格、流

動性、市場、法律、信譽及策略等風險，也會造成金融監理或社會的成本，目前「卡奴」風波或許有其相互關聯性。

二、網路銀行

1. 美國網路銀行使用率於 2005 年達到全美 38%家庭單位使用，部份優質銀行網路銀行戶數已超過 50%如 Bank of America、Wells Fargo、Citibank 等，而歐盟國家如英國、德國等網路銀行戶數亦已超過 50% ，可見網路銀行的交易與通路對銀行業務重要性已不可同日而語。
2. 環顧國外使用率較高的網路銀行，除提供多元化的服務項目及內容外，在用戶系統易於安裝、操作簡易或功能改進等方面，也是決定客戶是否接受新業務的重要關鍵。而企業電子金融在新技術不斷導入之下，功能及應用方面亦持續推陳出新。另行銷策略及後續追蹤改善等皆為提高網路銀行使用率不可或缺。
3. 為避免客戶免於網路銀行線上交易損失的恐懼，銀行可在契約書上載明客戶在無過失之下，銀行負賠償之責，或可透過保險方面降低整體風險。
4. 目前各國優質銀行網路銀行使用率相對較高，並已成為國際化及競爭力的重要領先指標之一。因而，如何提高國內銀行在網

路銀行使用比率，將可列為未來國內銀行發展或應用創新之研究議題。

貳、風險監理方面

各國對電子銀行風險監理採取模式為：

1. 將電子銀行視同銀行業務的一部份，原有法規適用或如有未決事項由法院判決，對電子貨幣或網路支付技術並無直接的監理機制，如加拿大、英國、瑞士等。

2. 為避免過於詳細的法規，反而因技術發展的階段而產生反效果，採取電子銀行不需要經過事先的許可，惟納入監理範疇如德國、香港等。

3. 採取嚴密的監控，並適切的評估這些發展所衍生之風險面及效率面者如日本，惟為避免對整體支付系統的交易量、交易總值及本質造成系統性的影響，目前尚未制定相關法規。美國聯邦銀行當局不斷更新、改進現行的銀行檢視程序，以納入考量電子金融的發展及其相關之風險。

4. 目前我國現行法令規章對電子銀行風險管理或安全已訂定相關準則或規範，供銀行業自律之參考，至於所採取監理的模式似乎比較傾向中立的角色。

第七章、結論與建議

銀行是否能穩定的成長與營運是各國銀行監理單位所重視的，尤其電子銀行與銀行未來發展密不可分，而風險控管的目的在於做到事前防範，提昇銀行經營效能及降低損失。本研究比較國際先進國家之電子銀行業務發展及風險控管，認為我國於風險監理規範的完整性與涵蓋面不亞於國外之規範。因此除主管機關法制規範及監理制度外，首要強化銀行高層重視電子銀行業務發展之趨勢，並建立銀行內部風險控管文化及觀念，尤其董事會及高階管理階層應體認這是責無旁貸的責任，並提高全機構員工的警覺心，出錯的機率自然降低。

金融監理機構監理的目的，在於穩定金融、強化銀行及金融市場效率及競爭力，並保護消費者免於銀行經營不善或不當而受害。因而在電子商務快速變化下，對於電子銀行業務或作業所訂定各項法規或基準，如以風險管理為唯一考量，可能會扼殺銀行業務發展之契機。所以，如何設計一套符合電子商務及市場多變的需求，又同時能兼顧銀行服務效能及安全的監理制度，並以務實的態度解決彼此之間的衝突，將是未來必然面對的挑戰。

茲將本研究之相關建議以及未來研究方向分述如下。

一、網路銀行業務發展

近年來國內外網路銀行業務持續快速成長，特別是客戶使用線上交易的比率不斷成長，數據指出 2005 年美國 38%家庭使用網路銀行交易，預計今年將達到 40%。根據本研究結果顯示，我國網路銀行使用率與美國差異的主要原因，除了地理環境與文化上的差異外，主要係因為國人使用網路銀行進行線上交易，對資訊安全方面信心仍不足。其次是我國網路銀行對企業電子金融或理財服務等服務仍待加強。再者，國內銀行整合帳戶服務(Aggregate Account)仍處於規劃或建置中的階段，尚未能提供以顧客需求導向設計產品並發揮共同行銷(Cross Selling)之效益。此外，美國網路銀行所提供的服務項目、服務內容、使用者操作介面、通路整合及後勤支援(客服中心)等方面，其優點亦值得作為我國網路銀行業務規劃或發展之參考。

有鑑於此，為期我國網路銀行業務之良好發展，本研究提出以下值得進一步探討之議題，供未來規劃網路銀行走向之參考。

1. 國內銀行對資訊作業委外顧慮尚在，造成技術服務能量未能滿足環境變遷或顧客快速回應的需求。因此建議強化資訊服務業者之專業知識及技能，以提升資訊服務業者之能量。

2. 為消弭使用者使用電子銀行之焦慮及增強信心，可試圖研擬出銀行在有條件下承擔顧客的損失，或透過保險方式在某限額之下予以理賠。

3. 為落實銀行與企業金流系統整合，有關企業端系統之建置如各產業「資金管理系統或平台」，可試圖研擬提供補助誘因，委託公協會結合資訊服務業者負責推動，藉由企業帳務自動化，加速簡化收付流程，並提高企業電子金融業務之發展。

4. 為強化我國企業金融ｅ化研發及供給能量，可試圖研擬以輔導或補助等方案，加速資訊服務業者對系統研發、人員培訓及應用推廣等持續投入，俾健全金融產業供需鏈ｅ化體系。

二、電子銀行風險控管

在電子銀行風險管理方面，我國除了應遵守巴賽爾銀行監理委員協議外，目前銀行公會等所訂定之相關電子銀行作業基準、安控準則或自律規範等，可作為現階段國內銀行在規劃電子銀行系統或風險控管之參考。

依據國外相關作法，以下幾點值得我們參考：

1. 鼓勵銀行服務創新並勇於承擔風險,以公司治理的方式由董事會承擔最終的責任，並以管理風險模式積極開拓新局。
2. 以資訊科技治理建構資訊作業安全及管理架構,鼓勵銀行採行國際 BS7799、COBIT(Control Objectives for Information and Related Technology)、ITSM 等資安認證、科技控制及服務管理等運作模式，以降低系統風險及確保服務品質。
3. 強化員工相關管理技能及加強訓練，並鼓勵取得國際專業證照，或聘請外部專家進行風險評估。
4. 電子銀行風險控管與科技應用演變息息相關,在科技快速變化之下,政府機關、金融業或公協會等應持續就相關議題加以研究及宣導,俾使國內銀行在電子銀行風險控管技能上與世界並駕齊驅。

三、國內小額消費付款

國內小額消費市場廣大，約佔整體消費總金額 80%，本研究針對國內小額付款需求，提出以下值得進一步探討之議題：

1. 為迎合電子商務發展新需求,非銀行業者提供小額第三者支付服務方興未艾，如日本 SONY　BitWallet 公司 Edy 卡或美國

PayPal、SpeedPass、Western Union 等，如何在滿足國人小額消費市場之殷切需求之下，並能達成監理階段目標，值得探討。

2. 為提高我國消費支付體系電子化，可研究聯合政府、銀行及民間企業等力量，共同導入我國晶片金融卡或小額支付工具之消費應用，或藉由國內便利商店普及與行銷優勢，加速打開我國支付電子化發展之瓶頸。
3. 為提供無銀行戶頭大眾便利需求，國外零售業或連鎖體系所開辦店對店之現金匯款或解款、代理政府發放津貼或提供小額外幣現金兌換等金流服務議題，亦值得探討。

最後感謝工作期間金管會銀行局、中華民國銀行公會、台灣金融研訓院、財金資訊公司、政治大學商學院、安侯企業顧問、IBM、台灣優利公司、台灣微軟、銀行界先進及評審委員等機構及專家之協助與指導，並提供寶貴資料與意見，如沒有各位先前累積的知識，本報告就無能量可言。惟本研究團隊礙於能力及時間有限之下，使本報告未盡理想或不足之處仍多，尚請業界先進持續不吝予以匡正及指導。當然，本報告中所提意見或建議，皆為本研究團隊各自看法，**並不代表委託機關之立場**。