台灣金融研訓院
Taiwan Academy of Banking and Finance

105 年自提研究計畫

銀行業因應網路金融發展之風險監理及稽核研究

補助單位：中華民國銀行商業同業公會全國聯合會

計畫主持人： 何宗武

顧　　問： 盧陽正、張麗珠、王志誠

共同主持人： 林士傑、賴建宇

協同主持人： 張凱君、林盟翔

研　究　員： 戴郁文、蘇秋惠

中華民國 105 年 11 月

財團法人台灣金融研訓院自提研究計畫

銀行業因應網路金融發展之風險監理及稽核研究

補助單位：中華民國銀行商業同業公會全國聯合會

本報告內容純係研究團隊之觀點，

不應引申為補助單位中華民國銀行商業同業公會全國聯合會之意見。

計畫主持人： 何宗武

顧　　問： 盧陽正、張麗珠、王志誠

共同主持人： 林士傑、賴建宇

協同主持人： 張凱君、林盟翔

研　究　員： 戴郁文、蘇秋惠

中華民國 105 年 11 月

摘要

本研究首先分析銀行傳統風險在網路金融業務之延伸，並探討金融科技趨勢下，創新網路金融業務帶來之新種風險類型。其次，研析歐美、亞洲、中國大陸及我國等主要國家，其新興網路金融業務之法令規範及監理架構。最後，再就銀行業因應網路金融業務之風險監理，以國際金融科技監理環境之趨勢為導管，提出網路金融資訊安全之偵測與預防，以及稽核措施與監理要點之見解，進而對我國銀行業與主管機關提供具體建議。我國面對 FinTech 趨勢雖步調較慢，但其全球化特性促使我們積極因應，如金管會仿照英國及新加坡，於 2015 年 9 月成立金融科技辦公室，並參酌監理沙盒制度提出「領航計畫」，目的致力於全面發展包括數位金融、機器人理財、大數據應用、雲端及物聯網建設等，結合金融與科技之創新金融服務。

誠言之，在數位金融時代下，銀行業面臨之競爭不僅來自於同行業內部，外部挑戰亦日益嚴峻，特別是擁有網路、電子商務等技術之新興企業，其在創新能力、市場敏感度、數據處理經驗等方面均較銀行業具有明顯優勢。但透過網路科技進行金融業務之創新，同時伴隨著風險之發生，包括政策風險、監理風險、法律風險、交易風險、技術風險及信用風險等類型，除了對網路金融企業或客戶本身產生直接影響，其風險亦可能傳導至傳統金融行業及實體經濟，此時稽核部門或制度是否可適時提出風險查核結果並向董事會報告，顯得格外重要。鑒於金融監理係以消費者保障與法令遵循為兩大核心任務，爰本研究以研究成果提出綜合具體建議如下。

（一）密切注意國際相關網路金融之監理措施可能發展之新方向。各國較缺乏有關網路金融業務之配套法規，為普遍存在之情況，且在網路金融交易者身份之認證、電子合約有效性確認等方面，時常面臨權利義務之糾紛，以致對網路金融交易雙方產生不確定性，而增加網路金融交易成本。爰建議金融機構應密切注意並預應國際網路金融監理措施可能發展之新方向，以完善各項內部基礎建設及準備工作予以因應。

（二）以風險導向概念引導內部稽核策略規劃。由於市場風險對網路金融交易者之資產、負債及損益變化，以及金融衍生工具交易帶來之風險等，在網路金融

交易中均受有影響，未來銀行基於強化內部資訊安全之內部控制，以及承作網路金融商品及服務業務之特殊性，應考量以網路金融及金融科技風險導向概念，引導銀行內部稽核作業執行及策略規劃，應建立相關作業措施。

（三）銀行業加強稽核暨風險查核部門任務重要性。以風險為基礎之查核策略，由各銀行業務經理人確認業務風險並建立控制點，維持有效監控並確保可及時更正已確認之缺失。而稽核暨風險查核部門應先辨識緊急風險及趨勢，有效說明並承擔管理上已發現缺失，並建議由資訊部門、策略暨支援部門、政策法令遵循部門共同執行該項任務。

（四）落實業務單位對網路金融客戶實名認證之內部稽查工作。隨網路及行動金融業務之普及，線上及行動支付成為電子商務市場競爭焦點，如網路支付身份未進行實名認證，非實名支付可能成為網路金融犯罪之來源，為避免客戶在網路支付業務中發生如資金盜領、個資洩漏、洗錢犯罪等風險，須及早因應落實業務單位對網路金融客戶實名認證之內部稽查工作。

（五）以風險導向稽核建構對網路金融業務內部控制三道防線。內控三道防線攸關金融機構有效自我管理及長期健全經營，為提升管理水準，要求金融業仿照公司治理運作，依其機構規模與業務複雜性，訂定明確最佳運作範本，未來主管機關將透過實地檢查要求機構妥善建置。

（六）風險導向監理檢查機制強調持續性監理。導入風險導向監理檢查機制時，應設立各專業檢查小組，以增進監理人員對整體營運管理模式之瞭解，並定期聚集研討分享檢查技巧及業者作法，建立監理資訊交流分享平台。如係透過場外監控須產出相關監理報告，促使檢查人員取得各銀行業務監理資訊，以利檢查前風險評估及檢查重點篩選。

（七）以個案模擬試作研討方式，訓練監理檢查人員管理評估及查核能力。因檢查人員專業訓練與一般金融人員不同，除了金融業務與商品專業知識外，尚須具備金融機構整體營運與風險管理品質之評估能力及實務查核技巧，如期望透過訓練課程提升相關能力，以個案研討與模擬試作係較佳之方式。

（八）落實銀行業建立資安演練機制，評估定期檢討更新網路應用程式。例如資安防駭之演練，係模擬資訊系統遭駭的知況為主，以及數位證據之蒐集與封存演練、模擬遭駭後系統證據之蒐集、封存與初步分析過程等，作為提升金融機構資安人員面對駭客入侵之應變策略。然金融交易背後需有複雜、費時之軟體開發週期，通常應用程式更新係錯誤修正，新功能增加約每年兩次。雖更新網路應用程式有其成本，但金融業者應評估成本效益後執行，定期檢討是否更新網路應用程式之必要性。

（九）採行網路金融「風險為本」、「科技中立」及「降低監理成本」監理原則。在制定及執行監理架構與規範時，係根據金融活動或交易本質及其衍生之風險作為基礎，但網路金融業務監理雖以風險為本，但應考量以不阻礙金融科技發展為原則。故依據科技中立原則建立監理原則，促使市場參與者可在有利創新及公平競爭之環境下營運。另金融監理機關、中央銀行、財政部，以及金融、電信、金融科技業與金融消費者保護機構間，應維持協調機制，藉由金融機構風險內部控制自律及市場紀律，可達成降低監理成本目標。

（十）要求銀行業應確實控管客戶整體信用風險。銀行業建立社群分析可補強銀行信用分析不足，降低信用風險，且銀行辦理網路金融金融商品業務，應落實銀行商品銷售控管及風險管理制度，並確認商品與客戶承擔風險能力可適切配合，以避免產生金融消費爭議，甚至遭受到主管機關嚴厲裁罰，影響銀行聲譽及業務之發展。

（十一）銀行業應定期衡量、監控及資訊管理系統。開發新型網路金融商品或作業程序重大改變時，除了辨識及評估風險外，須有法律、稽核、行銷、資訊安全、營運及主要業務人員參與。故銀行在開發網路金融風險指標時，須聚焦於最重要風險須定期驗證，董事會及高階經理人應定期收到作業風險報告並設計妥適風險指標。

（十二）銀行業應提升資安治理之管理層級。資訊安全不僅在營運作業層面，應與銀行業發展策略息息相關，過去資安非經營作業需面對之風險，而為資訊

部門之職責，但自 ATM 盜領事件發生後，銀行業之風險觀念應調整，思考將資安納入 KPI 管理指標。爰建議董事會應要求高階管理階層，定期評估網路安全控管之適當性，包括緊急網路威脅因應，以及建置可信網路安全控管基準。

目錄

表目錄

圖目錄

第一章　前言

第一節　研究目的

網路金融係網路與金融之結合，連結網路技術及行動通訊技術，而達成資金融通、支付及資訊仲介功能之新型金融模式。網路金融就本質上而言，仍是金融服務，僅是借助網路技術及行動通訊技術發展而產生之創新金融發展模式，目前主要網路金融模式，包括網路支付結算、網路理財、網路貸款、網路證券、網路保險等金融業務。網路金融交易之雙方均透過網路進行金融交易活動，網路金融交易平台之提供者，可分為金融機構與非金融機構二種，前者係以網路銀行提供網路金融服務；後者則結合資訊通訊科技，提供線上網路金融服務，經營之業務包括「支付」與「投、融資」兩大類。

在網路金融發展過程中，將使我們面臨不同於傳統金融之新型風險，故如何同時兼顧便利性及安全性，一直是業者執行業務之大課題。不可諱言地，在網路金融時代來臨之今天，銀行必須面臨業務型態變革衍生之風險控管問題，而另一方面，主管機關亦須適時訂定相關規範及稽核監理原則，促使網路金融業務得以健全發展，為避免兩者相互制約，研究網路金融風險之種類、原因及特色，建立網路金融風險之防範及管理機制，對未來我國銀行業發展健全及完善之網路金融業務，可謂至關重要之課題。

第二節　研究重點

（一）整理分析銀行網路金融之業務模式，以及其與傳統銀行業務所面臨風險之異同，並探討因應大數據、雲端計算可能引發之風險控管與監理問題。

（二）整理歐美、亞洲、我國及中國大陸等網路金融之風險監理法律規範，以及適用網路金融風險之稽核原則及監理架構，並對目前我國監理法令及稽核實務之影響加以探討。

（三）金管會為提升 Bank3.0 之成效，不僅將 2015 年訂為「行動金融元年」，並啟動開放 e 化十二項銀行業務項目，本研究亦將對銀行 e 化業務項目研究其所可能產生之網路金融風險。

（四）配合實地訪查，以取得國內外業者對網路金融新種業務之興起發展及可能產生之風險等資訊，並徵詢對後續可能持續增加之稽核、監管規定與法律規範走向之見解。

第三節　研究方法及預期成果

一、研究方法

（一）文獻分析法

蒐集整理及分析國際間網路金融風險之法律規範及稽核原則，以及金融監理機關之監理規定等重要議題文獻，並參酌專家學者之學術論著、相關主題研討會之意見等，進行綜合歸納分析，以求對各研究面向進行充分之瞭解及掌握。

（二）比較分析法

透過前述蒐集整理國際網路金融規範及監理原則等文獻，針對主要國家進行跨國比較，包括發展模式、監理措施、法律規範等，並配合因應金融科技之法規及制度調整，以求對我國銀行業在因應網路金融發展之參考。

（三）實地調查法

對銀行因應網路金融業務發展過程中，可能面臨之法令規範適用、監管制度規定、實務運作及內部稽核問題等，並透過與專家訪談、實地訪查及召開座談會等方式深度拜訪，聽取銀行業者、網路金融公司之意見，實際瞭解其對相關議題之處理看法及因應對策。

二、預期成果

（一）網路風險種類及與傳統風險異同之處，包括法令、技術、作業、道德、流動性、犯罪等風險。

（二）國際上銀行對網路金融風險之管理經驗及相應法律規範、適用之監管架構及後續稽核模式，對現行法律法規及解決機制之影響，金融體系革新監管態度及因應對策。

（三）歸納整理各國經驗，以及與傳統銀行融資在風險面及監管面之差異，提出銀行網路金融風險管理及防範措施之建議。

（四）網路金融業務新種風險將對下列研究內容進行研究：

1、新資訊科技帶來之作業風險問題。

2、消費者權益相關之風險問題。

3、異業結合之關聯性風險問題。

4、雲端計算、大數據對網路金融服務之資安保護衝擊 。

（五）未來銀行業網路金融風險對新種業務之發展影響，包括社群、電子支付及電子商務等，彙整作為各界瞭解網路金融及相關法律規範之參考，並妥適提出研究結論，以及主管機關與我國銀行業之具體因應建議。

第二章　網路金融及風險種類之發展

開發網路金融業務促使金融業者之營銷成本下降，銀行客戶申購金融商品或服務所需花費之時間減少，金融市場之供需雙方得以獲益。惟另一方面，伴隨著網路金融業務而來之各項風險，同樣不可不察，亦即網路金融快速發展帶來經濟社會之變革，同時在一定程度上引發了新挑戰與風險。而該挑戰及風險既有傳統金融理論架構下之支付清算風險、金融創新對中央銀行貨幣政策挑戰，亦有異於傳統金融模式之資訊風險。唯有掌握網路金融之風險類型與特點，始能對其進行有效之識別、界定並建立動態及前瞻性之預警、監測，從而保證金融體系之安全有效運行。本章主要從網路金融模式對支付清算、提供價格資訊、風險管理功能之影響等出發，透過對網路金融模式之資訊風險、道德風險、作業風險及流動性風險之觀察，識別當前網路金融模式在我國可能面臨之挑戰及風險。

第一節　銀行傳統風險種類在網路金融業務之延伸

「網路金融業務」仍是一種金融業務，且多數業務早於網路出現之前，即已存在，僅是營運之形式不同，該類金融業務挾帶之風險，其本質上並未因網路之使用而消失，特別是部分風險可能因此被放大。本節本研究先檢視銀行傳統業務面臨風險在網路金融之延伸。金融交易雙方，原本即存在包括信用風險在內、因訊息不對稱造成之風險，但此一風險在網路金融世界中以不同面貌出現。與傳統金融服務相比，網路金融中一切業務活動，如交易資訊傳遞、支付結算等，均在由電子資訊構成之虛擬世界中進行，因此金融機構之物理結構、服務網點等實物資產之重要性大幅降低。得益於網路金融服務方式之虛擬性，交易雙方不需直接見面，僅透過網路進行交易，如此雖可克服地理空間之障礙，但亦使得對交易者身份、交易真實性之驗證難度增大。換言之，交易者之間在身份確認、信用評價方面之資訊不對稱程度提高，進而導致資訊風險加劇。

為分析方便起見，網路金融商業模式大致上可簡化成「支付」與「投融資」兩大類概念。支付（指資金流通）類的商業模式旨在使資金流通更便捷安全，如虛擬貨幣與第三方支付；而投融資類型的商業模式旨在媒合有閒置資金者與需要

資金者，使放借款更便捷，如 P2P 網路貸款與群眾募資。金流、物流及資訊流三者之結合，促進電子商務及網路貸款業務之發展，又出於資金流對支付之便捷性要求，第三方支付平台亦應運而生。一方面，第三方支付平台為買賣雙方整合眾多銀行，提升買賣雙方支付之便捷性，二方面第三方支付平台為銀行整合零售電子商務、小額信貸之結算業務，大幅節省銀行之行銷成本，然第三方支付平台之資金運作不易監管，形成無法掌控之風險。

首先，就交易過程而言，供需雙方在完成交易前，須在第三方支付平台上開設帳戶，資金支付僅經由公正之第三方支付平台始得流轉。而在資金調撥過程中，雖依舊無法脫離銀行業之服務，但就業務性質來看，第三方支付平台已從事與銀行結算類似之業務。而當第三方支付平台扮演起銀行業在電子商務中，中小規模之支付結算業務後，作為支付仲介之一般存款帳戶，實際成為銀行無法控制之內部帳戶。

其次，在網路金融模式下借貸平台之資金轉帳過程中，資金並非是由出借人之帳戶直接轉入借款人帳戶，而是須透過網路平台方能流通，過去多數網路借貸平台係經由第三方支付之形式完成。誠言之，網路借貸平台具有匿名性及即時性之特點，監管部門對網路金融模式下資金流向之追蹤更加困難。與傳統商業銀行之借貸不同，網路借貸係在借款人及放款人間直接進行，屬於直接融資而非間接融資領域。其中協力廠商平台僅發揮撮合交易作用，而不直接從事借貸活動，故並不屬金融機構，由於該交易未有金融機構之直接參與，通常借貸額度不高，亦缺抵押擔保，本質上可謂一種信用借貸。而信用借貸即意味著風險主要係由借款人承擔，雖在網路借貸模式下，憑藉平台累積之註冊資料、銷售額金流及歷史成交記錄等資訊，可為放款人提供一定程度之借款人資訊，但仍無法完全消除借款人之信用風險。

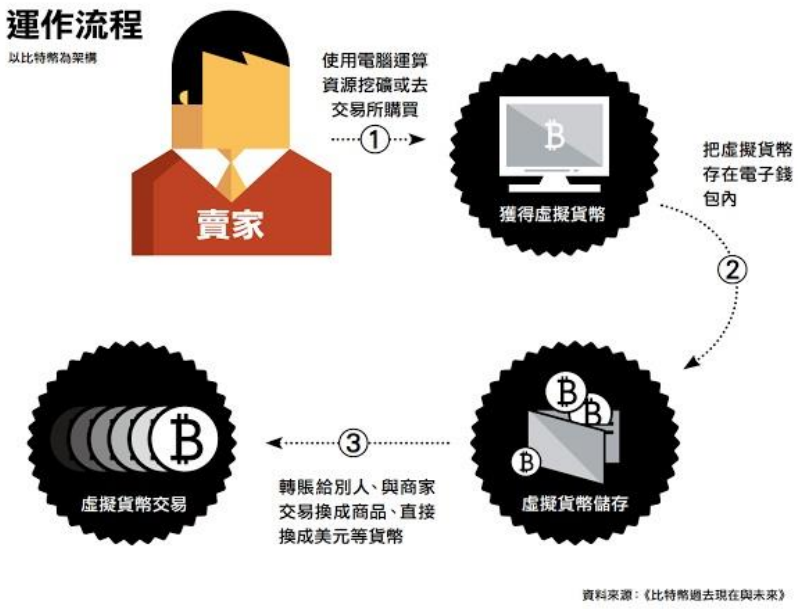


圖 2-1：虛擬貨幣交易示意圖

資料來源：整理自數位時代。

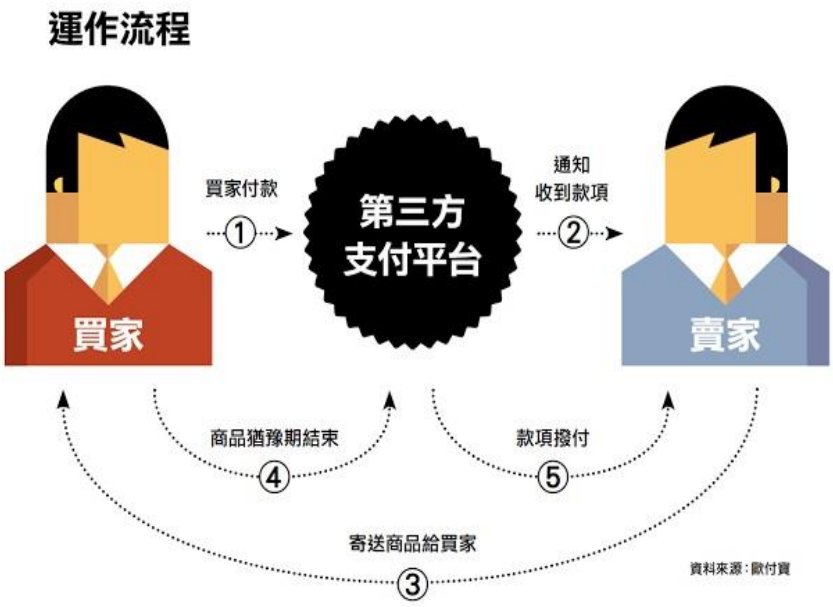


圖 2-2：第三方支付示意圖

資料來源：整理自數位時代。

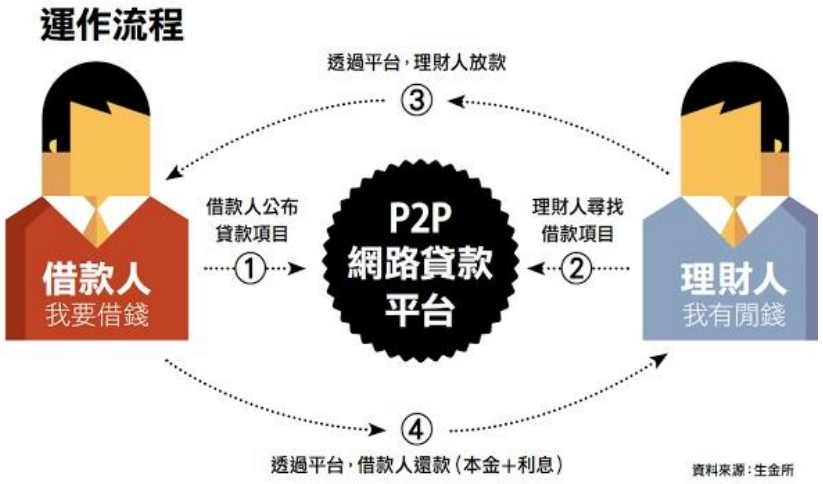


圖 2-3：P2P 網路借貸平台示意圖

資料來源：整理自數位時代。

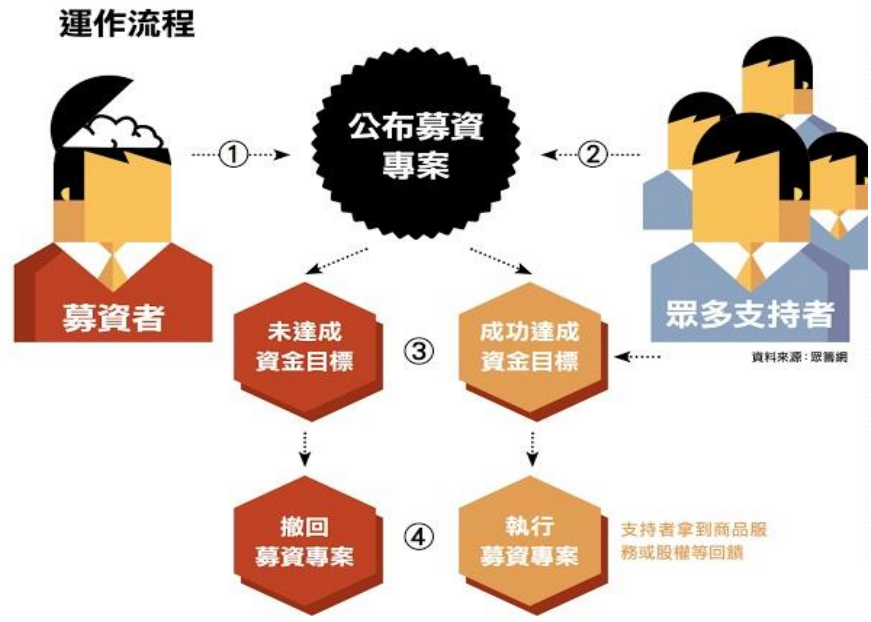


圖 2-4：群眾募資示意圖

資料來源：整理自數位時代。

對 P2P 網路借貸而言，其一，網路借貸企業或個人無法經協力廠商取得借款人客觀之信用歷史資料，但如借款人之徵信記錄、財務狀況、借款用途等資料無法充分取得，僅憑藉借款人自身提供之基本資料，難以建構客觀且全面之信用評級體系。其二，在各網路借貸平台資訊相互隔絕之情況下，一家平台對借款人進

行審核時，無法得知該使用者是否在其他網路借貸平台亦申請貸款，若一旦借款人故意隱瞞相關資訊，而審核人仍按照正常流程審核並放出貸款，即可能形成不可避免之風險。再者，對電商小貸而言，儘管可根據自身累積之使用者交易，售後及客戶評價等資訊對貸款申請者進行有效之信用評估，但該模式仍無法有效降低借款者之信用風險。如以電商信用體系建立之機制來看，歷史交易記錄未能充分類比及預測未來，貸款申請者亦可透過製造虛假交易、提高交易頻率及取得更多好評提高其信用評價，在信用體系中偽造出較高之信用評級，進而獲得信用貸款與交易之優勢。

應注意者，由於網路金融業務及服務提供者具有顯著之虛擬性特徵，以致在交易者身份之確認及信用評價等資訊方面，容易產生明顯之不對稱性。且在實際業務中，出借人無法對借款人之資金使用情況進行有效監控，而網路借貸平台亦不如商業銀行對貸款之使用進行審查，因此借款人可能隱瞞部分資訊，而有不利網路金融服務提供者及放款人之決策，從而使得放款人在選擇客戶時，處於更加不利之地位。此外，隨著網路金融與金融科技日益發達，資料總量爆發式增長，在帶來資料採擷與分析便利之同時，亦加劇金融市場之資訊不對稱程度。就觀察而言，資訊收集成本之提高，包括軟硬體設施在內之前期投入，可謂資訊收集之第一項成本，雖資訊技術之發展將記錄、存放裝置之價格變得不再高不可及，但對一般企業或個人，該資訊收集之前期成本不可忽略，而除了有形成本外，資訊之收集亦需付出相當時間。

誠如前述，大數據之形成需要一定時間累積之過程，在網路金融之資訊收集領域中，最先進入者即擁有先動之競爭優勢。如阿裡巴巴雖於 2003 年成立，但直至 2013 年始開展互聯網金融業務，其中一項重要之原因即是商業資料之時間累積。故阿裡金融之所以雖被普遍看好但難以複製之關鍵，在於其累積大量先動優勢，後進者如要重新累積消費者交易與信用資料，相當困難。不可諱言地，資訊時代到來使得社會間資訊溝通之規模及速率增強，但並不意味著，有用資訊之取得可變得更為迅捷及容易，主要原因在於網路資訊具有之無限性、廣泛性、廉價性、共用性、無序性等特點，在使用者在取得有用資訊之同時，亦會被大量之

虛假資訊、無用資訊所幹擾。換言之，資訊大爆炸造成資訊環境污染及噪音資訊之蔓延，增加民眾識別、判定及利用有效資訊之困難。

整體而言，資訊解讀技術之要求不斷提高，亦是當前數位化時代之產物，其增加取得有效資訊之難度。一般而言，透過傳統搜尋引擎所得之資訊，僅是網路之表層資訊，層次更加豐富及專業之深層資訊，通常儲存在網路檢索介面而無法觸及之後端，包括 Access、Oracle、SQL Server、DB2 等資料庫，該部分資料之讀取須使用網站之搜索工具進行直接互動式查詢。由於當前搜尋引擎之資訊抓取程式仍不具備在互動式檢索表單中填寫，或選擇所需欄位資訊之能力，並無法向資料庫提交檢索關鍵字，因而具有價值之資訊對使用者來說，無法直接得。與此同時，資訊在網路中具有傳播速度快、範圍廣之特點，使得金融資產價格亦更加容易受到網路突發資訊之影響。總言之，網路金融脫胎於傳統金融發展模式，故沿襲傳統金融之本質特徵，但不同之處在於，網路金融模式借助網路之力量分散及化解部分風險之同時，亦透過傳導效應放大另一部分之風險。

第二節　銀行網路金融新種風險研析

網路金融具有新型風險特徵，且風險類型更加多樣，其中以技術風險或作業風險最為突出。金融業務與網路技術結合後，帶有網路特色之技術風險，亦隨之而來，包括終端安全風險、平台安全風險、網路安全風險等，其中終端安全風險主要係指進行網路金融交易之電腦、移動設備等存在漏洞而帶來之風險，而平台安全風險是指網路金融平台存在之安全威脅，所謂網路安全風險，則係網路金融交易依託數據傳輸網路帶來之隱患。不可諱言地，技術風險帶來最大問題即資訊安全問題，包括技術之不成熟，可能導致資訊洩露、丟失、被截取或篡改而影響資訊保密性、完整性及可用性，進而威脅用戶之資訊及資金安全。隨著資訊技術之發展，作業風險之發生高頻率及其產生之重大影響，使其開始受到民眾廣泛之關注，正因如此，巴塞爾資本協議之兩次修訂，不僅將作業風險放在相當重要之篇幅，且新巴塞爾協議中，對作業風險之資本補償更作出明確之規定。

依據新巴塞爾協議，作業風險係指由不完善或具有問題之內部程式、人員及系統或外部事件所造成損失之風險。就其定義上來看，所有金融仲介及金融市場之內部程式，在任何環節出現之問題、相關業務人員有意無意之疏漏等，均係屬作業風險之範疇。在大數據時代中，對系統安全性及穩定性提出更高之要求，如需要企業建立有效之防範控制體系，以減少由於人為操作或系統缺陷，而導致之問題，同時避免因系統延遲、癱瘓造成之資訊遺失，以及資訊堵塞導致交易失敗及客戶財產損失，外部事件則包括駭客集團之惡意攻擊導致系統癱瘓、資訊洩露等，一系列危害金融機構安全性及金融穩定性之事件。由於網路金融模式根植於網路，隨著網路技術之發展，網路金融企業資訊技術部門須隨時應對可能出現之駭客攻擊、資金盜用、資訊篡改及竊取等行為。

有效防範及控制作業風險之前提，在於掌握作業風險之來源，然作業風險之涵蓋內容廣泛，且在不同網路金融模式下，即會產生不同形式之作業風險。如以第三方支付為例，因中國大陸電子商務交易之蓬勃發展，促進第三方支付業務之興起，為企業及個人用戶提供便捷、簡易之支付交易功能；但與此同時，第三方支付業務亦暴露不少風險。中國銀監會 2009 年 3 月發布《關於「支付寶」業務的風險提示》明確提出五大風險，包括第三方支付機構信用風險、網路駭客盜用資金風險、信用卡非法套現風險、發生洗錢等犯罪行為風險及法律風險。而在該五大風險中，網路駭客盜用資金風險及信用卡非法套現風險，均係屬作業風險之範疇，事實上，作業風險主要來自於技術安全及資訊真實性兩大層面。

另一與技術風險相關之議題則是虛擬貨幣。根據歐洲中央銀行之定義，虛擬貨幣係一種未經監管之數位貨幣，該數位貨幣之發行及流通，一般均由其開發者控制，並在某一類特定之虛擬社群（virtual community）中，被廣泛接受並流通使用。就虛擬貨幣與實體經濟之關係言，虛擬貨幣可分為三類：第一類是封閉之虛擬貨幣體系，主要應用於網路遊戲（如虛擬道具及裝備之購買）；第二類虛擬貨幣係單向之資金流動，通常對虛擬貨幣之購買已有兌換比率，主要應用於虛擬商品與服務之購買；第三類虛擬貨幣則有著雙向之資金流動，在該情況下之虛擬貨幣與中央銀行發行之貨幣無實質區別，可用於真實商品與服務之購買，比特幣

（Bitcoin）即是第三類虛擬貨幣之典型代表，隨著第三類虛擬貨幣日益成熟，與其相關之網路安全問題亦逐漸引起關注。

在網路金融模式下，其內部各部分之風險權重相對傳統模式有所不同，其中由內部程式及系統造成之損失風險，較傳統模式上升，須在監管時予以重視。以商業銀行為代表之信用創造機構及借款人之相關特性，使得金融體系具有天然之內在不穩定性，隨著經濟週期之進展，現實經濟中，冒險融資之行為增多，任何打斷信貸資金進入生產部門之事件，均有可能引起一連串之破產，最終一旦導致金融機構破產，勢必引發另一起金融危機之出現。再者，在經濟繁榮時期，隨著中小企業融資需求加大，傳統商業銀行體系難以滿足中小額貸款之需求下，更多民營資本進入網路金融平台，滿足中小企業之資金及擔保需求，但如該情況由於作業風險引發信貸資金之投放或使用不當，具有缺陷之融資機制設計，可能導致資金周轉困難甚至資金鏈斷裂，進而造成金融體系局部之不穩定，並在金融部門之間傳導。

Diamond 與 Dybvig（1983）認為，銀行是金融仲介機構，其基本功能係將不具流動性或流動性較差之資產轉化為流動性強之資產，但因銀行之負債及資產在時間、數量上不對稱，在面臨信貸風險時，如各類準備金總和低於同期貸款之損失，銀行即失去清償能力[1]。在網路金融時代，許多信貸服務類企業正扮演著商業銀行此一仲介機構角色，儘管該網路金融仲介機構，在功能上彌補傳統商業銀行不足，但亦面臨及承擔與商業銀行類似之風險，且其面臨之資金供需雙方之不穩定因素較傳統商業銀行更多、更難以預測。換言之，如其由於作業管理不善及資訊系統漏洞而導致作業風險，則可能帶來更大之恐慌而引發擠兌風潮。不可諱言地，隨著網路金融模式之發展，不難看到金融工具、金融機構及金融市場將不再是簡單之數量加總，而是相互間有機之結合，一旦某一環節產生風險，且無風險隔離與保險制度之設計，風險相當容易傳導至其他網路金融業務中，甚至是放大至整個金融體系。

[1] See Douglas W. Diamond and Philip H. Dybvig, "Bank Runs, Deposit Insurance, and Liquidity", *The Journal of Political Economy*, Vol. 91, No. 3. (Jun., 1983), pp. 401-419.

整體而言，由作業風險暴露金融工具、金融機構及金融市場之脆弱性，可能帶來更大之損失，但如企業及監管部門有效防範作業風險，建立良好之協調運作機制，則有可能借助網路金融平台，分散或吸收風險，並將損失減到最小，進而降低整個金融體系之脆弱性。換言之，確保金融之穩定方能保證金融機構、金融市場之健康發展及金融體系運行之效率，從而促進金融服務實體經濟。誠言之，就網路金融與實體經濟關係來看，網路金融不僅是豐富金融產品，由於網路技術之發展與普及，該模式可使得普羅大眾以較低成本，享受金融服務所帶來之便利及便捷，協助企業部門有效籌措及運用募集資金，但相對而言，傳導途徑亦更加多元及複雜，甚至可能產生間接管道之溢出效應，且金融風險對融和實體經濟之穩定性亦因變得更加複雜。隨著網路資訊技術之日新月異，以及金融產品與金融服務之不斷創新，金融風險勢必會逐漸增多。

接下來我們以去年（2015）底中國大陸爆發「e 租寶」詐騙事件為案例，管窺網路金融興起後，層出不窮之新風險模式。金易融（北京）網路科技有限公司於 2014 年 2 月經工商局註冊成立，註冊資本金 1 億元人民幣，隸屬於鈺誠集團，而鈺誠集團於 2014 年 7 月改造該平台並命名為「e 租寶」，以「網路金融」旗號上線營運，曾被中國新聞社中國新聞周刊評為 2015 年中國大陸「最有責任感」網路金融企業之一。「e 租寶」平台採用首創 A2P 模式，即資產對個人（Asset to Peer），意即融資租賃業務中形成的融資租賃債權資產，通過網路金融平台轉讓普通投資者。該種以融資租賃債權轉讓為基礎之網路金融服務模式，係屬於網路金融領域之一種創新模式，該平台推出六款投資產品，如 e 租財富、e 租穩盈、e 租年享、e 租年豐、e 租富盈、e 租富享等，其中五款產品預期年化收益率超過 13%。所有產品均為融資租賃債權轉讓，存款期限分為 3 個月、6 個月及 12 個月，贖回方式分「T+2」和「T+10」兩種。

但在 2015 年 12 月 3 日，e 租寶深圳寶安分公司突遭偵查，12 月 8 日官方網站與手機應用已無回應。到 12 月 16 日，廣東省公安廳發布通報，稱各地公安機關均已對 e 租寶及其關聯公司涉嫌犯罪問題依法立案偵查，涉案資產亦被查封、凍結、扣押。事證顯示，e 租寶事件屬「龐氏騙局」，即不靠「計畫」、「項目」、

「產品」賺錢，而是以高利息為誘餌，靠不斷發展下線來賺錢。經統計至 2015 年 12 月 8 日，e 租寶總成交量為 745.68 億元人民幣，總受騙投資人數 90 萬 9 千 5 百人，待收總額 703.97 億元人民幣。2016 年 1 月 31 日，中國大陸官方媒體新華社披露，「e 租寶」非法吸收資金 500 多億元人民幣，受害投資人遍布中國大陸各地區。據報導稱，「e 租寶」的分支機構遍布全國，涉及投資人眾多，且公司財務管理混亂，經營交易數據量龐大，僅需要清查的存儲公司相關數據的伺服器就有 200 餘台。

第三節　銀行網路金融業務風險未來發展

由於科技持續創新及金融機構間之激烈競爭，許多銀行均透過數位管道銷售商品或提供服務。鑒此，巴塞爾銀行監理委員會（BCBS）撰擬一份題為「電子金融之風險管理原則（Risk Management Principles for Electronic Banking）」之技術報告，該報告中，就電子金融彙整相關風險管理原則共計十四項，並分為管理高層監督、安全性控制、法律與信譽風險管理等三類。其中董事會與高階經理人肩負銀行發展商業策略，以及建立有效風險管理機制之責任，對銀行是否要承作某項數位金融業務及如何承作，自應有明確而完整之想法，且在決策之初即應對相關風險之究責制度與控制有所規劃。具體而言，屬管理高層監督該範疇之風險管理原則有三，如（1）對數位金融業務行為之有效管理監控；（2）全面安全性控制程式之建立；（3）對委外對手或其他協力廠商廠商須有周全之實地查核與管理監督程式。

儘管董事會與高階經理人有責任確保適當之數位元金融監控程式充分運作，但該程式之主要內容仍有賴專責單位建立。應注意者，與該類監控程式相關之風險管理原則共有七項，包括（1）數位金融業務之客戶的認證；（2）電子交易的責任歸屬；（3）採取適當措施確保責任劃分；（4）數位金融系統與資料庫的適當監控；（5）電子交易、紀錄、與訊息之資料整合；（6）建立電子交易之審計紀錄；（7）關鍵資訊之保密等。而為使銀行在商業與法律風險上獲得保護，數位

金融服務須建立在一致與即時之基礎上，以滿足客戶之高標準期待，同時銀行亦須有能力將服務傳遞至所有客戶，並在任何環境維持相同之服務能力。此外，與法律及信譽風險有關之風險管理原則亦有四項，即（1）對數位金融服務之適當揭露；(2) 注重顧客個人資料之私密性；(3) 確保數位金融系統服務能力之長遠計畫；(4) 做好事故應變規劃。

由於慮即現代科技之發展一日千里，巴塞爾銀行監理委員會刻意僅提出風險管理之原則以保持彈性，可免於太過細節之規範不合時宜，但另一方面，擬將該原則性之陳述落實至銀行業實際經營環境中，仍須耗費大量之時間及人力。不可諱言地，數位化技術確實提高銷售與營運之效率，帶動銀行獲利能力之改善，惟事實上，數位金融之潮流撼動已持續超過兩百五十年之銀行營銷模式，如以英國為例，1990 年時該國境內銀行分行共有 17,637 家，至 2014 年僅剩 9,500 家，就研究顯示，預期 2018 年將縮小至 7,500 家分行，較 2014 年減少 27%。銀行客戶持續增加線上或行動服務需求，年輕世代之銀行使用者重度依賴數位服務，甚至多數民眾生平未曾踏進過銀行大門，而該種全新之營銷模式，如實地改變銀行業之風險結構。

整體而言，風險主要表現在享受網路金融服務族群之金融知識、風險識別及承擔能力之相對欠缺，容易遭受誤導、欺詐及不公正待遇，同時由於其投資小額而分散，網路金融風險一旦爆發，對社會整體影響相當大。因此在考慮網路金融風險時，有必要將網路非法集資及網路金融加以區別，如近期 e 租寶在中國大陸發生之全國性風險事件，牽涉群眾廣，涉案金額大。事實上，該企業在宣傳中均標榜自身是網路金融創新，但此類打著網路金融旗幟而行非法集資之行為，形成另類之網路金融風險。誠言之，防範網路金融風險要採取針對性措施，如就信用風險問題，可對行業準入門檻、行業經營準則進行明確規定，包括網路金融平台有責任及時、準確之進行資訊揭露，惟同時亦要強化個人徵信體系，加快資訊之共用。而就流動性風險而言，則是建立流動性管理指標體系，對該風險進行實時監測評估，甚至可利用大數據對流動性風險進行預測。

此外，因應大規模擠兌之緊急配套亦勢在必行，包括對法律合規風險，必須利用相關法律限定網路金融行業之經營條件，並明確法律底線，以促使網路金融企業合規經營，但法律制定無法一蹴而就，有待與時俱進，不斷對法律法規進行調整，以適應行業發展之新動態。與此同時，法律制定亦需重視國際合作，如以作業風險為例，一方面要減少終端、平台、網路之設計缺陷，以提高使用之單純性並減少操作失誤之可能性，二方面則需增加對網路金融從業人員及交易對象之培訓，提高其對設備操作之熟悉度。當然在面對技術風險時，則應加強技術團隊之建設，開發新型可靠安全技術並不斷對漏洞進行修補，並透過包括多重用戶名稱、密碼、校驗碼、短信驗證等方式實現身份驗證。不可諱言地，對相關之安全措施，監管部門需建立一套有效之技術標準，並保證該技術標準之適用性及符合國際規格。

第三章　主要國家網路金融風險之法令規範及監理

第一節　歐美國家網路金融風險之之相關規範及監理

一、美國

（一）監理政策

有論者指出，FinTech 早在 1980 年已經使用，FinTech 業界之出現亦在美國特殊環境下自然形成，並在供需環境自發性成長，政府並未介入。2008 年金融海嘯衝擊下，傳統金融業務之營運受到影響，僅得減少放款、提高利率，但小型企業貸款尋找不易，爰積極求助於 FinTech，而造成許多創業潮。面對 FinTech 介入，雖美國銀行業採取許多因應對策，整體而言，美國並未對 FinTech「生態系（ecosystem）」積極介入，而係使其自然成型，但由於金融海嘯之發生，美國政府瞭解傳統金融體制之缺陷，強化監理實屬必要。與此同時，FinTech 興起可更新金融體制，提供替代性金融中介功能，輔助傳統金融體制弱點與缺陷，明確 FinTech 之地位[2]。

（二）P2P 網路借貸

針對 P2P 美國並無單一規範法制，論者指出，P2P 融資仍是依美國現行法制分別就融資面與投資面進行規範。其中在融資面，P2P 業者需依據各州業法辦理登記，接受監理。美國 P2P 融資業者為規避各州利率上限之規定，均透過與聯邦存款保險會員之銀行合作，排除上限。在投資面，P2P 融資業者將債權小額化對不特定多數人銷售時，視為公開募集，但為規避公開募集之管制，多半採用私募程式將債權分授給機構投資人，或採用有限合夥方式募集資金於貸款債權上[3]。

然另有論者指出，美國 P2P 金融監理體系主要在消費者保護身上，係以公平對待所有消費者（投資者）、保護消費者隱私（借款人）及消費者意識教育（借款人與投資者）。應注意者，在聯邦監理角度上，P2P 平台需將每天貸款列表提

[2] 參閱李儀坤，Fintech 2.0 金融結合科技，即將顛覆金融業的遊戲規則！，凱信企管，2016 年 7 月，第 120-121 頁。

[3] 同前註，第 192 頁。

交給美國證管會，保證當金融消費者與 P2P 平台進行法律訴訟時，有相關保存記錄可證明是否有誤導金融消費者之錯誤訊息產生。P2P 平台申請需公開揭露之訊息包括經營狀況、潛在風險因素、管理團隊結構、薪資報酬及公司財務狀況等內容。至於州監理角度上，美國各州存在些許差異，部分州僅要求訊息公開揭露即可；或需監理機關判斷 P2P 是否具有公平、公正、合理發行證券；或對投資者設置財務適合性標準，如規範投資者最低年收入或財產總數、投資額度佔年收入或財產總額最高比例[4]。

表 3-1：美國營利性 P2P 公司適用主要聯邦借貸及消費者金融保護法制

法案名稱	相關要求或規定之例
誠實借貸 (Truth in Lending Act[5])	要求債權人對於借貸及信用交易條款提供統一性便於理解之揭露訊息；對信用及借貸廣告進行監理；賦予借款人更新相關公開揭露資訊及信貸餘額處理之相關權利[6]。
平等信用機會法 (Equal Credit Opportunity Act[7])	禁止債權人基於信貸申請人之以下訊息產生歧視對待情事：種族、膚色、宗教、國籍、性別、婚姻情形、年齡、申請人之收入是否來自公共援助計畫、申請人是否根據聯邦消費者信保護法或其他可適用之州法律，誠實信用地行使權利[8]。
服役人員民事救助法 (Servicemembers Civil Relief Act[9])	賦予現役服役人員為借款人時，利率設定上限之權利，並允許現役軍人及預備人員暫停或延遲一定之民事義務[10]。
公平信用報告法 (Fair Credit Reporting Act[11])	於取得同意的前提下(需要一個允許之目的)，可以獲得金融消費者之信用報告；要求相關人士向信用監理機關報告確實之信貸訊息；要求債權人制定及實施預防身分盜用方案[12]。
美國聯邦貿易委員會法第 5 條 (Section 5 of the Federal Trade Commission Act[13])	禁止不公平或欺詐性之商業行為與方式[14]。

[4] 參閱姚文平，互聯網金融-即將到來的新金融時代，中信出版社，2014 年 2 月，第 288-290 頁。
[5] Pub. L. No. 90-321, Title I, 82 Stat. 146 (1968), codified at 15 U.S.C. §§ 1601-1667f.
[6] Requires creditors to provide uniform, understandable disclosures concerning certain terms and conditions of their loan and credit transactions; regulates the advertising of credit and gives borrowers, among other things, certain rights regarding updated disclosures and the treatment of credit balances.
[7] Pub. L. No. 93-495, Title V, 88 Stat. 1521 (1974), codified at 15 U.S.C. §§ 1691-1691f.
[8] Prohibits creditors from discriminating against credit applicants on the basis of race, color, religion, national origin, sex or marital status, or age, or the fact that all or part of the applicant's income derives from any public assistance program or the fact that the applicant has in good faith exercised any right under the federal Consumer Credit Protection Act or any applicable state law.
[9] 54 Stat. 1178 (1940), codified at 50 App. U.S.C. §§ 501-596.
[10] Entitles borrowers who enter active military service to an interest rate cap and permits servicemembers and reservists on active duty to suspend or postpone certain civil obligations.
[11] Pub. L. No. 91-508, Title VI, § 601, 84 Stat. 1128 (1970), codified at 15 U.S.C. §§ 1681-1681x.
[12] Requires a permissible purpose to obtain a consumer credit report, and requires persons to report information to credit bureaus accurately; imposes disclosure requirements on creditors who take adverse action on credit applications based on information contained in a credit report; requires creditors to develop and implement an identity theft prevention program.
[13] § 5, 38 Stat. 719 (1914), codified at 15 U.S.C. § 45.
[14] Prohibits unfair or deceptive business acts or practices.

金融服務現代化法 (Gramm-Leach-Bliley Financial Modernization Act[15])	限制金融機構向非關聯協力廠商洩漏消費者非公開揭露之個人訊息；要求金融機構通知客戶訊息共用方式，並告知金融消費者若他們不希望自己的訊息被非關聯協力廠商共用時，有選擇退出(拒絕)之權利[16]。
電子資金轉帳法 (Electronic Fund Transfer Act[17]	為金融消費者提供從自己銀行帳戶中劃撥電子資金之權利。
全球及國內電子簽名商業法 (Electronic Signatures in Global and National Commerce Act[18])	授權建立使用電子記錄與簽名具有法律約束力及強制執行力之協議；要求希望在消費交易中使用電子記錄及簽名之企業並需取得金融消費者之事前允許[19]。
銀行保密法 (Bank Secrecy Act[20])	要求金融機構實施反洗錢程式，並將聯邦政府指定、資產被動結集通常被要求禁止與其交易之國家及公司列入黑名單中[21]。
公平債務催收法 (Fair Debt Collection Practices Act[22])	對協力廠商債務追償之行為提供指引及限制；要求進行債務通知；禁止在債務追償過程中實施威脅、騷擾等行為[23]。

資料來源：PERSON-TO-PERSON LENDING-New Regulatory Challenges Could Emerge as the Industry Grows(GAO-11-613)， U.S. Government Accountability Office， July 2011， 33 (last visited 15 August 2016)；整理自姚文平，互聯網金融-即將到來的新金融時代，中信出版社，2014 年 2 月，第 289 頁。

（三）第三方支付

美國第三方支付監理機關分為聯邦存款保險公司（Federal Deposit Insurance Corporation, FDIC）及州政府層級，適用法規上亦可分為聯邦「統一資金服務法（Uniform Money Services Act）」及各州適用「資金移轉法（Money Transmitters Act）」。論者指出，美國聯邦對第三方支付之監理，係放在「貨幣服務業務」之

[15] Pub. L. No. 106-102, 113 Stat. 1338 (1999) (codified in scattered sections of 12 U.S.C. and 15 U.S.C.).

[16] Limits when a "financial institution" may disclose a consumer's "nonpublic personal information" to nonaffiliated third parties; requires financial institutions to notify their customers about their information-sharing practices and to tell consumers of their right to "opt out" if they do not want their information shared with certain nonaffiliated third parties.

[17] Pub. L. No. 95-630, Title xx, § 2001, 92 Stat. 3728 (1978), codified at 15 U.S.C. §§ 1693-1693r.

[18] Pub. L. No. 106-229, 114 Stat. 464 (2000), codified at 15 U.S.C. §§ 7001-7006, 7021, 7031.

[19] Authorizes the creation of legally binding and enforceable agreements utilizing electronic records and signatures and requires businesses that want to use electronic records or signatures in consumer transactions to obtain the consumer's affirmative consent to receive information electronically.

[20] Pub. L. No. 91-508, Titles I, II, 84 Stat. 1114-1124 (1970), codified at §§ 12 U.S.C. 1951-1959.

[21] Requires financial institutions to implement anti-money-laundering procedures, apply customer verification program rules, and screen names against the federal list of Specially Designated Nationals, whose assets are blocked and with whom companies are generally prohibited from dealing.

[22] Pub. L. No. 95-109, 91 Stat. 874 (1977), codified at 15 U.S.C. §§ 1692-1692.

[23] Provides guidelines and limitations on the conduct of third-party debt collectors in connection with the collection of consumer debts; limits certain communications with third parties, imposes notice and debt validation requirements, and prohibits threatening, harassing, or abusive conduct in the course of debt collection.

項目，角色被界定為「資金移轉服務商（Money Transmitters）」，蓋其資金特色會短暫停滯在第三方支付業者，該金額之使用或利息應受到管制，否則第三方支付業者會等同於銀行。FDIC 將滯留在第三方支付業者之資金定義為「負債」，而非聯邦銀行法定義之存款，故第三方支付業者並非存款保險公司認定之銀行或其他金融之存款機構，成立無需取得銀行之許可執照，該滯留資金無法得到存款保險之保障[24]。

以 PayPal 為例，FDIC 回函告訴 PayPal 其並非存款保險法涵攝之範圍，其非銀行且其用戶資金無法得到存款保險之保障[25]，雖對滯留資金的監理及安全維護係通過 FDIC 所提供之「存款延伸保險（Pass Through Insurance Coverage）」部分實現。亦即任何 P2P 網上支付服務提供者，在將所有滯留資金存入 FDIC 保險之商業銀行，修改使用者服務條款及滿足其他資訊揭露要求，使用者資金每戶保險達到 10 萬美元。但此保險僅是在存款銀行倒閉有效，如是支付服務提供者本身倒閉，存款延伸保險將不適用[26]。應注意者，此類延伸保險對消費者而言，無法適用在 PayPal 客戶選擇投資在 PayPal 資金市場基金，而對 PayPal 本身負擔責任亦不能被 FDIC 認定為其客戶之代理人，故延伸保險該方案僅解決部分資金安全問題[27]。

---

[24] 參閱李儀坤，Fintech 2.0 金融結合科技，即將顛覆金融業的遊戲規則！，凱信企管，2016 年 7 月，第 174-175 頁。

[25] Online payment service PayPal Inc., which recently went public, said that the U.S. independent deposit insurance agency that oversees the nation's financial system declared that PayPal is not a bank or savings association for purposes of the Federal Deposit Insurance Act. The FDIC said that when PayPal acts as an agent for its customers and places funds into an FDIC-insured institution, those funds would be insured up to FDIC limits. However, the PayPal Money Market Fund is not covered by FDIC insurance and is not guaranteed by any bank. (Investors should also understand that the fund may lose value.) See Ina Steiner, FDIC Tells PayPal It Is Not Covered under FDIC Act, PayPal Is Not a Bank(March 13, 2002). *Available at* : http://www.ecommercebytes.com/cab/abn/y02/m03/i13/s03(last visited 15 August 2016).

[26] 參閱金融時報，美國支付市場。*Available at*: https://news.99bill.com/modules/news/article.php?storyid=94 (last visited 15 August 2016)

[27] PALO ALTO, Calif., March 12 /PRNewswire-FirstCall/ --PayPal, Inc. (Nasdaq: PYPL) today announced that it has received a finaladvisory opinion from the FDIC Legal Department to the effect that, when PayPal acts as agent for customers and places PayPal customer funds with well-capitalized FDIC member banks, those funds will qualify for federal deposit insurance up to $100,000 per customer, per bank, in the event of a failure of a bank at which the funds were placed. This "pass-through" insurance for customers does not apply to funds that PayPal customers choose to invest in the PayPal Money Market Fund, to liabilities of PayPal itself, nor if PayPal was deemed by the FDIC not to be acting as an agent for its customers. In order to ensure that PayPal is treated as an agent for its customers, PayPal places all customer funds not invested in the PayPal Money

本研究認為，借鏡歐盟將支付款項定性為「電子錢」性質觀之，雖具有回贖性質，但儲存在電子設備之儲值金額並非存款[28]。然從美國 PayPal 提供之預付款儲值服務可知，如要受美國存款保險保障，須依據其與消費者約定條款所示，將個別消費者儲值之預付款項，全部集中至一個單一帳戶中，再將此帳戶所有儲值預付款金額，儲蓄至受存款保險保障體系之銀行，故該儲蓄至銀行之儲值預付款金額，受到存款保險制度之保護[29]，亦即儲值之預付款項本質上並非存款[30]。然從其發展狀況得知，依舊可依照契約約定客戶獲得存款保險保障金額，業者存入受存款保護之銀行與金融機構。

美國對第三方支付使用規範為「統一資金服務法」，此法係對貨幣服務進行監理，並強調以發放執照的方式管理規範從事貨幣服務之非銀行機構。而從事貨幣服務之機構，即包括電子貨幣及信用卡代收付之支付方式，須向各州政府申請獲得專項業務經營許可，同時符合有關資本額、財務狀況、從業經驗、投資主體及營業場所等相關資格要求。貨幣服務機構須保持交易資金之高度流動性及安全

Market Fund in accounts at FDIC-insured banks and has adopted internal procedures intended to maintain its status as agent for its customers. See PayPal, Inc., PayPal Receives FDIC Advisory Opinion on Insurance for Customer Funds FDIC Legal Opinion Holds That Funds Deposited by PayPal on Behalf of Customers At FDIC Member Institutions Would Qualify for Insurance On a Per-Customer Basis(Mar 12, 2002). *Available at*: http://www.prnewswire.com/news-releases/paypal-receives-fdic-advisory-opinion-on-insurance-for-customer-funds-76421017.html (last visited 15 August 2016).

[28] See DIRECTIVE 2009/110/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 16 September 2009: "(18) Electronic money needs to be redeemable to preserve the confidence of the electronic money holder. Redeemability does not imply that the funds received in exchange for electronic money should be regarded as deposits or other repayable funds for the purpose of Directive 2006/48/EC. Redemption should be possible at any time, at par value without any possibility to agree a minimum threshold for redemption. Redemption should, in general, be granted free of charge. However, in cases duly specified in this Directive it should be possible to request a proportionate and cost-based fee without prejudice to national legislation on tax or social matters or any obligations on the electronic money issuer under other relevant Community or national legislation, such as anti-money laundering and anti-terrorist financing rules, any action targeting the freezing of funds or any specific measure linked to the prevention and investigation of crimes."

[29] See PayPal User Agreement : "You are not required to keep funds in the PayPal system (i.e., carry a balance in your PayPal agency account) in order to use the Service. If you do carry a U.S. Dollar balance in your PayPal account and do not enroll in the PayPal Money Market Fund, PayPal will pool your funds together with funds from other Users, and will place those funds in accounts at one or more non-interest bearing FDIC-insured banks ("Pooled Accounts"). Those funds may be eligible for FDIC pass-through insurance. Balances held in currencies other than U.S. Dollars will not be eligible for FDIC insurance." Available at：http://claudelafleur.qc.ca/ PayPalPoli cies.html（last visited 2015.10.10）.

[30] 參閱林盟翔，電子支付機構金融監管之爭議問題研析，上海財經大學法學院第二屆金融法治論壇會，2015 年 10 月，第 30-31 頁。

性，不得從事類似銀行存放款業務，且不得擅自使用或留存客戶交易資金。由此可知，美國電子支付法規是建立在維護客戶合法權益上，且對提供電子支付機構設置一定門檻、並建立檢查及報告制度，亦即透過履約保證等規定以維護客戶權益，加強電子支付機構之退出及撤銷等管理[31]。

以紐約州為例，2010 年「紐約州之資金移轉法（Article 13-B of the New York Banking Law 2010）」係規定在銀行法第 13-B 資金移轉部分（第 640-652B 條）及行政規則第 406、416、417 及 300 條[32]。所謂「支付工具」係指任何支票、匯票、匯款單或其他文書及資金支付命令，無論該文書或命令係可商談，或出賣給一人或數人，但支付工具不包括旅行支票，且任何工具在發行人之商品或服務係可贖回，信用證券或被允許之支付工具（permissible investments，如現金、商業票據等）均被本節定義所包含在內。規範重點如下[33]：1、監理機關應依申請人之財務狀況、信用度、營運經驗、適格性進行審查（第 642 條）[34]。2、第三方支付業者於許可及營業時，為保護消費者權利，業者應交付紐約州經認可之保險公司或保險公司保證證書，該保證金額最低 50 萬美元，若為旅行支票之銷售須

[31] 參閱李書儀，參加美國紐約梅隆銀行舉辦之「全球客戶資金服務研討會」心得報告，台灣銀行，2015 年 8 月，第 14-15 頁。

[32] See Information and Resources for Money Transmitters of New York State. *Available at*：http://www.dfs.ny.gov/banking/moneytransmit.htm（last visited 2015.10.10）.

[33] 參閱李儀坤，Fintech 2.0 金融結合科技，即將顛覆金融業的遊戲規則！，凱信企管，2016 年 7 月，第 177-179 頁。

[34] § 642. Action by superintendent. 1. As a condition for the issuance and retention of the license, applicants for a license and other licensees shall, within thirty days after notice by the superintendent, or such longer or shorter period as he or she shall prescribe, file with the superintendent one or more corporate surety bond or bonds, as required below, in form satisfactory to him or her and issued by a bonding company or insurance company authorized to do business in this state. One bond shall be in favor of the superintendent and in such principal amount as he or she shall determine is necessary or desirable for the protection of the purchasers and holders of New York instruments sold or to be sold by the applicant or licensee, provided, however, that until June first, nineteen hundred seventy-seven, the principal amount of such bond shall be no less than two hundred ten thousand dollars and on and after June first, nineteen hundred seventy-seven, the principal amount of such bond shall be no less than five hundred thousand dollars. If the applicant or licensee intends to engage or engages in the sale of New York traveler's checks, such applicant or licensee shall file with the superintendent a separate bond. Said bond shall be in favor of the superintendent and in such principal amount as he or she shall determine is necessary or desirable for the protection of the purchasers and holders of the New York traveler's checks sold or to be sold by the applicant or licensee; provided, however, that the principal amount of such bond shall not be less than seven hundred fifty thousand dollars, unless the superintendent, for good cause shown, shall have determined that a lesser amount will adequately protect the purchasers and holders of the New York traveler's checks sold or to be sold by such applicant or licensee.

另增提 75 萬美元，總計 125 萬美元（第 643 條）[35]。3、並未有兼營禁止規定（第 646 條）[36]。若兼營資金服務業務，包括匯兌、支票兌現、旅行支票及預附卡之發行銷售變現、匯款等任一業務，應依據「銀行秘密法（Bank Secrecy Act）」與「美國愛國法（USA Patriot Law）」向美國「財政部金融犯罪執行網」（Financial Crime Euforcement Network，FinCEN）辦理登記。4、匯款、網購支付金額無上限（第 647 條）[37]。5、監督代理行之義務（第 648 條）[38]。6、第三方支付業者

[35] § 643. Bond or securities. 1. As a condition for the issuance and retention of the license, applicants for a license and other licenseesshall, within thirty days after notice by the superintendent, or such longer or shorter period as he or she shall prescribe, file with the superintendent one or more corporate surety bond or bonds, as required below, in form satisfactory to him or her and issued by a bonding company or insurance company authorized to do business in this state. One bond shall be in favor of the superintendent and in such principal amount as he or she shall determine is necessary or desirable for the protection of the purchasers and holders of New York instruments sold or to be sold by the applicant or licensee, provided, however, that until June first, nineteen hundred seventy-seven, the principal amount of such bond shall be no less than two hundred ten thousand dollars and on and after June first, nineteen hundred seventy-seven, the principal amount of such bond shall be no less than five hundred thousand dollars. If the applicant or licensee intends to engage or engages in the sale of New York traveler's checks, such applicant or licensee shall file with the superintendent a separate bond. Said bond shall be in favor of the superintendent and in such principal amount as he or she shall determine is necessary or desirable for the protection of the purchasers and holders of the New York traveler's checks sold or to be sold by the applicant or licensee; provided, however, that the principal amount of such bond shall not be less than seven hundred fifty thousand dollars, unless the superintendent, for good cause shown, shall have determined that a lesser amount will adequately protect the purchasers and holders of the New York traveler's checks sold or to be sold by such applicant or licensee. In making any determination under this subdivision, the superintendent may take into account the financial condition of the licensee, the number of locations in this state at which the licensee, either directly or through agents, transacts the business of selling New York instruments or New York traveler's checks, the controls imposed on such agents or, and the possible exposure of purchasers and holders of New York instruments and New York traveler's checks to loss in the event of the insolvency, bankruptcy or other financial impairment of the licensee. The proceeds of each bond shall constitute a trust fund for the exclusive benefit of the purchasers and holders of the New York instruments and New York traveler's checks, as the case may be. Except as otherwise provided in the following sentence, in the event of the insolvency or bankruptcy of any licensee, the proceeds of the bond or bonds held for the exclusive benefit of the purchasers and holders of New York instruments and the proceeds of the bond or bonds held for the exclusive benefit of the purchasers and holders of New York traveler's checks shall be paid to the superintendent forthwith for disposition in accordance with the provisions of this article. If any New York instruments have been assigned to the fund, the proceeds of the bond held for the exclusive benefit of the purchasers and holders of New York instruments shall constitute a trust fund for the benefit of, and shallbe payable to, the fund to the extent of such assignment. From time to time, the superintendent may require, upon thirty days notice or suchlonger or shorter period as he or she shall prescribe, that such bond or bonds be increased if he or she shall determine that such increase is necessary or desirable for the protection of the purchasers and holders of New York instruments and New York traveler's checks.

[36] § 646. Investigations, hearings and reports. 1. The superintendent shall have the power to make such investigations and conduct such hearings as he shall deem necessary to determine whether any licensee or any other person has violated any of the provisions of this article, or whether any licensee has conducted himself in such manner as would justify the suspension or revocation of his license.

[37] § 647. Judicial review. The refusal by the superintendent of an original license, in the case of an applicant which, prior to January first, nineteen hundred sixty-three, and upon the date of filing such application, has lawfully been engaged in this state in the business of selling or issuing checks or of

平時應經許可而為投資（permissible investment：包括現金、票據、支息債權、其他經認可之投資或資產）。投資額度市價評估額，應高於支付工具餘額及旅行支票餘額之合計總額（第 651 條）[39]。

（四）群眾籌資

基於保護投資人及維護市場秩序，美國聯邦證券交易法將具有證券性質股票及債券，甚至投資契約均列入保護範疇，然導致小型企業籌措資金不易（小型企業根本無法負擔財務、會計等成本），遂有論者提出應試圖鬆綁前述限制。美國政府為提升就業率，由總統歐巴馬於 2012 年 4 月簽署 JOBS 法案（Jumpstart Our Business Startups Acts, JOBS Act[40]，創業企業融資法案），企圖藉此方式減低小微或新創企業因各種證券法規所承受之募資負擔，俾利小微或新創企業得以更迅速籌措資金。該法案第三章群眾籌資（Crowdfunding[41]）容許於網路平台進行資金籌措，並得以股權、現金、紅利等金錢利益作為回饋投資人之方式，惟該企業須合於下列條件，始得豁免於向證管會（SEC）申報生效之規定：（1）單一案最高

receiving money for transmission or transmitting the same, and in all cases the suspension or revocation of any license by the superintendent, shall be subject to judicial review in the manner in such cases made and provided by law.

[38] § 648. Agents. A licensee may conduct its business at one or more locations within this state, as follows: (a) The business may be conducted through or by means of agents as the licensee may from time to time designate or appoint and, in no event, shall the business of money transmission be conducted through a subagent. (b) No license under this article shall be required of any agent of a licensee in cases in which such agent is acting on behalf of a licensee under, and in accordance with, an agency contract except as provided in subdivision (c) of this section. (c) An agent, other than a person expressly excepted from the application of this article, who sells or delivers the licensee's checks over-the-counter to the public shall not be exempt from licensing under this article if such agent in the ordinary conduct of such business receives or at any time has access to (1) the licensee's checks which, having been paid, are returned through banking channels or otherwise for verification or for reconciliation or accounting with respect thereto or (2) bank statements relating to checks so returned. No license under this article shall be required of an agent, including a general or managing agent, of a licensee who does not directly sell or deliver the licensee's checks over-the-counter to the public.

[39] § 651. Investments. Every licensee shall at all times maintain permissible investments having (i) a market value, computed in accordance with generally accepted accounting principles, at least equal to the aggregate of the amount of all its outstanding payment instruments and all its outstanding traveler's checks or (ii) a net carrying value, computed in accordance with generally accepted accounting principles, at least equal to the aggregate of the amount of all its outstanding payment instruments and all its outstanding traveler's checks so long as the market value of such permissible investments is at least eighty per centum of the net carrying value. Notwithstanding the foregoing provisions of this section, the superintendent shall have the authority, for good cause shown, to exempt from the requirements of this section any licensee.

[40] http://www.sec.gov/spotlight/jobs-act.shtml，最後瀏覽日：2016 年 9 月 20 日。

[41] http://www.gpo.gov/fdsys/pkg/BILLS-112hr3606enr/pdf/BILLS-112hr3606enr.pdf，最後瀏覽日：2016 年 9 月 20 日。

募集資金之上限（12 個月內不得募集超過 100 萬美元）以下之有價證券；（2）單一投資人投資上限（年收入或是淨資產低於十萬美元者，年度可投資金額限於 2,000 美元以下或其年收入（或是淨資產）5%，投資人可擇中較高者計算；若年收入或淨資產高於十萬美元者，年度可投資金額上限為年收入或淨資產 10%）；（3）不得直接銷售或是推銷有價證券，須經由仲介單位為之（仲介單位限於證券經紀商、承銷商或募資平台）。

二、英國

（一）監理政策

論者指出，英國政府提出「金融科技未來願景（FinTech Futures）」此一項具指標意義報告，明確表示金融科技絕非洪水猛獸，其亦可能產生良性循環，創造全新市場與新客戶，從而展現更多之「普惠金融（financial inclusion）」；換言之，受惠於金融科技與 Bank 3.0，未來不分族群、身分，均可輕易使用嶄新金融服務並享受其所帶來之便利性。而就金融主管機關立場，金融科技固然帶來諸多重要課題，然其中最為關鍵者，仍是如何建置適當之監管制度，除了因應對傳統金融機構及固有商業模式產生之劇烈衝擊外，放置於天平上之考量因素，尚應包括在評估納管金融科技之餘，能否保持其充分靈活性，以持續促進金融環境之創新與成長[42]。其研究指出，英國政府確信有效之金融監理法規，將是英國金融產業及金融科技未來發展之成功關鍵因素。

為因應金融服務模式及產業版塊快速變遷，英國金融監理總署（FCA）提出相關計畫，以利英國金融監理法規跟上金融體系出現之創新商業模式。英國科技辦公室明確指出金融科技規範上之重大挑戰，在於許多 FinTech 模式似乎自外於既有管理規範，以網路 P2P 借貸為例，相關業者在善加運用資訊科技下，網路

[42] 參閱郭戎晉，從國際趨勢談金融科技(FinTech)與 Bank 4.0 推動策略，第 1-2 頁。*Available at* : http://www.tfsr.org.tw/Uploads/files/201511%20 從國際趨勢談金融科技(FinTech)與 Bank%204_0 推動策略_郭戎晉組長.pdf(last visited 15 August 2016).

P2P 借貸不必然存在特定仲介者（intermediary）角色，能否逕以既有法規加以規範，存在適用上之疑義[43]。另亦有論者指出，由於英國金融科技創事業約占全歐洲 50%，但英國監理制度尚須顧及新市場參與者、破壞式創新者及新創業者之利益，故由 FCA 主導「新創計畫」應運而生，目的即在檢視並排除對金融科技創新之障礙。此外，金融科技發展亦帶動「監理科技（RegTech）」，亦即在監理活動之透明化，以及業者自動化資訊揭露與分析上帶來改變，落實以資料為導向之監理與法令遵循制度（Data-Driven Regulation and Compliance），監理效率勢必因而增加[44]。

（二）P2P 網路借貸

2014 年是英國對 P2P 之監理分界點，論者指出，自 2005 年 Zopa 取得英國公平交易辦公室信貸許可，成為英國信用行業欺詐防範機構成員，並在訊息專員辦公室註冊，其原因在於 1974 年英國消費者信貸法，要求大部分向消費者提供信貸、租賃、債務催收等產品或服務之企業，均須要擁有信貸許可證，否則可能構成犯罪。2011 年 8 月英國 P2P 金融協會（The Peer-to-Peer Finance Association, P2PFA）成立，以非官方、非營利性性之行業協會方式管理 P2P 業者，對貸款人之保護設定最低標準要求，並促進 P2P 市場之有效監理[45]。2014 年 3 月依據金融服務市場法（Financial Service and Market Act 2000）由 FCA 訂定「關於網路眾籌及透過其他方式發行不易變現證券之監理規則（The FCA's regulatory approach to crowdfunding over the internet and the promotion of non-readily realisable securities by other media， PS14/4）」[46]，區分二類群眾籌資納入監理：第一類是「P2P 網路借貸型眾籌（Loan-based Crowdfunding）」；第二類則是「股權投資型

[43] 參閱郭戎晉，從國際趨勢談金融科技(FinTech)與 Bank 4.0 推動策略，第 10-11 頁。*Available at* : http://www.tfsr.org.tw/Uploads/files/201511%20 從國際趨勢談金融科技(FinTech)與 Bank%204_0 推動策略_郭戎晉組長.pdf(last visited 15 August 2016).

[44] 參閱李慧芳，英國金融科技發展及監理沙箱(Regulatory Sandbox)機制對我國的啟示。*Available at* : http://portal.stpi.narl.org.tw/index/article/10260(last visited 15 August 2016).

[45] 參閱姚文平，互聯網金融-即將到來的新金融時代，中信出版社，2014 年 2 月，第 290 頁。

[46] See The FCA's regulatory approach to crowdfunding over the internet, and the promotion of non-readily realisable securities by other media Feedback to CP13/13 and final rules(March 2014) . Available at : https://www.fca.org.uk/your-fca/documents/policy-statements/ps14-04(last visited 15 August 2016).

眾籌（Investment-based Crowdfunding 《and the promotion of non-readily realisable securities》）」，並制定不同監管標準，從事以上二類業務之公司，均需取得 FCA 授權。監理規則之目標在於提供消費者取得額外保護，以及在消費者利益中推動有效之競爭。

1、最低資本需求

監理規則建立網路借貸型眾籌固定資本與浮動資本之規定，自 2014 年 4 月至 2017 年 3 月為 2 萬英鎊，2017 年 4 月後為 5 萬英鎊。此外，為抵禦將來產生之金融危機，監理規則要求依據平台借貸狀況採取差額累進之補充資本制度，其詳細規定以下表 3-2 呈現。

表 3-2：英國 P2P 固定資本及浮動資本措施

項目	平台規模	草案內容		定案內容	
時間		2014.4.1-2017.3.31	2017.4.1 以後	2014.4.1-2017.3.31	2017.4.1 以後
固定資本		2 萬英鎊	5 萬英鎊	2 萬英鎊	5 萬英鎊
浮動資本	0-£50m	0.3%	0.3%		
	> £50m - £500m	0.2%	0.2%		
	> £500m	0.1%	0.1%		
浮動資本	0-£50m			0.2%	0.2%
	> £50m - £250m			0.15%	0.15%
	> £250m - £500m			0.1%	0.1%
	> £500m			0.05%	0.05%

資料來源：The FCA's regulatory approach to crowdfunding over the internet， and the promotion of non-readily realisable securities by other media Feedback to CP13/13 and final rules (March 2014) ，18-19.*Available at* : https://www.fca.org.uk/your-fca/documents/policy-statements/ps14-04 (last visited 15 August 2016).

2、客戶資金規定（client money rules）

客戶資金規定係源自「客戶資產規章（Client Assets Sourcebook, CASS）」之要求。「P2P 網路借貸型眾籌」類型，平台應將客戶資金分類管理，並定期每年向監理機關報告資金分類結果。蓋此種類型係平台將客戶資金交付銀行託管，亦當平台為客戶開立銀行帳戶，該帳戶資金仍為平台帳戶客戶所有，銀行不得使用

該筆資金，而平台應對銀行進行盡職調查，確保客戶資金不被銀行私自動用。但平台或銀行發生「失卻償付能力（insolvency）」時，客戶尚未貸出之資金應立即返還客戶[47]。依據規定，平台業者須依據企業規模大小，由公司經營基層或專責人士，每年或每月定期向監理機關進行客戶資金持有狀況之報告，但有業者認為依照 CASS 分類之方式造成企業過大之負擔，但不被監理機關接受[48]。

表 3-3：英國 P2P 客戶資金規定

CASS 分類企業	持有客戶資金規模	監理需求
小型企業(small firms)	0 - < £1m	公司經營階層：每年向監理機關報告持有客戶資金規模。
中型企業(medium firms)	≧ £1m - ≦ £1bn	公司經營階層：每年向監理機關報告持有客戶資金規模。 公司配置專門人員：每月向監理機關報告持有客戶資金規模。
大型企業(large firms)	> £1bn	

資料來源：The FCA's regulatory approach to crowdfunding over the internet， and the promotion of non-readily realisable securities by other media Feedback to CP13/13 and final rules (March 2014) ，22-24. *Available at* : https://www.fca.org.uk/your-fca/documents/policy-statements/ps14-04 (last visited 15 August 2016).

3、公開揭露制度（Disclouse）

平台之風險等訊息公開揭露，不僅是保護消費者最佳方式，亦為最佳之監理措施。FCA 要求公開訊息包括平台業務訊息及平台提供之服務訊息，前者包括過去與未來投資狀況、過去與預期之違約率、計算預期違約率所使用之假設因素及信貸狀況之評估描述、擔保狀況、可能實際收益以及稅捐計算、延遲給付與違約處理程式等。後者則是有關聯繫方式、FCA 授權文書揭露、營運狀況、平台費用說明、風險等相關準備金提撥之狀況等[49]。

[47] 英國 P2P 行業是如何監管的？*Available at* : https://read01.com/GPmBG.html (last visited 15 August 2016).

[48] See The FCA's regulatory approach to crowdfunding over the internet, and the promotion of non-readily realisable securities by other media Feedback to CP13/13 and final rules(March 2014) ,23-24. Available at : https://www.fca.org.uk/your-fca/documents/policy-statements/ps14-04(last visited 15 August 2016).

[49] See The FCA's regulatory approach to crowdfunding over the internet, and the promotion of non-readily realisable securities by other media Feedback to CP13/13 and final rules(March 2014), 10；30-31；40. *Available at* : https://www.fca.org.uk/your-fca/documents/policy-statements/ps14-04 (last visited 15 August 2016).

4、解除權（Cancellation rights）

「遠程銷售指令（Distance Marketing Directive, DMD）」要求多數金融服務契約形成一個遠程時（不包括供應商或仲介與客戶之同時實際存在），應給客戶在一定期限可撤銷之權利，無任何罰則亦無需附理由。基此，英國將 DMD 轉換為國內法律，係為「2004 年金融服務（遠程銷售）規章（The Financial Services《Distance Marketing》Regulations）」，於 2004 年 10 月生效，而相關銷售由英國財政部負責。應注意者，雖解除權藉由 EU 立法程式且適用於「P2P 網路借貸型眾籌」類型平台，而監理機關亦無挑戰之意，惟須加以探討者，部分情況下平台機構不採用此類權利之原因，以及考慮是否要賦予投資人撤銷權因素為何，若有賦予撤銷權之場合，該權利應於開始與平台協議中即須賦予，而非基於一個單一借貸契約，然監理機關並無強制機構該如何提供此類權利[50]。

5、經營失敗（failure）

當平台經營失敗（或破產）、遭遇償付不能（insolvency）之狀況時，對尚在契約期間內之契約應繼續管理，並對貸款管理亦須提出合理安排，例如對未到期貸款、分配返還資金、違約金與遲延追償等事項。具體行為包括（1）未到期之借貸可以由其他網路借貸型眾籌平台或債務管理人管理，由未到期借貸收益支付管理費用；（2）客戶資金應該依據客戶資金規定分配予客戶，於破產清算中產生之破產管理人或清算人之費用向客戶分配資金之費用由客戶依據比例分擔；（3）為客戶設立之新的銀行帳戶以接受未到期貸款之本息償還；（4）不可發生新借貸關係，但既有借貸依據契約之條件繼續有效[51]。

[50] See The FCA's regulatory approach to crowdfunding over the internet, and the promotion of non-readily realisable securities by other media Feedback to CP13/13 and final rules(March 2014) ,29. *Available at* : https://www.fca.org.uk/your-fca/documents/policy-statements/ps14-04(last visited 15 August 2016).

[51] See The FCA's regulatory approach to crowdfunding over the internet, and the promotion of non-readily realisable securities by other media Feedback to CP13/13 and final rules (March 2014), 27. *Available at* : https://www.fca.org.uk/your-fca/documents/policy-statements/ps14-04(last visited 15 August 2016).

6、爭端解決機制

當投資人對平台提供之服務不愉快（不滿意）時應有權利申訴。若平台回應仍造成投資人不滿，可將該申訴送至英國公評人服務機構（Financial Ombudsman Service, FOS）[52]進行投訴，但爭端解決機制並無強制程式，僅投訴處理係公平與即時。監理機關期盼平台業者開發適合其商業模式之爭端解決程式，且期望不會導致不成比例之成本。應注意者，所謂「申訴（complaint）」範圍非常廣泛，如「從任何口頭或書面表示產生之不滿足、無論是否合理、來自於或代表、一個人有關規定或未能提供金融服務或補救之決定等，申訴人聲此舉使申訴人遭受經濟損失、實際損害或實際困擾[53]」。至於「投資型群眾籌資」因處理客體為未上市股票及債券，應受 FCA 監理並適用 FCA 核心標準，對投資人而言，投資型群眾籌資之風險遠高於融資型群眾籌資，亦因此監理強度必須嚴格[54]。

（二）第三方支付

英國於 2007 年依據歐盟「支付服務指令（Directive on Payment Services，PSD， 2007/64/EC）」、金融服務市場法，2009 年發布「支付服務法（The Payment Service Regulations 2009，PSRs 2009）[55]」。2012 年 FCA 發布「在 2009 年支付服務法 FCA 之角色（The FCA's role under the Payment Services Regulations 2009 Our approach[56]）」一文，其公布支付服務法之修正重點在於[57]：（1）支付業監理主管

[52] See Annex K of Appendix 2 of PS14/3, Detailed rules for the FCA regime for consumer credit, February 2014, for DISP 2.7.6R(15)

[53] The definition of a complaint in our Handbook is deliberately broad. It includes 'any oral or written expression of dissatisfaction, whether justified or not, from, or on behalf of, a person about the provision of, or failure to provide, a financial service or a redress determination, which alleges that the complainant has suffered (or may suffer) financial loss, material distress or material inconvenience'. See The FCA's regulatory approach to crowdfunding over the internet, and the promotion of non-readily realisable securities by other media Feedback to CP13/13 and final rules (March 2014) ,32. *Available at* : https://www.fca.org.uk/your-fca/documents/policy-statements/ps14-04(last visited 15 August 2016).

[54] 參閱李儀坤，英美日 P2P 融資內涵與相關監理，存款保險季刊，第 29 卷第 2 期，2016 年 6 月，第 162 頁。

[55] FINANCIAL SERVICES AND MARKETS：The Payment Services Regulations 2009, 2009 No. 209. *Available at*: http://www.legislation.gov.uk/uksi/2012/1791/pdfs/uksi_20121791_en.pdf?utm_source=Concep%20Send&utm_medium=email&utm_campaign=FSi:%20An%20overview%20of%20recent%20key%20financial%20services%20and%20regulatory%20developments_07/31/2012(last visited 15 August 2016).

[56] See Financial Conduct Authority, The FCA's role under the Payment Services Regulations 2009 Our approach (June 2013). *Available at* :

機關由 FSA 變更為 FCA；（2）大型與小型第三方支付業者[58]，資本額需求規範與原則細緻化；（3）安全、報告、監理之強化；（4）消費者保護強化、業者彈性營運及其功能發揮；（5）清算支付系統運用嚴謹。「支付服務法」於 2012 年公布（The Payment Services Regulations 2012, PSRs 2012[59]），該法主要是對「2007 年金錢借貸法」（Amendment of the Money Laundering Regulations 2007）、「2009 年支付服務法」（Amendment of the Payment Services Regulations 2009）及「2011 年電子錢法」（Amendment of the Electronic Money Regulations 2011）進行修正。

表 3-4：英國不同支付業者適用電子支付法之情形

支付服務提供業者	授權支付機構	註冊支付機構	EEA 授權支付機構[60]	其他支付機構
Chapter 1 – Introduction	●	●	●	●
Chapter 2 – Scope	●	●	●	●
Chapter 3 – Authorisation and registration	●	●		
Chapter 4 – Changes in circumstances of authorisation and registration	●	●		
Chapter 5 – Appointment of agents	●	●		
Chapter 6 – Passporting	●		●	
Chapter 7 – Use of the FSA and FCA logos	●	●	●	●
Chapter 8 – Conduct	●	●	●	●

https://www.fca.org.uk/your-fca/documents/ payment-services-approach(last visited 15 August 2016).

[57] 參閱李儀坤，Fintech 2.0 金融結合科技，即將顛覆金融業的遊戲規則！，凱信企管，2016 年 7 月，第 173-174 頁。

[58] 所謂「小型協力廠商支付業者 (Small payment institutions, SPI)」，係指該業者具有不超過 300 萬歐元之平均每月價值，且不提供跨境支付服務之前提下，該業者可以申請註冊成為小型支付機構，並可以從授權及審慎要求中豁免。需注意的是，成為小型支付機構之前提，一定要向 FCA 申請註冊。You can apply for registration as a small payment institution and be exempt from authorisation and prudential requirements if your firm: has an average monthly payment value of no more than €3 milliondoes not intend to provide payment services on a cross-border basisYou must register with us if you wish to become registered as a small PI. *Available at* : https://www.the-fca.org.uk/firms/apply/ small-payment-institution-spi(last visited 15 August 2016).

[59] FINANCIAL SERVICES AND MARKETS The Payment Services Regulations 2012(2012 No. 1791）. *Available at* : http://www.legislation.gov.uk/uksi/2009/209/pdfs/uksi_20090209_en.pdf(last visited 15 August 2016).

[60] 歐洲經濟區域(European Economic Area, EEA)。在 PSD 的架構及要求下，全部 30 個歐洲經濟區域(EEA)國家均被要求依據 PSD 之規定進行國內立法，該指令引入了新之許可制度來鼓勵非銀行機構進入到支付市場體系。

of Business Requirements				
Chapter 9 – Capital resources and requirements	●			
Chapter 10 – Safeguarding	●	●		
Chapter 11 – Complaints handling	●	●	●	●
Chapter 12 – Supervision	●	●	●	●
Chapter 13 – Reporting requirements	●	●	●	
Chapter 14 – Enforcement	●	●	●	●
Chapter 15 – Fees	●	●	●	●
Chapter 16 – Access to payment systems	●	●	●	●

資料來源：Financial Conduct Authority， The FCA's role under the Payment Services Regulations 2009 Our approach (June 2013)， 12-13. *Available at* : https://www.fca.org.uk/your-fca/documents/payment-services-approach (last visited 15 August 2016).

應注意者，依據資策會科技法律研究所公布之資訊可知，2012 年歐洲議會發表之綠皮書「邁向信用卡、網路以及手機支付的整合歐洲市場（Towards an integrated European market for card，internet and mobile payments）」，並進行廣泛之公眾意見徵詢、舉辦公聽會，最後決議進行現有歐洲支付法制架構修正。歐盟支付服務指令修正案（revised Payment Service Directives, PSD2[61]）於 2013 年 7 月由執委會提出，2015 年 10 月歐洲議會通過，2016 年 1 月生效，本次修正大幅提升支付創新應用之發展可能。PSD2 重大修正，包括針對支付服務之內容作出修正，新增第三方支付服務提供人（third party payment service provider, TPP）為支付服務內容（附件一第 7 項）。TPP 內涵係透過對其他支付服務提供者之支付帳戶存取，提供包含支付發動服務及帳戶資訊服務。依據第 58 條規定 TPP 服務提供者具備下列義務：（1）確保支付服務使用者的個人化安全資訊不會被其它人取得；（2）以明確方式向帳戶之支付服務提供者認證自己之身分；（3）不儲存支付服務使用者的敏感支付資訊或個人化安全憑證[62]。

[61] Revised Directive on Payment Services (PSD2)：The European Parliament adopts the revised Directive on Payment Services (08.10.2015). *Available at* : http://ec.europa.eu/finance/payments/framework/index_en.htm(last visited 15 August 2016).

[62] *Available a*t : https://stli.iii.org.tw/ContentPage.aspx?i=7192 (last visited 15 August 2016).

（三）群眾籌資

英國金融業務監理局（Financial Conduct Authority, FCA）於 2014 年 3 月公布群眾籌資之政策說明書（The FCA's regulatory approach to crowdfunding over the internet, and the promotion of non-readily realisable securities by other media），同時確立對於借貸模式（Loan-based crowdfunding）及投資模式（Investment-based crowdfunding）之監管政策。2014 年 5 月，英國群眾籌資法（The FCA's regulatory approach to crowdfunding over the internet, and the promotion of non-readily realisable securities by other media Feedback to CP13/13 and final rules）生效，針對前揭借貸模式及投資模式提出新之管制規定，投資模式除須合於借貸模式（即前述關於 P2P 網路借貸平台之部分）外，其投資人仍需另符合後述要求[63]：投資屬性上被化歸類為成熟之投資者（例如金融接觸、風險投資接觸或被評定為高淨值客戶（HNW））、零售客戶之可投資金額不得逾越淨投資資產 10%、須通過線上妥適性測驗，亦即對投資人之身份多所限制。

表 3-5：英美網路金融發展及監管規範比較

比較項目		英國	美國
發展模式		第三方支付(Skrill) P2P 網路借貸(Zopa) 股權群眾籌資(Crowdcube)	第三方支付(PayPal) P2P 網路借貸(Lending Club) 股權群眾籌資(Kickstarter)
監管架構	第三方支付	金融業務監理局(FCA)	聯邦存款保險公司(FDIC)
	P2P 網路借貸		證券管理委員會(SEC)，並採取聯邦政府及州政府之雙重監管
	群眾籌資		
法律規範	第三方支付	支付服務法(The Payment Service Regulations 2009)	統一資金服務法案(Uniform Money Services Act)
	P2P 網路借貸	對網路眾籌與其他媒體對未實現證券化的促進監管辦法(包括借貸模式及投資模式)	無專法，僅有 P2P 網路貸款之規制與挑戰報告，搭配證券監管及消費者信貸保護法案。
	群眾籌資		創業企業融資法案(JOBS) 第三章
發展特色		在監管當局頒布相關法律規範之前，該行業組成自律組織並制定規則，用以要求行業會員共同遵守。	注重政府監管及立法規範，即是採用最嚴格證券類之法規監管網路金融業務，降低對金融體系帶來衝擊。

資料來源：本研究整理。

[63] http://www.entrepreneurhandbook.co.uk/changes-in-uk-crowdfunding-regulation-what-it-all-means/ 最後瀏覽日：2015 年 5 月 24 日。

第二節　亞洲國家網路金融風險之之相關規範及監理

一、日本

（一）監理政策

根據 2015 年 3 月麥肯錫公司發表之報告指出[64]，其對 2014 年亞洲個人金融服務調查結果，數位銀行滲透率（指使用網路銀行或智慧手機銀行服務占所有銀行客戶比率）首位係韓國及澳洲 96%，其次為新加坡 94%、香港 93%，我國以 92%位居第五，高於排名第六位日本 83%。前五名僅差距 4%，而日本與我國差距 9%，實難想像先進技術、製造業興盛、科技進步者之日本在數位銀行滲透率上排名不如印象中之高。論者指出，數位銀行滲透率與數位化程度、人口結構及業務推展相關，在此方面日本較我國為低，或因其金融消費者使用習慣及高齡人口比例較高有關[65]。國發會指出，我國 65 歲以上老年人口比率於 2018 年將達 14.36%，正式邁入「高齡社會」； 至 2026 年更將走入「超高齡社會」，老年人口比率達 20.63%。應注意者，由「高齡化社會」進入「高齡社會」，台灣歷時約 25 年，與日本相當，但與法國歷時長達 115 年、美國 72 年、英國 47 年相較，我國轉變時程快速[66]。故包括高齡人口照顧及安養需求等，已成為政府所關注之重要課題，相對歐美之 Finrech 政策，日本受高齡化社會影響而對 FinTech 之相關政策內容，對我國之未來發展，誠屬重要。

日本於 2015 年（平成 27 年）9 月公布「平成 27 事務年度金融行政方針」，其中「4、鑑於 IT 技術之進展金融業及市場變革之戰略性對應」（4. IT 技術の進展による金融業・市場の変革への戦略的な対応）之具體重點政策第（1）點即

---

[64] McKinsey & Company, Digital Banking in Asia: What do consumers really want？(March 2015). *Available at* : https://www.google.com.tw/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=0ahUKEwjDka_blcbOAhVFOJQKHXpkBIkQFggcMAA&url=http%3A%2F%2Fwww.mckinsey.com%2F~%2Fmedia%2Fmckinsey%2520offices%2Fmalaysia%2Fpdfs%2Fdigital_banking_in_asia_what_do_consumers_really_want.ashx&usg=AFQjCNEoK9gWXHW4HLJlI1T2N7nW0OGaCA&sig2=-UJ2OdPK6leB2ZJEpGYLeg(last visited 15 August 2016).

[65] 參閱劉玉枝，參加「2015 銀行公會日本新興金融交流考察團」心得報告，2015 年 10 月，第 29 頁。

[66] 2018 年台灣進入高齡社會。Available at : http://news.ltn.com.tw/news/business/paper/105329(last visited 15 August 2016).

FinTech 之對應[67]。基本上金融與 IT 融合、智慧型手機開始、人工智慧（AI）之授信審查、投資顧問及資產運用等，FinTech 活用範圍非常廣泛，金融業「機能分化」之結構性改變，市場分野、交易所機能改變未來可預見。而日本金融廳為確保對變動極快之 FinTech 產生對應，以及未來金融業務優位性，協請民間部門對海外事業調查與對話，以金融業及市場發展與顧客之便利性提升為目標，積極活用日本國內外專家之貢獻，透過技術革新整備日本經濟與金融環境。

論者指出，日本金融廳彙整日本 FinTech 與其他各國 FinTech 差異[68]：(1) 營運模式不同：其他國家之營運模式不一定適合日本運作。美國為英美法系與日本大陸法系之根本性不同將造成 FinTech 引進之障礙;(2)資本市場活絡之差異：美國市場如天使投資人、創投資金活絡，投資 FinTech 非常積極。日本則為美國 1%，等同 FinTech 新創事業在日本之發展困難;(3) 開戶條件不同：美國低所得（信用評分在 650 分以下）無法在銀行開戶，以及 underbanked 階層為多，日本銀行開戶往來相對容易，與銀行交易極為便利;(4) 業務獨佔性：美國貸款業務非銀行所獨占，非銀行亦可取得許可後，辦理貸款業務。同時美國貸款業務市場膨大，FinTech 跨足經營空間廣，但日本市場規模小，競爭有限;(5) 使用習慣：美國對信用卡、轉帳卡、支票取代現金深入生活習慣，FinTech 在使用上本質並無不同，但日本習慣以現金為主，FinTech 影響日本人民消費習慣仍屬有限。

---

[67] FinTech への対応：足元、すでにスマートフォンでの金融取引等の決済サービスを起點に、人工知能(AI)による 與信審查、投資アドバイスや資產運用等、FinTech を活用した動きが広がっており、金融業の 「アンバンドリング化」とも言うべき構造変化が見られ始めている。市場分野においても、取引所 等の機能の変容等、同様の動きを展望する見方がある。翻って現狀を見ると、こうした構造変化の動きを敏感に捉え、IT ベンチャー等のノンバンク・プ レーヤーと金融機関との連攜・協働等の動きが見られている歐米の狀況に比べ、我が國ではこ のような有機的な対応が遲れている。また、我が國金融機関(金融機関ネットワークを含む)が 提供する決済サービスは、國際的に活動する企業・個人のニーズ(グローバルなキャッシュマネ ジメントサービス、全銀システムの仕様の國際標準化、安価な海外送金手數料等)に十分に対 応出來ていないという課題もある。金融庁としては、我が國が、FinTech の動きに速やかに対応し、將來の金融ビジネスにおけ る優位性を確保するため、民間部門と協働しつつ、海外事例の調查や內外の擔い手との対話 等を通じて FinTech の動向を出來る限り先取りして把握していく。その上で、利用者保護等の金 融行政上の課題と両立させつつ、將來の金融業・市場の発展と顧客利便性の向上につなげて いくとともに、內外の專門家の知見を積極的に活用し、技術革新が我が國経済・金融の発展につながるような環境を整備する。日本金融庁,平成 27 事務年度金融行政方針,2015 年,第 27 頁。*Available at* : http://www.fsa.go.jp/news/27/20150918-1/01.pdf(last visited 15 August 2016).

[68] 參閱李儀坤，Fintech 2.0 金融結合科技，即將顛覆金融業的遊戲規則！，凱信企管，2016 年 7 月，第 129 頁。

（二）P2P 網路借貸

論者指出，就融資面而言，日本與美國類似，P2P 業者適用融資公司法，而在投資面，日本 P2P 機構之投資人，除了適用融資公司法規範外，尚須受「金融商品交易法」規範。為規避上述法令限制，P2P 業者有以隱名合夥持分方式，在網路上募集資金，投資人以不超過 500 人為限，符合私募條件避免成為公開募集資金。然採取隱名合夥之風險在於，投資人並非直接出資融資申請人，雖可免除融資公司法之適用，但日本 P2P 業者除了依據金融商品交易法進行登記外，亦須依融資公司法進行登記，受到日本金融廳監理。論者亦指出，日本小型企業融資本身已有政策性金融機構及區域性銀行及信用合作社提供，日本監理機構並未對 P2P 業務非常重視[69]。然如前述，日本自 2015（平成 27）年 4 月重視 FinTech 之影響，刻正在研擬 P2P 融資法制監理之完備。

（三）第三方支付

論者指出，日本在 2009 年通過「資金決済に関する法律（資金決算相關法律）」，其主要章節包括儲值支付（前払式支払手段）、資金移動（代收付業務）及資金清算（銀行間資金清算，類似財金公司的角色）等三種業務樣態，並對各該業務範圍進行資格、業務內容及風險管理等規範[70]。日本金融廳金融審議會自 2014 年 10 月開始審議有關決算法制問題，自 2015 年 4 月開始彙整相關資料直至同年 12 月公布，並於 2016 年 3 月正式向國會提出「為了對應情報通信技術進展等環境變化之銀行法一部改正法律案」（情報通信技術の進展等の環境変化に対応するための銀行法等の一部を改正する法律案，下稱「銀行法修正案」），於同年 5 月通過參議院審議後即於 6 月公布[71]。

[69] 參閱李儀坤，Fintech 2.0 金融結合科技，即將顛覆金融業的遊戲規則！，凱信企管，2016 年 7 月，第 192-193 頁。李儀坤，英美日 P2P 融資內涵與相關監理，存款保險季刊，第 29 卷第 2 期，2016 年 6 月，第 164 頁。

[70] 我們需要協力廠商支付專法嗎？從各國相關法規看協力廠商支付業務發展，2012 年 6 月 8 日。*Available at* : https://buzzorange.com/techorange/2012/06/08/taiwan-3rd-party-payment-law/(last visited 15 August 2016).

[71] *Available at* : http://www.shugiin.go.jp/internet/itdb_gian.nsf/html/gian/keika/1DBF6D6.htm(last visited 15 August 2016).

其重點為[72]：1、銀行集團規範審查方面：(1) IT 進展伴隨著技術革新之對應：A、銀行集團對金融關聯企業等出資之柔軟化。B、集團內外結算關聯事務受託容易化（修正日本銀行法第 16-2 條及第 52-23 條）。C、利用 IC 晶片支付之預付額裝置（預付卡）表示義務履行方法之合理化（修正日本資金結演算法第 13 條）。D、預付卡發行人面對投訴系統維護之整備（修正日本資金結演算法第 21-2 條）；(2) 通過匯集共通、重複性業務強化金融仲介機能：A、允許執行控股公司型之集團內共通、重複性業務。B、集團內子公司業務匯集容易化（修正日本銀行法第 12-2 條第 3 項）。C、在集團內銀行間資金融通之容易化（修正日本銀行法第 13-2 條）；(3) 銀行集團經營管理之充實：期望銀行集團經營管理機能明確化（修正日本銀行法第 16-3 條、52-21 條）。

2、朝向結算高度化之審查方面：(1) 虛擬貨幣法制度整備：對虛擬貨幣、洗錢與恐怖主義（マネーローンタリンク、テロ）資金提供對策及利用者保護規範整備。A、許可註冊制（登錄制）之導入（修正日本資金結演算法第 63-2~7 條、第 107 條第 5 款）。B、對使用虛擬貨幣者之保護：a.資訊安全管理（修正日本資金結演算法第 63-8 條）。b.對利用者之資訊提供義務（修正日本資金結演算法第 63-10 條）。c.利用者預託之金錢及虛擬貨幣之分別管理義務（修正日本資金結演算法第 63-11 條）。d.導入金融 ADR 制度（修正日本資金結演算法第 63-12 條、第 99-101 條等）。e.外部監理措施整備：事業報告書、進入檢查、業務改善命令等處分之權限（修正日本資金結演算法第 63-13-16 條）。f.洗錢與恐怖注意資金提供對策：開戶時對本人之確認義務；(2) 認定資金結算事業者協會：自律組織建立（修正日本資金結演算法第 87 條）；(3) 其他改正事項：電子記錄收款系統對應電子終端類型預付卡之審查。

[72] 金融庁，情報通信技術の進展等の環境変化に対応するための銀行法等の一部を改正する法律案要綱，*Available at* : http://www.fsa.go.jp/common/diet/190/01/youkou.pdf(last visited 15 August 2016)；横山淳，FinTech、仮想通貨などを巡る銀行法等改正法案の概要 5%ルール、グループ経営管理、仮想通貨交換業者など，大和総研，2016 年 3 月 25 日，第 1-6 頁。*Available at* : http://www.dir.co.jp/research/report/law-research/securities/20160325_010760.pdf(last visited 15 August 2016)；金融審議會，決済業務等の高度化に関するワーキング・グループ報告 ~決済高度化に向けた戦略的取組み ~，2015(平成 27)年 12 月 22 日，第 1-31 頁。*Available at* : http://www.fsa.go.jp/singi/singi_kinyu/tosin/20151222-2/01.pdf(last visited 15 August 2016).

二、新加坡

（一）監理政策

金融科技（FinTech）風潮自歐美吹進亞洲國家，其中新加坡為全球第四大金融中心起跑較快，不僅該國政府大力支持，其公股投資公司整合民間組織打造一站式服務平台，凝聚市場參與者及現有資源，而形成健全金融科技生態圈。該平台串聯政府、銀行、保險公司、投資者及新創公司，由新加坡政府於 2016 年 5 月成立跨部會「金融科技辦公室（FinTech Office）」負責相關事務，鼓勵全球 FinTech 新創業者在新加坡設立據點，而該計畫係新加坡金管局（MAS）及國家研究基金會（NRF）共同宣布。前項 FinTech Office 主要職責一是審查、對應並提高跨政府機構之 FinTech 相關補助計畫；二是關注產業基礎設施、人才培養與人力需求間之斷層，並提出目標戰略、政策及改進方案，三是透過 FinTech 活動與相關倡議推動，管理新加坡金融科技品牌及行銷戰略，致力成為全球金融科技樞紐中心。

事實上，新加坡金管局於 2015 年 6 月揭露新加坡金融科技發展現況與主要關注技術重點，除了行動支付、生物識別驗證、區塊鏈（Blockchain）、雲端運算及大數據等，亦提出成立金融創新推動計畫、打造電子支付基礎架構、建立智慧化監管通報系統、打造 FinTech 生態圈、FinTech 技術與技能培育計畫。此外，同年 8 月新加坡政府成立 FTIG（FinTech & Innovation Group）組織，負責 FinTech 領域政策發展及監管，分為支付與技術方案、技術基礎建設、技術創新實驗室等三個辦公室。並繼英國自 2015 年 3 月提出「監理沙盒（Regulatory Sandbox）」概念後，新加坡金管局於 2016 年 6 月正式提出指導原則，並明確表示在沙盒中註冊 FinTech 公司，可在一明確定義之場所、期間、新加坡金管局提供法規支援情境下進行實驗，且允許在事先報備之情況下，從事與目前法律規範尚有衝突之業務，即便日後被官方終止相關業務，亦不追究其相關法律責任。

誠言之，新加坡金管局設立「監理沙盒」並放寬相關監管條例，目的係鼓勵金融機構或非金融業者在指定範圍與時限，試行創新科技或服務，且可與金管局

共同探討相關條例之放寬範圍。而金管局評估各方案之創新程度、業者是否有意在新加坡廣泛實行方案及該方案是否有利於消費者等因素，作為是否准許試行之依據[73]。換言之，監理沙盒有助減少金融監理摩擦，並為金融科技試驗提供更加安全之環境，以利於創新更有機會生根，但監理沙盒之目的並非防止失敗，而是提供適當保障，掌握失敗對消費者之影響。應注意者，新加坡 FinTech Office 自上線以來至今，僅有 PolicyPal 新創團隊提案，但尚未通過，主要是評估提案所需時間取決於其複雜性，以及具體法律與監管要求參與，惟監理沙盒係屬於探索性質，申請人可允許對重新提交之提案進行調整（詳見圖 3-1）[74]。

[73] FinTech Regulatory Sandbox Guidelines, 2.THE REGULATORY SANDBOX APPROACH: 2.1. MAS would like to encourage more FinTech experimentations so that promising innovations can be tested in the market and have a chance for wider adoption, in Singapore and abroad. 2.2. To achieve this objective, FIs or any interested firm (the "Applicant") can adopt a Sandbox to experiment with FinTech solutions in the production environment but within a well-defined space and duration. The Sandbox should include appropriate safeguards to contain the consequences of failure and maintain the overall safety and soundness of the financial system. 2.3. The Sandbox would be deployed and operated by the Applicant, with MAS providing the appropriate regulatory support by relaxing specific legal and regulatory requirements prescribed by MAS, which the Applicant would otherwise be subject to, for the duration of the Sandbox. Depending on the FinTech solution, the Applicant involved and the proposal made to MAS, MAS will determine the specific legal and regulatory requirements which it is prepared to relax for each case.

[74] FinTech Regulatory Sandbox Guidelines, 8.APPLICATION AND APPROVAL PROCESS: 8.1. The Applicant should ensure that the objective, principles and criteria specified under Section 5 and Section 6 are satisfied before submitting the proposal and ANNEX B to the MAS Review Officer if the Applicant is an MAS regulated FI or xxxxxx@mas.gov.sg. 8.2. The following diagram depicts the application and approval process, and the estimated time frame upon receiving the proposal: a. At the "Application Stage", MAS shall review the proposal and endeavour to inform the Applicant of its potential suitability for a Sandbox within 21 working days after MAS receives a complete and final set of information necessary for the assessment (T0). b. At the "Evaluation Stage", the time required to assess the proposal (T1) is dependent on its complexity and the specific legal and regulatory requirements involved. Due to the exploratory nature of the Sandbox approach, the Applicant is allowed to make adjustments to the proposal for resubmission (for example, refining the boundary conditions) after discussing with MAS. The Applicant would be informed in writing whether to proceed with the Sandbox. c. Upon approval of the proposal, the Sandbox is launched into the "In-Progress Stage", and Section 7 shall apply.

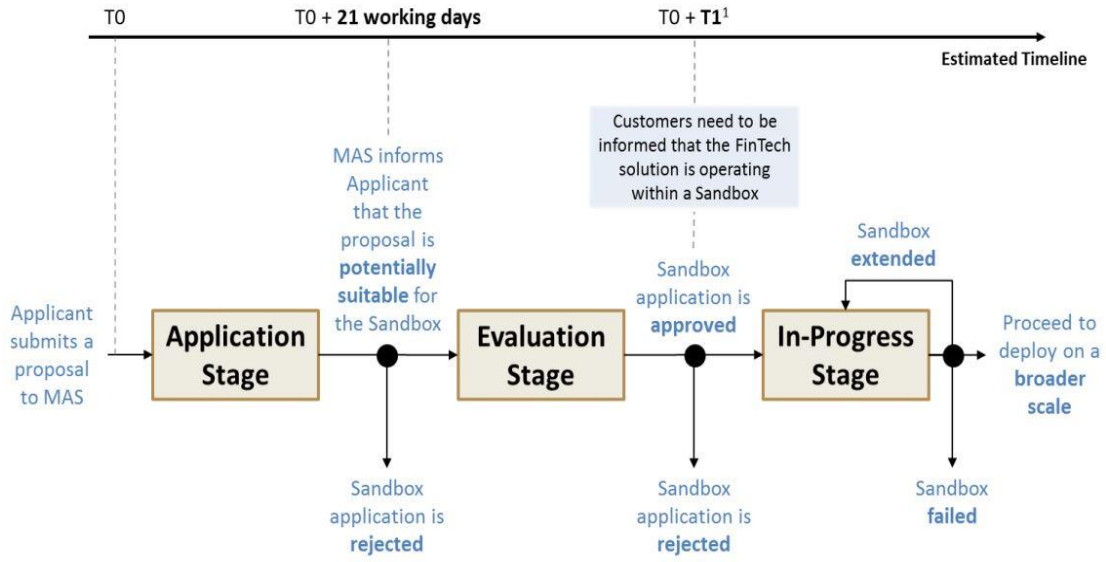


圖 3-1：新加坡 FinTech 監理沙盒申請及核准程式

資料來源：整理自新加坡 FinTech Regulatory Sandbox Guidelines。

（二）P2P 網路借貸

新加坡 P2P 網路借貸平台服務對象以中小企業為主，而非個人借款者，主要新加坡金管局對放貸人資格嚴格控管，無抵押借款僅得提供低收入之新加坡公民或永久住民[75]。新加坡金管局以「放債人法（Moneylenders Act 2010）」、「放債人規則（Moneylenders Rules 2009）」為資金借貸之規範，其中「放債人法」主要是設置消費者保護機制，以保障小額借款人之權益，亦是嚴格監管放債人經營業務之目的，如放債人需經新加坡金管局許可，並取得牌照始得營運。而對 P2P 網路借貸之監管限制，則落實在「證券暨期貨法（Securities and Futures Act, SFA）」及「財務顧問法（Financial Advisers Act, FAA）」，其中 SFA 第 239 條復規定平台

[75] Money Lenders Rule 2009 of Singapore, 19.Unsecured loans only for persons with minimum income or assets: (1) A moneylender shall not grant any unsecured loan to a Singapore borrower, if the total of -(*a*)the amount of the loan; and (*b*)the outstanding amount of every unsecured loan previously granted by him (including, if it is a corporation, its affiliated corporation) to the borrower or jointly to the borrower and one or more other persons, exceeds $3,000 unless, at the time of the grant of the loan, the annual income of the Singapore borrower is at least $20,000, or his total net personal assets exceeds $2 million. (2)A moneylender shall not grant any unsecured loan jointly to 2 or more persons any of whom is a Singapore borrower, if the total of -(*a*)the amount of the loan; and (*b*)the outstanding amount of every unsecured loan previously granted by him (including, if it is a corporation, its affiliated corporation) to the Singapore borrower or jointly to the Singapore borrower and one or more other persons, exceeds $3,000 unless, at the time of the grant of the loan, the annual income of the Singapore borrower is at least $20,000, or his total net personal assets exceeds $2 million. (3)Any moneylender who contravenes paragraph (1) or (2) shall be guilty of an offence and shall be liable on conviction -(*a*)in a case where the offender is an individual, to a fine not exceeding $10,000; and (*b*)in any other case, to a fine not exceeding $20,000.

業者除了向新加坡金融局註冊招股說明書、符合 P2P 借貸業務範圍外，且應取得資本市場服務許可證（Capital Market Services license）[76]。

新加坡將 P2P 網路借貸定位為債權型群眾籌資，並以中小企業為主，該網路借貸平台係透過借款人向投資者簽發本票（Promissory Note），其面額 10 萬美元以上，而每位貸款人投資低於票面總額之金額，由於該商業模式被新加坡金管局認定為「債券」發行，如擬繼續從事借貸業務即須取得許可證[77]。雖以簽發本票之債權型群眾籌資無法免除招股說明書要求，但有符合本票條款者除外[78]，前述所謂除外條款係指排除短期票據，包括商業票據、公司為因應短期融資所簽發之本票（允諾付款票據），但多筆貸款會總之合併本票不在此限[79]。當然每項資金籌集案件不盡相同，如一家籌資企業向二十位貸款人發行面額 10 萬美元，每筆 5,000 美元；或一家籌資企業向三位貸款人發行面額 20 萬美元，一筆 10 萬美元及兩筆 5 萬美元等形式，均須應要求在招股說明書中載明。

（三）群眾籌資

---

[76] See Overview of the Regulatory Framework for P2P Lending and Equity-based Crowdfunding in Singapore (2016), (last visited on Oct. 13, 2016) http://www.p2p-banking.com/countries/asian-overview-of-the-regulatory-framework-for-p2p-lending-and-equity-based-crowdfunding-in-singapore/

[77] Frequently asked questions (FAQs) on lending-based crowdfunding, 10.MAS is aware that some lending-based crowdfunding and P2P lendingplatform operators facilitate the raising of funds by having the borrowers issue asingle promissory note of face value $100,000 or more to multiple lenders, with eachlender lending less than $100,000. Such consolidated promissory notes issued by a borrower under such business models are considered by MAS to be "debentures" and hence are subject to the Prospectus Requirements. Platform operators should nowensure that the participants on their platforms are aware that each lender has tolend at least $100,000 if the borrower is to fall within the Promissory NoteExclusion. Offers of consolidated promissory notes commenced after the date ofthese FAQs must comply with the Prospectus Requirements.

[78] Frequently asked questions (FAQs) on lending-based crowdfunding, 8.Crowdfunding through promissory notes is not exempted from the Prospectus Requirements unless the promissory note in question falls within the Promissory Note Exclusion. A promissory note will only qualify for the Promissory Note Exclusion if it is issued by one borrower to one single lender and has a face value of not less than $100,000, as well as a maturity period of not more than 12 months. A promissory note which is an aggregation of multiple loans from multiple lenders, consolidated into one promissory note which has a face value of not less than $100,000 and a maturity period of not more than 12 months ("consolidated promissory note"), does not qualify for the Promissory Note Exclusion.

[79] Frequently asked questions (FAQs) on lending-based crowdfunding, 9.The Promissory Note Exclusion is meant to exclude short-term notes likecommercial papers and promissory notes issued for short-term financing needs ofcompanies, typically issued by entities with solid credit profiles and bought byaccredited or institutional investors. The Promissory Note Exclusion is not meant toexclude consolidated promissory notes.

股權群眾籌資在新加坡仍是起步階段，而 FundedHere 為第一家以股權群眾籌資為主，同時從事債權籌資之平台，於 2016 年 3 月取得資本市場服務許可證後成立，亦即須依據「證券暨期貨法（SFA）」向新加坡金管局註冊。事實上，新加坡金管局於 2015 年 2 月對股權集資行為發表諮詢文件，對投資者類型僅限合格投資人及機構投資人參與投資，主要考量該類投資人較具有投資經驗及風險管理能力[80]，其中合格投資人（Accredited Investors, AI）對募資企業可投資金額為 3,675 美元[81]，但須在股權眾籌平台登記個人資料及提供證明檔。另對股權群眾籌資平台而言，僅經營機構投資人交易其最低設立資本 25 萬美元，如處理合格投資人交易者，最低設立資本為 50 萬美元，且須向新加坡金管局繳交維持保證金 10 萬美元，並依據 SFA 規定限制其廣告行為。

應注意者，新加坡金管局於 2016 年 6 月提出改善初創公司與中小企業取得資金之機會，並加強對投資人之保護，其相關改善內容，包括簡化對投資人資格審查，股權眾籌平台確定其具財務能力及適合投資即可；下修股權群眾籌資平台最低資本為 5 萬美元，並取消維持保證金制度，有助業者在符合 SFA 相關規定下申請許可證；未單獨向特定人公開消息，不禁止籌資業務之廣告行為[82]。整體而言，新加坡金管局對股權群眾籌資採取開放態度，同時明確其相關法律規定及準則，藉以協助群眾籌資業務在新加坡發展。此外，新加坡金管局除了積極參與 FinTech 新創企業，並理解相關新興創新技術外，亦協助其設計考量金融業法規及風險特性之解決方案[83]。

---

[80] Under Singapore law, individual AIs are required to have at least S$2 million in net personal assets, excluding the primary residence, or earn an annual income of at least S$300,000 (US$200,000). Corporate AIs are required to have at least S$10 million (US$7.4 million) in net assets.

[81] See Singapore's equity and debt crowdfunding platform FundedHere goes live (2016), (last visited on Oct. 13, 2016) https://e27.co/singapores-equity-and-debt-crowdfunding-platform-fundedhere-goes-live-20160321/

[82] New guidelines, to clarify and guide SCF platforms on the parameters within which they can publicise their platforms and services, have been published. In particular, the guidelines will clarify that the advertising restrictions under the SFA do not prohibit SCF platform operators from publicising their services provided no information on specific issuers are disclosed.

[83] See Ravi Menon(Jun 2015), A Smart Financial Centre, Development Initiatives for a Smart Financial Centre: supporting a FinTech ecosystem, The effort to grow a Smart Financial Centre must go beyond the financial industry, to help nurture a wider FinTech ecosystem. We need a strong FinTech community that can: generate ideas and innovations that FIs could adapt and adopt; and provide a platform for collaborations with the industry to produce innovative solutions for defined problems and needs.

表 3-6：日本及新加坡網路金融發展及監管規範比較

比較項目		日本	新加坡
發展模式		第三方支付(GMO-PG) P2P 網路借貸(CrowdBank) 股權群眾籌資(Crowd Equity)	第三方支付(MasterPass) P2P 網路借貸(Funding Societies) 股權群眾籌資(FundedHere)
監管架構	第三方支付	日本金融廳	新加坡金融管理局
	P2P 網路借貸		
	群眾籌資		
法律規範	第三方支付	資金決算相關法律(資金決済に関する法律)	安全支付法(Security Of Payment Act)
	P2P 網路借貸	1.融資公司法 2.金融商品交易法	1.證券暨期貨法(SFA) 2.財務顧問法(FAA)
	群眾籌資	1.金融商品交易法 2.投資型眾籌行業促進條例	
發展特色		與美國同重視立法規範及英國自律規則，經主管機關核准後並符合規定始得經營，但對金融法因應 Fintech 趨勢進行修正，則較我國快速。	雖注重政府監管及立法規範，並以證券類相關法規，但同時採取開放態度，與 Fintech 新創公司互動以順利網路金融業務。

資料來源：本研究整理。

第三節　中國大陸互聯網金融風險之相關規範及監理

近年中國大陸互聯網金融產業快速成形，互聯網金融企業密集度較高之一線城市，該地方政府相繼發布產業扶持政策以推動其穩定發展，包括北京市海澱區人民政府《關於促進互聯網金融創新發展的意見[84]》、北京市石景山區金融服務辦公室《石景山區支持互聯網金融展業發展辦法（試行）[85]》、上海市黃浦區人民政府《關於印發黃浦區建設外灘金融創新試驗區實施意見的通知[86]》、深圳市人民政府《關於支持互聯網金融創新發展的指導意見[87]》，以及天津市人民政府於 2016 年 7 月發布《天津開發區推進互聯網金融產業三年行動方案》等，但僅具象徵性意義或認定標準參考，並無實質規範及監管之功能。直至中國人民銀行於 2015 年 7 月與十部委出台《關於促進互聯網金融健康發展的指導意見[88]》，始有明確監管責任之政策性檔。

[84] 北京市海澱區人民政府 2013 年 10 月 11 日海行規發[2013]3 號。
[85] 北京市石景山區金融服務辦公室 2013 年 8 月 30 日石金融發[2013]48 號。
[86] 上海市黃浦區人民政府 2013 年 8 月 9 日黃府發[2013]18 號。
[87] 深圳市人民政府 2014 年 5 月 13 日深府[2014]23 號。
[88] 中國人民銀行 2015 年 7 月 18 日銀發[2015]221 號。

一、非金融機構之互聯網金融監管規範

（一）P2P 網路借貸

中國銀監會會同工信部、公安部等部會於 2015 年 12 月起草《網路借貸資訊仲介機構業務活動管理暫行辦法（徵求意見稿）》，該辦法明確提出不得吸收公眾存款、不得歸集資金設立資金池、不得自身為出借人提供任何形式之擔保等多項禁止行為，用以補強網路借貸行業形成以來，因監理政策及體制缺失、業務邊界模糊、經營規則不健全等，並在快速發展時所暴露出之問題及風險隱患，進一步引導投資人風險自負，並保障其合法權益。事實上，中國大陸對從事 P2P 借貸之定位，最早可追溯至中國人民銀行於 2014 年 4 月發布《中國金融穩定報告》中「互聯網金融的發展及監管」專題。除了闡述對互聯網金融之定義及概念，亦對 P2P 借貸之特點及國際監理經驗加以描述，並提出互聯網金融監理之立場及原則底線。而國務院於 2015 年 10 月發布《關於進一步做好防範和處置非法集資工作的意見[89]》，其中第 18 點項下提及「儘快出台非存款類放貸組織條例，規範民間融資市場主體」及「儘快出台 P2P 網路借貸、股權眾籌融資等監管規則，促進互聯網金融規範發展」等語，係用於呼籲正視防範非法集資之重要性。

（二）群眾籌資

為規範私募股權群眾籌資業務，同時保護投資者權益及防範金融風險，中國證券業協會於 2014 年 12 月起草《私募股權眾籌融資管理辦法（試行）（徵求意見稿）》，明文股權群眾籌資係採取非公開發行方式，且須通過一定程式自律管理要求，並符合包括投資者應為特定對象、投資者累計不得超過 200 人，以及股權群眾籌資平台與融資者均不得進行公開廣告宣傳、推薦或勸誘等規定，而該平台亦不得兼營 P2P 網路借貸或網路小額貸款業務，但該辦法至今尚未落地。而隨著《關於促進互聯網金融健康發展的指導意見》出台，中國證監會於 2015 年 8 月發布《關於對通過互聯網開展股權融資活動的機構進行專項檢查的通知[90]》，明

[89] 中國國務院 2015 年 10 月 19 日國發[2015]59 號。
[90] 中國證監會 2015 年 8 月 7 日證監辦發[2015]44 號。

文指出如未經中國證監會構核准，不得從事股權群眾籌資活動，而市場上機構冠以「股權群眾籌資」名義之活動，係以互聯網形式進行非公開股權募資行為，非屬前述《指導意見》所定股權群眾籌資之範圍。同一時間，中國證券業協會亦發布《關於調整<場外證券業務備案管理辦法>個別條款的通知[91]》，並將《場外證券業務備案管理辦法》第二條第十項之「私募股權眾籌」修改為「互聯網非公開股權融資」，以確保論述之準確性。

（三）第三方支付

信用卡使用早期在中國大陸未普及，加上實體支付不易、消費者對網路交易信心不足，當具有擔保交易模式之第三方支付服務上市後，即深受消費者喜愛及推崇。為促進支付服務之發展，規範非金融機構支付服務行為，中國人民銀行於 2010 年 6 月制定並公布《非金融機構支付服務管理辦法[92]》，確立第三方支付機構之法律地位，並限制取得「支付業務許可證」始得提供服務，逾期未取得則禁止第三方支付機構繼續從事支付業務，相關實施細則於同年 12 月發布，共同成為第三方支付規範之主要法源依據。為進一步規範客戶備付金管理、網路支付及預付卡業務，中國人民銀行分別發布相關管理辦法，包括 2012 年 9 月《支付機構預付卡業務管理辦法[93]》、2013 年 6 月《支付機構客戶備付金存管辦法[94]》及 2015 年 12 月《非銀行支付機構網路支付業務管理辦法（徵求意見稿）[95]》，其中在網路支付業務方面，分別對綜合類及消費類支付帳戶進行限額管理，包括採用不少於兩類驗證要素，且具有安全級別較高之數位憑證或電子簽名，如無高安全級別驗證，則按照商業銀行之監管要求。

[91] 中國證券業協會 2015 年 8 月 10 日中證協發[2015]170 號。
[92] 2010 年 6 月 14 日中國人民銀行令[2010]第 2 號。
[93] 2012 年 9 月 27 日中國人民銀行令[2012]第 12 號。
[94] 2013 年 6 月 7 日中國人民銀行令[2013]第 6 號。
[95] 2015 年 12 月 28 日中國人民銀行公告[2015]第 43 號。

二、金融法規因應互聯網金融之調整

（一）中國人民共和國商業銀行法

銀行扮演資金供需者之媒合橋樑，除了對企業提供融資資金援助，並在扶持產業發展方面發揮金融仲介功能外，對地方經濟、就業、社會安定等方面亦具有重大貢獻。然由於銀行擁有廣大金融資源，受到高度金融監管，辦理銀行業務須依據《中華人民共和國商業銀行法》及《中華人民共和國銀行業監督管理法》等法律規定，以及最高人民法院司法解釋之規範。其中銀行貸款業務遵守資產負債比例管理之規定，包括（1）資本充足率不得低於 8%；（2）貸款餘額與存款餘額比例不得超過 75%（存貸比）；（3）流動性資產餘額與流動性負債餘額比例不得低於 15%；（4）對同一借款人貸款餘額與商業銀行資本餘額比例不得超過 10%（商業銀行法第 39 條）。但在存貸比方面，全國人大常委會於 2015 年 8 月決議修改商業銀行法，同意將存貸比由法定監管指標轉為流動性風險監測指標，亦即取消存貸比不得超過 75%之要求，而該修正自 2015 年 10 月 1 日起生效。

近年由於互聯網金融興起、直接金融增加等因素導致銀行存款增速放緩，而受制於存貸比考核，銀行貸款投放亦相應受到限制。與此同時，銀行存款利率如維持較高水準，將使得銀行負債成本高居不下，取消存貸比考核有助於貸款利率之下行，推動社會融資成本下降。存貸比監管標準 1995 年推出，當時係為約束銀行信貸規模過快擴張，發揮防範及控制銀行流動性風險，但隨著銀行審慎監管指標體系持續提升，在嚴控流動性風險方面，如流動性覆蓋率、存款準備金率及淨穩定資金比例等，更細緻及準確反映銀行之流動性風險狀況，存貸比監管早已不適用銀行資產負債多元化及業務創新發展之需要。據中信建投證券觀察，存貸比監管指標取消後，16 家上市銀行可釋放 6.6 兆元貸款資金規模，有助於增強銀行服務實體經濟之投放能力。

（二）中國人民共和國證券法

中國大陸《證券法》自 2005 年 10 月首次大幅修訂後，迄今已有十年，由於近年資本市場持續發展，且金融創新進入高峰期，市場環境不可同日而語，相關

法律規範必須順應市場，並修訂升級。爰第十二屆全國人民代表大會常務委員會第十四次會議於 2015 年 4 月召開，會中財經委員會推出《證券法》草案，除了提出股票發行註冊制改革外，亦允許互聯網群眾籌資方式之公開發行模式。此次修訂係以推動市場化、放寬管制鼓勵創新，以及強化對投資者合法權益保護作為主要思維。應注意者，《證券法》草案中，第十三條規定如經由證券經營機構或中國證監會認可之其他機構，以互聯網群眾籌資之方式公開發行證券，發行人及投資者符合中國證監會規定之條件，可豁免註冊或核准。事實上，作為新創公司之風險融資工具，在缺乏明確法律依據之環境下，股權群眾籌資常被與非法集資類比，而此次《證券法》修訂即是明文確立其合法性。

（三）關於改進個人銀行帳戶服務加強帳戶管理通知

中國人民銀行於 2015 年 12 月發布《中國人民銀行關於改進個人銀行帳戶服務加強帳戶管理的通知[96]》，用以落實個人銀行帳戶實名制、建立銀行帳戶分類管理機制、規範代理開立個人銀行帳戶、強化銀行內部管理及改進銀行帳戶服務等五大面向，對個人銀行結算帳戶進行規範。其中在銀行帳戶方面，過去經銀行臨櫃開立之帳戶劃為Ⅰ類銀行帳戶，而日後申請人可透過臨櫃、遠端視頻櫃員機及智慧櫃員機等自助機具、網路銀行及行動銀行等電子通路，開立Ⅰ類、Ⅱ類或Ⅲ類銀行帳戶[97]。Ⅰ類銀行帳戶可辦理存款、購買投資理財產品、轉帳、消費及繳費支付、支取現金等業務；Ⅱ類銀行帳戶辦理存款、購買投資理財產品、限定金額之消費及繳費支付等業務，而Ⅲ類銀行帳戶，則僅可辦理限定金額之消費及繳費支付服務。Ⅱ類及Ⅲ類帳戶之設置，係用以滿足客戶個性化需求及電子商務交易需要，具有靈活性及較強之便利性，但為有效控制客戶資金風險，Ⅱ類帳戶設有單日 10,000 元人民幣支付限額，Ⅲ類帳戶則有 1,000 元餘額之限制。

[96] 中國人民銀行 2015 年 12 月 25 日銀發[2015]392 號。

[97] (1)臨櫃受理銀行帳戶開戶申請，銀行可為開戶申請人開立Ⅰ類、Ⅱ類或Ⅲ類帳戶。(2)透過遠端視頻櫃員機、智慧櫃員機等自助機受理銀行帳戶開戶申請，如銀行工作人員現場核驗開戶申請人身份資訊，銀行可為其開立Ⅰ類帳戶；未現場核驗開戶申請人身份資訊，僅可為其開立Ⅱ類或Ⅲ類帳戶。(3)以網路銀行及行動銀行等電子通路受理銀行帳戶開戶申請，銀行可為開戶申請人開立Ⅱ類或Ⅲ類帳戶。

前項《通知》公布前，銀行即須依據《人民幣銀行結算帳戶管理辦法》相關規定開立之個人銀行帳戶，納入Ⅰ類帳戶管理，並將試點開立其他個人銀行帳戶劃為Ⅱ類帳戶管理，且應於 2016 年 4 月 1 日前完成對通過自助機具、電子通路開立之個人銀行帳戶進行核實。而於 2016 年 4 月 1 日在系統中對Ⅰ類、Ⅱ類及Ⅲ類帳戶進行有效區分，並按規定向人民幣銀行結算帳戶管理系統報備，同時將銀行帳戶區分及標識方法向中國人民銀行備案。目前銀行可採取多種方式對開戶申請人之身份資訊進行交叉驗證，但生物特徵辨識尚無法運用，其因係中國大陸缺乏生物特徵識別技術之基礎標準，亦無應用於金融領域之國家認定標準，不具作爲核驗存款人身份資訊方式之條件。事實上，匯豐銀行於 2016 年開始在英國引進聲音及指紋辨識，客戶以手機登入網路金融服務系統，可錄製聲軌取代傳統密碼，大為簡化線上金融服務流程。

（四）銀行業金融機構全面風險管理指引

事實上，為進一步引導銀行業樹立全面風險管理意識及體系，持續提高風險管理水準，中國銀監會參照巴塞爾銀行（BCBS）「有效銀行監管核心原則」，於 2016 年 6 月起草《銀行業金融機構全面風險管理指引（徵求意見稿）》，其中在各類風險中除了信用風險、市場風險、流動性風險外，加入資訊科技風險，並應建立可供識別、計量、評估、監測、報告、控制之管理方法，以及與業務規模及風險狀況等相符合之資訊科技基礎設施。再者，在資料品質上，該指引要求銀行業建立資料品質控制機制，用以蒐集及運用具有準確、連續與完整之內部與外部資料，同時需訂立可確保及時應對，以及處理緊急或危機情況之應急計畫。整體而言，雖前項指引尚在徵求社會意見階段，但不可諱言，其係銀行業風險管理之綜合性規則，並更加嚴格且明確要求在銀行創新業務發展過程，新種風險產生時可迅速掌握，進而防範跨境、跨業風險。

三、銀行業因應互聯網金融發展之作法

誠如前述，2015 年 7 月國務院十部委出台《關於促進互聯網金融健康發展的指導意見》，同年 12 月中國人民銀行發布《非銀行支付機構網路支付業務管理辦法》及《關於改進個人銀行帳戶服務加強帳戶管理通知》，中國銀監會亦會同工信部、公安部、國家網信辦等部門研究起草《網路借貸資訊仲介機構業務活動管理暫行辦法（徵求意見稿）》。該等一系列監理新規代表監理部門對互聯網金融業態之監管尺度逐漸轉嚴，相較過去，即從包容性監管轉為至審慎監管，以避免互聯網金融脫離金融本質、脫離與金融機構相同強度之對稱監管。而伴隨著監理規範之確立，以及投資人受到詐欺及巨額資金損失之風險警示，中國大陸社會對互聯網融之風險偏好，較過去更加客觀及理性之看待。事實上，互聯網金融本質仍屬金融，並未改變金融風險之廣泛性及傳遞性，隨著「互聯網+金融」之深度發展，在金融業務不斷豐富，且金融服務及產品存在民眾日常生活中，如影隨形之信用危機、資訊不對稱、虛假資訊及詐欺取財等問題，勢必帶來新法律風險、資訊安全及金融穩定風險。

雖金融數位時代來臨，但銀行固有文化，並未將便利性及用戶體驗視為首要重點，無法提供便捷地提供標準化及低門檻之金融服務，然技術創新與金融脫媒帶來之創新，銀行業已體會隨著互聯網金融持續發展下，應運而生之新商業模式勢必對傳統業務造成衝擊。對此，銀行業對創新轉型之共識逐漸成形，從早期之網路銀行、行動銀行等電子通路商品轉移及服務延伸，發展至向互聯網企業或是金融科技公司學習，快速更迭金融商品，並開發互聯網模式之營運。然互聯網之高頻場景及流量入口，早已被阿裡巴巴等互聯網龍頭佔據，在金融服務場景拓展及互聯網獲客方面受到擠壓同時，銀行業開始在通路宣傳、客戶情感訴求洞察等方面重新打造流程。從銀行業觀察角度來看，銀行業之互聯網轉型主要呈現在其內部透過互聯網新技術創新，以提高服務效率、降低營運成本，如銀行根據客戶信用卡消費紀錄，挖掘客戶生命週期並主動推銷消費金融服務，以達到提高客戶忠誠度之目的。

再者，銀行業與金融科技公司合作，達到提升服務黏性或開拓全新客戶群之目標，例如大通銀行與 MCX 合作，將其 8,900 萬隻個人客戶開放給 MCX，作為使用掃碼支付之天使客戶，用意在於為自身零售客戶提供全新支付體驗。其次則直接投資成立互聯網金融公司，為日後傳統業務萎縮面臨之經營週期轉折，安排主營業務切換之戰略準備。綜前所述，銀行業面對互聯網金融之競爭力，來自於大數據之採集及應用能力，由於逐漸體會大數據對全球生產、流通、分配、消費活動，以及經濟運行機制、社會生活方式產生重大影響，國務院於 2015 年 8 月發布《關於促進大數據發展的行動綱要[98]》，從頂層設計之層面推動，包括大數據開放共用、大數據技術研發、大數據安全運用等任務目標，對銀行業利用大數據提升互聯網金融創新及經營能力，提供底層之基礎設施。該行動綱領首要工作係於 2018 年前，推動政府與公部門資料統一彙整並向社會開放，同時建立政府資料蒐集及安全管理標準，加強政府資料開放之標準化。

誠言之，隨著網路、行動載具、智慧手機及數位科技之演進，掀起傳統產業版圖之轉移，該版圖轉移現象亦出現在金融業中，金融業之客戶行為與經營環境正面臨著極大之變化。如以銀行業為例，當可隨時使用銀行服務之網路銀行出現時，其所提供之控制感與多元選擇特性，符合年輕世代客戶之需求，短時間內即接納虛擬通路，甚至網路銀行之發展可能超越實體分行，而成為年輕族群與銀行間最主要之通路[99]。而當智慧手機問世後，更加迅速催生行動銀行，其可在任何時間、任何地點操作現金以外銀行業務之情境，銀行不再是一個「地方」，而是一種「行為」。應注意者，中國銀監會於 2016 年 7 月公布《中國銀行業資訊科技「十三五」發展規劃監管指導意見（徵求意見稿）》，主要是督促指導銀行業加強資訊化建設，並依託銀行業長期積累之風險控管、公司治理、資料優勢等，適應互聯網金融創新發展之趨勢，同時加強跨業、跨界之合作，以促進金融互聯網與互聯網金融之融合。

---

[98] 中國國務院 2015 年 8 月 31 日國發[2015]50 號。

[99] 參閱安怡芸，數位化金融環境 3.0 下金融監理政策規劃方向之探討，國會月刊，第 44 卷第 1 期，2016 年 1 月，第 74 頁。

前項指導意見明確指出，「十三五」規劃期間逐步落實《關於積極推進「互聯網+」行動的指導意見[100]》、《促進大數據發展行動綱要》及《關於促進雲計算創新發展培育資訊產業新業態的意見[101]》，並持續推動對新興科技之研究及成果應用，用以優化客戶體驗、增加客戶黏性，進而支援銀行業務之轉型，始能鞏固現有金融服務之能力。此外，銀行業面臨更加複雜之網路及資訊安全威脅，常規攻擊不斷進化，包括分散式阻斷服務攻擊（DDoS）、進階持續性威脅（APT）等攻擊手段推陳出新，且釣魚、假基地台等欺詐手段對客戶資訊安全之威脅進一步擴大，因而新技術迅速應用帶來之潛在風險隱患亦不容忽視。應注意者，該指導意見要求需加強資料中心運營管理能力之建設，截至「十三五」規劃末期，按照相關標準[102]，大中型銀行資料中心服務能力成熟度不低於 III 級，而其他機構資料中心服務能力成熟度則不低於 II 級。

第四節　我國網路金融風險之相關規範及監理

一、非金融機構之網路金融法律規範

由於電子科技快速發展，促使金流支付模式隨之推陳出新，特別是以網路技術與各類行動載具所發展之新興電子支付服務。在此一趨勢潮流下，為加強電子支付機構之管理，以建立消費者使用電子支付之信心，同時降低小額交易之支付成本，我國於 2015 年 2 月制定公布「電子支付機構管理條例[103]」（以下稱「管理條例」），允許支付機構從事代收代付業務、儲值業務、電子支付帳戶間款項移轉業務，亦可將支付款項運用於購買政府債券、國庫券、定存單及經主管機關核准之其他金融商品。「管理條例」所稱之電子支付機構，係經主管機關許可以網路或電子支付平台作為仲介，接受使用者註冊及開立記錄資金移轉與儲值情形之帳戶（以下稱電子支付帳戶），並利用電子設備以連線方式傳遞收付訊息，於付款

[100] 中國國務院 2015 年 7 月 1 日國發[2015]40 號。
[101] 中國國務院 2015 年 1 月 6 日國發[2015]5 號。
[102] 資料中心服務能力成熟度之標準，由工信部國家資訊技術服務標準工作組制訂。
[103] 中華民國 104 年 2 月 4 日總統華總一義字第 10400012581 號令。

方及收款方間經營代理收付實質交易款項、收受儲值款項、電子支付帳戶間款項移轉。如有涉及外匯部分，則應依中央銀行之相關規定辦理，且實質交易之標的須為經主管機關核准代理收付款項之金融商品或服務。

再者，「管理條例」對電子支付機構亦訂有最低實收資本額，如經營「管理條例」第 3 條所列示之業務，實收資本額新台幣 5 億元以上，但僅從事代理收付實質交易款項業務之電子支付機構，實收資本額新台幣 1 億元以上，惟主管機關仍有視社會經濟情況及實際需要調整之裁量權。當然，電子支付機構經營「管理條例」核准之業務，自取得營業許可後六個月內，必須向主管機關申請核發營業執照，並應在開始營業之日起算五個營業日內，以書面通知主管機關。而除了非金融機構之電子支付機構外，「管理條例」允許銀行、中華郵政公司或電子票證發行機構均得申請兼營支付業務，其中銀行及中華郵政公司兼營業務所收受理之儲值款項，除了依據規定提列準備金外，亦是存款保險制度之標的。其次，在業務限額上，專營支付業務之電子支付機構所收受儲值款項，不得超過新台幣 5 萬元，而辦理電子支付帳戶間款項移轉，每筆亦不得超過新台幣 5 萬元，而當收受儲值款項合計達一定金額，則應依法繳存足額之準備金。

應注意者，由於電子支付機構保管支付款項非屬存款業務性質，且基於洗錢防制目的，以及使實際資金流向及歸屬得以確認，如當使用者提領電子支付帳戶款項時，其應將提領款項轉入該使用者銀行存款帳戶，不得以現金支付。就支付款項之動用及運用方式而言，電子支付機構對代理收付款項，應以專用存款帳戶儲存及保管為限，但儲值款項得在一定比率內以銀行存款，或購買政府債券、國庫券或銀行可轉讓定期存單，以及經主管機關核准之金融商品等方式為之。此外，在客戶資料保護方面，電子支付機構應建立使用者身分確認機制，並留存確認使用者身分程式所得之資料，以及使用者電子支付帳戶之帳號、交易項目、日期、金額及幣別等必要交易紀錄至少五年。對使用者之往來交易資料及其他相關資料，亦應保守秘密，不得利用使用者個人資料為第三人從事行銷行為。不可諱言地，電子支付除了提供用戶更親民、便利之支付工具外，在跨境支付應用上，亦支援電商跨境銷售參與他國之消費市場。

二、金融機構從事網路金融業務之規定

（一）創櫃板管理辦法

我國微型創新企業雖經營規模小且缺乏資金，但創意本質具發展潛力，亟須扶植其成長茁壯，並響應政府政策扶植微型及小型創新企業之發展，以活絡資本市場動能，證券櫃檯買賣中心（以下稱櫃買中心）在金融監督管理委員會（以下簡稱金管會）支援下籌設創櫃板。該「創櫃板管理辦法[104]」於 2013 年 11 月核予備查後公告全部條文，並於 2014 年 1 月正式啟用「創櫃板」專區，以協助我國創新創意企業發展順利籌資。創櫃板基本概念係參考美國 JOBS 法案，鼓勵新興成長企業上市豁免規定，以及股權型群眾籌資平台等規範而建置。申請在創櫃板募資之募資公司，實收資本額以低於新台幣 5,000 萬元為限，募資公司辦理登錄前增資作業，須將員工及原股東放棄而原應洽特定人認購之股份，全數於創櫃板籌資專區進行籌資，以近一年增加股本面額累計低於新台幣 1,500 萬元為限。

在投資人認購金額方面，非專業投資人最近一年內對所有創櫃板公司認購投資股票累計金額不得超過新台幣 15 萬元，並簽署「風險預告書」，專業投資人則不受限。但美國 JOBS 法案將投資人等級分為五類（詳表 3-7），且募資公司一年內籌資不超過 100 萬美元為限，惟創櫃板設立宗旨，係扶植微型及小型創新企業之發展，故設定募資公司在申請登錄創櫃板時，其資本額不宜大於得申請上櫃之公司。在轉售限制上，取得創櫃板股票後原則上一年內不得轉售，賣回原發行人除外，而美國 JOBS 法案則允許轉賣合格投資人、原購買人家族成員，以及買方為設立家族信託之委託人等對象[105]。此外，我國證券交易法未如同美國證券法上設有籌資平台（Funding Portal）之概念，募資公司僅得透過經註冊合格之證券商

[104] 金融監督管理委員會 102 年 11 月 12 日金管證發字第 1020042930 號函備查；證券櫃檯買賣中心 102 年 11 月 15 日證櫃審字第 10200286981 號公告。

[105] Regulation Crowdfunding: A Small Entity Compliance Guide for Issuers, 5. Restrictions on Resale: Securities purchased in a crowdfunding transaction generally cannot be resold for a period of one year, unless the securities are transferred: (1) to the issuer of the securities; (2) to an "accredited investor"; (3) as part of an offering registered with the Commission; or (4) to a member of the family of the purchaser or the equivalent, to a trust controlled by the purchaser, to a trust created for the benefit of a member of the family of the purchaser or the equivalent, or in connection with the death or divorce of the purchaser or other similar circumstance.

發行股票以募集資金，故如有商品型群眾籌資平台擬從事股權募資行為，須申請註冊為合格證券商後始得為之。

表 3-7：美國 JOBS 法案投資人等級分類

Investor Annual Income	Investor Net Worth	Calculation	Investment Limit
$30,000	$105,000	Greater of $2,000 or 5% of $30,000 ($1,500)	$2,000
$150,000	$80,000	Greater of $2,000 or 5% of $80,000 ($4,000)	$4,000
$150,000	$100,000	10% of $100,000 ($10,000)	$10,000
$200,000	$900,000	10% of $200,000 ($20,000)	$20,000
$1,200,000	$2,000,000	10% of $1,200,000 ($120,000), subject to $100,000 cap	$100,000

資料來源：本研究整理。

（二）證券商經營股權性質群眾籌資管理辦法

為兼顧保障投資人權益，並適度結合民間業者能量共同活絡我國創新創業之風潮，金管會授權櫃買中心訂定「證券商經營股權性質群眾籌資管理辦法[106]」，協助富有創新創意之微型企業得以順利籌措所需資金，該法於 2015 年 4 月正式發布。由於公開募資行為屬證券交易法規範業務，僅限證券商始得為之，爰平台業者須申請為證券商，並向金管會申請許可及核發許可證。有別於創櫃板之處，證券商僅得受理實收資本額新台幣 3,000 萬元以下之募資公司，在募資平台辦理股權募資，並揭示募資公司之基本資料及現金增資等資訊。而從事股權群眾籌資業務之平台業者，與櫃買中心簽約後，始得經營該項業務（契約關係），並依據相關標準規範訂定內部控制制度。該募資平台僅得採取單一募資平台方式，專營股權性質群眾籌資業務，其辦理股權募資之有價證券，僅限於募資公司之普通股股票，對募資公司收取之手續費及服務費用亦須揭露在公開網站上。

應注意者，因網路經濟及創新經濟之需，行政院於 2015 年 4 月通過經濟部擬具「公司法」部分條文修正草案，經立法院審議後，於同年 6 月三讀通過增修

[106] 中華民國 104 年 4 月 29 日金融監督管理委員會金管證發字第 1040015319 號函。

閉鎖性股份有限公司之規定[107]。相較一般股份有限公司，閉鎖性公司股東人數以五十人為限，且出資種類包括現金、公司所需財產、技術、勞務或信用等，利於吸引優秀人才加入創業圈，惟非以現金出資須全體股東同意、章程載明，並公開於資訊網站上。此外，閉鎖性公司原則上不得公開發行或募集有價證券，但得向主管機關許可之證券商群募平台公開募資，即賦予募資公司較大自治空間，以及多元化籌資工具、更具彈性之股權安排。惟應注意者，閉鎖性公司雖可發行複數特別股，但證券商群募平台僅得以普通股進行募資，且限制股東人數與公開募資性質或許有些許悖離。

三、主管機關因應金融科技之法規及制度調整

（一）現行銀行業務適用法規修正

由於行動通訊、社群媒體、大數據、雲端科技等資訊訊技術進步，金融服務勢必須順應時代潮流、配合資訊發展，以提升消費者便利性。為促進我國金融業全面朝向「網路化」及「行動通訊」之升級，金管會於 2014 年 6 月首次宣布將打造台灣數位化金融環境 3.0 版本，並提出「調整法規因應業者需求」、「資訊安全是未來管理重點」、「強化消費者保護工作」及「強化金融資訊專業能力」作為四大因應策略。而為進一步落實該項政策，金管會於 2015 年 1 月起推動「打造數位化金融環境 3.0」計畫，除了對既有存款戶在網路銀行與行動銀行得辦理之金融業務外，新增 12 項業務[108]（包括存款業務、授信業務、信用卡業務、財富管理業務及共同行銷業務）可於線上申辦，同時修正三項自律規範[109]及提出配合

[107] 中華民國 104 年 7 月 1 日總統華總一義字第 10400077151 號令修正；中華民國 104 年 9 月 3 日行政院院台經字第 1040047867 號令發布定自 104 年 9 月 4 日施行。

[108] 新增線上申辦業務項目：(一)存款業務 3 項：線上申請(1)結清銷戶、(2)約定轉入帳號、(3)受理客戶傳真指示扣款無須再取得客戶扣款指示正本。(二)授信業務 1 項：線上申辦貸款，係指無涉保證人之(1)個人信貸、(2)房貸、車貸於原抵押權擔保範圍內之增貸、(3)客戶線上同意銀行查詢聯徵中心信用資料。(三)信用卡業務 3 項：線上申辦(1)信用卡、(2)長期使用循環信用持卡人轉換機制中之「信用卡分期方案」、(3)線上取得客戶同意信用卡分期產品約款。(四)財富管理業務 4 項：線上申辦(1)信託開戶、(2)認識客戶作業(KYC)、(3)客戶風險承受度測驗及(4)客戶線上同意信託業務之推介或終止推介、(5)共同行銷業務 1 項。

[109] 「銀行銷戶處理程式自律規範」、「金融機構代客戶辦理存提款作業範本」及「金融機構辦理電子銀行業務安全控管作業基準」。

電子化申辦及交易之相關消費者保護措施，並於同年 2 月，修正「現金卡應注意事項」、「信用卡管理辦法」、「信託業行銷訂約辦法」及「金控公司子公司間共同行銷辦法」等規定（詳見表 3-8），以便利消費者使用各項線上申辦業務。

表 3-8：我國打造數位化金融環境 3.0 之法規修正重點

銀行業務	適用法規	修正重點	修正效益
授信	金融機構辦理現金卡業務應注意事項	1. 刪除「當面宣讀」。 2. 重要事項之確認機制，增列可以「其他得以辨識申請人同一性及確定申請人意思表示之方式確認」。 3. 不良債權讓與及申訴專線通知方式，增列「電子檔」通知方式。	便利民眾線上申辦現金卡業務時，得以更簡捷作業方式辦理。
信用卡	信用卡業務機構管理辦法	同上 2、3	便利民眾線上申辦信用卡業務時，得以更簡捷作業方式辦理。
財富管理	信託業營運範圍受益權轉讓限制風險揭露及行銷訂約管理辦法	1. 增訂「所稱書面，依電子簽章法之規定，得以電子檔為之。」 2. KYC 作業，增訂得經客戶以蓋用原留印鑑或其他雙方同意之方式確認資料內容及分析結果。 3. 境內結構型商品之客戶須知，增訂得以電子設備方式向非專業投資人告知，並留存相關作業過程之軌跡。	便利民眾線上申辦信託業務時，得以更簡捷作業方式辦理。
共同行銷	金融控股公司子公司間共同行銷管理辦法	增列得以其他可辨識客戶同一性及確認其意思表示之方式，作為取得客戶同意資料交互使用之方式。	金控公司子公司得以「電子檔」方式取得，以利業者推動金融數位化。

資料來源：整理自金融監督管理委員會新聞稿，「打造數位化金融環境 3.0 推動情形」，2015 年 2 月 10 日。

（二）主管機關金融科技發展政策

再者，金管會為持續推動金融業運用科技創新服務，以提升金融業之效率及競爭力，並促進金融科技產業發展，除了推出「打造數位化金融環境 3.0」計畫外，更於 2015 年 9 月設立「金融科技辦公室」，並發布「銀行及金融控股公司申請轉投資資訊服務業及金融科技業規定」，將金融科技業及資訊服務業一併認定為金融相關事業，亦即持股最高可達 100%，其中資訊服務業及金融科技業之年

度營業成本或營業收入，係來自金融事業及金融服務之比率下限為 51%。所謂資訊服務業，係指主要業務為從事與金融機構資訊處理作業密切相關之電子資料處理、涉及金融機構帳務之電子商務交易資訊之處理，或研發設計支援金融機構業務發展之金融資訊系統者，而金融科技業則是指利用資訊或網路科技，從事輔助金融機構業務發展之資料蒐集、處理、分析或供應，以提升金融服務或作業流程之效率或安全性[110]。

此外，金管會在研析國際金融科技發展趨勢及國內推動現況後，於 2016 年 5 月公布「金融科技發展策略白皮書」，將發展金融科技（FinTech）定調為提升國家競爭力之重要戰略，並以 2020 年為期，分別就金融服務、創新研發、人才培育、風險管理、基礎建設等五大構面發展金融科技。事實上，金管會已於 2014 年 8 月首度開放保險業辦理網路投保業務，初期僅開放強制汽車責任保險、任意汽車保險、住宅火災及地震基本保險、住（居）家綜合保險及旅遊不便險、旅行平安保險、傷害保險及定期人壽保險等特定險種之網路投保，金融消費者不必再親簽檔。第二階段放寬於 2014 年 12 月起，以網路方式首次註冊之非有效契約客戶，得藉由本人信用卡或本人存款帳戶，作為加強身分輔助驗證機制進行網路投保。2015 年 6 月開放第三階段保險業辦理網路投保業務，如放寬保險業辦理網路投保之險種及提高投保額度，增加網路保險服務。第四階段則是配合內政部開放自然人憑證適用範圍（身分識別及資料保護），於 2016 年 3 月放寬要保人及被保險人不同人，可以自然人憑證投保。

整體而言，數位金融日趨盛行之重要原因，即科技與網路之發展，因而參與數位金融業務之業者，並非是傳統定義下之金融機構，甚至其所從事之業務是否屬於金融業務、是否歸於金融主管機關監理，仍容有討論空間。但不可諱言地，隨著數位金融與行動支付之興起，以網路或行動交易系統為攻擊目標之惡意程式亦日漸流行，促使資訊安全與個資保護之問題再度受到重視，包括偽裝銀行網路應用系統之「宙斯（ZeuS）」，或以在鎖定對象附近架設訊號基地台之方式，透過

[110] 銀行及金融控股公司申請轉投資「資訊服務業」及「金融科技業」，屬於銀行法 74 條第 4 項所稱「其他經主管機關認定之金融相關事業」及金融控股公司法第 36 條第 2 項第 11 款所稱「其他經主管機關認定與金融業務相關之事業」。

「綁架」病毒攔截被害人之手機簡訊、應用程式等。我國尚無銀行推出行動銀行以指紋等生物辨識系統，而係普遍採用雙步驟或雙因數身分認證，仍有無法加強資安維護之作用。在面對未來可能產生新興金融業態時，除了金融機構積極擴展數位金融業務外，金融、經濟、治安、通訊或科技等相關主管機關，尚須建立較緊密之橫向聯繫機制，避免由單一主管機關監理，不僅較難進行全面性監控，其監理模式及強度亦有所不足。

（三）小結

雖我國現既存處理銀行體系之信用風險內部大型資料庫，已運行多年，但在大數據及雲端技術之完備下，實有運用雲端資料、大數據等創新科技，強化國內銀行業可動態取得及掌控授信交易對手之借款行為軌跡，確實有效提升信用風險之因應能力必要性，特別是對法人外部訊息資料庫之大數據分析，即時掌控法人企業之財務行為，提升我國金融機構對信用風險之因應能力[111]。事實上，金管會於 2000 年核准銀行開辦網路銀行業務（Internet Banking）後，全體銀行業均已建置自行網路銀行系統，惟各金融機構之網路銀行業務作法，僅係基於傳統銀行服務作業模式，視網路為前端通路介面。亦即僅在既有實體服務上增加虛擬服務介面，即使網路銀行業務日趨成熟，業務服務成效不易大幅成長。

誠言之，金融科技高度利用資通訊技術開發新型態服務之同時，需特別注重相關金融資訊及個人資料之隱私與安全。所謂資安威脅係來自非法管道，但跨境之金融科技服務，則是藉由合法管道進入國內市場，並廣泛地蒐集相關之大數據情資，對來自特定國家或有特定目的之機構，須維持我國經濟與金融資訊之高度自主性。其中在徵信方面，過去金融聯徵中心長期累積國人之信用資料，但支付服務屬於挖掘未來之消費行為，而該類金融資訊之蒐集，顛覆我國金融業者徵信工具之基礎，進而可能影響其之競爭力。對此，為因應銀行業運用新興科技，如雲端服務、社群媒體及自攜裝置所可能面臨資訊安全需求，銀行公會研訂「運用新興科技應注意事項」，協助業者建立必要之資訊安全防護機制。

[111] 參閱金融監督管理委員會，金融科技發展策略白皮書，2016 年 5 月，第 24-26 頁。

表 3-9：主要國家及台灣網路金融發展與監管規範比較

比較項目		英國	美國	日本	新加坡	中國大陸	台灣
發展模式		第三方支付(Skrill) P2P 網路借貸(Zopa) 股權群眾籌資(Crowdcube)	第三方支付(PayPal) P2P 網路借貸(Lending Club) 股權群眾籌資(Kickstarter)	第三方支付(GMO-PG) P2P 網路借貸(CrowdBank) 股權群眾籌資(Crowd Equity)	第三方支付(MasterPass) P2P 網路借貸(Funding Societies) 股權群眾籌資(FundedHere)	第三方支付(支付寶) P2P 網路借貸(陸金所) 股權群眾籌資(人人投)	第三方支付(歐付寶、永豐銀行) P2P 網路借貸(鄉民貸) 股權群眾籌資(創櫃板)
監管架構	第三方支付	金融業務監理局(FCA)	聯邦存款保險公司(FDIC)	日本金融廳	新加坡金融管理局	中國人民銀行	金融監督管理委員會，但對 P2P 網路借貸，一不納入金融監理二不設立專法
	P2P 網路借貸		證券管理委員會(SEC)，並採取聯邦政府及州政府之雙重監管			中國銀監會	
	群眾籌資					中國證監會	
法律規範	第三方支付	支付服務法(The Payment Service Regulations)	統一資金服務法(Uniform Money Services Act)	資金決算相關法律(資金決済に関する法律)	安全支付法(Security Of Payment Act)	非金融機構支付服務管理辦法	電子支付機構管理條例
	P2P 網路借貸	對網路眾籌與其他媒體對未實現證券化的促進監管辦法(包括借貸模式及投資模式)	無專法，僅有 P2P 網路貸款之規制與挑戰報告搭配證券監管及消費者信貸保護法案。	1.融資公司法 2.金融商品交易法	1.證券暨期貨法(SFA) 2.財務顧問法(FAA)	網路借貸業務管理暫行辦法(草案)	無專法，直接適用現行法規
	群眾籌資		創業企業融資法案(JOBS)第三章	1.金融商品交易法 2.投資型眾籌行業促進條例		1.私募股權眾籌融資管理辦法 2.證券法	1.創櫃板管理辦法 2.證券商經營股權性質群眾籌資管理辦法
發展特色		在監管當局頒布相關法律規範之前，該行業組成自律組織並制定相關規則，用以要求行業會員共同遵守。	因注重政府監管及立法規範，即是採用最嚴格證券類之法規監管網路金融業務，降低對金融體系帶來衝擊。	與美國同重視立法規範及英國自律規則，經主管機關核准後並符合規定始得經營，但對金融法因應 FinTech 趨勢進行修正，則較我國快速。	雖注重政府監管及立法規範，並以證券類相關法規，但同時採取開放態度，與 FinTech 新創公司互動以順利網路金融業務。	監管制度及自律規則均落後於業務發展，但其發展模式相較英美兩國多元，並開創符合國情之創新服務及產品。	與美國同注重政府監管及立法規範，經主管機關核准並符合規定始得經營，但起步較英美及中國大陸晚。
監理重點		英國政府確信有效金融監理法規，為英國金融金融科技未來發展之關鍵因素。FCA 提出創新計畫，協助金融監理法規適應金融變革。	美國政府對 FinTech 係任其自然成型，並視為替代性金融中介功能，輔助傳統金融體制弱點與缺陷，但仍採聯邦及州層級之雙向監理。	日本金融廳為確保對快速變動之 FinTech 產生對應，彙整日本與其他各國 FinTech 差異，評估是否適合日本後，調整金融監理政策。	新加坡金管局設立監理沙盒制度，並放寬相關監管條例，以指導原則明確 FinTech 可在法規支援情境進行實驗，以減少金融監理摩擦。	中國銀監會公布銀行業資訊科技發展規劃指導意見，督促指導銀行業加強資訊化建設，並依其風險控管優勢，適應互聯網金融創新發展。	金管會以金融環境 3.0 計畫開放部分銀行業務可於線上申辦，並參酌監理沙盒制度提出領航計畫，但相較其他國家，我國對金融科技開放仍以金融業為主體。

資料來源：本研究整理。

第四章　銀行網路金融業務發展之風險控管及稽核監理

第一節　國際金融科技監理環境趨勢-兼論反 BSA 及 AML 之監管審查

對監理機關來說，法規與監理措施如何設計方能有效監理，同時避免不成熟階段之過度監理而阻礙金融科技發展，確實為一難題。對金融科技業而言，發展過程須將法令遵循架構納入營運計畫中，考慮與監理機關間之關係與互動，以及長期欠缺互動與規避法令之影響，例如虛擬貨幣（Virtual Currency）當成為洗錢工具時，金融科技業者可能面臨刑事追訴（Popper, 2015）。因此，金融科技發展已經幾乎成為主流之今日，監理法規制度如何設計，始得發揮監理作用，又不致妨害創新，並創造與金融科技業者良性互動環境，可謂金融科技發展成功一重要拼圖。

金融穩定理事會（FSB）於2016年3月在日本召開第十六屆年會，首次正式討論金融科技之系統性風險與全球監管問題，此意謂金融科技監理告別各國單打獨鬥之局面，正式邁入全球協調協作之新階段，同時金融穩定亦成為重要之考量因素。事實上，FinTech浪潮下，金融相關產業面臨極大衝擊，主管機關應考量業務發展與監理間之衡平性，對科技業者加以適度管理外，亦應放寬對金融業者之監理尺度，加速引進沙盒機制（Regulatory Sandbox），提供獎勵制度，以鼓勵業者尋求創新營運模式。而應用科技提升金融服務便利與效率同時，仍必須兼顧公平、安全及消費者保護，共創金融、產業及消費者三贏局面。

英國政府科技辦公室（Government Office for Science）提出在未來十年內，金融科技推動上最為重要之關鍵領域，包括（1）機器學習（machine Learning）及認知計算（cognitive computing）；（2）數位貨幣（digital currency）及區塊鏈（blockchain）相關技術；（3）巨量資料分析（big data analytics）、數據優化及組合相關技術；（4）分散式系統（distributed system）、行動支付（mobile payment）與 P2P 應用（peer-to-peer applications）。然英國科技辦公室亦同時提醒相關技術

所隱含之龐大發展潛力與經濟效益，絕非單純出自技術本身，而是在資訊安全之前提下，如何妥適地採行並運用各項技術，就政府立場而言，其在金融科技議題應對上所須扮演之角色，即是促使各項嶄新技術透過金融監理，而運用在正確之用途。目前全球金融科技之監理法規精神及目的，如按照國家及地區之金融市場之發展程度，可區分為以下三大類。

（一）先進金融市場

包括歐元區、美國、英國、澳洲、新加坡、香港等國金融業服務先進，網路基礎設施及行動裝置普及度高。基本上，金融先進國家監理機關，對金融科技之監管在「公平」、「穩定」前提下，以促進產業發展為主要之監理目的，重點在於先確保商業行為符合現行法令規定，強化金融業內控以預防系統性風險，進一步透過金融科技監理強化金融服務之提供。

（二）高度開發中金融市場

以中國大陸為例，金融監理原則係降低小微企業與民眾之資金取得成本，以緩解信用分配不均及避免不當之監管套利行為。

（三）低度開發中金融市場

例如肯亞及菲律賓，監理係以實踐普惠金融（Financial Inclusion）為目的。由於該地區之金融資源缺乏且分配不均，但持有智慧型手機之人口不少，因而在監理方面，更強調如何利用行動裝置提供不受地理疆界限制之支付服務，故金融監理目標為鼓勵業者創新、提高消費者之使用意願及頻率。

再者，以英國金融科技發展現況與趨勢來看，根據 UK Trade & Investment（2014）分析，英國金融科技發展趨勢影響監理則有以下三大面向：

（一）資料貨幣化（Monetization of Data）：金融業透過大數據掌握之客戶資料數量增加，在客戶逐漸同意以對價支付之方式，將資料有償移轉予其他第三人作為特定目的運用時，產生資料交易安全之問題。

（二）預防詐欺及個資保護（Fraud and Data Protection）：由於在金融科技之服務模式中，新型詐欺案件層出不窮，故資訊安全之維護及測試設備建置之重要性提高。

（三）基礎設施置換（Infrastructure Replacement）及去中介化：基礎設施置換及去仲介化係指金融科技新型交易基礎設施之建構，促使客戶不再執著使用金融機構之仲介功能，例如機器人點對點交易網路或電子貨幣交易平台之出現，該交易上較不注重傳統金融機構與客戶間之信賴關係。

誠言之，金融監理制度之建構無法精確量化，制度之設計涉及普遍社會價值與社會利益之判斷，必須綜合考量一國之金融體制、歷史文化、社會環境、金融市場穩定、消費者保護意識、政府行政效率等面向。故我國金融科技監理之原則是「防弊」與「興利」並重，避免因個案之防弊而影響整體產業興利及金融科技之健全發展。2008 年金融海嘯，大型銀行業金融機構受到嚴重影響。政府監理部門將危機主要歸因於大型金融機構所形成之系統風險，巴塞爾銀行監管委員會將部分大型銀行金融機構定義為系統重要性金融機構（SIFIs），增加銀行之監理資本要求，進而發展出一系列衡量及管理系統風險與增提資本之監理措施。

FinTech 風潮自美國矽穀開始吹起後，至英國、香港、新加坡、澳洲、日本及中國大陸。美國近五年已投資逾新台幣 1 兆元在 FinTech 公司，而英國由商業銀行籌措資金引入小型新創公司，並建立法規試驗框架，在新監管架構下，鼓勵實驗及創新。新加坡則打造成國家智慧金融中心（Smart Financial Centre），除了新加坡金融管理局（MAS）成立專門發展相關策略及條例部門，以及各類金融科技創新項目外，2015 年更推出總值新台幣 50 億元基金，以協助金融機構研究金融科技。澳洲金融服務為對該國經濟貢獻最大之產業，澳洲政府推出租稅獎勵措施，包括對每人每年低於 20 萬澳元之創新投資提供 20%抵稅獎勵；十二個月以上之投資案提供十年免資本利得稅獎勵，且該國政府亦設立早期階段創資有限合夥公司（ESVCLP），可得到投資額 10%之抵稅獎勵，作為提供稅務優惠予在初期階段即投資新創事業投資人之投資工具。

就金融監理來看，英國可謂歐洲 FinTech 重鎮，金融科技新創事業占全歐洲50%以上，故英國之監理制度須顧及新市場參與者、破壞式創新者及新創業者之利益。前述由 FCA 主導之「新創計畫」，其目的即是檢視並排除對金融科技創新之障礙，目前「監理科技（RegTech）」（或「法遵科技」）已繼 FinTech 後，成為另一個熱門議題。「監理科技」係指監管機構應用科技執行現有監管程式，促進有效之風險識別、進行風險加權、監測及數據分析，此類應用方案即稱之為監理科技。監理科技之精神在於透過監理透明化，以及 FinTech 業者資訊揭露自動化機制及分析，轉變為以資料導向之監理與法令遵循制度（Data-Driven Regulation and Compliance），以在 FinTech 時代中進一步強化監理效率。根據近期國際機構研究報告，監理科技發展趨勢可歸納如下。

（一）去中心化之監理機制

由於金融科技及區塊鏈技術去中心化之結果，系統性風險之控管比以往更加困難，而傳統以大型銀行為首及高度監理對象之監理建制（Regulatory Regime）亦開始調整。

（二）跨產業之監理整合（inter-industry integration）

由於金融服務提供者除了以銀行為首外，亦有可能以行動業者、網路業者及電信業者為主體（如肯亞 M-PESA），因而產生高強度與密度之跨產業監理整合需求來得重要。金融科技產業已跨出金融業之範疇，監理科技相較傳統金融監理更需要高度跨業協調及整合，金融監理者開始肩負跨產業監理之任務。

（三）無國界之監理整合

過去傳統之跨國監理，較注重金融機構跨國經營所產生之相關監理協調，但網路金融之發展，包括區塊鏈、比特幣、P2P 借貸、股權群眾籌資等，金融服務已跨國界，為跨國監理帶來全新挑戰。

（四）消費者導向之科技監理

科技來自於「互動」及「創意」，金融科技相較傳統產品與服務更加強調對

消費者即時、行動及互動體驗之功能，客戶體驗成為金融科技服務重要元素，而金融消費者保護亦成為科技監理之核心。應注意者，在消費訴訟上，FinTech 之訴訟案件可能更加多元，且須面臨交由不甚熟悉該領域法規之檢察官偵辦，影響金融消費者保護之成效。

（五）即時（Real-Time）監理

傳統金融監理邏輯，係透過預先設計之程式或標準，例如銀行資本適足率之要求，就不同情形採取相應之監理措施，而金融科技之發展則使得金融監理機關可利用監理科技相關技術，監控金融業者之服務安全，達到即時（Real-Time）監理之目的。

（六）低成本導向之監理

RegTech 係金融監理之高度創新，利用科技降低監理風險，而金融監理機構發展監理科技技術，透過科技監控系統之導入，可大幅降低監理人力、監理成本、法令遵循成本及訴訟，該概念已受到英國等先進國家之高度重視。

（七）兼具產業發展功能之監理

金融科技監理之重要趨勢，係監理機制設計，不僅以追求金融體系之安全及穩定為唯一要求，而是逐漸朝向金融體系安全穩定以及鼓勵金融創新的雙元思維前進，金融監理機構未來可能會採取更多實驗性（experimental）監理措施。

近年，英國金融科技產業發展在全球位居領先地位，每年金融科技利潤可達 200 億英鎊（UK Trade & Investment, 2014）。根據英國政府報告，英國金融監理機關，包括金融審慎監理局（Prudential Regulation Authority, PRA）及英國金融業務監理局（Financial Conduct Authority, FCA），均對金融科技業務建立新監理目標，亦較積極與私部門間就監理議題與要求進行溝通。其中 FCA 提出「創新計劃」，目的在於探索金融市場之新興商業模式，且 FCA 亦在國家科技辦公室之支持下，建立「監理沙盒」金融科技監理模式。2015 年 3 月英國科技政府辦公室在政策報告中，首度提到沙盒（sandbox）一詞之概念，並提到監理沙盒係將

金融監管單位、金融機構、FinTech 新創與學界合作之一種創新監管方式。監理沙盒（Regulatory Sandbox）之概念，原意係指在科技應用軟體開發過程，先行建立一個與外界環境隔絕之測試環境，而工程師則會在沙盒內，放置軟體以測試其功能。

所謂監理沙盒機制，即是開放新興金融服務可對少數民眾試辦，在測試服務其間享有法規豁免，目前英國、新加坡均已引入監理沙盒機制發展 FinTech，並將該理念念應用在金融科技創新上，新創公司在沙盒內，即可在一定範圍內自行測試創新服務及商業模式，而毋需受到政府法律之規範。根據 Financial Conduct Authority（2015）及 Woolard（2016）研究，採行監理沙盒制度原因有三：一是降低進入市場之時間及成本，避免法規上不確定對金融科技業者造成疑慮而妨害創新；二是金融科技仍有賴投資，法規阻礙及其不確定性，容易造成投資人裹足不前之可能，而監理沙盒可消除此一疑慮；三是消除法規不確定性，促使多元且特別是在初期被放棄或未經測試之產品或商業模式進入市場。應注意者，FCA 監理沙盒之主要執行措施如下。

（一）監理沙盒納入創新計畫（Project Innovate）之範圍，使創新計劃小組可審查並監控測試之過程；

（二）訂定申請進入沙盒資格條件；

（三）進入沙盒之業者，FCA 將提供策略選擇，以協助其在測試期間可調適法規上遇到之障礙；

（四）監理沙盒為彈性機制，且由 FCA 與業者間以逐案方式協議測試與運作；

（五）FCA 就監理沙盒須建立模擬空間，業者在商品或服務未上市前，可在其中進行測試；

（六）私部門利害關係人可共同設立一非營利之上層公司，代表其下層之新創業者進入沙盒中；

（七）FCA 在觀察測試結果後，決定是否修訂法規及適當法規之調整措施。

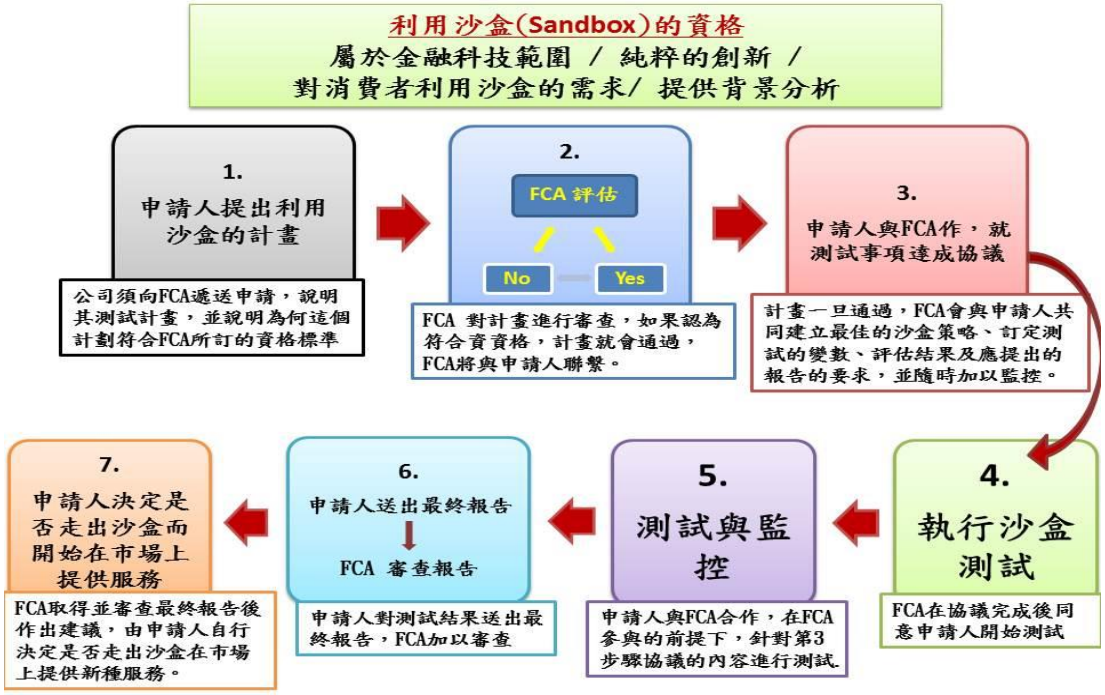


圖 4-1：英國監理沙盒（Sandbox）之運作流程

資料來源：整理自李慧芳，英國金融科技發展及監理沙盒機制對我國的啟示，國家實驗研究院，2016 年 7 月。

兆豐銀紐約分行被美方重罰一事引發過內外關注，美國紐約金融服務署（DFS）發現兆豐紐約分行對於涉及與巴拿馬分行的交易風險未能處理，總行也未予高度重視，而巴拿馬正是國際已確認的洗錢高風險區。兆豐銀行在巴拿馬市（Panama City）及科朗自由貿易區（Colon Free Zone）設有分行。從 DFS 針對兆豐金因違反反洗錢法而公告的處置合意令（consent order），以及美國紐約州金融服務署（NYDFS）裁罰兆豐銀行的檢查報告新聞稿，可看出 DFS 罕見嚴厲的用字遣詞，包括**內控機制，組織任命利益衝突、未落實客戶審查（KYC）及定期稽查制度、未善盡反洗錢督導職責**等。

茲引用紐約州金融服務署（DFS）金檢局負責人 Maria T. Vullo 所描述的：「金檢局將不寬容公然漠視反洗錢法規，而且決心採取決然、嚴厲的措施來對付那些在本地沒有法遵計畫去阻止不法交易的機構」；「金檢局發現兆豐紐約分行的法遵失敗是嚴重的、持續的，而且影響整個兆豐銀行事業；這也顯示該行對於強有力的法遵基礎建設需求缺少真正的瞭解。金檢局揭露兆豐銀行的法遵計畫僅具形式，因此合意令對於保證將來的法遵是必要的。」

自 2001 年 10 月「美國愛國者法案（USA Patriot Act）」頒布以來，美國聯邦監管機構對涉嫌違反「銀行保密法（Bank Secrecy Act, BSA）」及「洗錢防制法（Anit-Money Laudering Act, AML）」之金融機構，共祭出超過 54 億美元之民事罰款、罰金及沒收等行政處分。此前已於 1990 年 4 月在財政部下設立之「金融犯罪執法網路（FinCEN）」反洗錢情報體系，其核心職能在於執行 BSA 為美國國內境外執法部門提供情報，而展開洗錢資訊收集及傳遞工作。前項美國愛國者法案係增加金融機構之義務，包括修正現有執行政策及程式、更嚴格之客戶辨別標準、增強謹慎義務履行、禁止美國銀行與外國空殼銀行保持商務聯繫、加強防制洗錢國際合作等。但美國聲浪質疑國家安全局（NSA）出於反恐，而大量蒐集美國公民通訊紀錄之合法權力，故美國眾議院於 2016 年 5 月通過「美國自由法案（The USA Freedom Act）」取代愛國者法案，未來政府僅得在獲得法院核准之情況下，始能取得特定案例之電話記錄。

事實上，歷經 2008 年金融海嘯襲擊後，FinCEN 強調個人及企業對銀行保密法與洗錢防制法合規性之責任，並在執法行動中更加積極，除了要求提交「可疑活動報告（SAR）」外，亦對金融機構與金融犯罪行為人及其和解協議過於寬鬆提出批評[112]，此前 HSBC 曾於 2003 年被美國聯邦監管機構警告「應更好地監視可疑資金動向」。事實上，美國對洗錢防制立法進程快速，如美國國會於 1986 年頒布「洗錢控制法案（Money Laundering Control Act）」，用於補充 BSA 未將洗錢行為視為一項犯罪之法律缺漏，而後美國國會分別於 1988 年通過「洗錢檢控改善法案（Money Launder Prosecution Improvement Act, MLPIA）」，擴大金融機構定義，並對出於過失協助洗錢之銀行從業人員規定其義務條款及罰則；1992 年「Annuzio-Wylie Anti-Money Laundering Act」則強化金融機構及其董事、雇員及代理人貫徹洗錢防制方案、保存資金交易記錄、報告可疑交易等義務；1998 年則通過「打擊洗錢與金融犯罪戰略法案（The Money Launderingand Financial Crimes Strategy Act）」，要求財政部與司法部須在全國範圍內，協調執法力量阻止洗錢活動。

[112] See Sharon Brown-Hruska, Developments in Bank Secrecy Act and Anti-Money Laundering Enforcement and Litigation, NERA ECONOMICCONSULTUNG, page 2. (Jun. 2016)

應注意者，美國司法部於 2015 年 9 月將 FinCEN「個人問責制」之行動方式以「Yates Memo」為名發布聯邦政策，並以「個人對企業錯誤負責」之主題廣泛傳達給所有聯邦檢察官，闡明司法部打擊企業不當行為之有效方法，在於透過向個人追究責任，促使該違法者承擔責任並阻止未來錯誤行之立場[113]。事實上，自備忘錄（Yates Memo）發布以來，監管機構表示其意圖強制金融機構、董事與其高階管理人員承認日後結算中之瀆職行為；如成功，可在與自身有關之訴訟中向第三方原告提出承認書。此外，美國紐約州金融服務署（NYDFS）擬於 2017 年 1 月起實施洗錢防制新規定，相關受監督機構需檢視其交易監控及過濾計畫，以確保符合風險監管保障措施，且該機構亦須通過年度董事會決議或高階管理人員法遵調查，以證明法令遵循制度符合 DFS 規定。誠言之，就最近執法行動趨勢而言，預期金融機構將持續面臨更加激烈對違反 BSA 及 AML 之監管審查，而金融機構亦因響應執法行動及有關可疑活動報告之指導，增加報告申請數量及可疑活動數量。

第二節　銀行網路金融資訊安全之偵測、控管及預防

Morgan and Hunt（1994）提出承諾-信任理論（Commitment-Trust Theory），該理論表示服務品質、顧客滿意度與信任是牽動著顧客行為。其將信任定義為對交易伙伴是否提供合理的且完整產品的信心接受程度，當消費者相信賣主是可靠且誠實時，便稱為信任。Jones et al（2002）以應用系統的角度提出網站本身之可用性（availability）、可靠性（reliability）及安全性（security）是影響網路使用者信任網站的基本因素。Koufaris 及 Hamptom-Sosa（2004）認為網站在吸引消費者瀏覽後，若無法建立良好的信任，則消費者並不會進行消費，而且極可能轉至使用其他的網站，網路信任則決定於消費者對網站呈現的知覺（Bart、Shankar、Sultan、Urnban，2005）。

[113] 同前註，page 3.

據國內外研究顯示，資訊安全為阻礙消費者使用網路銀行服務主要原因。因銀行網路金融業務之交易迅速，且不受地點、時間限制之優勢，符合現今社會之需求。據市場研究機構對台灣地區網路銀行及線上理財行為綜合調查，約有六成民眾表示半年內使用網銀，該民眾中高達 92%表示未來將會繼續使用，未使用者中亦有 40%表示將考慮使用。如去除不了解功能、申請流程麻煩，以及難以改變交易習慣等因素，阻礙消費者最主要原因即對交易安全之顧慮，Turkey（2009）亦指出安全性是阻礙網銀使用之主要因素。顯示網銀使用者持續增加之趨勢。故銀行應對網路銀行業務規劃風險導向內部稽核，持續追蹤重大資安風險事件。就近期第一銀行 ATM 盜領事件之偵查過程，以及引申之銀行網路金融資訊安全之偵測、內部控制及預防等，本研究說明如下：

（一）第一銀行 ATM 盜領事件偵查過程

第一銀行轄下 22 家分行共計 41 部 ATM，於 2016 年 7 月遭到英國駭客攻擊入侵，累計遭盜走 8,327 萬元，而第一銀行倫敦分行鎖在鐵櫃之電話錄音伺服器主機，即成為駭客遠端遙控 ATM 大量吐鈔之工具。我國調查局資安鑑識實驗室全力解析相關犯罪手法，找到遠端遙控的惡意程式及可能入侵路徑等，成功偵破我國歷史上第一次沒有提款卡也能盜領大量現金的犯罪案件，並透過綿密的監控設備，逮到洗錢嫌犯並追回贓款。此次第一銀行盜領案問題，包括（一）俄羅斯黑道份子如何遠端遙控 ATM 盜領大筆金額；（二）一銀倫敦分行是否是駭客入侵的端點；（三）控管嚴謹的銀行內部網路（Intranet），駭客入侵並且植入惡意程式的風險；（四）ATM 封閉網路的安全性；（五）銀行業者的資安防護機制。

調查局資安鑑識團隊發現，惡意程式因具備自毀匿蹤之能力，導致事後追查難度高，先前多台受駭 ATM 中找不到任何證跡，主因就是這些惡意程式中有一用於刪除之批次檔 cleanup.bat，透過系統內建加密刪除工具 sdelete.exe 移除藏在 ATM 內部所有惡意程式及相關檔案，而調查局發現惡意程式的 ATM，係因自毀程式執行失效才留下紀錄。找出惡意程式確認 ATM 遭駭，但這些惡意程式來源更是要解決的問題，由於這些木馬都不具備遠端連線功能，無法透過駭客常用的

伺服器遙控，駭客勢必得遠端手動操控才能執行。調查局清查第一銀行內部網路之各種異常連線記錄，找到 2016 年 7 月大量來自海外第一銀行倫敦分行連線至台灣 ATM 的記錄，發動大量連線系統是倫敦分行之電話錄音伺服器。

但第一銀行倫敦分行沒有 ATM 業務，不需連線回台灣 ATM，不應出現任何連線記錄，而對位於台灣的 ATM 設備，亦不應出現對外之異常連線，故調查局推斷第一銀行倫敦分行是造成這次事件的駭客入侵端點之一。第一銀行倫敦分行之受駭主機，可能為受駭的主機之一，調查局不排除除了倫敦分行外，駭客還從其他可能受駭主機端點入侵。調查局從進階持續性威脅（APT）之角度分析，有可能是透過魚叉式釣魚郵件（Spear Phishing）的方式，先入侵倫敦分行行員的個人電腦後，再藉由內部橫向移動的方式，進一步掌控倫敦分行內網主機以及電話錄音系統，駭客入侵電話錄音伺服器做為跳板，再進一步攻入總行 ATM。網銀業務安全標準及設計內容包含交易面與管理面之安全需求及設計，銀行業網金業務之管理與設計雖有法律面的規範，然由於其各項服務高度仰賴資訊系統，隨著資訊技術變動或是因資訊系統的弱點或不當使用帶來營運的風險。

根據美國聯邦調查局（FBI）與美國電腦安全協會（CSI）曾經針對財星 500 大企業、金融組織、政府單位、醫療院所，以及大學院校等 538 個單位調查發現，大約有 85%的組織遭受過資訊安全破壞，而因資訊安全的相關破壞事件而產生組織的損失，其中 70%源自網路。例如 2004 年微軟病毒「殺手（Sasser）」曾造成台灣約 1/3 的郵局因 420 處電腦系統當機癱瘓而影響民眾存匯款進行破壞金融秩序，為當時政府機構及公營機構最重大的資安事件。面對日益複雜的網路攻擊手法，企業開始重視資安管理，惟大部分對資安的認知仍停留在病毒與駭客入侵的議題上，面對千變萬化的資訊安全風險，金融業對於資訊資產的保護、系統管理安全的重視程度及內控稽核的機制仍然有持續加強的必要性。根據調查局所揭露的資料，可以將駭客入侵一銀 ATM 的流程，分成 6 個階段，包括了階段 1、從分行入侵內網。階段 2、建立內網潛伏基地。階段 3、暗中蒐集入侵情報。階段 4、ATM 入侵準備、階段 5、開啟 ATM 遠端控制、階段 6、植入 ATM 控制木馬，發動盜領。

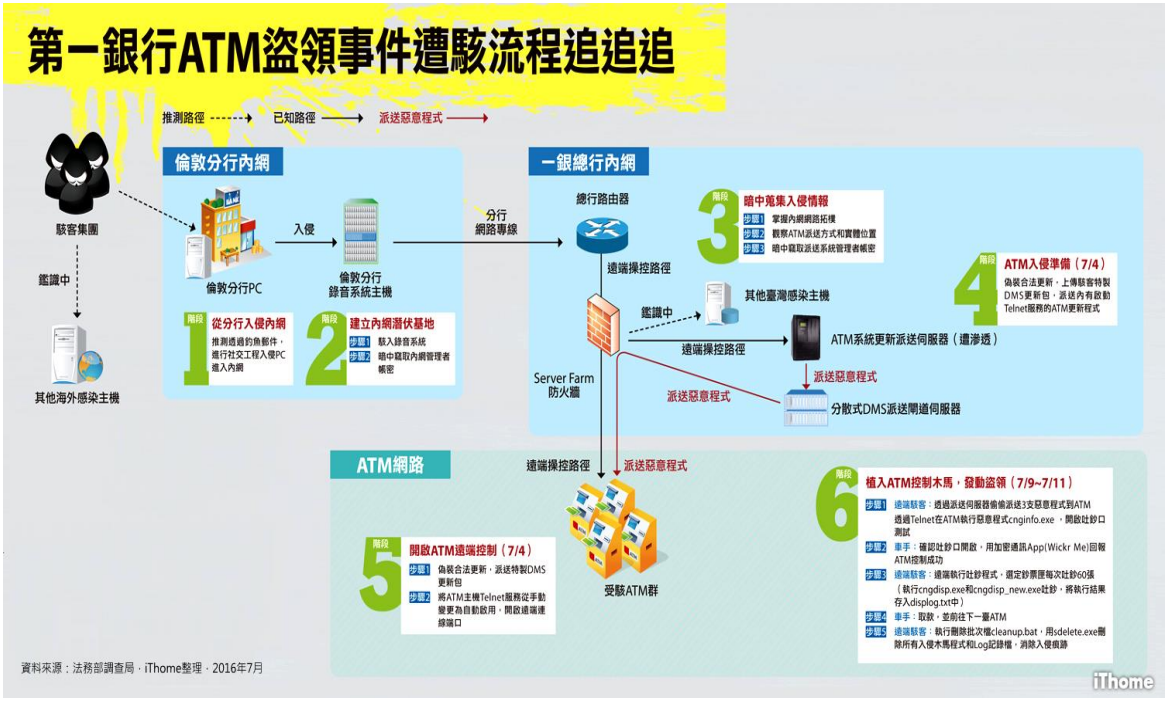


圖 4-2：第一銀行 ATM 盜領事件遭駭流程示意圖

（二）第一銀行 ATM 盜領事件論銀行網路業務內部控制之重點

根據我國調查局所公布的調查結果，第一銀行 ATM 盜領事件有六個重要階段，從此事件看銀行網路業務內部控制的重點，分述如下：階段一：從分行入侵內部網路：駭客首先入侵的是個人電腦。從 APT（進階持續性威脅）攻擊的角度來分析，駭客有可能透過魚叉式釣魚郵件的方式，騙取倫敦分行行員點選連結，下載木馬軟體，入侵其個人電腦後取得進入內部網路的能力。階段二：建立內部網路潛伏基地：攻佔內部網路 PC 之後，駭客下一步就是建立一個具備管理者權限的內部網路潛伏基地，可提供對外連線能力和入侵銀行內部網路的跳板，駭客取得內部網路 PC 的控制權後，很容易取得更多內部網路情報，甚至是管理者帳號密碼。

目前海外分行都各自有專線連回台灣的總行，從駭客入侵的程度來看，總行對於海外分行登入連線的部分，很可能沒有進行相當嚴格的身分確認，加上內部網路專線的設置，使得海外分行和總行系統，並沒有明顯的區隔。也就是說，銀行業者在保護客戶資料的資料庫系統方面採取了非常嚴謹的防護措施，但是對於

內部系統及內部網路之間的資安認證程序為了使用方便往往較為便利，使得海外分行和總行連接的系統只需要簡單的帳號、密碼就可以順利登入，造成資安的漏洞產生，也因此國際駭客憑藉控制錄音系統伺服器，進一步透過伺服器建立潛伏基地，進行對總行內部網路的行動，此點值得銀行內控部門特別加強稽核及關注。

階段三：蒐集 ATM 入侵情報：錄音系統也是內部系統之一，穿透防火牆的存取連線行為是合法行為，不易遭監控軟體發現。我國調查局發現儲存在 ATM 系統的木馬程式，是儲存在 C：\install 以及 C：\Documents and Setting\Administrator\兩個目錄中。透過軟體發送的惡意程式，在上述兩個資料夾中都有發現，就邏輯推論，可能更早在 1 到 2 個月之前，駭客發送的軟體就已經進入分行的內部系統中放置木馬，進而取得管理員權限的程式，在這段期間，駭客可能掌握了總行內部網路的網路拓樸（Network Topology）[114]。

另外銀行更新 ATM 程式的方式，不是過去的實體光碟更新，而是透過一套軟體發送到伺服器來更新 ATM 程式，駭客只要竊取了發送系統管理者帳密，再蒐集到 ATM 的實體位置和 IP 的對應，就能明確攻擊特定位置的 ATM，我國調查局調查第一銀行案，檢調人員發現有 38 台 ATM 被植入「cngdisp.exe」及「cngdisp_new.exe」等兩款新種惡意程式，亦即駭客集團利用 ATM 系統更新時破解更新系統，再利用主機統一更新 ATM 機會，直接將惡意程式植入主機，再由車手於特定時點，透過手機、平板等載具啟動程式，ATM 即大量吐鈔，因此銀行更新 ATM 程式的方式值得注意。

階段四：ATM 入侵準備：駭客透過 ATM 軟體發送伺服器，發送開啟 ATM 遠端連線服務（Telnet Service）的 DMS 更新包，將 Telnet 服務從手動模式轉為自動開啟模式。階段五：開啟 ATM 遠端控制：收到更新程式的 ATM 系統，自動按照例行系統更新程序執行，等到下一次系統重新開機後，ATM 就會自動開啟了遠端連線服務，讓駭客可以遠端控制 ATM。[115]

---

[114] 網路拓樸(Network Topology)又稱為網路結構，為電腦網路中端點間連接的方式。網路上各端點藉由鏈(Link)、節點(Node)或交換中心(Switch)互相連接。

[115] 根據調查局統計，除了 41 台成功遭駭的 ATM，另有 3 台 ATM 也遭植入木馬，但駭客沒有成

階段六：植入 ATM 控制木馬，發動盜領：駭客從遠端登入，開始將木馬程式發送到 ATM 設備中，包括了控制 ATM 遠端吐鈔程式 cngdisp.exe 及 cngdisp_new.exe，以及顯示受駭 ATM 資訊的惡意程式 cnginfo.exe。另外有一批次檔 cleanup.bat，可用來執行微軟內建加密刪除工具 sdelete.exe，銷毀所有木馬程式。遠端駭客先透過 Telnet 在 ATM 執行惡意程式 cnginfo.exe 開啟吐鈔口，負責取款的車手早在幾天前就先入境台灣，在遠端駭客指定的時間到特定 ATM 面前，來確認吐鈔口是否開啟，若成功開啟表示該 ATM已遭控制，車手就回報給遠端駭客進行下一個動作。

遠端駭客確認入侵成功後，開始執行遠端執行 cngdisp.exe 或 cngdisp_new.exe 吐鈔，每次吐鈔 60 張。所以，從 ATM 監視影片上才看到，車手完全不用接觸 ATM 或輸入密碼，就能取款。清空某 ATM 的鈔票後，車手再前往下一 ATM 繼續盜領。而遠端駭客也會執行自動刪除批次檔 cleanup.bat，用 sdelete.exe 刪除所有入侵木馬程式和 Log 記錄檔。綜上，三支木馬程式透過合法的 ATM 更新發送系統，透過電話錄音伺服器穿過內部網路資安系統的監控，植入 ATM 系統中，等到領錢車手就定位，遠端（英國、東歐等）操控的駭客一舉控制 ATM 吐鈔，事後使用系統內建加密刪除工具，將入侵的作案木馬程式和軌跡都清除。若不是調查局在木馬銷毀失敗的 ATM 中，發現了木馬程式，進而從其他 ATM 中反組回遭刪除的程式，才找到破案的關鍵線索。

此外，國際上近期發生著名資安案例，首推 2016 年 2 月孟加拉央行遭駭客入侵事件，該案例與我國第一銀行遭受攻擊之手法類似，駭客先入侵孟加拉央行某台端點電腦後進入內部網路，約潛伏二至三個月後，再透過惡意程式觀察內部系統、風控稽核機制如何運作，進行交易轉帳須取得何人審核通過，並側錄帳號密碼。孟加拉央行係透過 Alliance Access 軟體（SWIFT 的產品之一）連接 SWIFT 網路，根據參與鑑識的 BAE 公司指出，駭客進一步研究該軟體之設定檔，找出漏洞以繞過系統檢查機制，全面掌握來自 SWIFT 網路所傳回的確認訊息，了解

功控制 ATM。可推測，可能是因這 3 台 ATM 還未重開機，因此沒有套用駭客客制的更新包而躲過一劫。

何時回應及如何回應，甚至操控印表機阻擋系統自動列印轉帳後之記錄報表，而變成列印竄改後之文件。潛伏期間駭客極盡所能隱藏行蹤，以便讓後端有更充裕時間洗錢。

一切準備就緒後，駭客假冒孟加拉央行發出轉帳請求，成功轉走孟加拉央行存放於紐約聯邦準備銀行帳戶中的$8,100 萬美元外匯存底。事件發生後，導致總裁 Atiur Rahman 為此下台，而包括越南 Tien Phong 銀行、菲律賓銀行也陸續傳出 SWIFT 系統曾遭攻擊。同時，更多銀行紛紛尋求鑑識服務，以調查內部可疑活動。根據外電報導，駭客對聯邦準備銀行共發出 35 筆轉帳請求，總金額將近 10 億美金，其中 30 筆遭擋下，而 4 筆之所以成功地轉到菲律賓 RCBC 銀行，則是利用 2 月 5 日隔天是休假日，Fed 無法聯繫上孟加拉央行，加上轉帳過程所有憑證、程序皆正常，Fed 因而放行，緊接著資金被菲律賓銀行轉到賭場進行洗錢，而另一筆則是轉到斯里蘭卡銀行後欲轉給某非營利機構，然而駭客卻在轉帳時誤把"foundation"拼成"fandation"，引起銀行關注而轉向孟加拉央行進一步確認時，才揭發整起詐騙事件。

銀行資安如出現狀況，帶來最大損失其實是商譽受損以及客戶信任。但目前台灣企業風險管理委員會並未納入資安，加上許多資安與 IT 風險很難量化，使得台灣企業資安和資訊治理層級，一直未能有效拉高。我國銀行業者近年在主管機關的要求下，以取得 ISO 27001 作為資安的標準，但是 ISO 27001 資安認證主要是針對資訊部門，資訊部門的資安控管目前雖然可以解決 80%的資安問題，但是目前仍產生二個主要問題：第一，銀行開發新的網路及數位金融服務，並無法納入既有 ISO 27001 控管範圍；第二，海外分行資訊系統必須仰賴國內總行的大型主機提供服務，但許多海外分行都已經先通過當地主管機關的同意，要為了資安需求作流程修正有困難；在地的委外與法令遵循仍有一定需求時，在 IT 管理上很難出現零缺失；上述二點使得銀行仍有加強內部資安控制及稽核空間。

我國銀行在治理上一向相當嚴謹，許多都已經取得包括 ISO 27001 與 ISO 20000 雙認證的單位，加上金管會對於銀行向來是高度控管，而且在 ATM 上也

一直都還是採用 SNA 封閉網路架構的銀行，爆發 ATM 盜領事件，顯示 ATM 網路和內部辦公網路並沒有有效隔離，對 ATM 上啟動服務和作業系統日誌未能有效監控，未來應建立預警機制防範危害資安及金融秩序的產生。

ISO27001 資訊安全管理系統規範為英國標準協會（British Standards Institution, BSI）於 2005 制定的資安管理規範，是全球公認最完整的資通安全架構及認證標準，ISO27001 最早源於 BSI 發布之 BS7799 標準，用以評估檢討組織之資安作業，提供組織進行資訊風險的評估與處理，防範意外的發生及對組織的衝擊（BSI, 2002）。[116] ISO27001 標準之風險管理流程首先是界定組織安全的需求及管理範圍，以進行資訊資產的鑑別，進而實施系統風險的評鑑，根據評鑑結果訂定風險管理的優先順序，在管控成本與降低風險效益中取得平衡。因此應用 ISO27001 是在組織資源及管理時間有限的情況下，分析可能造成危害的潛在因素，找出威脅資訊安全的重大風險，優先配置資源進行控管，以將風險對組織資訊資產的危害降至最低。

表 4-1：網路金融之資安風險來源

事件類型	定義	事件細分	業務舉例	可能發生模式
內部詐欺	故意騙取、盜用財產或違反監管規章、法律	未經授權的活動和項目	交易不報告(故意) 交易品種未經授權(存在資金損失) 計價錯誤(故意)	P2P 借貸、金融大數據、基於第三方支付的財富管理
		竊盜和詐欺	詐欺/信貸詐欺/假存款 竊盜/勒索/挪用公款 盜用資產 惡意毀損資產 偽造 多戶頭支票詐欺 竊取帳戶資金/假冒開戶人 賄賂/回扣 內幕交易(不用企業帳戶)	所有網路金融模式
外部詐欺	第三方故意騙取、盜用財產或逃避法律導致的損失	竊盜和詐欺	竊盜/ 偽造多戶頭支票詐欺	P2P 借貸、金融大數據、群眾募資
		網路系統安全性	駭客攻擊損失 竊盜資訊(存在資金損失)	所有網路金融模式
客戶、產品及業務操作	因疏忽未對特定客戶履行義務(如信託責任和適當性要求)或產品性質或設計缺	適當性、披露和信託責任	違背信託責任/違反規章制度 適當性/披露問題 洩漏私密	所有網路金融模式

[116] 行政院國家資通安全會報要求國土安全、能源設施、金融服務等列入資安等級 A 級的單位必須於 2004 年以前通過此項認證(行政院國家資通安全會報，2004)。

	陷導致的損失		冒險銷售 為多收手續費反覆操作客戶帳戶 保密資訊使用不當 貸款人責任	
		不良的業務或市場行為	反壟斷 不良交易/市場行為 操縱市場 內幕交易(不用企業的帳戶) 未經當局批准的業務活動 洗錢	第三方支付，P2P借貸等
		產品瑕疵	產品缺陷(未經授權等) 模型誤差	
		客戶選擇，業務提起和風險暴露	未按規定審查客戶超過客戶的風險限額	P2P 借貸、群眾募資
實體資產損壞	實體資產因自然災害或其他事件丟失或損壞導致的損失	災害和其他事件	自然災害損失 外部原因(恐怖襲擊、故意破壞)造成的人員傷亡	P2P 借貸、金融大數據、群眾募資
業務中斷和系統失敗	業務中斷或系統失敗導致的損失	系統	硬體 軟體 電信 動力輸送損耗/中斷	所有網路金融模式
執行、交割及流程管理	交易處理或流程管理失敗和因交易對手及外部銷售商關係導致的損失	交易認定，執行和維持	錯誤傳達資訊 數據登入、維護或登載錯誤 超過最後期限或未履行義務 模型/系統錯誤操作 會計錯誤/交易方認定紀錄錯誤 其他任務履行失誤 交割失敗 擔保品管理失敗 交易相關數據維護	所有網路金融模式
		監控和報告	為履行強制報告職責 外部報告失準	P2P 借貸
		招攬客戶和文件紀錄	客戶許可/免責聲明缺失 法律文件缺失/不完備	所有網路金融模式
		個人/企業客戶帳戶管理	未經批准登錄帳戶 客戶紀錄錯誤(導致損失) 客戶資產因疏忽導致的損失或損壞	
		交易對手	非客戶對手方的失誤 與非客戶對手方的糾紛	
		外部銷售商和供應商	外包 與外部銷售商的糾紛	第三方支付

資料來源：本研究整理。

第三節　銀行網路金融業務之稽核措施

探討銀行網路金融業務之稽核措施，必須先討論「風險導向內部稽核制度」以及「內部控制三道防線架構」，世界先進各國及領導企業已採行三道防線架構建置風險管理及內部監控系統框架，其被視為風險管理之最佳實務。

一、國銀導入「風險導向內部稽核制度」分析

隨著銀行業朝向區域化及全球化發展，銀行業務變得多樣化、產品更為複雜化，銀行的經營風險也跟著大為提高。金管會日前宣布 2017 年開始推動國內銀行業導入「風險導向內部稽核制度」，強化公司治理能力。隨著主管機關監理趨勢的演進與監理機構管理思維變革與推動，國際性銀行稽核策略因應主管機關監理趨勢走在前端，傳統偵錯角色已經無法滿足內部與外部使用者對於稽核部門的要求，被賦予更高的期待。風險導向稽核是近年來國內外普遍採行的稽核制度，意指稽核人員採用辨認、衡量、監視與控制風險暴露之技術與程序，有效掌握組織之風險，並依風險等級之高低順序，實施差異化監督與查核規劃，即在高風險者投入高資源、低風險者投入低資源的原則下，妥善分配其監督及查核資源，以健全組織業務經營。此外，當稽核人員發現組織管理階層有刻意提供錯誤或誤導之資料，抑或迴避提供重要資料時，則應擴大執行實地查核之範圍，並採取後續適當之監督措施及專案查核。

近年來，內部稽核的新角色已從傳統財務報表相關內控的稽核，擴充至策略規劃與執行、作業效率效果及法令遵行。以風險為導向將組織目標、風險承受度及策略加以連結，並積極協助管理階層確保風險在可接受的範圍以內，並作為董監事、高階管理者、各營運單位、外部稽核與主管單位之溝通橋樑，並積極協助管理階層掌握機會、辨認及處理整個組織所有相互關聯之風險、評估合理資源需求及分配。以風險為導向之稽核制度，係透過風險評估與分析結果規劃稽核工作，集中資源在偵測較高風險的業務區塊與產品，檢視其制度及程序是否可達成有效風險控管與偵知，因其具有高度集中且深度查核的特性，較易於發揮聚焦風險查核的效益。

目前我國銀行業可以依據「金融控股公司及銀行業內部控制及稽核制度實施辦法」第十五條之一第一項規定申請採行風險導向內部稽核制度，主管機關藉由申請核准的方式，陸續開放各家銀行採行以風險為導向之稽核制度，允許將風險評估結果連結至查核頻率，以差異化管理的方式協助國內銀行業者建立以風險為導向之稽核制度，漸與其他先進之國家及銀行作法一致。全面性的風險導向概念引導內部稽核策略規劃與稽核作業執行，從內部稽核的角色出發，由稽核設計面與稽核作業面更為積極參與風險偵知，協助管理階層能夠針對風險所在洞燭機先，提出能協助公司營運及發展的有效改善意見及建議，協助銀行強化公司治理能力，並彰顯內部稽核單位價值。

傳統的稽核作業模式也由測試各作業循環、法令遵循情形等，逐漸調整為依據各銀行業務類別，產品複雜度與風險集中度引導稽核頻率與強度，更能夠積極有效運用稽核資源。以風險為導向的查核項目通常根據風險評估的結果，來決定相關查核目標、範圍、方法、稽核程序及查核頻率，以提昇稽核品質，並持續性監督查核項目的風險。這些方法可讓稽核資源分配依風險評估結果作有效運作，不但能充分利用稽核資源，也可將稽核資源運用在高風險的業務或單位上，增加查核深度以及達到聚焦的效果，讓內部稽核程序有效率，也避免稽核資源過度運用在風險度較低的項目。

為使金融機構得依內部風險評估結果，訂定內部稽核之查核頻率，提升風險辨識、評估能力，使內部稽核資源更有效配置，推動風險導向內部稽核制度。爰金管會於 2016 年 7 月增訂「金融控股公司及銀行業內部控制及稽核制度實施辦法」第 15-1 條文，本國銀行得向主管機關申請核准採行「風險導向內部稽核制度」；本國銀行經採行風險導向內部稽核制度者，不適用同法§15 第 1 項查核頻率之規定。經核准採行風險導向內部稽核制度的國銀，其執行品質將作為金管會調整檢查週期之參考。對銀行影響及效益包括：稽核角色更具獨立性、風險聚焦檢查、依差異化評比結果決定查核頻率，以及稽核資源有效配置。有關國銀申請「採行風險導向內部稽核制度」辦法如以下表所述。

表 4-2：申請「採行風險導向內部稽核制度」辦法

項目	說明
申請期限	應於申請年度八月底前向金管會提出申請，經金管會核准後，自次一年度起採行風險導向內部稽核制度。
內部陳核程序	為本項申請時，應先將相關申請書件交付監察人(監事會)或審計委員會合議並做成紀錄。如未設置審計委員會者，應先送獨立董事表示意見，並報經董(理)事會通過。
應檢附之申請書件	1.申請採用風險導向內部稽核制度自評表。 2.監事會或審計委員會合議結果與提報董(理)事會通過之提案及相關會議記錄，未設審計委員會者，監察人或獨立董事如有反對意見或保留意見者，亦應一併檢附。

資料來源：整理自資誠企業管理顧問公司。

二、內部控制原則及三道防線實務守則

內控制度之原則應包括管理階層之監督及控制文化、風險辨識與評估、控制活動與職務分工、資訊與溝通、監督活動與更正缺失。而配合採行之措施包括內部稽核制度、法令遵循制度、風險控管機制、自行查核制度、會計師查核制度。

圖 4-3：內控制定及內控目標

資料來源：整理自金融監督管理委員會。

根據國際內部稽核協會（IIA）與 COSO 委員會於 2015 年 7 月發布「運用 COSO 於三道防線」研究報告指出，企業應該藉由建立內部控制之三道防線，重新檢視如何強化風險管理與內部控制減少弊端發生。國際內部稽核協會（IIA）

立場聲明書之「內部控制三道防線實務守則」，所謂「內部控制制度」三道防線之概念，即第一道防線：銀行各單位就其功能及業務範圍，承擔各自日常事務所產生之風險謂第一道防線，其應該負責辨識及管理風險，針對該風險特性設計並執行有效的內部控制程序以涵蓋所有相關之營運活動（詳見圖 4-4）。第二道防線：第二道防線係獨立於第一道防線且非為第三道防線的其他功能及單位，依其特性協助及監督第一道防線辨識及管理風險。第二道防線包含風險管理、法令遵循及其他專職單位，其就各主要風險類別負責銀行整體風險管理政策之訂定、監督整體風險承擔能力及承受風險現況、並向董（理）事會或高階管理階層報告風險控管情形（詳見圖 4-5）。第三道防線：第三道防線係內部稽核單位，應以獨立超然之精神，執行稽核業務，協助董（理）事會及高階管理階層查核與評估風險管理及內部控制制度是否有效運作，包含評估第一道及第二道防線進行風險監控之有效性，並適時提供改進建議，以合理確保內部控制制度得以持續有效實施及作為檢討修正內部控制制度之依據（詳見圖 4-6）。

圖 4-4：內控第一道防線

資料來源：整理自金融監督管理委員會。

圖 4-5：內控第二道防線

資料來源：整理自金融監督管理委員會。

圖 4-6：內控第三道防線

資料來源：整理自金融監督管理委員會。

控制活動與職務分工為每日整體營運之一部分，訂定內控程序，有適當之職務分工（第一道）；而監督活動與更正缺失為持續監督內控有效性，管理、營業單位、內部稽核或其他內控人員發現缺失，應向適當層級報告，並採取改正措施（第二道、第三道）。在第一線與第二線內控機制防線中，倘若未能發揮既有監督與制衡功能，除舞弊警訊可能遭到長期忽視外，同時，作業流程中將存在越來越多的內控弱點，而第三道防線的內部稽核人員可能會疲於奔命偵測潛在內部問題，卻失去讓組織有效從根本改善內控缺失、降低風險的目標。在董（理）事會及高階管理階層方面，應注意以下三項要點：

（一）銀行的董（理）事會及高階管理階層應積極協助及指導三道防線之建立，清楚界定各道防線之角色功能及權責。

（二）管理階層建立三道防線架構時，應考量各銀行活動的性質、大小、複雜程度及風險狀況進行調整，但其調整需能確保三道防線之有效性。

（三）董（理）事會及高階管理階層應持續確保組織架構符合三道防線原則，督導該架構之有效運作，並對其有效性負最終之責任。

根據我國銀行內控制度規定，銀行自行查核制度，每半年一次一般自行查核，每月專案自行查核，法遵單位應督導各單位法遵自評，每半年至少一次，辦理結果應送法遵單位備查；銀行應設置獨立之專責風險控管單位，建立各項業務風險之管理。有關三道防線預警機制發展可參考以下方向[117]：

1. 落實第一線人員作業 SOP，透過第二線人員建置與實施自我檢查機制。
2. 內部稽核落實督導第二線自我檢查作業品質以及持續追蹤改善進度。
3. 針對特定高舞弊風險作業流程，增加查核頻率外，對於已發現之內部控制弱點持續追蹤評估改善進度。
4. 重視內部稽核專案查核結果，將專案查核結果列入重要績效評估指標外，及時向審計委員會與管理當局報告。
5. 強化舉報機制（Hot-Line/ Whistleblower program），設定專責單位接收、調查與處理舉報資訊。
6. 善用資訊科技工具與鑑識資料分析的方法（Forensic Data Analytics），以增加突擊檢查對象的廣泛性以及深入性檢查項目。

[117] 參閱安侯建業會計師事務所研究報告，2016 年。

圖 4-7：銀行內部控制三道防線架構

資料來源：IIA Position Paper: THE THREE LINES OF DEFENSE IN EFFECTIVE RISK MANAGEMENT AND CONTROL, JANUARY 2013.

表 4-3：有關「內部控制三道防線實務守則」規定

條文	條文內容
第 7 條	第一道防線負責及持續管理營運活動所產生的相關風險，包含下列各款： 一.辨識、評估、控制及降低營運活動所產生的風險，確保營運活動與銀行目標及任務一致。 二.第一道防線應將風險控制在其單位可承擔之範圍內，依需要向第二道防線報導其曝險狀況。 三.建立內部控制程序。 四.執行風險管理程序並維持有效的內部控制。 五.當流程及控制程序不足時，應立即提出改善計畫。 第一道防線應定期或不定期就前項內容辦理自我評估，以確保風險有被適當控管。
第 8 條	第二道防線的功能係在訂定整體政策及建立管理制度，協助及監督第一道防線管理風險與自我評估執行情形。依照不同的功能性質，第二道防線之權責包含協助辨識及衡量風險、定義風險管理角色及責任、提供風險管理架構及定期將風險管理結果呈報高階管理階層。說明如下： 一.風險管理功能負責建立獨立有效的風險管理機制，以評估及監督整體風險承擔能力、已承受風險現況、決定風險因應策略及風險管理程序遵循情形。 二.法令遵循功能負責法令遵循制度之規劃、管理及執行，訂定法

	令遵循之評估內容與程序，並督導各單位定期辦理法令遵循自行評估及綜理法令遵循事務。 三.其他專職單位，包含但不限於財務控制、人力資源、法務等。
第 9 條	內部稽核單位係第三道防線，負責查核與評估第一道及第二道防線所設計並執行之內部控制與風險管理制度之有效性，並適時提供改進建議。

資料來源：整理自資誠企業管理顧問公司。

三、銀行網路金融業務對抗駭客稽核分析

銀行網路金融業務稽核有一重要目的，即是對抗駭客攻擊，而現在最常見之攻擊手法如下：

（一）Cross-site scripting（XSS）：網路銀行最常見攻擊手法，係釣魚攻擊最容易進入管道。一旦 XSS 攻擊成功，駭客可使用的手段包括：以假網頁取得密碼、轉帳、刪除或修改資料，而駭客成功得手以後，受害客戶根本無從得知。

（二）SQL injection：網路金融系統設計相當繁複，必須設計相當多網頁輸入與輸出欄位。駭客以查詢語法輸入欄位後進行 SQL Injection 攻擊，騙取系統並得到帳號及個資等敏感資料。事實上，SQL Injection 是最容易取得資料庫內容的攻擊手法。

（三）提升權限：這種攻擊手法有兩大類：（1）垂直式：駭客取得最高權限後新增/刪除使用者資料，並進行轉帳。（2）水平式：駭客取得受害客戶的資料後，進行後續攻擊。銀行無法得知客戶資料已經洩漏，而且也無法得知是否為正常客戶的正常使用行為。

網路銀行提供使用者處理銀行交易很大的方便，用戶可以用更簡單的方法進行理財、轉帳和支付。但這並非沒有風險，許多網路犯罪工具和伎倆讓無辜的網銀使用者變成受害者。根據趨勢科技提出的研究報告，銀行木馬從第一隻開始就不停在進化，直到今日高度複雜化的惡意軟體，例如 2014 年趨勢科技偵測到的 TROJ_WERDLOD 木馬程式，一種新形網路銀行惡意程式攻擊日本，這項威脅

藉由兩項系統設定變更來讓它能直接在網路層次竊取資訊。其優點是不需重新開機或在感染系統上執行任何常駐程式。2015 年 10 月的 Sphinx 被視為最新的 ZeuS 變種，這種銀行木馬程式包括表格擷取、IE、Firefox 和 Tor 瀏覽器網頁注入、鍵盤側錄程式及 FTP 和 POP3 擷取程式。趨勢科技研究 Sphinx 可在 Windows Vista 和 Windows 7 上運作，即便是在使用者帳戶控制（UAC）已經啟用的電腦上。這代表 Sphinx 可以用較低權限的使用者帳號運作，用 C++編寫的 Sphinx 也是基於惡名昭彰的 ZeuS 銀行惡意軟體原始碼。值得注意的是利用 Tor 網路的匿名性，駭客聲稱 Sphinx 能逃過黑名單追踪工具的銀行木馬程式，還包含憑證擷取程式，可以在憑證使用時加以攔截，以逃避安全警告並繞過防惡意軟體程式。

自從竊取網路銀行憑證相關資訊的金融木馬惡意程式 ZeuS 現身後，網路犯罪份子即透過這種手法取得受害者重要個資及金融交易資料。此類攻擊成功的原因可能是因為 ZeuS 利用了模組化的作法，利用網頁應用程式竊取金錢，讓犯罪份子得以繞過雙因子認證，竊取網路銀行客戶憑證和操縱網銀交易，也由於有利可圖，導致此類的銀行木馬程式攻擊目前日益猖獗。隨著行動網路世代逐漸成為所得及消費主流，愈來愈多的金融商品及服務都透過網路銀行提供，銀行惡意程式偵測已經成為金融單位與駭客之間的重要戰爭，網路金融交易安全議題更是目前最重要的關鍵議題。網路駭客使用隱身技術閃避偵測，得以竊取網路銀行客戶憑證和操縱網銀交易，導致銀行木馬程式日益猖獗，建議銀行業應針對網路金融業務提出新的網路銀行安全框架，如趨勢科技公司曾於 2015 年 8 月提出「惡意軟體注入防禦系統（Malware Inject Prevention System, MIPS）」，藉由有效的軟體開發與測試給銀行資訊人員和網頁應用程式開發者，提升軟體安全能力，並建議運用短、中、長期及多層次的網銀戰略防禦機制提供更安全的服務。

四、銀行業風險導向內部稽核制度及網路金融業務稽核分析

採行風險導向內部稽核制度，銀行業首先應決定決定受查主體：包括單位組織、產品、業務、作業流程等，其次應訂定風險評估程序：內部稽核所訂定之風

險評估程序與方法，以書面交付監察人（監事、監事會）或審計委員會核議，並作成紀錄，未設審計委員會者，應先送獨立董事表示意見。第三，決定風險評估程序與方法，包括：[118]

（一）固有風險：擬訂固有風險評估因子，描述評估風險時應考量因素，以及評估固有風險之等級。控制措施則須包括：(1) 評估控制措施設計及執行之有效性；(2) 評估控制措施有效性之等級。

（二）剩餘風險：評估剩餘風險等級，內部稽核應訂定受查主體之綜合風險評估結果與查核頻率連結之標準，就風險等級為高者，應至少每年執行一次或一次以上查核；就風險等級為低者，至少每四年執行一次查核。

（三）訂定內部稽核計畫：年度稽核計畫應併同內部稽核單位風險評估結果以書面交付監察人（監事、監事會）或審計委員會核議，並作成記錄，未設審計委員會者，應先送獨立董事表示意見。年度稽核計畫應經董（理）事會通過；修正時亦同。

（四）定期檢視機制：內部稽核應定期就整體外部環境或內部業務發展變化檢視風險評估結果，並據以決定是否修訂年度稽核計畫。包括：(1) 國內外主管機關監理重點與重要法令及金融環境變化；(2) 經營策略目標與重要政策變化；(3) 業務營運管理資訊及重要監控指標；(4) 主要利益關係人意見；(5) 重大風險事件發生情形。

有關銀行網路金融業務之風險評估與檢查技巧如下：

（一）瞭解網路金融業務風險之來源、類型及評估風險程度應考量之條件、不同風險程度之定義。

（二）評估網路金融業務風險管理品質應考量之 4 大因素，包括董事會與高階管理人員之有效監督，政策、作業流程及限額之妥善訂定及執行，風險衡量、監控及資訊管理系統之妥適與確實性，以及內部控制及獨立驗證。

[118] 參閱資誠企業管理顧問公司，採行風險導向內部稽核制度，2016 年 11 月。

（三）不同網路金融業務管理品質之定義。

（四）網路金融業務剩餘風險之判定及風險趨勢之評估。

在金融科技的時代，金融業應從流程的角度來辨識、評估／衡量、管理、監控及回應，新種業務或是新產品也應依照風險框架來管理。金融科技新興業務須辨識可能的各項風險，瞭解在流程、人員、系統及各種因子下的各項衝擊。資安管理及治理是董監事層級議題，並非 IT 課題。董事會必須根據現狀與未來風險變革，關注組織風險、執行風險決策與排序，進而決定任務排序、決定可接受風險與預算核定。建議落實網路金融業務內部控制重點如下：

（一）網路銀行內部控制包括管理面之「網路銀行風險評估」、「網路銀行安全需求」、「網路銀行風險管理及措施」；技術面之「內部網路控管」、「緊急應變措施」、「應用程式檢核」，內部稽核面之「稽核人員素養與內控評估」、「績效控管」、「訂定查核程式」，以及安全控管品質之「客戶信用」、「品質需求」、「實名認證」等重要內控事項。

（二）網路金融的業務及風險控制工作是由電腦程式和軟體系統完成，所以系統的技術性和管理性安全內部控制就成為網路金融的重要工作，網路金融中，安全風險會導致整個網路的癱瘓，是一種系統性風險。因此包括電腦系統當機、網路外部的駭客攻擊，以及電腦病毒破壞等因素，利用網路的漏洞進入主機、竊取信息、程式被感染、發送假冒電子郵件等，都是內部控制的重點。

（三）未來銀行商譽及形象將已取決於網路金融業務使用的網路開發技術，因此網路金融業務的開發技術檢核非常重要，若未能隨時新更成熟的技術解決方案，可能影響網路金融業務競爭力甚至失去市場，而客戶可以在家輕鬆的上網使用網路銀行，駭客也同樣能輕鬆的想辦法竊取這些資料，因此包括網路金融商品開發的技術系統檢核、提升軟體安全等級以及客戶終端軟體的相容性檢核非常重要是內部控制的重點。

（四）銀行內部網路檢核：駭客使用電子郵件對網路銀行客戶進行「釣魚」。在國際實務上，約有 60%銀行曾遭受釣魚手法攻擊，儼然成為最新網路銀行攻擊手法，一旦網銀系統被成功入侵，帳號資料也勢必曝光。以近期 ATM 盜領成因來看，加強銀行內部網路管理系統、郵件伺服器系統查核、定期檢核內部釣魚郵件及通訊設備等，十分重要。

（五）網路銀行內部控制因素共可分為管理面、技術面、內部稽核三構面，並藉由三構面因素來達成網路銀行安全控管品質目標。銀行採用防火牆，防毒軟體等工具保護內部應用程式與資料，而這些工具正是駭客攻擊之標的。網路銀行真正的資安挑戰在應用程式層，必須用更積極的資安觀念與改良的軟體開發流程。應定期檢核銀行應用程式和軟體開發流程技術保護網路銀行系統的能力。

隨著銀行業近年發展網路數位及科技金融，產品及服務更為多樣化且複雜，銀行的經營風險亦大為提高，因此各國金融主管機關的監理也從過去消極的發現錯誤與糾正功能，逐漸轉換為風險導向與積極預防性的監理機制，以彈性因應金融業的發展與改變。國銀內部稽核應思考導入風險導向內部稽核制度、風險導向內部稽核策略規劃與稽核作業執行。以風險為導向之稽核制度要有效的提升國內銀行業內部控制品質與提升風險聚焦查核能力，而銀行必需具備明確的內部控制三道防線機制及差異化評比標準，儘早與國際接軌，以利銀行國際化及科技金融浪潮發展。

五、我國洗錢防制法配合國際趨勢修正

我國「洗錢防制法」修正草案經行政院於 2016 年 8 月院會審查通過，係為因應國際社會對不法金流誘發之各種犯罪，以及產生各種弊端之重視與關注日益升高，修正重點包括回應國際強化洗錢防制、接軌國際規範、加強司法實務打擊跨境電信詐欺與人肉運鈔洗錢等犯罪。誠言之，舉凡高度政治性人物貪污洗錢、金融機構或專業人士（如會計師及律師）協助資產配置洗錢、跨境夾帶大額現鈔

洗錢、不法金流挹注恐怖犯罪，國際規範對該不法所得之追討、不法金流之遏止極為關注。近期兆豐銀行紐約分行遭裁罰案件，即係因涉未遵循當地國洗錢防制法令之缺失，突顯我國洗錢防制體質亟需調整，爰修正草案於 2016 年 12 月順利經立法院三讀通過，並在公布後六個月施行。相較現行「洗錢防制法」僅得沒收犯罪所得財物或財產上之利益，並未及於洗錢行為標的之財物或財產上利益，而修正後「洗錢防制法」則明定如有事實足以證明行為人所得支配之財產或財產上利益，係取自其他違法行為所得者，得沒收之。

應注意者，我國「洗錢防制法」自公布後歷經五次修正，惟過去修正多數集中於洗錢罪名及協助國際間執行不法利得沒收。但亞太防制洗錢組織（APG）於 2007 年指出我國「洗錢防制法」未符合洗錢防制金融行動工作組織（FATF）所發布之洗錢防制及打擊資恐主義與武器擴散國際標準，包括列為「部分遵守（PC）」及「未遵守（NC）」等 24 項缺失，再加上近期社會矚目之跨境詐騙案件、跨境人肉運鈔集團等犯罪頻傳，實有其積極透過檢討現行洗錢防制法制之必要。事實上，對金融機構及「特定非金融事業與專業人士」之要求，係建議事項指出「應該（should）」或「依照法規必須」（should be required by law or regulation to）採取某些行動，適用申報可疑交易報告義務，爰修正草案不同於過去僅限「機構」而未及於自然人，故第 5 條第 2 項增列指定之非金融事業或人員，如律師、公證人、會計師、不動產仲介業等從事不動產買賣交易及相關契約之公證、為客戶管理財產與帳戶，蓋特定之交易型態，由於交易金額較高或其行業本質，均納入洗錢防制體系。

再者，該修正草案為改善洗錢行為罪刑化之缺失，對修正前「洗錢防制法」第 11 條參照維也納公約對洗錢行為加入處罰未遂犯（修正條文第 14 條），是以不法金流未必可與特定犯罪進行連結，但依犯罪行為人取得該不法金流方式，已明顯與洗錢防制規定相悖，有意規避洗錢防制規定時亦應處罰，即不以可疑金流與特定犯罪有所連結為必要。此外，增加重大犯罪所得之認定，不以其重大犯罪行為經有罪判決為必要之規定（修正條文第 4 條第 2 項），由於洗錢犯罪之追訴主要是透過不法金流流動之軌跡發掘不法犯罪所得，經由洗錢犯罪追訴遏止犯罪

誘因，是以洗錢犯罪之追訴，不必然可以特定重大犯罪本身經有罪判決確定視為唯一認定方式。且 FATF 四十項建議之第三項建議，要求各國於進行洗錢犯罪之立法時，應明確規定「證明某資產是否為重大犯罪所得時，不須其前置重大犯罪經有罪判決為必要。」其他修正重點列示如下，修法最終目的在於建立全民對於洗錢防制之共識，並提升我國洗錢防制體質。

（1）修正洗錢行為之態樣，以符合國際規範。（修正條文第 2 條）

（2）將現行重大犯罪之門檻，由最輕本刑五年以上有期徒刑之罪，修正為最輕本刑三年以上有期徒刑之罪；另擴大本條重大犯罪之範圍，刪除犯罪所得門檻之規定。（修正條文第 3 條）

（3）修正本法所稱重大犯罪所得定義，明定重大犯罪行為所得之證明不以其重大犯罪行為須經法院為有罪判決為必要。（修正條文第 4 條）

（4）將現行銀樓業及其他有被利用進行洗錢之虞的機構修正為指定之非金融事業或人員，並增訂法務部會同中央目的事業主管機關報請行政院核定其適用交易類型及適用本法規定之範圍。（修正條文 5 條）

（5）增訂金融機構及指定非金融事業或人員應訂定防制洗錢注意事項之義務；增訂主管機關查核及規避、拒絕或妨礙查核之處罰規定；增訂對客戶審查之法律依據；增訂負交易資料保存義務之法律依據，以及違反義務之處罰規定；修正對未依規定申報大額交易之處罰規定，增訂金融機構依法通報可疑交易業務應守秘密之免責規定，並明定違反義務之裁罰機關；增訂金融目的事業主管機關得對洗錢及資恐高風險國家或地區採取防制措施之法源依據。（修正條文第 6 條至第 11 條）

（6）將旅客入出境通關申報義務擴大至非隨旅客入出境情形之申報義務，並將新台幣、人民幣、黃金及經指定有被利用為洗錢之虞之物品亦納入申報標的之列。（修正條文第 12 條）

（7）增訂規避洗錢規定所取得之不明財產罪及其未遂行為之處罰；擴大本法沒

收範圍及於洗錢犯罪之財物或財產上利益標的。（修正條文第 18 條）

（8）增訂法務部辦理防制洗錢業務得設置基金之依據。（修正條文第 20 條）

（9）增訂中央目的事業主管機關委辦直轄市、縣（市）政府之法律依據。（修正條文第 22 條）

總言之，我國法務部提出「洗錢防制法」修正草案，係繼刑法沒收新制修法推行及推動資恐防制法立法施行。我國「資恐防制法」於 2016 年 7 月經立法院三讀通過，除了資助恐怖主義犯罪者最高處七年以下有期徒刑，得併科 1,000 萬元以下罰金外，如資助恐怖組織或個人者，亦列為洗錢防制法之重大犯罪。而為強化我國洗錢防制及打擊資恐機制，金管會即於 2016 年 12 月修正發布「銀行業防制洗錢及打擊資恐注意事項」，其中如強化董事會治理、內控三道防線及教育訓練，塑造銀行業重視洗錢防制文化；透過集團層次及指派國外營業單位之洗錢防制人員，以強化總行對海外分支機構之管理；強化有關帳戶及交易持續監控之規範，以提升銀行業發現可疑交易之能力，以及針對特定風險事項，明定應採取額外措施，以降低其風險。主要參酌 FATF 2014 年 10 月發布「銀行業風險基礎方法指引」，以及巴塞爾銀行監理委員會 2014 年 1 月發布「健全有關防制洗錢及打擊資恐之風險管理」等文件，其他修正重點分述如下。

（1）增訂客戶為法人或信託之受託人時，金融機構應瞭解其業務往來之性質、所有權與控制架構及法律形式等資訊。另並應瞭解客戶是否可發行無記名股票，以及對已發行無記名股票之客戶採取適當措施以確保其實際受益人之更新。（參酌 FATF 第十項及第二十四項建議）

（2）增訂銀行業完成確認客戶身分措施前，不得與客戶建立業務關係或進行臨時性交易，但在已完成客戶身分之辨識及風險可有效控管等條件下，得於建立業務關係後再完成客戶資料之驗證，以兼顧實務之執行。（參酌 FATF 第十項建議）

（3）配合資恐防制法公布施行，並參考美國紐約州金融署「防制洗錢之交易監

控與篩選程序最終規範」，增訂姓名檢核計畫與帳戶及交易持續監控之相關規範。

（4）增訂金融機構對於現任及曾任國外政府或國際組織之重要政治職務人士與其家庭成員及有密切關係之人（close associates）等之客戶審查措施。（參酌 FATF 第十二項建議）

（5）增訂匯款行辦理匯款應提供匯款人及受款人資訊之規定（參酌 FATF 第十六項建議）

（6）明定銀行業內部控制應包括洗錢及資恐風險評估、防制洗錢及打擊資恐計畫等。另銀行業之董事會及高階管理人員應瞭解其洗錢及資恐風險，以及其防制洗錢及打擊資恐計畫之運作，並採取措施以塑造重視防制洗錢及打擊資恐之文化。（參酌 FATF 第一項及第十八項建議）

（7）金融機構應指定一專責人員負責防制洗錢及打擊資恐法令遵循事宜，至是否成立專責單位則由金融機構依其規模或風險自行決定。惟考量本國銀行之規模及所面臨之洗錢及資恐風險，爰明定其應設置獨立之防制洗錢及打擊資恐專責單位，並由董事會指派高階主管一人擔任專責主管，賦予防制洗錢及打擊資恐第二道防線之充分職權。

（8）要求銀行業國內外營業單位應指派資深管理人員擔任督導主管，負責督導所屬營業單位執行防制洗錢及打擊資恐政策及程序之相關事宜，並辦理自行查核，以落實第一道防線之功能。

（9）銀行業每年應出具防制洗錢及打擊資恐內部控制制度聲明書，提報董事會通過後，於網站公告。

（10）明定員工任用應檢視其是否具廉正品格及相關專業，並就防制洗錢及打擊資恐專責主管、人員及國內營業單位防制洗錢及打擊資恐督導人員之資格條件及在職訓練等進行規範。

第四節　銀行網路金融業務之監理要點

金融業遭駭客攻擊事件頻傳，台灣及全球發展金融科技都是一大挑戰，資誠（PwC）於 2016 年 7 月公布「2016 全球經濟犯罪調查報告：金融服務業」，該受訪者為全球 115 國，共計 1,513 位金融服務業之高階主管及各部門主管。調查顯示半數金融業過去一年曾發生網路經濟犯案，較上次調查增加 10%，儘管企業在法令遵循之投資持續增加，亦持續受到法令之審查規範，但金融業犯罪事件仍持續增加，代表企業須在資安防護上有一嶄新思維，以利更有效打擊經濟犯罪及增加法令遵循投資之價值。就上開調查報告結果及近來駭客事件，提供台灣發展金融科技一省思機會，企業追求創新、技術與速度同時，尚不得忽略風險之重要性。有論者謂：「資安為永遠做不完之專案，但不是補不完之破網」，期待資安與新興科技發展同步並進，為台灣發展金融科技帶來契機。以下為前項調查報告之重點結果：

（一）53%金融業在過去一年增加打擊經濟犯罪支出，55%受訪者認為未來仍將持續增加該支出。

（二）46%全球金融業在過去一年曾發生經濟犯罪事件，較上屆調查增加 1%。

（三）16%曾發生經濟犯罪事件之金融業，遭受逾 100 個犯罪事件；6%曾發生經濟犯罪事件之金融業甚至遭受超過 1,000 件犯罪事件。

（四）49%金融業曾經歷網路犯罪，較上一屆增加 10%。

（五）37%金融業坦承，過去一年來受到網路犯罪事件之影響。

全球金融科技自開始發展以來，係科技業（Technology Sector）而非金融業主導，金融科技新創事業（FinTech Start-ups）更是如此，在此趨勢下，金融經營環境已在雲端、行動、大數據、社群及物聯網等重大科技發展中快速轉變，除了帶來交易型態、商業模式及產業價值鏈創新外，未來新型態科技風險亦挑戰當前金融監理思維。有論者言，金融科技新創事業與監理機關及其監理規範間，存在緊張關係（Douglas, 2016），其主要原因包括一是新創企業欠缺金融業經營背景

而不知可能受何項法律規範；二是已知相關法規限制，因而在開始營業前，即以規避作法設計商業模式；三是新創企業自始意圖違反法規。對前二類情形，新型科技或商業模式係在監理機關思考，如何將其納入現行規範體系前先行到位。對金融監理機關而言，監理措施如何設計始能有效監理，並避免不成熟階段之過度監理阻礙金融科技發展，可謂困難之所在。

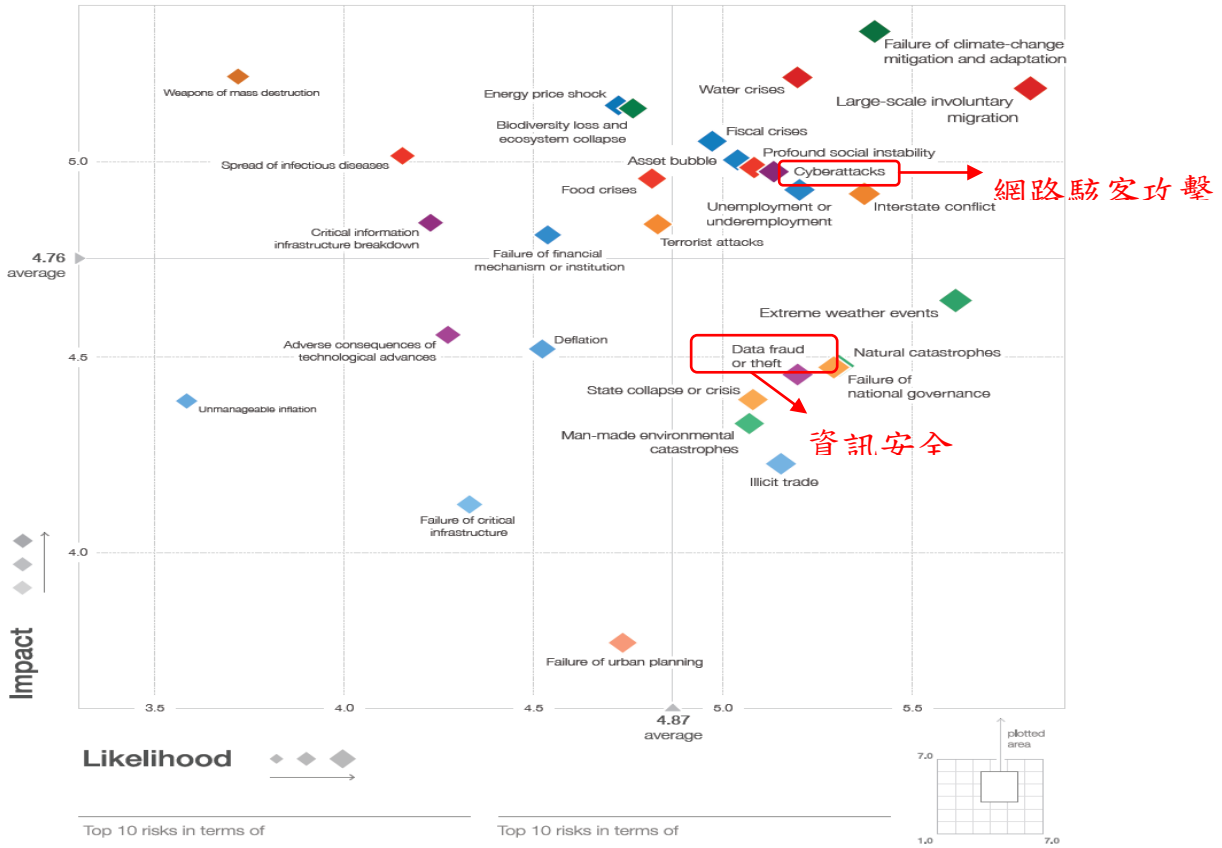


圖 4-8：2016 全球風險分佈

資料來源：The Global Risks Report 2016 11th Edition, World Economic Forum.

由於在全球各國網路利用擴大，網路安全解決方案之採用數量亦增加，加上隨著行動裝置（智慧型手機、平板電腦、筆記型電腦等）無線網路之廣泛使用，IT 系統對電腦網路攻擊變得更脆弱。再者，由於雲端基礎服務之引進與 IoT（物聯網）之興起，IT 系統對電腦網路攻擊之漏洞增大。國際研究機構預估 2016 年至 2020 年資安事件複合成長率（CAGR）13.39%。在網路金融使用方面，台灣網路資訊中心及國立政治大學 2016 年 7 月最新公布「2016 年台灣寬頻網路使用調查」，台灣使用行動銀行及使用行動支付情形結果如下：

（一）使用行動銀行情形

1. 曾經行動上網的 2,171 位受訪者中，26.0%有使用行動銀行，而 74.0%表示沒有使用行動銀行。

2. 有使用行動銀行的 564 位受訪者中，使用過的行動銀行服務以「帳戶查詢」的比例最高，占 64.5%，其次是「轉帳」，占 59.2%。

3. 有使用行動銀行的 564 位受訪者中，會擔心的事情以「個人資訊外洩」的比例最高，占 53.3%，其次是「帳戶被盜用」，占 38.2%。

4. 沒有使用行動銀行的 1,608 位受訪者中，沒有使用的原因以「不需要」的比例最高，占 56.2%，其次是「安全考慮」，占 32.4%。

（二）使用行動支付情形

1. 曾經使用行動上網的 2,171 位受訪者中，21.8%有使用行動支付，而 78.2%表示沒有使用行動支付經驗。

2. 有使用行動支付的 474 位受訪者中， 支付的費用項目以「生活用品」的比例最高，占 56.3%，其次是「LINE 貼圖」，占 22.0%。

3. 沒有使用行動支付的 1,698 位受訪者中， 沒有使用的原因以「不需要」的比例最高，占 54.3%，其次是「擔心它不安全」，占 36.3%，再次是「不知如何使用」，占 11.4%。

對金融科技業而言，在發展過程亦須同步將現行法令遵循架構，納入其營運計畫中，並考慮與監理機關間之關係與互動，以及長期規避法令之影響，如電子貨幣成為洗錢工具時，金融科技業者即可能面臨刑事追訴（Popper, 2015）。我國金管會於 2016 年 5 月公布「金融科技發展策略白皮書」，其中將「建立虛擬法規調適機制，打造友善的法規環境」列為金融科技施政重點，但對「虛擬法規調適機制」之定義為何，以及如何打造友善法規環境之具體落實，並未有提及。目前英國金融科技發展居於全球領先地位，根據英國政府報告，包括歐洲銀行監理署

（European Banking Authority）、金融審慎監理局（Prudential Regulation Authority, PRA）、英國金融業務監理局（Financial Conduct Authority, FCA） 等，均嘗試與金融服務業與金融科技業建立新關係，並在監理機關間就預期監理目標進行公開對話，亦與私部門間就監理議題進行溝通。

英國 FCA 建立「創新計劃（Project Innovate）」，目的在於追蹤進入金融市場之新興商業模式，並在國家科技辦公室（Government Office for Science）之建議下，FCA 開始研議對金融科技監理，建立「監理沙盒」之可行性。換言之，當英國發展金融科技時，對監理環境及監理措施之調控與規劃亦同步進行，對我國法規環境欠缺具體規劃之現況，深具參考價值。對此金管會於 2016 年 9 月提出研議推展 FinTech 之「領航計畫（pilot program）」，該計畫係為鼓勵銀行運用金融科技提供創新金融服務，相當監理沙盒之實質意涵，但後續仍需參考各國對監理沙盒制度政策與試行之經驗，進而調整「領航計畫」之作法。誠言之，有論者言監理沙盒制度之益處有三，一是降低進入市場時間及成本，二是融資取得容易並排除現行法規上之阻礙，三是消除法規不確定性可帶動多元商業模式，或新興商品進入市場[119]。

整體而言，金融科技重視即時客戶體驗及意見反饋，監理思維應由傳統被動之顧客權益保障，轉變以消費者為中心之金融消費者保護建構。有論者言，金融監理中，以消費者保障與洗錢防制為兩大核心任務，而金融科技服務下客戶身份核實、信用紀錄、償債能力查核、風險取向等須透過數位方式互動實踐[120]。儘管各國金融科技之創新性及成熟度不同，故監理措施各異，但總體原則趨同，包括堅持監管一致性原則以防止監管套利、秉承漸進適度原則（Progressiveness）在預防風險及鼓勵創新中尋求平衡、市場自律原則（Market Discipline），以及注重消費者保護（Consumer Protection）及資訊揭露[121]。應注意者，美國紐約州金融

[119] 參閱李慧芳，英國金融科技發展及監理沙箱(Regulatory Sandbox)機制對我國的啟示，科技政策觀點，2016 年 7 月 22 日，http://portal.stpi.narl.org.tw/index/article/10260，最後瀏覽日：2016 年 10 月 13 日。

[120] 參閱李沃牆，金融科技創新、監理與消費者保護，2016 年 8 月 19 日，第 9-12 頁，最後瀏覽日：2016 年 10 月 13 日，https://www.foi.org.tw/Download.ashx?Id=461&Lang=1

[121] 參閱廖岷，金融科技的發展版圖與監管挑戰，2016 年 5 月 17 日，最後瀏覽日：2016 年 10

服務署（New York State Department of Financial Services, DFS）近期公布「防制洗錢交易監控與篩選程式最終規範」，其中對交易監控及篩選計畫之要求，即係以風險預防為基礎之監理思維。

（一）預防性風險導向之監理原則

巴塞爾資本協定以風險為依據之監理方式，鼓勵金融機構根據實際風險情況及影響程度，進行自我測試與風險管理，而監理機關之監管力度可按新科技造成之風險程度，予以情境測試及設定監理門檻等措施，如此可將非金融業從事網路金融營業活動，明確歸入特定業務別，並精確掌握風險業務核心。換言之，監理工作之出發點及落腳點，均聚焦在資訊科技風險之預防，相關監理政策之推出及監理方式改變，其核心目的在於增強銀行對科技風險之掌控能力，進而降低銀行對受到金融科技衝擊之影響程度。事實上，以預防性風險為導向之監理策略，在美國、香港、澳洲、中國大陸等國家，均導入其金融監理政策中[122]。

風險導向之金融監理機制，其係透過檢查分析銀行財業務、營運管理及監理檢查資訊，以有效辨識潛在高風險事項，並將該等事項列為金融檢查重點，促使有限檢查資源投入最須關注項目，再藉由實地檢查逐一檢視實際辦理情形，一旦發現受檢機構確有相關制度性或重大缺失，即進一步督促其採取立即且有效改善措失，以增進營運健全性，並避免類似缺失重覆發生[123]。惟風險導向監理機制之設計目的，主要在改善傳統作業模式傾向發現金融機構當下問題與缺失，較無法確實瞭解造成問題之原因。故須要求對機構之風險管理品質（包括董事會與高階管理之監督、政策與作業流程規範、風險監控與資訊管理、內控與稽核等）進行評估，找出管理與制度面之可能弱點，透過實際交易抽查以確認實際情況，如此提出之檢查意見可點出問題源頭，以及實際負責單位並進行導正。

月 31 日，https://read01.com/mR8JKB.html

122 參閱閻慶民、謝翀達、駱絜飛，銀行業金融機構資訊科技風險監管研究，中國金融出版社，2013 年 4 月，第 63-68 頁。

123 參閱周鳴皋，參加「APEC 金融監理人員訓練倡議-風險導向金融監理及風險評估研討會」會議摘要與心得報告，行政院金融監督管理委員會出國報告，2012 年 6 月，第 7-13 頁。

（二）強化金融科技風險之動態監測

由於資訊科技風險可能隨著市場環境、金融業務種類及規模、新興技術開發等變化而影響銀行正常經營，故監理單位對資訊科技風險之敏感度至關重要。其監理要點應遵循在最短時間內，監測單體銀行或銀行業總體之科技風險變化，以建立動態性之資訊科技風險評估指標，尋求在最短時間內預警風險變化趨勢。有論者謂[124]，如網路金融服務涉及資金籌集、借貸相關授信業務，比照為消費金融業務，或其他可歸類為資產管理業務、收付清算業務，可考慮給予適用風險係數而應用在現有金融業監理指標。事實上，金融科技未改變金融業務風險屬性，但潛在之資訊科技風險及作業風險更加突出，對此美國金融穩定監管理事會將資訊科技安全列為影響金融穩定之主要風險，而加以動態、及時監控。

（三）「監理沙盒」鼓勵創新之監理模式

在電腦領域中所謂「沙盒」技術，係指在電腦中規劃一獨立區域，提供指定程式僅在該被隔離之區域中執行、讀寫資訊，而「沙盒」中資料交換或訊息讀寫等工作，不會與沙盒以外之環境相互影響或混淆。事實上，防毒軟體其實亦內建沙盒功能，可將疑似病毒、木馬等可疑程式置於沙盒中，試用是否有問題，既可執行該程式之功能、又可不讓電腦中毒，當使用電腦時產生之各種暫存檔、網頁瀏覽記錄或各種私人資訊，均在沙盒中獨立運作，在不使用時刪除沙盒中之內容即可讓電腦操作記錄完全消失，完全不會留下記錄。

在金融科技發展趨勢下，銀行業與金融科技公司持續互動及結合，美國貨幣監理署（OCC）於 2016 年 3 月發布「支持在聯邦銀行體系進行負責任創新」，其提出支持「負責任創新（Responsible Innovation）」之監理架構。就意義而言所謂負責任創新係是指在符合穩健風險管理及銀行整體經營戰略前提下，創新或改良金融產品、服務及流程，以滿足消費者、企業不斷變化之需求。對此 OCC 提出其基本原則，包括建立評估 FinTech 創新方案之「中央創新辦公室」；培育負責

[124] 參閱柯瓊鳳、黃一敏，非金融機構在網路金融業務監理風險之探討-以中國大陸電子商務公司為例，兩岸金融季刊，第四卷第三期，2016 年 9 月，第 129-130 頁。

任創新之監理內部文化；鼓勵銀行業提供公平金融服務及對待金融消費者；銀行業須透過有效風險管理及良好公司治理，促進安全穩健經營；鼓勵各類規模銀行均將負責任創新納入戰略規劃等。惟應注意者，創新監理模式不應完全脫離現有之監理架構，同時確保創新業務風險不從 FinTech 公司轉移至金融消費者。

（四）強化資訊揭露範圍及分類

由於 FinTech 服務對象可能是傳統金融體系未觸及之新創企業，甚至是信用評分較低之個人，其金融專業知識及風險承受能力相對較少，因而各國監管單位無不將資訊揭露及消費者權益保護，視為重要議題。如英國 FCA 於 2014 年發布「對網路眾籌與其他媒體對未實現證券化的促進監管辦法」中，即要求 P2P 借貸平台須以大眾化語言向投資人揭露投資商品之收益及風險等資訊，包括過去實際違約率、未來預期違約率、預期違約率計算假設條件、借貸風險評估情況、可能實際收益率、處理延遲支付及違約程式等。而法國於 2014 年發布「參與性融資法令」，要求股權群眾籌資平台須設置「分步訪問程式」，意即首先向投資人告知投資之性質及風險，二在投資者認購前，平台應對投資人進行適當性測試，包括投資人經驗等[125]。誠言之，市場紀律方面可透過資訊透明度提高，而消費者保護方面則透過消費者教育增進消費者保護，達到金融監理之目的。

（五）推動監理科技（Regtech）之有效發展

誠如前述，Regtech 繼 FinTech 後成為另一個熱門議題，所謂監理科技係指監理單位應用科技執行現有監管程式，達到有效風險識別、進行風險加權、監測及數據分析。近年英國、香港等國家或地區研究提出積極發展監理科技，一方面監理單位利用資訊科技升級監理工具及方法，以及時掌握金融體系之風險關聯性與集中度變化，甚至評估金融機構報送資料之真實性及準確性。二方面由於新興資訊科技在金融領域之應用，可謂大勢所趨，對從事金融監理人員須強化其資訊科技知識培訓，以提高金融監理檢查效率。

[125] 參閱朱太輝、陳璐，Fintech 的潛在風險與監管應對研究，2016 年 10 月 28 日，最後瀏覽日：2016 年 11 月 9 日，http://chuansong.me/n/1047983846743

（六）即時監理保護消費者

由於美國金融監理成熟，故運用科技強化監理，以致於 RegTech 議題在美國相當盛行。美國專業財報資料庫解析公司，未來協助主管機關即時（real time）監理，而主管機關透過監管科技（RegTech）對受監管業者之營運活動進行即時監控，協助業者做到即時之法令遵循。例如透過區塊鏈技術（Block-Chain）改變銀行運作之模式、降低銀行之作業成本；不但能讓金融服務安全提升，亦可降低消費者支付的費用，改善監理程序。因此未來在消費訴訟上，FinTech 訴訟案件可能更為多元，科技金融個案研究作為制定金融消費者保護，將在 RegTech 當中扮演重要之角色。

第五章　結論與建議

第一節　結論

為分析方便起見，網路金融商業模式大致上可簡化成「支付」與「投融資」兩大類概念。支付（指資金流通）類的商業模式旨在使資金流通更便捷安全，如虛擬貨幣與第三方支付；而投融資類型的商業模式旨在媒合有閒置資金者與需要資金者，使得借款更加便捷，如 P2P 網路貸款與群眾募資。不過未來網路金融商品及服務會愈來愈複雜，包括利用網路技術和行動通訊甚至大數據及人工智慧運算等技術進行資金支付及供需的新興金融模式。

據台灣金融研訓院（2014）研究，網路金融之主要目的，即是將金融體系之基本功能，包括（1）清算與結算、（2）聚集及分配資源、（3）風險管理與風險分散等功能，透過網路達成。以目前網路金融發展情況，以上幾個主要功能均已能達成，特別在支付方面，各國以第三方支付及行動支付為代表之網路金融業務取得較快進展。據高盛（Goldman Sachs）2015 年發布資料顯示，全球行動支付預計未來五年以年均 42%速度增長。基本上，網路金融模式在消費者端有三管道，一是透過社交網路，可生成及傳播各類與金融相關之資訊，特別是可獲取部分個人或機構無義務揭露之資訊；二是搜尋引擎對資訊之組織、排序及檢索，可緩解資訊超載問題，滿足資訊需求，大幅提高資訊蒐集效率；三是巨量資訊高速處理能力。上述組成部分正是發展網路金融之主要誘因與趨勢，甚在傳統金融業務之融資與風險管理方面，網路亦可憑藉資訊處理能力，以及組織模式方面之優勢，大幅降低金融交易成本。

再者，台灣金融研訓院（2014）研究認為，在大數據時代下，銀行所面臨之競爭不僅來自同行業內部，外部之挑戰亦日益嚴峻。擁有網路、電子商務等新興企業，在產品創新能力、市場敏感度及大數據處理經驗等方面，均擁有其明顯之優勢，若這些企業開始涉足金融領域，將對銀行形成較大的威脅。因此，對銀行來說，建構銀行業強大的數據處理能力，必須與網路業者、電子商務等企業進行合作，獲取更多的使用者行為資訊，與各類資料分析的專業廠商合作，對銀行已

經存在的大數據庫進行綜合處理與分析。其次由於台灣網路銀行業務發展較早，銀行的網路金融行銷多數透過自有網站或是電子郵件進行，在後續智慧型手機普及後，才開始將原有網路銀行介面轉到手機 app 進行，但規劃思維仍以過去的網路銀行規劃方向進行。而目前中國大陸較為新式的網路金融業務包括微信紅包、群眾籌資等，主要都是基於幾個重要主軸，在網路進行業務宣傳、行銷及資金募集等金融活動最後達到提高客戶使用率目標。

網路金融業務風險議題主要包括以下幾項：(1) 新資訊科技帶來之作業風險問題。(2) 消費者權益相關之風險問題。(3) 異業結合之關聯性風險問題。(4) 雲端計算、大數據對網路金融服務之個資保護衝擊。而與網路金融交易相關之風險管理原則共有七項，包括 (1) 數位金融業務之客戶的認證；(2) 電子交易的責任歸屬；(3) 採取適當措施確保責任劃分；(4) 數位金融系統與資料庫的適當監控；(5) 電子交易、紀錄、與訊息之資料整合；(6) 建立電子交易之審計紀錄；(7) 關鍵資訊之保密等。而為使銀行在商業與法律風險上獲得保護，數位金融服務須建立在一致與即時之基礎上，以滿足客戶之高標準期待，同時銀行亦須有能力將服務傳遞至所有客戶，並在任何環境維持相同之服務能力。此外，與法律及信譽風險有關之風險管理原則亦有四項，即 (1) 對數位金融服務之適當揭露；(2) 注重顧客個人資料之私密性；(3) 確保數位金融系統服務能力之長遠計畫；(4) 做好事故應變規劃。

整體而言，風險主要表現在享受網路金融服務族群之金融知識、風險識別及承擔能力之相對欠缺，容易遭受誤導、欺詐及不公正待遇，同時由於其投資小額而分散，網路金融風險一旦爆發，對社會整體影響相當大。因此在考慮網路金融風險時，有必要將網路非法集資及網路金融加以區別，如近期 e 租寶在中國大陸發生之全國性風險事件，牽涉群眾廣，涉案金額大。事實上，該企業在宣傳中均標榜自身是網路金融創新，但此類打著網路金融旗幟而行非法集資之行為，形成另類之網路金融風險。誠言之，防範網路金融風險要採取針對性措施，如就信用風險問題，可對行業準入門檻、行業經營準則進行明確規定，包括網路金融平台有責任及時、準確之進行資訊揭露，惟同時亦要強化個人徵信體系，加快資訊之

共用。而就流動性風險而言，則是建立流動性管理指標體系，對該風險進行實時監測評估，甚至可利用大數據對流動性風險進行預測。

目前主要國家對於網路金融業務風險監理的措施如下：

（一）美國

美國目前採功能性監管，較嚴格以穩定平衡為主。2008 年金融海嘯後監管趨嚴，惟在金融海嘯發生後，FinTech 提供替代性金融中介功能，輔助傳統金融體制之弱點與缺陷。美國人才資本濟濟，創意無限， FinTech 仍在美國特殊環境下形成，並在供需環境中自發性成長，且美國政府亦未對 FinTech「生態系」積極介入，頗有平衡監理的意味。美國對 P2P 雖無單一規範法制，但對採取多頭監管方式，包括除了聯邦層級管制外，各州政府亦有相關規定，其中在聯邦監理角度上，P2P 平台需將每天貸款列表提交美國證管會，在州監理角度上，各州則存在些許差異。美國第三方支付監理機關分為存款保險公司（FDIC）及各州，而適用法規亦可分為聯邦「統一資金服務法」及各州適用之「資金移轉法」。美國聯邦對第三方支付監理係放在「貨幣服務業務」項目，角色被界定為「資金移轉服務商」，其資金非聯邦銀行法所定義之存款。

（二）日本

日本受到美國的影響，目前較保守嚴謹。日本於 2015 年 9 月公布「平成 27 事務年度金融行政方針」中，「4、鑑於 IT 技術之進展金融業及市場變革之戰略性對應」之具體重點政策，即為 FinTech 之對應。日本金融廳為確保對變動極快之 FinTech 產生對應，彙整日本 FinTech 與其他各國 FinTech 之差異，包括營運模式、資本市場活絡程度、業務獨佔性、使用習慣等。日本 P2P 業者除了須依金融商品交易法進行登記外，亦應依融資公司法進行登記，並受到日本金融廳監理，但日本監理機構並未對 P2P 業務非常重視。日本政府於 2016 年 3 月向國會提出「為了對應情報通信技術進展等環境變化之銀行法一部改正法律案」，重點包括 IT 進展伴隨著技術革新之銀行對應、銀行集團內子公司業務匯集容易化、虛擬貨幣法制度之整備等。

（三）英國

英國身為國際金融中心，採政府主動監管主導。英國政府提出「金融科技未來願景」表示金融科技非洪水猛獸，可能產生良性循環，展現更多「普惠金融」。但就金融主管機關立場而言，最為關鍵仍是如何建置適當之監管制度，在評估納管金融科技之餘保持充分靈活性。英國中央監管單位金融行為監管局（Financial Conduct Authority, FCA）主導「新創計畫（Project Innovate）」，目的在檢視並排除對金融科技創新之障礙，與此同時，亦帶動「監理科技」之改變，以增加監理效率。2016 年 5 月正式推出監理沙盒（Regulatory Sandbox）計畫。英國對 P2P 監理始於 2014 年 3 月之「金融服務市場法」，其分別將「P2P 網路借貸型眾籌」與「股權投資型眾籌」制定不同監管標準。2009 年英國參採歐盟「支付服務指令」及其金融服務市場法發布「支付服務法」，並於 2012 年修正，旨在對第三方支付體系詳加規範。

（四）中國大陸

中國大陸方面，目前則採被動型監管，以市場商業模式驅動。由於大陸法系之監管靈活度及成熟度不如英美，負面表列較容易造成灰色地帶。國務院十部委於 2015 年 7 月出台《關於促進互聯網金融健康發展的指導意見》，此後一系列監理新規陸續公布，即代表監理部門對互聯網金融之監管尺度轉嚴。在非金融機構之互聯網金融規範方面：

1、銀監會會同工信部、公安部等於 2015 年 12 月起草《網路借貸資訊中介機構業務活動管理暫行辦法（徵求意見稿）》，對網路借貸行業之定位及其禁止活動行為，進一步引導投資人風險自負。

2、證券業協會於 2014 年 12 月起草《私募股權眾籌融資管理辦法（試行）（徵求意見稿）》，明文以非公開發行方式進行股權群眾募資活動，但該辦法至今尚未落地。而隨著前開指導意見出台，證監會發布通知，未經許可不得從事公開股權群眾募資活動。

3、中國人民銀行於 2010 年 6 月公布《非金融機構支付服務管理辦法》，其確立第三方支付機構之法律地位，並對規範客戶備付金管理、網路支付及預付卡業務分別發布相關管理辦法。

4、金融法規因應互聯網金融調整：

（1）全國人大常委會於 2015 年 8 月決議修改商業銀行法，取消存貸比不得超過 75%要求，考量要點之一為互聯網金融對銀行貸款投放相應受到限制。

（2）第十二屆人大常委會第十四次於 2015 年 4 月召開時，財經委員會推出《證券法》草案，其中該草案第十三條規定，經中國證監會核准以互聯網群眾募資之方式公開發行證券，可豁免註冊或核准。但草案尚未三讀通過。

（3）中國人民銀行於 2015 年 12 月發布《中國人民銀行關於改進個人銀行帳戶服務加強帳戶管理的通知》，其中建立銀行帳戶分類管理機制方面，主要是區分 I 類 II 類及 III 類，並可採取多種方式對開戶申請人身份資訊進行交叉驗證。

（4）中國銀監會於 2016 年 6 月起草《銀行業金融機構全面風險管理指引（徵求意見稿）》，在各類風險中加入資訊科技風險，並要求建立可供識別、評估、監測等管理方法及資訊科技基礎設施。

（五）台灣

台灣方面，已有相關網路金融業務法規修訂。我國於 2015 年 2 月公布「電子支付機構管理條例」，允許支付機構從事代收代付業務、儲值業務、電子支付帳戶間款項移轉業務，同時開放銀行、中華郵政及電子票證發行機構得申請兼營支付業務。櫃買中心於 2013 年 11 月公告「創櫃板管理辦法」，而該「創櫃板」專區於 2014 年 1 月正式啟用，其主要參考美國 JOBS 法案，以協助創新創意企業發展順利籌資。櫃買中心於 2015 年 4 月發布「證券商經營股權性質群眾募資管理辦法」，僅限證券商得申請經營股權性質群眾募資平台，並受理微型創業之募資公司。金管會於 2014 年 6 月宣布打造台灣數位化金融環境，並於 2015 年 1

月起推動相關計畫，包括新增 12 項銀行業務可在線上申辦，並陸續修正管理辦法、自律規範及消費者保護措施，旨在便利消費者使用各項線上申辦業務。金管會於 2015 年 9 月設立「金融科技辦公室」，同時發布「銀行及金融控股公司申請轉投資資訊服務業及金融科技業規定」，其將金融科技業及資訊服務業一併認定為金融相關事業，持股最高可達 100%。金管會於 2016 年 5 月公布「金融科技發展策略白皮書」，將發展金融科技定調為提升國家競爭力之重要戰略，並以 2020 年為期，分別就金融服務、創新研發、人才培育、風險管理、基礎建設等五大構面發展金融科技。

本研究首先分析銀行傳統風險在網路金融業務之延伸，並探討金融科技趨勢下，創新網路金融業務帶來之新種風險類型。其次，研析歐美、亞洲及中國大陸等主要國家，其新興網路金融業務之法令規範及監理架構。最後，再就銀行因應網路金融業務之風險監理，以國際金融科技監理環境趨勢為導管，提出網路金融資訊安全之偵測與預防，以及稽核措施與監理要點之見解，進而對我國銀行業與主管機關提供具體建議。對此，本研究以討論在金融科技趨勢下，應重視之網路金融風險管控、稽核及監理措施與時俱進地調整等研究成果，歸納整理如下：

（一）主要國家網路業務及金融風險之法令規範及監理

參照各主要國家網路金融業務，未來網路金融業務的主要發展模式包括第三方支付、P2P 融資平台、大數據徵信、眾籌、網路智慧銀行、區塊鏈金融、供應鏈金融及物聯網金融等模式。FinTech 風潮自美國矽谷吹起後，傳遞至紐約、倫敦，並擴及亞洲之香港、新加坡，而中國大陸亦於 2011 年從電子商務產業崛起後迅速發展。FinTech 席捲全球各地，至今發展最為成熟仍是美國，全球前 50 強 FinTech 公司占半數以上即可得知，包括 Paypal、Lending Club、Wealthfront 等。事實上，美國 FinTech 之興起可謂拜 2008 年金融風暴之賜，在金融機構大舉裁員，政府亦訂定新法令以加強風險控管之環境下，非具銀行身分之 FinTech 公司不受相關法令限制，加上被裁員者具備金融及科技領域之專業技能，而得以運用於聚焦顧客需求，發展出創新性金融服務。在面對 FinTech 跨足金融業務時，

美國銀行業亦採取許多因應對策，但美國政府並未對 FinTech「生態系（ecosystem）」積極介入，而使其自然成型，惟引發金融海嘯前車之鑑，美國政府瞭解傳統金融體制之缺陷，強化監理實屬必要，故注重政府分層監管及立法規範，並採用較為嚴格之證券類法規監理新興網路金融業務。

繼美國 FinTech 發跡後，英國政府亦宣示將倫敦打造成為全球 FinTech 中心之目標，除了主動就現行金融法規在 FinTech 領域之適用進行說明外，金融業務監理局（FCA）亦推動「監理沙盒（Regulatory Sandboxe）」計畫，提供創新金融服務可實際營運之測試環境，並觀察可能之產業衝擊及影響，以作為法規調適之依據[126]。誠言之，英國政府提出「金融科技未來願景（FinTech Futures）」此項具指標意義報告，明確表示金融科技絕非洪水猛獸，其亦可能產生良性循環，創造全新市場與新客戶，從而展現更多之「普惠金融（financial inclusion）」。如就金融主管機關立場而言，金融科技固然帶來諸多重要課題，其中最為關鍵者仍是如何建置適當之監管制度，故英國政府確信有效之金融監理法規，將是英國金融產業及金融科技未來發展之成功關鍵因素。而金融科技業者，則在監管當局頒布相關法律規範前，該行業即組成自律組織並制定規則。

新加坡金管局於 2015 年 6 月揭露新加坡金融科技發展現況與主要關注技術重點，同時提出成立金融創新推動、打造 FinTech 生態圈、FinTech 技術及技能培育等計畫，同年 8 月新加坡政府即成立 FTIG（FinTech & Innovation Group）組織 FinTech 領域政策發展及監理工作。更繼英國經驗，先於 2016 年 5 月成立跨部會「金融科技辦公室（FinTech Office）」負責 FinTech 相關事務，鼓勵全球 FinTech 新創業者在新加坡設立據點，再於同年 6 月正式提出「監理沙盒」指導原則，明確表示在監理沙盒註冊之 FinTech 公司，可在一明確定義之場所、期間及新加坡金管局提供法規支援情境下進行實驗，且允許在事先報備情況下，從事與目前法律規範尚有衝突之業務，即便日後被官方終止相關業務，亦不追究相關法律責任。新加坡對新網路金融業務雖注重政府監管，並以證券類相關法規加以

[126] 參閱範秉航，台灣 FinTech 的下一步，P2P 借貸平台？，台灣經濟研究院，2016 年 1 月 15 日，http://www.tier.org.tw/comment/pec5010.aspx?GUID=73eb4243-4409-4196-bd7e-1a7478a5412e，最後瀏覽日：2016 年 10 月 13 日。

規範，但同時採開放態度，積極與 FinTech 新創企業互動，並理解相關新興創新技術，以協助其設計考量金融業法規及風險特性之解決方案。

日本金融廳為確保對變動極快之 FinTech 產生對應，以及未來金融業務之優位性，協請民間部門對海外事業調查與對話，以金融業及市場發展與顧客之便利性提升為目標，積極活用日本國內外專家之貢獻，透過技術革新整備日本經濟與金融環境。日本政府於 2015 年 9 月公布「平成 27 事務年度金融行政方針」，其中「4、鑑於 IT 技術之進展金融業及市場變革之戰略性對應」之具體重點政策第（1）點即是說明 FinTech 之對應。此外，日本金融廳進一步彙整日本 FinTech 與其他各國 FinTech 之差異，提出營運模式、資本市場活絡程度、開戶條件、業務獨佔性及使用習慣等不同之處。但因 FinTech 活用範圍非常廣泛，金融業「機能分化」之結構性改變，市場分野、交易所機能改變未來可預見，因而對金融法規因應 FinTech 趨勢進行修正較我國為快，如日本金融廳於 2016 年 3 月正式向國會提出銀行法及資金結演算法修正案，包括對應 IT 進展伴隨著技術革新、充實銀行集團經營管理、虛擬貨幣使用者保護等。

我國面對 FinTech 趨勢雖步調較慢，但其全球化特性促使我們積極因應，如金管會仿照英國及新加坡，於 2015 年 9 月成立金融科技辦公室，並致力於全面發展包括數位金融、機器人理財、大數據應用、雲端及物聯網建設等，結合金融與科技之創新金融服務。再將共同投資大數據資料庫、新創事業創新基地、金融科技發展基金等列為後續推動措施，亦宣布打造不動產授信統計資訊平台、分析投資機構與投資人之交易行為等十一項資料應用計畫，預期提升金融業競爭力及發揮投資總體效益，即如同國外 FinTech 成為創業投資熱點，站在數位金融創新之風口上，創造成功之金融營運模式。此外，金管會再於 2016 年 9 月提出研議推展 FinTech 之「領航計畫（pilot program）」，為鼓勵銀行運用金融科技提供創新金融服務，相當監理沙盒之實質意涵，但後續仍需參考各國對監理沙盒制度政策與試行之經驗，進而調整「領航計畫」之作法。

（二）銀行網路金融業務發展之風險控管及稽核監理

稽核部門應提出主要風險查核結果並向董事會報告，稽核範圍及資訊不受限制，稽核人數應與銀行規模及複雜度相當，且應有稽核技術以查核相關風險，並應定期訓練以符實際需求；稽核計畫應提出個別及整體的作業風險計劃，並隨情況改變調整，稽核頻率應以辨識風險程度為基礎，稽核計畫執行，應明確表達所辨識出的作業風險，其交易測試應充分驗證作業風險的控制，且應包括法令遵循之測試；稽核報告應清楚標示作業及控制缺失，並依嚴重性或重要性區分等級，例外事項應建立稽核軌跡直至問題解決為止，未解決的例外事項應有陳報程序，稽核應驗證改善措施之完整性及有效性。

金融科技重視即時客戶體驗及意見反饋，監理思維應由傳統被動之顧客權益保障，轉變以消費者為中心之金融消費者保護建構。事實上，金融監理以消費者保障與洗錢防制為兩大核心任務，而金融科技服務下客戶身份核實、信用紀錄、償債能力查核、風險取向等則透過數位方式互動實踐。雖各國金融科技之創新性及成熟度不同，監理措施各異，但總體原則趨同，如堅持監管一致性原則以防止監管套利、秉承漸進適度原則在預防風險及鼓勵創新中尋求平衡、市場自律原則及注重消費者保護與資訊揭露。美國紐約州金融服務署（DFS）近期公布「防制洗錢交易監控與篩選程式最終規範」，其中對交易監控及篩選計畫之要求，即係以風險預防為基礎之監理思維。

網路金融風險包括政策風險、監理風險、法律風險、交易風險、技術風險及信用風險等類型，除了對網路金融企業或客戶本身產生直接影響，其風險亦可能傳導至傳統金融行業及實體經濟。其中政策法律風險主要有法律風險及政策風險二類，後者政策風險為來自國家有關網路金融政策調整帶來之不確定風險；前者法律風險之一是刑事行政法律風險，由於觸犯非法集資類犯罪或行政違法、非法經營類行政違法或犯罪及非法證券類行政違法或犯罪的刑事法律風險。二是民事法律風險，指因交易結構本身所造成的各類民事法律風險，導致集團性訴訟案件爆發。

再者，監管風險主要來自分業監管模式與混業經營模式的不匹配。跨行業、跨部門、業務交叉性強等特徵是網路金融領域普遍存在，網路金融企業之經營範圍可能既包括銀行業務，亦涉及證券及保險業務，而形成數類金融業務以網路為基礎進行深度融合之模式。而目前中國金融業實行分業監管模式，不免存在著九龍治水和監管真空現象。交易風險包括交易系統及交易特性風險，前者係諸如網路仿冒、病毒威脅、系統中斷或其他不可預見之事件，導致機構無法提供安全產品或服務，該風險普遍存在於每一個網路金融產品或服務中。而網路金融交易特性風險產生於經濟主體之決策，主要由交易者間的之信息不對稱引起信用風險，該信用風險係指網路徵信系統建設不足，資訊不透明及信用資訊缺乏導致信任危機及風險聚集。

其次，技術風險係網路技術本身存在著技術風險，包括所信賴的信息系統之技術安全及技術容量、駭客攻擊、密碼洩露、帳戶資金被盜。交易者身份和真實性難以確認，存在著較高之消費者資訊洩露及受欺詐、誘騙等風險。與銀行封閉運行業務系統相比，網路金融之用戶敏感信息及個人財產，不僅存在更大之安全隱患，亦加速支付、清算等風險之擴散，使得風險在非傳統金融機構與傳統金融機構間出現轉移。認知風險則是網路金融創新之處，在於創造新業務技術、交易渠道及方式，主要功能仍是資金融通、價格發現、支付清算等方面，而金融業之兩大核心詞彙即資金與風險，但由於網路拓展金融交易之可能性邊界，大量傳統金融覆蓋不到之人群被納入金融服務範圍，該部分人群風險識別能力及風險承受能力相對欠缺，個體及集體非理性更容易出現，提高風險發生機率。

第二節　建議

我國金管會業於 2016 年 7 月正式公布「銀行業建立風險導向內部稽核制度實務守則」，將風險管理及內控內稽做更進一步結合。其中第六條風險評估因子與方法，規定內部稽核應就各受查主體所面臨之固有風險、控制措施之有效性等進行評估後，確認受查主體之風險評估結果（剩餘風險），並據以決定年度稽核

計畫。因此預期未來主管機關將加強要求各銀行實施較過去更為預應導向、積極及彈性，更以不同業務屬性的風險為評估依據的內部稽核管理計畫，強化聚焦在業務重要風險因子監測，從自行查核、法令遵循、風險管理及內部稽核四大構面訂定計畫加強內控稽核深度。

從英國金融科技創新計畫中可以發現，金融監理單位肩負計畫成功的重要責任，包含提供法令諮詢與說明、商品與服務審查、評估市場等。所以，金融監理單位至少須擁有以下三項能力：

（一）新科技接受力：金融監理單位對於新科技在金融服務的應用要抱持著開放態度，並願意使用或感受新科技應用（如智慧型手機），否則申請沙盒後，因為看不懂科技層面而被拒絕的機率應該會大幅增加。

（二）容許出錯能力：創新商品與服務必定有一些明顯或隱含的缺漏與問題，只要這些缺漏與問題在一個可控範圍內，都有改善空間。沙盒並不是要測試一個完美無誤的解決方案，而是一個有機會成功的方案。

（三）主動積極協助的意願與能力：金融監理應能主動積極協助 FinTech 業者才是沙盒成功運作的必要條件。在監理沙盒文件中，有七次提到金融監理單位應該要幫助或與創新業者一起共同尋求解決方案，所以金融監理單位並非金融科技的主導者，而是站在與業者平等的地位，主動協助業者了解法令規章、提供法令諮詢與解釋，甚至在必要時考慮修改因科技發展而可能不合時宜的規定。

2008 年金融海嘯後國際金融組織及歐美主要金融監理機關提出多項金融監管改革方案，保護金融消費者權益以及促進整體金融市場的健全。巴塞爾銀行監理委員會（BCBS）於 2008 年金融危機後，為改善銀行體系承擔來自經濟及金融層面衝擊之能力，提升銀行體系穩健性，於 2010 年 12 月發布「巴塞爾資本協定三：強化銀行體系穩健性之全球監理架構」（Basel III：A global regulatory framework formore resilient banks and banking systems，以下簡稱 Basel III），提出強化全球資本規範之改革方案，其內容包括修正銀行自有資本之組成項目、逐年

提高最低資本要求、建立槓桿比率及授權各國主管機關訂定抗景氣循環緩衝資本措施。BCBS 於 2011 年 1 月再發布「確保銀行在發生無法存續事件時吸收損失之最低要求（Minimum requirements to ensure loss absorbency at thepoint of non-viability）」，以強化銀行非普通股權益之其他第一類資本及第二類資本工具承擔損失之能力。

表 5-1：本國銀行合併及銀行本行資本適足率

	2013 年	2014 年	2015 年	2016 年	2017 年	2018 年	2019 年起
資本適足率(%)	8.0	8.0	8.0	8.625	9.25	9.875	10.5
第一類資本比率(%)	4.5	5.5	6.0	6.625	7.25	7.875	8.5
普通股權益比率(%)	3.5	4.0	4.5	5.125	5.75	6.375	7.0

資料來源：金融監督管理委員會。

參照各主要國家網路金融業務，未來網路金融業務的主要發展模式包括第三方支付、P2P 融資平台、大數據徵信、眾籌、網路智慧銀行、區塊鏈金融、供應鏈金融及物聯網金融等模式，由於網路金融業務發展十分快速，並不限於消金、企金或金融交易業務，銀行業未來可能會面臨網路金融業務，以及在反洗錢防制及反恐金融法令遵循方面的專業法令遵循專業人才的短缺問題。因應金融海嘯後網路金融與金融科技浪潮的興起，BCBS 亦陸續研議相關規範之修正，提案修改現有銀行自有資本與風險性資產計算方法，希望各銀行能以更嚴格的方式來計算面臨網路金融及網路資安攻擊、欺詐或巨額罰款時所需之營運資本。本研究提出綜合建議如下：

（一）密切注意國際相關網路金融之監理措施可能發展之新方向。一般主要國家之金融立法架構仍以傳統金融業務為主，如銀行法、證券法、保險法及財務揭露制度等，事實上各國仍缺乏有關網路金融業務之配套法規，此亦是多數國家發展網路金融普遍存在之情況。由於網路金融業務發展十分快速，部分商品及業務尚處於起步階段，利用網路提供或接受金融服務，在網路金融交易者之身份認證、電子合約之有效性確認等方面，勢必面臨在權利義務上容易產生糾紛，結果促使網路金融交易雙方產生較大不確定性，增加網路金融之交易成本，甚至影響網路

金融業務發展。隨著國際監理趨勢演進，與監理機構管理思維變革與推動，國際性銀行之稽核策略成為主管機關監理趨勢，且傳統偵錯角色已無法滿足內部與外部使用者對稽核部門之要求，於是被賦予更高期待。爰建議金融機構應密切注意並預應國際相關網路金融之監理措施可能發展之新方向，以做好各項內部基礎建設及準備工作予以因應。

（二）以風險導向概念引導內部稽核策略規劃。由於市場風險，即利率、匯率等市場價格的變動對網路金融交易者的資產、負債及損益變化，以及金融衍生工具交易帶來的風險等，在網路金融交易中一樣有影響。參考金管會民國 105 年 1 月修正「銀行辦理衍生性金融商品業務內部作業制度及程序管理辦法」，未來銀行基於強化內部資訊安全的內部控制，以及銀行承作網路金融商品及服務業務之特殊性，應考量以網路金融及金融科技風險導向概念來引導銀行內部稽核作業執行以及稽核策略規劃應建立相關作業措施，並建議國銀對銀行之風險導向稽核目標、策略、組織等預做規劃。

（三）銀行加強稽核暨風險查核部門任務重要性。以風險為基礎（Risk-based coverage）查核策略，由各銀行業務經理人責任確認業務風險並建立控制點，以維持有效監控並確保可及時更正已確認之缺失。稽核暨風險查核部門應先聚焦並辨識緊急風險及趨勢，有效說明並承擔管理上已發現缺失，並負責稽核、監控所採取改正措施，再向風險管理委員會及稽核工作小組報告稽核結果及趨勢，內控與業務部門共同努力以強化控制環境。並建議資訊系統暨基礎結構（Technology &Infrastructure）建置部門、策略暨支援組（Strategy & Support）建置部門、政策法令遵循建置部門（Policy Compliance Group）共同執行該項任務。

（四）落實業務單位對網路金融客戶實名認證之內部稽查工作。隨著網路及行動金融業務的普及，線上及行動支付已成為電子商務市場競爭焦點，中國大陸《非銀行支付機構網絡支付業務管理辦法》於 2016 年 7 月正式生效，未來如網路支付身份沒有進行實名認證，網路非實名支付將成為網路金融犯罪的重要來源，透過帳號竟能查到該用戶真實姓名、身份證字號以及手機號碼，不法集團得以製作

假身份證實施盜刷，客戶在網路支付業務中可能產生資金盜領、個資洩漏、詐騙、洗錢犯罪、非法融資等風險，因此應及早因應落實業務單位對網路金融客戶實名認證之內部稽查工作。

（五）以風險導向稽核建構對網路金融業務內部控制三道防線。內控三道防線攸關金融機構有效自我管理及長期健全經營，目前金融機構在三道防線之架構、組織建置及具體功能之實際運作差異甚大，為提升業者管理水準，建議要求業者仿照公司治理運作，依機構規模與業務複雜性，訂定明確之最佳運作範本，未來主管機關將透過實地檢查要求機構妥善建置。從風險導向內部稽核出發，透過內部三道防線機制對網路金融業務在稽核設計與稽核作業評估風險偵測，讓前線管理人員簡化內部控制程序，透過歷史交易及其他參數建立風險預警機制，進而協助管理階層能夠針對風險所在提出銀行營運及發展計畫，強化銀行公司治理、舞弊預警機制。

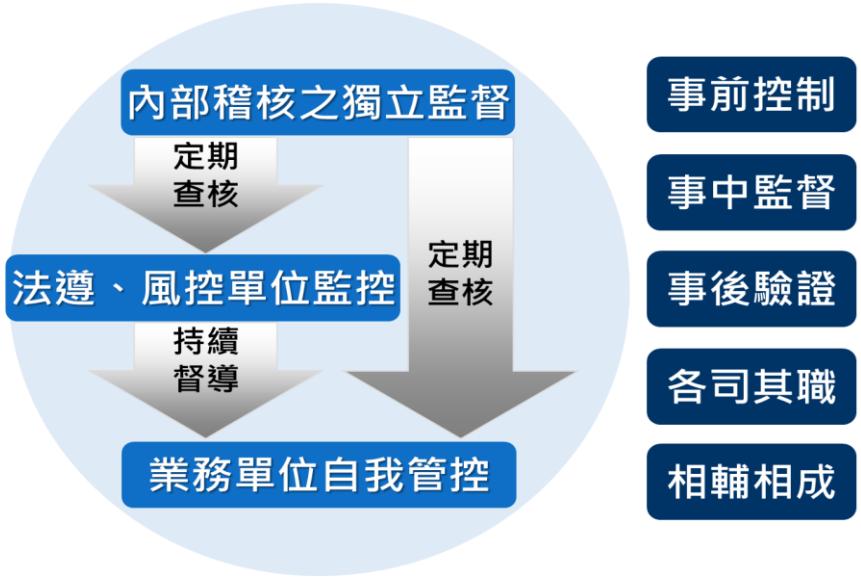


圖 5-1：內部控制三道防線之溝通、協調與合作

（六）風險導向監理檢查機制強調持續性監理。於導入風險導向新監理檢查機制時，應設立各專業檢查小組增進監理，以及檢查人員對整體業界營運管理模式之瞭解，並定期聚集研討分享檢查技巧及作法，建立監理資訊交流分享平台，透過場外監控時須產出相關監理報告，使檢查人員取得各銀行業務監理重要資訊（如

董事會會議紀錄內容及審核結果、業務申請及審核結果、負責人與經理人異動情形、機構重要內規增修訂情形等），以利檢查前風險評估及檢查重點篩選。

（七）以個案模擬試作研討方式，訓練監理檢查人員管理評估及查核能力。檢查人員之專業訓練與一般金融人員訓練不同，除金融業務與商品專業知識外，另須具備金融機構整體營運與風險管理品質之評估能力及實務查核技巧，如欲透過訓練課程提升相關能力與技巧，個案研討與模擬試作係較佳之方式，透過金檢知識網之各業務檢查案例，提升學習成效。建議未來檢查人員訓練課程納入個案試作，提供實際銀行完整財務業及管理性資料（去識別化），模擬檢查人員至受檢機構之可能情境，以學習機構整體風險評估、檢查重點挑選、個案抽樣作業及檢查提問等實際檢查技巧。

（八）落實銀行建立資安演練機制，評估定期檢討更新網路應用程式。例如資安防駭的演練，模擬資訊系統遭駭的情況為主，以及數位證據的蒐集與封存演練、模擬遭駭後系統證據的蒐集、封存與初步分析過程等，作為提升金融機構資安人員面對駭客入侵的應變策略，以及如何具備基礎的數位鑑識能力和協調溝通能力。而所有的資安應變都會分「事前準備」以及「事後應變與鑑識」兩個階段，事前準備階段應建立資安事件通報的 SOP 與制定資安應變暨化，並做好定期的防駭演練，讓銀行業將資安應變的作法透過內部控制內化成工作流程的一部分，從平日規劃妥善的資安應變。網路銀行業務之範圍，包括一般銀行貸款及消費金融，以及投資與財富管理業務，應用程式規模龐大，目前的網銀系統通常使用 Java、.NET、PLSQL（Oracle）或 TSQL（MS SQL）開發。而金融交易背後需要複雜、費時的軟體開發週期，通常應用程式更新針對的是錯誤修正，而新功能增加是每年兩次。由於更新網路應用程式有其成本，金融業者應評估成本效益後執行，建議定期檢討是否更新網路應用程式之必要性。

（九）採行網路金融「風險為本（Risk-Based Supervision）」、「科技中立（Technology-Neutral）」及「降低監理成本」（Low Cost Supervision）之監理原則。在制定及執行監理架構與規範時，通常根據金融活動或交易本質及衍生之風

險作為基礎，但網路科技金融業務監理雖然以風險為本，但應考量以不阻礙金融科技發展為原則。所謂科技中立原則，在民法對著作權的判例上，係指隨著科技之發展，著作所附著之媒介亦隨著科技而有不同之面貌，在此意涵下，媒介中立原則可延伸「科技中立原則」，亦即引申法律不因採用不同的科技而作出不合理的豁免或要求。依科技中立原則建立監理原則，使市場參與者能在有利創新和公平競爭的環境下營運，但不會因為金融科技的快速發展，而減少對投資者或消費者的保障。另外建議政策制定單位、金融監理機構、中央銀行、財政部會，以及金融、電信、金融科技業與金融評議消費者保護機構間應維持協調機制，藉由金融機構風險內部控制自律及市場紀律可達成降低監理成本目標。

（十）銀行業應確實控管客戶整體信用風險。建議銀行業建立社群分析補強銀行信用分析不足，降低信用風險。而銀行辦理網路金融金融商品業務，應落實銀行商品銷售控管及風險管理制度，包括瞭解客戶（KYC）、審慎核給客戶額度，並確認商品與客戶承擔風險能力可適切配合，以避免產生金融消費爭議，甚至遭受到主管機關嚴厲的裁罰，影響銀行聲譽及業務之發展。

（十一）銀行業應定期衡量、監控及資訊管理系統。開發網路金融新產品或網路金融作業程序重大改變時，須辨識及評估風險，將評估過程完整紀錄，並須有法律、稽核、行銷、資訊安全、營運及主要業務人員參與。稽核的重要缺失包括風險評估欠完整、風險辨識管理技術不足、評估工具不適當；未能辨識主要風險、未聚焦於現在及未來風險、未獨立驗證；缺乏定期監控報告、內容不一致性、不易了解、未將異常事項向上呈報等均應妥善記錄。銀行應開發網路金融風險指標時，且須聚焦於最重要風險須定期驗證，董事會及高階經理人，應定期收到作業風險報告並設計妥適風險指標。

（十二）銀行業應提升資安治理的管理層級。資安不只是營運作業層面的事情，更應該與銀行業發展策略息息相關，過去風險管理委員會獨立於資安風險問題，因為資安不是經營作業要面對的風險，而是 IT 部門的職責，但從 ATM 盜領事件發生之後，銀行業風險的觀念應該要調整，資安風險其實就是整體營運的風險。

銀行業應思考將資安納入 KPI 管理指標，除量化指標的管理，應進行資安壓力測試，例如資安風險沒有獲得控管，將對銀行帶來多少損失的評估，納入內部控制的機制。至於事後資安應變與鑑識方面，由於可能會面臨金融消費訴訟，因此銀行的數位證據保存技術及鑑識機制都必須要做到可以確保相關的證據能力。因此包括訂定資安處理與數位鑑識作業程序，資安事件與鑑識分析工具及資安應變與數位鑑識工作小組都是內部控制及稽核的重點。建議董事會應要求高階管理階層定期評估網路安全控管的適當性，包括緊急網路威脅因應，以及建置可信網路安全控管基準。

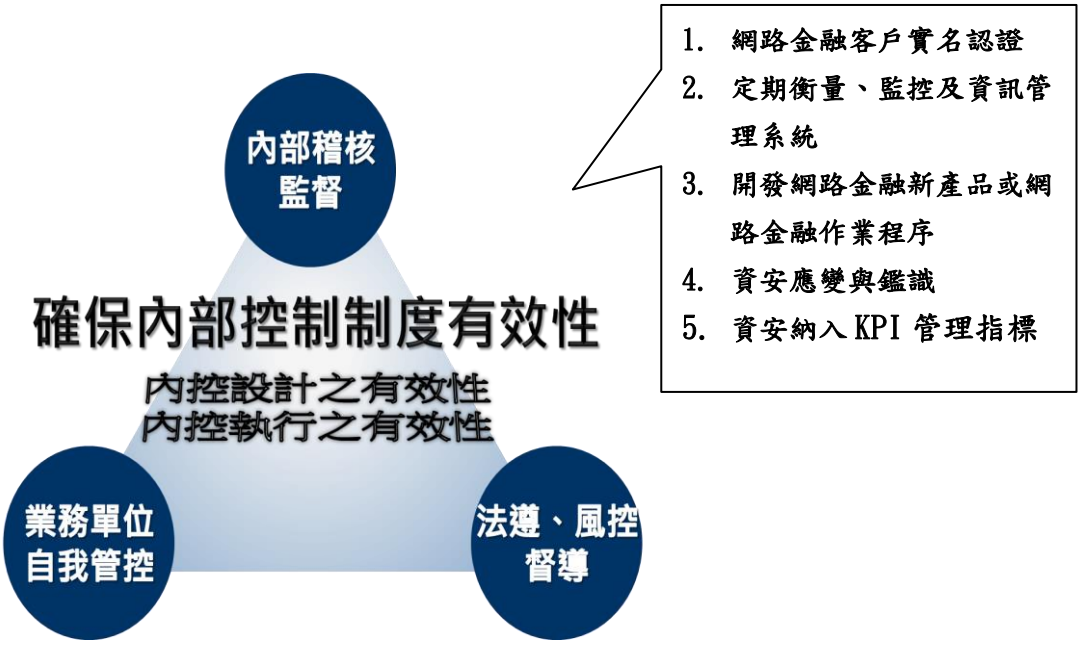


圖 5-2：網路金融內部稽核的角色

資料來源：整理自金融監督管理委員會

參考文獻

1. 王文宇，他山之石—中國台灣地區"電子支付機構管理條例草案"評析，互聯網金融法律評論第 1 期，2014 年 12 月。
2. 安怡芸，數位化金融環境 3.0 下金融監理政策規劃方向之探討，國會月刊，第 44 卷第 1 期，2016 年 1 月。
3. 台灣金融服務業聯合總會，網際網路及電子商務發展趨勢及其對金融業之影響與因應研究，2016 年 6 月。
4. 李儀坤，英美日 P2P 融資內涵與相關監理，存款保險季刊，第 29 卷第 2 期，2016 年 6 月。
5. 李儀坤，FinTech 2.0 金融結合科技，即將顛覆金融業的遊戲規則！，凱信企管，2016 年 7 月。
6. 李慧芳，英國金融科技發展及監理沙盒(Regulatory Sandbox)機制對我國的啟示，國家實驗研究院，2016 年 7 月。
7. 何啟嘉、呂桂玲，中國大陸非金融機構經營網路金融之現況、影響及監理，國際金融參考資料，第 67 輯，2014 年 12 月。
8. 林盟翔，電子支付機構金融監管之爭議問題研析，上海財經大學法學院第二屆金融法治論壇會，2015 年 10 月。
9. 姚文平，互聯網金融-即將到來的新金融時代，中信出版社，2014 年 2 月。
10. 柯瓊鳳、黃一敏，非金融機構在網路金融業務監理風險之探討-以中國大陸電子商務公司為例，兩岸金融季刊，第四卷第三期，2016 年 9 月。
11. 徐俊富，美國金融監理單位對銀行風險管理制度與措施，中央存款保險公司，2001 年 10 月。
12. 陳章正，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，行政院金融監督管理委員會銀行局委託，2006 年 5 月。
13. 郭戎晉，從國際趨勢談金融科技(FinTech)與 Bank 4.0 推動策略，財團法人

資訊工業策進會，2015 年 11 月。

14. 曾令寧、黃仁德，現代銀行監理與風險管理，台灣金融研訓院，2003 年 7 月。

15. 黃偉倫，從「金融機構辦理電子銀行業務安全控管作業基準」談網路銀行服務之安全機制，財金資訊季刊，第 68 期，2011 年 9 月。

16. 閻慶民、謝翀達、駱絜飛，銀行業金融機構資訊科技風險監管研究，中國金融出版社，2013 年 4 月

17. Douglas W. Diamond and Philip H. Dybvig, “Bank Runs, Deposit Insurance, and Liquidity”, *The Journal of Political Economy*, Vol. 91, No. 3. (Jun, 1983)

18. Douglas, J. L, New Wine into Old Bottles: FinTech Meets the Bank Regulatory World. North Carolina Banking Institute (Mar, 2016)

附錄一：專家訪談會議記錄

一、主辦單位：台灣金融研訓院金融研究所

二、舉辦時間：105 年 10 月 4 日（星期二）下午 4 時 30 分至 6 時

三、舉辦地點：台灣金融研訓院金融研究所會議室

四、訪談專家：何宗憲（台灣威睿資訊有限公司資深技術顧問）

許智偉（台灣威睿資訊有限公司業務協理）

五、出席成員：林士傑（台灣金融研訓院金融研究所副所長）

張凱君（台灣金融研訓院金融研究所副研究員）

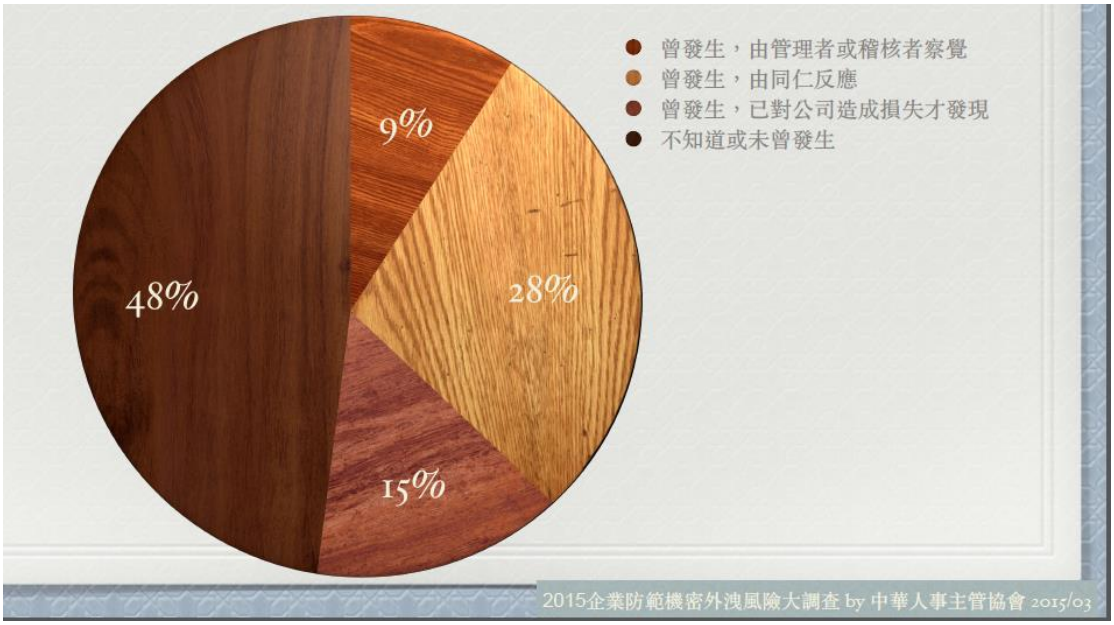
蘇秋惠（台灣金融研訓院金融研究所分析師）

李宛蓁（台灣金融研訓院金融研究所分析師）

六、會議重點：

本次會議由台灣威睿資訊有限公司針對網路資訊安全實務分享，重點觀念紀錄如下：

1. 是否發生過內部同仁竊取或洩漏機密的情況？

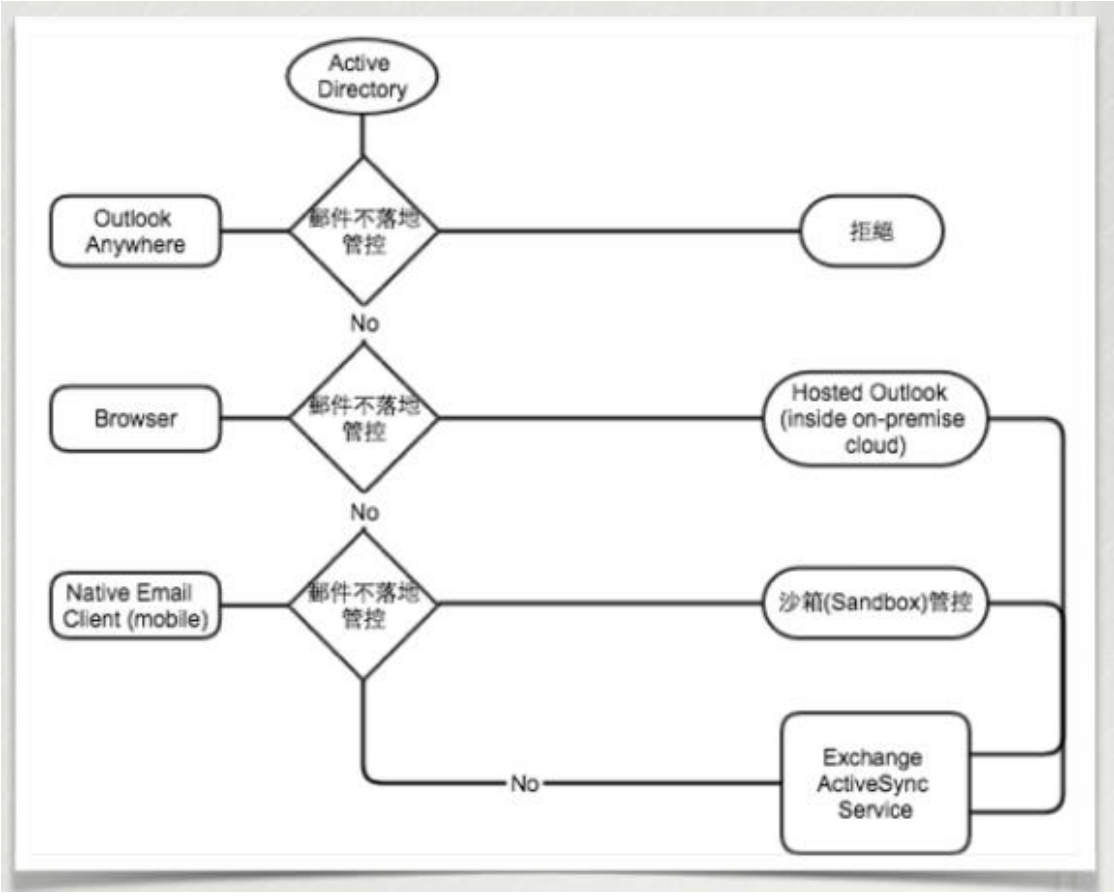


2. 可用於處理組織內部所定義的敏感性事務的行動裝置，組織都應證明有進行相關管控。

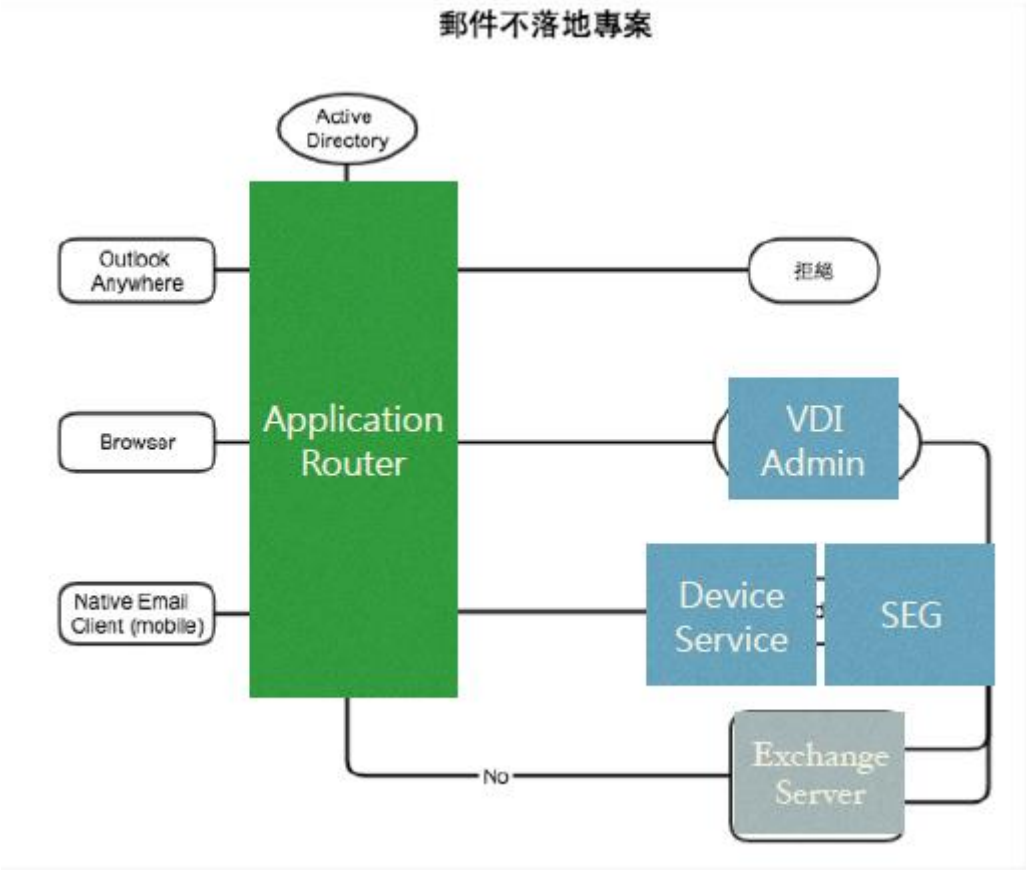
3. 為什麼郵件不落地難做？Exchange 主機信件的傳送方式：

	通訊方式	認證方式	管控瓶頸
Outlook Anywhere	RPC over HTTPs	Basic/ NTLM Authentication	Protocol複雜
Outlook Web App	HTTPs	Basic/ NTLM/ Digest/ Form-based Authentication	多瀏覽器/ 多種平台
Mobile App	ActiveSync	Basic Authentication	多個Free Mobile App 可收信

4. 推行郵件部落地最佳實踐，係以不影響員工現有的使用習慣為前提下，分階段導入並須同時考量 Outlook Anywhere、Browser、Native Email Client。



5. 客戶需求及解決方案，須依照 Client 裝置不同，與人員被管控與否，進行拒絕、Airwatch 管控、Horizon RDS(hosted Outlook)、或是直接導至 Exchange Server。



6. 建議透過 MDM，改變使用者習慣，減低被動洩密風險。透過 MCM+VDI，加強資料管控，減低主動洩密風險。可整合各家 Identity Manager 的 Application Router 進行分段導入，兼顧稽核壓力並紓解員工反彈。透過整合 Airwatch 與 Horizon，才可真正落實郵件不落地。

附錄二：金融控股公司及銀行業內部控制及稽核制度實施辦法

修訂日期：105 年 07 月 05 日

第 一 章 總則

第 1 條　本辦法依金融控股公司法第五十一條、銀行法第四十五條之一第一項、信用合作社法第二十一條第一項、票券金融管理法第四十三條及信託業法第四十二條第三項規定訂定之。

第 2 條　本辦法所稱銀行業，包括銀行機構、信用合作社、票券商及信託業。銀行業以外之金融業兼營票券業務及信託業務者，其內部控制及內部稽核制度，除其他法令另有規定外，應依本辦法辦理。

第 3 條　金融控股公司及銀行業應建立內部控制制度，並確保該制度得以持續有效執行，以健全金融控股公司（含子公司）與銀行業經營。

金融控股公司（含子公司）與銀行業應規劃整體經營策略、風險管理政策與指導準則，並擬定經營計畫、風險管理程序及執行準則。

第 4 條　內部控制之基本目的在於促進金融控股公司及銀行業健全經營，並應由其董（理）事會、管理階層及所有從業人員共同遵行，以合理確保達成下列目標：

一、營運之效果及效率。

二、報導具可靠性、及時性、透明性及符合相關規範。

三、相關法令規章之遵循。

前項第一款所稱營運之效果及效率目標，包括獲利、績效及保障資產安全等目標。

第一項第二款所稱之報導，包括金融控股公司及銀行業內部與外部財務報導及非財務報導。其中外部財務報導之目標，包括確保對外之財務報表係依照一般公認會計原則編製，交易經適當核准等目標。

第 5 條　金融控股公司及銀行業之內部控制制度，應經董（理）事會通過，如有董（理）事表示反對意見或保留意見者，應將其意見及理由於董（理）事會議紀錄載明，連同經董（理）事會通過之內部控制制度送各監察人（監事、監事會）或審計委員會；修正時，亦同。

第 二 章 內部控制制度之設計及執行

第 6 條　金融控股公司及銀行業應建立內部稽核制度、自行查核制度、法令遵循制度、以及風險管理機制，以維持有效適當之內部控制制度運作。

第 7 條　金融控股公司（含子公司）與銀行業之內部控制制度應包含下列組成要素：

一、控制環境：係金融控股公司及銀行業設計及執行內部控制制度之基礎。控制環境包括金融控股公司及銀行業之誠信與道德價值、董（理） 事會及監察人（監事、監事會）或審計委員會治理監督責任、組織結構、權責分派、人力資源政策、績效衡量及獎懲等。董事會與經理人應建立內部行為準則，包括訂定董事行為準則、員工行為準則等事項。

二、風險評估：風險評估之先決條件為確立各項目標，並與金融控股公司及銀行業不同層級單位相連結，同時需考慮金融控股公司及銀行業目標之適合性。管理階層應考量金融控股公司及銀行業外部環境與商業模式改變之影響，以及可能發生之舞弊情事。其評估結果，可協助金融控股公司及銀行業及時設計、修正及執行必要之控制作業。

三、控制作業：係指金融控股公司及銀行業依據風險評估結果，採用適當政策與程序之行動，將風險控制在可承受範圍之內。控制作業之執行應包括金融控股公司及銀行業所有層級、業務流程內之各個階段、所有科技環境等範圍、對子公司之監督與管理、適當之職務分工，且管理階層及員工不應擔任責任相衝突之工作。

四、資訊與溝通：係指金融控股公司及銀行業蒐集、產生及使用來自內部與外部之攸關、具品質之資訊，以支持內部控制其他組成要素之持續運作，並確保資訊在金融控股公司及銀行業內部與外部之間皆能進行有效溝通。內部控制制度須具備產生規劃、執行、監督等所需資訊及提供資訊需求者適時取得資訊之機制，並保有完整之財務、營運及遵循資訊。有效之內部控制制度應建立有效之溝通管道。

五、監督作業：係指金融控股公司及銀行業進行持續性評估、個別評估或兩者併行，以確定內部控制制度之各組成要素是否已經存在及持續運作。持續性評估係指不同層級營運過程中之例行評估；個別評估係由內部稽核人員、監察人（監事、監事會）或審計委員會、董事會等其他人員進行評估。對於所發現之內部控制制度缺失，應向適當層級之管理階層、董事會及監察人（監事、監事會）或審計委員會溝通，並及時改善。

第 8 條　內部控制制度應涵蓋所有營運活動，並應訂定下列適當之政策及作業程序，且應適時檢討修訂：

一、組織規程或管理章則，應包括訂定明確之組織系統、單位職掌、業務範圍與明確之授權及分層負責辦法。

二、相關業務規範及處理手冊，包括：

（一）投資準則。
（二）客戶資料保密。
（三）利害關係人交易規範。
（四）股權管理。
（五）財務報表編製流程之管理，包括適用國際財務報導準則之管理、會計專業判斷程序、會計政策與估計變動之流程等。
（六）總務、資訊、人事管理（銀行業應含輪調及休假規定）。
（七）對外資訊揭露作業管理。
（八）金融檢查報告之管理。
（九）金融消費者保護之管理。
（十）其他業務之規範及作業程序。

金融控股公司業務規範及處理手冊應另包括子公司之管理及共同行銷管理。銀行業務規範及處理手冊應另包括出納、存款、匯兌、授信、外匯、新種金融商品及委外作業管理。

信用合作社業務規範及處理手冊應另包括出納、存款、授信、匯兌及委外作業管理。

票券商業務規範及處理手冊應另包括票券、債券及新種金融商品等業務。

信託業作業手冊之範本由信託業商業同業公會訂定，其內容應區分業務作業流程、會計作業流程、電腦作業規範、人事管理制度等項。信託業應參考範本訂定作業手冊，並配合法規、業務項目、作業流程等之變更，定期修訂。

股票已在證券交易所上市或於證券商營業處所買賣之金融控股公司及銀行業，應將薪資報酬委員會運作之管理納入內部控制制度。

金融控股公司及銀行業設置審計委員會者，其內部控制制度，應包括審計委員會議事運作之管理。

金融控股公司及銀行業應於內部控制制度中，訂定對子公司必要之控制作業，其為國外子公司者，並應考量該子公司所在地政府法令之規定及實際營運之性質，督促其子公司建立內部控制制度。

前九項各種作業及管理規章之訂定、修訂或廢止，必要時應有法令遵循、內部稽核及風險管理單位等相關單位之參與。

第 三 章 內部控制制度之查核

第 一 節 內部稽核

第 9 條　內部稽核制度之目的，在於協助董（理）事會及管理階層查核及評估內部控制制度是否有效運作，並適時提供改進建議，以合理確保內部控制制度

得以持續有效實施及作為檢討修正內部控制制度之依據。

第 10 條　金融控股公司及銀行業應設立隸屬董（理）事會之內部稽核單位，以獨立超然之精神，執行稽核業務，並應至少每半年向董（理）事會及監察人（監事、監事會）或審計委員會報告稽核業務。

金融控股公司及銀行業應建立總稽核制，綜理稽核業務。總稽核應具備領導及有效督導稽核工作之能力，其資格應符合各業別負責人應具備資格條件規定，職位應等同於副總經理，且不得兼任與稽核工作有相互衝突或牽制之職務。

總稽核之聘任、解聘或調職，應經審計委員會全體成員二分之一以上同意及提董（理）事會全體董（理）事三分之二以上之同意，並報請主管機關核准後為之。

前項未經審計委員會全體成員二分之一以上同意者，應於董事會議事錄載明審計委員會之決議，未設審計委員會而設有獨立董事者，如有反對意見或保留意見，亦應於董事會議事錄載明。

內部稽核單位之人事任用、免職、升遷、獎懲、輪調及考核等，應由總稽核簽報，報經董（理）事長（主席）核定後辦理。但涉及其他管理、營業單位人事者，應事先洽商人事單位轉報總經理同意後，再行簽報董（理）事長（主席）核定。

銀行業以外之金融業兼營信託業務者，不適用本條第一項至第五項之規定。

金融控股公司總稽核得視業務需要，調動各子公司之內部稽核人員辦理金融控股公司及其子公司之內部稽核工作，並對確保金融控股公司及其子公司維持適當有效之內部稽核制度負最終之責任。

第 11 條　總稽核有下列情形之一者，主管機關得視情節之輕重，予以糾正、命其限期改善或命令金融控股公司或銀行業解除其總稽核職務：

一、有事實證明曾有從事不當授信案件或涉及嚴重違反授信原則或與客戶不當資金往來之行為。

二、濫用職權，有事實證明從事不正當之活動，或意圖為自己或第三人不法之利益，或圖謀損害所屬金融控股公司（含子公司）或銀行業之利益，而為違背其職務之行為，致生損害於所屬金融控股公司及其子公司或銀行業或第三人。

三、未經主管機關同意，對執行職務無關之人員洩漏、交付或公開金融檢查報告全部或其中任一部分內容。

四、因所屬金融控股公司（含子公司）或銀行業內部管理不善，發生重大舞弊案件，未通報主管機關。

五、對所屬金融控股公司（含子公司）或銀行業財務與業務之嚴重缺失，未於內部稽核報告揭露。

六、辦理內部稽核工作，出具不實內部稽核報告。

七、因所屬金融控股公司（含子公司）或銀行業配置之內部稽核人員顯有不足或不適任，未能發現財務及業務有嚴重缺失。

八、未配合主管機關指示事項辦理查核工作或提供相關資料。

九、其他有損害所屬金融控股公司（含子公司）或銀行業信譽或利益之行為者。

第 12 條　金融控股公司及銀行業應依據投資規模、業務情況（分支機構之多寡及其業務量）、管理需要及其他相關法令規章之規定，配置適任及適當人數之專任內部稽核人員，以超然獨立、客觀公正之立場，執行其職務，職務代理，應由內部稽核部門人員互為代理。

金融控股公司及銀行業內部稽核人員應具備下列條件：

一、具有二年以上之金融檢查經驗；或大專院校畢業、高等考試或相當於高等考試、國際內部稽核師之考試及格並具有二年以上之金融業務經驗；或具有五年以上之金融業務經驗。曾任會計師事務所查帳員、電腦公司程式設計師或系統分析師等專業人員二年以上，經施以三個月以上之金融業務及管理訓練，視同符合規定，惟其員額不得逾稽核人員總員額之三分之一。

二、最近三年內應無記過以上之不良紀錄，但其因他人違規或違法所致之連帶處分，已功過相抵者，不在此限。

三、內部稽核人員充任領隊時，應有三年以上之稽核或金融檢查經驗，或一年以上之稽核經驗及五年以上之金融業務經驗。

金融控股公司及銀行業應隨時檢查內部稽核人員有無違反前二項之規定，如有違反規定者，應於發現之日起二個月內改善，若逾期未予改善，應立即調整其職務。

第 13 條　內部稽核人員執行業務應本誠實信用原則，並不得有下列情事：

一、明知所屬金融控股公司（含子公司）或銀行業之營運活動、報導及相關法令規章遵循情況有直接損害利害關係人之情事，而予以隱飾或作不實、不當之揭露。

二、逾越稽核職權範圍以外之行為或有其他不正當情事，對於所取得之資訊，對外洩漏或為己圖利或侵害所屬金融控股公司（含子公司）或銀行業之利益。

三、因職務上之廢弛，致有損及所屬金融控股公司（含子公司）或銀行業或利害關係人之權益等情事。

四、對於以前曾服務之部門，於一年內進行稽核作業。

五、對於以前執行之業務或與自身有利害關係案件未予迴避，而辦理該等案件或業務之稽核工作。

六、直接或間接提供、承諾、要求或收受所屬金融控股公司（含子公司）或銀行業從業人員或客戶不合理禮物、款待或其他任何形式之不正當利益。

七、未配合辦理主管機關指示查核事項或提供相關資料。

八、其他違反法令規章或經主管機關規定不得為之行為。

金融控股公司及銀行業應隨時檢查內部稽核人員有無違反前項之規定，如有違反規定者，應於發現之日起一個月內調整其職務。

第 14 條　內部稽核單位應辦理下列事項：

一、規劃內部稽核之組織、編制與職掌，並編撰內部稽核工作手冊及工作底稿，其內容至少應包括對內部控制制度各項規定與業務流程進行評估，以判斷現行規定、程序是否已具有適當之內部控制，管理單位與營業單位是否切實執行內部控制及執行內部控制之效益是否合理等，並隨時提出改進意見。

二、督導業務管理單位訂定自行查核內容與程序，及各單位自行查核之執行情形。

三、擬訂年度稽核計畫，並依子公司或各單位業務風險特性及其內部稽核執行情形，訂定對子公司或各單位之查核計畫。

金融控股公司及銀行業應督促各單位（金融控股公司含子公司）辦理自行查核，並由內部稽核單位覆核各單位（金融控股公司含子公司）之內部控制制度自行查核報告，併同內部稽核單位所發現之內部控制缺失及異常事項改善情形，以作為董（理）事會、總經理、總稽核及法令遵循主管評估整體內部控制制度有效性及出具內部控制制度聲明書之依據。

第 15 條　銀行業內部稽核單位對國內營業、財務、資產保管及資訊單位每年至少應辦理一次一般查核及一次專案查核，對其他管理單位每年至少應辦理一次專案查核；對各種作業中心、國外營業單位及國外子行每年至少辦理一次一般查核；對國外辦事處之查核方式可以表報稽核替代或彈性調整實地查核頻率。

銀行業稽核單位應將營業單位辦理信託業務、財富管理及金融商品銷售業務有無不當行銷、商品內容是否充分揭露、相關風險是否充分告知、契約是否公平及其他依法令或自律規範應負之義務之執行情形，併入對營業單位之一般查核或專案查核辦理。

金融控股公司內部稽核單位每年至少應辦理一次一般業務查核；每半年至少應對金融控股公司之財務、風險管理及法令遵循辦理一次專案業務查核；另辦理一般業務查核如已涵蓋專案業務查核之項目及範圍，且查核結果無重大缺失事項並於內部稽核報告敘明者，該半年度得免辦理專案業務查

核。

內部稽核單位應將法令遵循制度之執行情形，併入對業務及管理單位之一般查核或專案查核辦理。

第 15-1 條　本國銀行得向主管機關申請核准採行風險導向內部稽核制度。主管機關得視銀行之資產規模、業務風險及其他必要情況，請本國銀行申請採行風險導向內部稽核制度。

本國銀行申請採行風險導向內部稽核制度，應符合下列條件：

一、最近一次申報自有資本與風險性資產比率，符合銀行資本適足性及資本等級管理辦法第五條之規定。

二、以最近一次金融檢查及最近一期經會計師查核簽證之財務報表為基準，均無備抵呆帳及各項準備提列不足。

三、最近一季逾期放款比率未超過百分之一。

四、已具備有效之內部控制制度，且最近一年內部控制執行無重大缺失，或缺失已具體改善。

本國銀行經採行風險導向內部稽核制度者，不適用前條第一項查核頻率之規定。

第 16 條　金融控股公司及銀行業應依子公司業務風險特性及其內部稽核執行情形，於年度稽核計畫中訂定對子公司之查核計畫。

金融控股公司及銀行業除銀行業之國外子行及其他經主管機關核准者外，其內部稽核單位應每半年對子公司之財務、風險管理及法令遵循辦理一次專案業務查核，並納入年度稽核計畫。

金融控股公司及銀行業之子公司，應向母公司呈報董（理）事會議紀錄、會計師查核報告、金融檢查機關檢查報告或其他有關資料，已設置內部稽核單位之子公司，並應將稽核計畫、內部稽核報告所提重大缺失事項及改善辦理情形併同陳報，由母公司予以審核，並督導子公司改善辦理。

金融控股公司及銀行業總稽核應定期對子公司內部稽核作業之成效加以考核，經報告董（理）事會考核結果後，將其結果送子公司董（理）事會作為人事考評之依據。

第 17 條　內部稽核單位辦理一般查核，其內部稽核報告內容應依受檢單位之性質，分別應揭露下列項目：

一、查核範圍、綜合評述、財務狀況、資本適足性、經營績效、資產品質、股權管理、董（理）事會及審計委員會議事運作之管理、法令遵循、內部控制、利害關係人交易、各項業務作業控制與內部管理、客戶資料保密管理、資訊管理、員工保密教育、消費者及投資人權益保護

措施及自行查核辦理情形，並加以評估。

二、對各單位發生重大違法、缺失或弊端之檢查意見及對失職人員之懲處建議。

三、金融檢查機關、會計師、內部稽核單位（含母公司內部稽核單位）、自行查核人員所提列檢查意見或查核缺失，及內部控制制度聲明書所列應加強辦理改善事項之未改善情形。

前項之內部稽核報告、工作底稿及相關資料應至少保存五年。

第 18 條　金融控股公司及銀行業因內部管理不善、內部控制欠佳、內部稽核制度及法令遵循制度未落實、對金融檢查機關檢查意見覆查追蹤之缺失改善辦理情形或內部稽核單位（含母公司內部稽核單位）對查核結果有隱匿未予揭露，而肇致重大弊端時，相關人員應負失職責任。內部稽核人員發現重大弊端或疏失，並使所屬金融控股公司（含子公司）或銀行業免於重大損失，應予獎勵。

金融控股公司及銀行業管理單位及營業單位發生重大缺失或弊端時，內部稽核單位應有懲處建議權，並應於內部稽核報告中充分揭露對重大缺失應負責之失職人員。

第 19 條　金融控股公司及銀行業應將內部稽核報告交付監察人(監事、監事會)或審計委員會查閱，除主管機關另有規定外，應於查核結束日起二個月內報主管機關，設有獨立董事者，應一併交付。

第 20 條　內部稽核單位之稽核人員於充任前均應分別參加主管機關認定機構所舉辦之下列訓練，並取得結業證書：

一、初任稽核人員應參加稽核人員研習班、電腦稽核研習班或票券稽核研習班六十小時以上課程，並經考試及格且取得結業證書。

二、領隊稽核人員應參加領隊稽核研習班十九小時以上課程。

三、總稽核及正副主管應參加稽核主管研習班十二小時以上課程。

內部稽核人員（含正副主管及總稽核）每年應參加主管機關認定機構所舉辦或稽核人員所屬金融控股公司（含子公司）或銀行業（含母公司）自行舉辦之金融相關業務專業訓練，其最低訓練時數，正副主管及總稽核應達二十小時以上，其餘內部稽核人員應達三十小時以上。當年度取得國際內部稽核師證照者，得抵免當年度之訓練時數。

參加主管機關認定機構所舉辦之金融相關業務專業訓練時數不得低於前項應達訓練時數二分之一。

派駐國外之稽核人員，得以參加符合當地法令規定所設立之金融專業訓練機構之訓練課程時數進行認定。

金融控股公司及銀行業應每年訂定自行查核訓練計畫，依各單位之業務性

質對於自行查核人員應持續施以適當查核訓練。

金融控股公司及銀行業應確認內部稽核人員之資格條件符合本辦法規定，該等確認文件及紀錄應留存備查。

第 21 條　金融控股公司及銀行業應將內部稽核人員之姓名及服務年資等資料，於每年一月底前依主管機關規定格式以網際網路資訊系統申報主管機關備查。

金融控股公司及銀行業依前項規定申報內部稽核人員之基本資料時，應檢查內部稽核人員是否符合第十二條第二項及第二十條規定，如有違反者，應於二個月內改善，若逾期未予改善，應立即調整其職務。

第 22 條　金融控股公司及銀行業應於每會計年度終了前將次一年度稽核計畫及每會計年度終了後二個月內將上一年度之年度稽核計畫執行情形，依主管機關規定格式以網際網路資訊系統申報主管機關備查。

金融控股公司及銀行業應於每會計年度終了前將次一年度稽核計畫以書面交付監察人（監事、監事會）或審計委員會核議，並作成紀錄，如未設審計委員會者，並應先送獨立董事表示意見。年度稽核計畫並應經董（理）事會通過；修正時，亦同。

前項提交稽核計畫內容至少應包括：計畫編列說明、年度稽核重點項目、計畫受檢單位、查核性質（一般檢查或專案檢查）、查核頻次與主管機關規定是否相符等，如查核性質屬專案檢查者，應註明專案查核範圍。

第 23 條　金融控股公司及銀行業應於每會計年度終了後五個月內將上一年度內部控制制度缺失與異常事項及其改善情形，依主管機關規定格式以網際網路資訊系統報主管機關備查。

第 24 條　銀行業具有業務或交易核准權限之各級主管，應於就任前具備下列條件之一：

一、曾擔任內部稽核單位之稽核人員實際辦理內部稽核工作一年以上者。

二、參加主管機關認定機構所舉辦之稽核人員研習班或電腦稽核研習班，經前述訓練機構考試及格且取得結業證書。

三、取得主管機關認定機構舉辦之銀行內部控制與內部稽核測驗考試合格證書，測驗內容應比照前款研習與考試內容。

國外營業單位具有業務或交易核准權限之各級主管，得參加國外專業機構舉辦之稽核專業訓練，或取得國外類似測驗證書，以取代第一項所列條件。

首次擔任國內營業單位之經理，除應符合第一項之規定外，其中符合第一

項第二款或第三款者，並應於就任前或就任後半年內參與內部稽核單位之查核實習四次以上，每次查核項目至少乙項，查核實習累計應至少查核四項以上，並應撰寫實習查核心得報告，呈報總稽核核可後，由總稽核出具證明書併同留卷備查。

外國銀行在台分行具有業務或交易核准權限之各級主管，業完成外國銀行對該分行要求之內部稽核所提供之訓練者，如其訓練課程有不低於第一項之條件，得不適用本條之規定。

第 二 節 自行查核檢查及內部控制制度聲明書

第 25 條　銀行業應建立自行查核制度。各營業、財務、資產保管、資訊單位及國外營業單位應每半年至少辦理一次一般自行查核，每月至少辦理一次專案自行查核。但已辦理一般自行查核、內部稽核單位（含母公司內部稽核單位）已辦理一般業務查核、金融檢查機關已辦理一般業務檢查或法令遵循事項自行評估之月份，該月得免辦理專案自行查核。

金融控股公司各單位及子公司每年至少須辦理一次內部控制制度自行查核，以及每半年至少須辦理一次法令遵循作業自行查核。

各單位辦理前二項之自行查核，應由該單位主管指定非原經辦人員辦理並事先保密。

第一項及第二項自行查核報告應作成工作底稿，併同自行查核報告及相關資料至少留存五年備查。

第 26 條　內部稽核單位對金融檢查機關、會計師、內部稽核單位（含母公司內部稽核單位）與內部單位自行查核所提列檢查意見或查核缺失及內部控制制度聲明書所列應加強辦理改善事項，應持續追蹤覆查，並將其追蹤考核改善情形，以書面提報董（理）事會及交付監察人（監事、監事會）或審計委員會，並列為對各單位獎懲及績效考核之重要項目。

金融控股公司及銀行業稽核工作考核要點，由主管機關定之。

第 27 條　金融控股公司及銀行業總經理應督導各單位（金融控股公司含子公司）審慎評估及檢討內部控制制度執行情形，由董（理）事長（主席）、總經理、總稽核及總機構法令遵循主管聯名出具內部控制制度聲明書（附表），並提報董（理）事會通過，於每會計年度終了後三個月內將內部控制制度聲明書內容揭露於金融控股公司及銀行業網站，並於主管機關指定網站辦理公告申報。

前項內部控制制度聲明書應依規定刊登於年報、股票公開發行說明書及公開說明書。

第一項規定對於經主管機關依法接管之銀行業，不適用之。

第 三 節 會計師對銀行業之查核

第 28 條　銀行業年度財務報表由會計師辦理查核簽證時，應委託會計師辦理內部控制制度之查核，並對銀行業申報主管機關表報資料正確性、內部控制制度及法令遵循制度執行情形、備抵呆帳提列政策之妥適性表示意見。

會計師之查核費用由銀行業與會計師自行議定，並由銀行業負擔會計師之查核費用。

第一項規定對於經主管機關依法接管之銀行業，不適用之。

第 29 條　主管機關於必要時，得邀集銀行業及其委託之會計師就前條委託辦理查核相關事宜進行討論，主管機關若發現銀行業委託之會計師有未足以勝任委託查核工作之情事者，得令銀行業更換委託查核會計師重新辦理查核工作。

第 30 條　會計師辦理第二十八條規定之查核時，若遇受查銀行業有下列情況應立即通報主管機關：

一、查核過程中，未提供會計師所需要之報表、憑證、帳冊及會議紀錄或對會計師之詢問事項拒絕提出說明，或受其他客觀環境限制，致使會計師無法繼續辦理查核工作。

二、在會計或其他紀錄有虛偽、造假或缺漏，情節重大者。

三、資產不足以抵償負債或財務狀況顯著惡化。

四、有證據顯示交易對淨資產有重大減損之虞。

受查銀行業有前項第二款至第四款情事者，會計師並應就查核結果先行向主管機關提出摘要報告。

第 31 條　銀行業委託會計師辦理第二十八條規定之查核，應於每年四月底前出具上一年度會計師查核報告報主管機關備查，其查核報告至少應說明查核之範圍、依據、查核程序及查核結果。

信用合作社依前項規定辦理時，應由直轄市政府財政局或縣(市)政府申報轉呈。

主管機關對於查核報告之內容提出詢問時，會計師應詳實提供相關資料與說明。

第 四 節 法令遵循制度

第 32 條　金融控股公司及銀行業應設立一隸屬於總經理之法令遵循單位，負責法令遵循制度之規劃、管理及執行，並指派高階主管一人擔任總機構法令遵循主管，綜理法令遵循事務，至少每半年向董（理）事會及監察人（監事、監事會）或審計委員會報告。

金融控股公司及銀行業之總機構法令遵循主管除兼任法務單位主管外，不得兼任

內部其他職務。但主管機關對信用合作社及票券金融公司另有規定者，不在此限。

金融控股公司及銀行機構之總機構法令遵循主管，職位應等同於副總經理，資格應分別符合「金融控股公司發起人負責人應具備資格條件負責人兼職限制及應遵行事項準則」及「銀行負責人應具備資格條件兼職限制及應遵行事項準則」規定。

金融控股公司及銀行業總機構、國內外營業單位、資訊單位、財務保管單位及其他管理單位應指派人員擔任法令遵循主管，負責執行法令遵循事宜。

金融控股公司及銀行業總機構法令遵循主管、法令遵循單位所屬人員，每年應至少參加主管機關認定機構所舉辦或所屬金融控股公司（含子公司）或銀行業（含母公司）自行舉辦十五小時之教育訓練，訓練內容應至少包含新修正法令、新種業務或新種金融商品。

金融控股公司及銀行業應以網際網路資訊系統向主管機關申報總機構法令遵循主管、法令遵循單位所屬人員之名單及受訓資料。

第 33 條　金融控股公司及銀行業總、分支機構對法令規章遵循事宜，應建立諮詢溝通管道，以有效傳達法令規章，俾使職員對於法令規章之疑義得以迅速釐清，並落實法令遵循。

金融控股公司及銀行業法令遵循單位對各單位就法令遵循重大缺失或弊端，應分析原因及提出改善建議，簽報總經理後，提報董（理）事會。

第 34 條　法令遵循單位應辦理下列事項：

一、建立清楚適當之法令規章傳達、諮詢、協調與溝通系統。

二、確認各項作業及管理規章均配合相關法規適時更新，使各項營運活動符合法令規定。

三、於銀行業推出各項新商品、服務及向主管機關申請開辦新種業務前，法令遵循主管應出具符合法令及內部規範之意見並簽署負責。

四、訂定法令遵循之評估內容與程序，及督導各單位定期自行評估執行情形，並對各單位法令遵循自行評估作業成效加以考核，經簽報總經理後，作為單位考評之參考依據。

五、對各單位人員施以適當合宜之法規訓練。

內部稽核單位得自行訂定所屬單位法令遵循之評估內容與程序，及自行評估所屬單位法令遵循執行情形，不適用前項第四款規定。

銀行業設有國外分支機構者，法令遵循單位應督導國外分支機構遵守其所在地國家之法令。

金融控股公司及銀行業法令遵循自行評估作業，每半年至少須辦理一次，其辦理結果應送法令遵循單位備查。各單位辦理自行評估作業，應由該單位主管指定專人辦理。

前項自行評估工作底稿及資料應至少保存五年。

第 五 節 風險管理機制

第 35 條　金融控股公司及銀行業應訂定適當之風險管理政策與程序，建立獨立有效風險管理機制，以評估及監督整體風險承擔能力、已承受風險現況、決定風險因應策略及風險管理程序遵循情形。

前項風險管理政策與程序應經董（理）事會通過並適時檢討修訂。

第 36 條　金融控股公司及銀行業應設置獨立之專責風險控管單位，並定期向董（理）事會提出風險控管報告，若發現重大暴險，危及財務或業務狀況或法令遵循者，應立即採取適當措施並向董（理）事會報告。

前項獨立專責風險控管單位之設置，信用合作社得指定一總社管理單位替代。

第 37 條　金融控股公司之風險控管機制應包括下列事項：

一、依金融控股公司及其子公司業務規模、信用風險、市場風險與作業風險狀況及未來營運趨勢，監控金融控股公司及其子公司資本適足性。

二、訂定適當之長短期資金調度原則及管理規範，建立衡量及監控金融控股公司及其子公司流動性部位之管理機制，以衡量、監督、控管金融控股公司及其子公司之流動性風險。

三、訂定金融控股公司及其子公司整體性之防制洗錢與打擊資助恐怖主義計畫，包括以防制洗錢與打擊資助恐怖主義為目的之集團內資訊分享政策與程序。

四、考量金融控股公司整體暴險、自有資本及負債特性進行各項投資配置，建立各項投資風險之管理。

五、建立金融控股公司及其各子公司一致性資產品質及分類之評估方法，計算及控管金融控股公司及其子公司之大額暴險，並定期檢視，覈實提列備抵損失或準備。

六、對金融控股公司與其子公司及各子公司間業務或交易、資訊交互運用等建立資訊安全防護機制及緊急應變計畫。

第 38 條　銀行業之風險控管機制應包括下列原則：

一、應依其業務規模、信用風險、市場風險與作業風險狀況及未來營運趨勢，監控資本適足性。

二、應建立衡量及監控流動性部位之管理機制，以衡量、監督、控管流動性風險

三、應建立辨識、衡量與監控洗錢及資助恐怖主義風險之管理機制，及遵循防制洗錢相關法令之標準作業程序，以降低其洗錢及資助恐怖主義風險。

四、應考量整體暴險、自有資本及負債特性進行各項資產配置，建立各項業務風險之管理。

五、應建立資產品質及分類之評估方法，計算及控管大額暴險，並定期檢視，覈實提列備抵損失。

六、應對業務或交易、資訊交互運用等建立資訊安全防護機制及緊急應變計畫

第 四 章 附則

第 39 條　金融控股公司及銀行業應確保金融檢查報告之機密性，其負責人或職員除依法令或經主管機關同意者外，不得閱覽或對執行職務無關之人員洩漏、交付或公開與金融檢查報告全部或部分內容。

金融控股公司及銀行業應依主管機關之規定，制定金融檢查報告之相關內部管理規範及作業程序，並提報董（理）事會通過。

第 40 條　金融控股公司及銀行業應於內部控制制度中訂定經理人及相關人員違反本辦法或其所訂內部控制制度規定時之處罰。

第 41 條　本辦法所稱金融控股公司之子公司，應依金融控股公司法第四條規定認定；銀行業之子公司應依公開發行公司建立內部控制制度處理準則第五條第三項規定認定。

第 42 條　內部稽核人員及法令遵循主管，對內部控制重大缺失或違法違規情事所提改進建議不為管理階層採納，將肇致所屬金融控股公司（含子公司）或銀行業重大損失者，均應立即作成報告陳核，並通知獨立董事及監察人（監事、監事會）或審計委員會，同時通報主管機關。

第 43 條　本辦法規定格式，由主管機關另定之。

第 44 條　信用合作社依本辦法規定向主管機關申報相關資料時，應另陳報直轄市政府財政局或縣（市）政府。

第 45 條　外國銀行在台分行應依本辦法之規定辦理。但外國銀行在台分行之內部控制及稽核制度，如依其總行所訂之相關內部控制及稽核制度規定，有不低於本辦法之規定者，得由外國銀行在台分行提出總行制度之詳細說明與我國制度之對照說明，經在台分行負責人簽署後，報經主管機關備查，依該制度辦理。

外國銀行在台分行之總行對於其內部控制及稽核制度如有任何變更適用於在台分行者，應於變更後即刻提出對照說明，並經在台分行負責人簽署後，報經主管機關備查。

外國銀行在台分行違反主管機關依前二項規定認可之內部控制及稽核制度，視同違反本辦法規定。

第 46 條　金融控股公司或銀行業不符本辦法第三十二條、第三十四條第一項第三款、第四款規定者，應自中華民國一○三年八月八日本辦法修正發布之日起六個月內，調整至符合規定。

第 47 條　本辦法自發布日施行。

中華民國一百零一年三月二日修正條文，除第八條第一項第二款第五目修正條文，信用合作社自一百零三年一月一日施行，及第八條第一項第二款第八目修正條文自一百年十二月三十日施行外，自發布後三個月施行。

附錄三：銀行業建立風險導向內部稽核制度實務守則

金融監督管理委員會 105 年 7 月 8 日
金管檢制字第 1050150241 號函准予備查

(依據)

一、 本實務守則係依據金融監督管理委員會 105 年 7 月 8 日金管檢制字第 10501502370 號令辦理。

(目的)

二、 銀行業實施風險導向內部稽核制度，係透過風險評估之方法，審慎評估稽核範疇內各個受查主體之風險，並依據評估結果決定稽核任務之查核重點、範圍、方法、稽核程序及查核頻率，將稽核資源做最有效的配置，聚焦於重要風險並加強查核深度，提升內部稽核執行效益，以有效協助銀行業完善內部控制制度及強健企業體質。

(風險導向內部稽核制度實施方法)

三、 為確保內部稽核之品質與有效性，銀行業實施風險導向內部稽核制度，應具備明確之內部控制三道防線架構，並建立以下機制：

(一)內部稽核風險評估之程序與方法。

(二)內部稽核品質評核機制。

(訂定風險評估程序)

四、 內部稽核應建立風險評估之程序與方法，以辨識並評估各受查主體所面臨之風險。

五、 確認風險評估範圍：

內部稽核應依據銀行業所經營業務範圍及單位組織，以及主管機關法令規範，辨識應辦理風險評估之受查主體，以確保風險評估範圍能完整涵蓋銀行業整體營運範疇。

內部稽核得以單位組織、產品、業務、作業流程或其他構面訂定受查主體

六、 風險評估因子與方法：

(一)內部稽核應就各受查主體所面臨之固有風險、控制措施有效性進行評估後，確認受查主體之風險評估結果(即剩餘風險)，並據以決定年度稽核計畫。

所稱固有風險、控制措施與剩餘風險定義如下：

1.固有風險：在管理階層尚未採取任何行動來改變風險發生的可能性或其影響之情況下，達成目標之風險。

2.控制措施：管理階層為管理風險及增加達成既定目標之可能性，而採取之任何行動。管理階層負責規劃、組織及指揮執行

足夠之行動，以合理保證目的及目標之達成。

3.剩餘風險：管理階層在設計及執行控制措施後，仍留下來無法達成組織目標之風險。

(二)固有風險之評量：

1.內部稽核應依據所屬銀行業之經營形態與發展策略目標，擬訂適合之固有風險評估因子。

風險評估因子之訂定可參酌 Basel Committee 所列舉之主要風險類型，並應描述評估各風險類型時應考量之因素(所述因素應能顯著代表各風險之表徵)。

2.依前項有關之固有風險因子，就受查主體發生風險事項之可能性與嚴重程度評估其固有風險：

(1)發生可能性：評估風險事件在可預期的未來中發生之可能性。

(2)嚴重程度：評估風險事件發生對財務、商譽及營運服務可能造成之影響。

(3)依據前二項構面評估固有風險，評估結果至少應區分為高、中、低等三個風險等級。

(三)控制措施有效性之評量：

1.以持續或個別評估的方式確認各受查主體之控制措施是否存在且發揮功效，並就控制措施設計及執行之有效性至少區分為高、中、低三個等級。

2.控制措施有效性評估至少應包含下列資訊：

(1)主要業務之內部控制運作情形。

(2)外部檢查意見，包含主管機關、會計師、母公司稽核單位及其他外部檢查。

(3)內部檢查意見，包含內部稽核、二道防線遵循測試、自行查核及內部控制制度聲明書所列應加強辦理改善事項。

(4)主管機關裁罰及重大風險事件之發生及處理。

(5)缺失追蹤改善及重覆發生情形。

3.運用前項評估資訊時，應考量相關資料之時效性。

(四)風險評估結果(剩餘風險)：

1.內部稽核單位依據固有風險及控制措施有效性之評估結果(即固有風險經執行控制措施後之剩餘風險)，確認各受查主體之綜合風險評估最終結果，並至少區分為高、中、低三個等級。

2.內部稽核應訂定受查主體之綜合風險評估結果與查核頻率連結之標

準，就風險等級為高者，應至少每年執行一次或一次以上查核；就風險等級為低者，至少每四年執行一次查核。

(五)內部稽核辦理風險評估，應考量主要利益關係人(Stake holder)對銀行業可能面臨之重大及潛在風險之意見，包含主管機關、董(理)事會及審計委員會、高階管理階層、風險管理與法令遵循單位等。

七、 內部稽核應依據其所訂定之評估方法，每年至少執行一次風險評估。執行風險評估時應指定合適之稽核人員辦理，並指派資深稽核人員覆核其評估結果後，呈總稽核核准。

八、 內部稽核所訂定之風險評估程序與方法，以書面交付監察人(監事、監事會)或審計委員會核議，並作成紀錄，未設審計委員會者，應先送獨立董事表示意見。風險評估程序與方法並應經董(理)事會通過；修正時，亦同

九、 內部稽核辦理風險評估應留存記錄並至少保存五年，包含確認風險評估範圍與受查主體、辨識與評量風險、訂定稽核計畫等過程，以及有關核准記錄。

(訂定內部稽核計畫)

十、 內部稽核應依據風險評估結果進行年度稽核計畫之規劃，包含受查主體、頻率、範圍及查核方式，並另依據主管機關其他個別指定事項，彙總訂定年度稽核計畫。

十一、受查主體若有主管機關要求年度辦理之查核範圍，則無論風險評估結果所對應之查核頻率為何，均應依主管機關要求納入年度稽核計畫。

十二、內部稽核應於年度稽核計畫擬訂完成後，檢附年度稽核計畫及風險評估結果，呈總稽核就主管機關監理重點及銀行業經營策略目標，審閱整體年度稽核計畫與風險評估結果之妥適性，並做必要之調整。

十三、年度稽核計畫應併同內部稽核單位風險評估結果以書面交付監察人(監事、監事會)或審計委員會核議，並作成紀錄，未設審計委員會者，應先送獨立董事表示意見。年度稽核計畫並應經董(理)事會通過；修正時，亦同。

(定期檢視風險評估結果與內部稽核計畫)

十四、內部稽核應定期就整體外部環境或內部業務發展變化檢視風險評估結果，以即時反應受查主體之風險，並據以決定是否修訂年度稽核計畫。

十五、內部稽核應依據其所制定之風險評估方法，持續蒐集內、外部監控資訊，如：國內、外主管機關監理重點與重要法令及金融環境變化、經營策略目標與重要政策變化、業務營運管理資訊與重要監控指標、主要利益關係人意見，以及重大風險事件發生情形等，俾確保風險評估過程能充分考量內、外部環境風險變化。

(內部稽核品質評核機制)

十六、內部稽核應訂定品質評核機制，以定期確認內部稽核業務執行是否確實遵循有關內部稽核制度與程序，並符合主管機關法令規範。

十七、內部稽核品質評核內容應涵蓋下列項目：

(一)稽核策略與目標之訂定與執行。

(二)稽核制度及程序之設計與運作。

(三)組織編制與稽核資源配置。

(四)人員專業之適足性及持續訓練。

(五)稽核方法與工具之持續精進與研發。

(六)對主管機關法令規範遵循情形。

(七)前次品質評核應改善事項。

十八、內部稽核辦理品質評核，得採內部自我評核或外部機構評核方式辦理：

(一)評核方式：

1.內部自我評核：由內部稽核單位指定人員，每年度至少辦理一次自我評核，負責辦理評核人員應不得檢查自身經辦之業務，內部稽核單位並應至少每五年委請外部機構驗證其評核結果。

2.外部機構評核：由內部稽核單位委請外部機構辦理評核，應至少每五年辦理一次。

(二)內部稽核單位委請負責辦理驗證或評核之外部機構，不得為其財務簽證會計師。

(三)內部稽核應就所採行之評核方式，及外部機構之資格與獨立性，以書面交付監察人(監事、監事會)或審計委員會核議，未設審計委員會者，應送獨立董事。評核方式及選定之外部機構應經董(理)事會通過。

前項各款所稱之外部機構，由中華民國銀行商業同業公會全國聯合會認定之。

十九、內部稽核應依據評核結果，就可能影響內部稽核整體運作事項擬訂改善計畫，總稽核應負責督導改善計畫之確實執行。

內部稽核品質評核結果與改善計畫應以書面交付監察人(監事、監事會)或審計委員會，未設審計委員會者，應送獨立董事。內部稽核品質評核結果與改善計畫並應提報董(理)事會備查。

(本實務守則修訂核准層級)

二十、本實務守則經本會理事會通過，並報金融監督管理委員會備查後施行；修正時，亦同。

附錄四：風險導向稽核相關注意事項

資料來源：安侯建業企管顧問公司、資誠企管顧問公司

一、風險導向稽核檢查流程

(一)傳統檢查方式與風險導向檢查之比較：

傳統檢查程序僅依受檢銀行之檢查頻率，在實地檢查期限前挑選某一特定檢查基準日，採用突擊檢查方式辦理檢查，查核重點多為驗證機構資產負債表及損益表內容、法令遵循情形及重要交易抽查，查核完畢後到下一次實地檢查前，除特殊情況須辦理專案查核及每季針對受檢機構申報監理資訊(Call Report)辦理場外分析外，不會再針對該機構執行相關監理或檢查作業，亦無相關監理或檢查文件之產出。

(二)風險導向監理檢查機制之導入：

(1)採用新機制之目的：透過評估機構風險管理與內部控制健全性，及早發現金融機構潛在營運風險，再透過實地檢查以確認管理面弱點是否確實存在，而非僅點出機構目前的問題。

(2)新機制的運作原則：

①要求機構建立完善三道防線(包括營業單位自我控管、風管與法遵之監控、內部稽核之檢核)，使其能有效自我管理，而非以實地檢查取代三道防線之功能。

②建立早期預警系統，以反應潛在風險。

③採行持續監理檢查機制，對小型機構至少每季與機構管理階層進行會談瞭解營運現況，大型機構則持續辦理專案檢查。

④針對個別機構設計監理計畫，將主要監理資源投注於大型及高風險機構。

⑤設計一系列監理檢查工作底稿，完整留存監理檢查過程與結論，惟為避免造成監理資源之不足，須先有效篩選檢查重點，並利用多層次查核程序以降低抽查案件之必要性。

(三)風險導向檢查流程

1.蒐集機構資料並進行整體概況瞭解（產出「機構概況」）。

2.評估機構各類風險規模及風險管理品質，確認主要潛在風險（產出「風險矩陣及風險評估」）。

3.研擬須採行之監理與檢查作業（產出「監理計畫及檢查計畫」）。

4.研擬檢查作業內容（產出「檢查範圍備忘錄」）。

5.決定實地檢查須提供資料（產出「檢查通知信函」）。

6.執行實地檢查（填寫各類檢查模組工作底稿）。

7.撰寫檢查結果（產出「檢查報告」、「彙整文件(Summary Documents)」、「美國營運信函(US Operations Letters)」、「與董事會及經營階層會談紀錄」）。

8.辦理場外監理作業（更新「風險導向文件」、「監理與監控報告」、「與管理階層會談紀錄」）。

(四)信用等 6 大固有風險(Inherent Risk)種類之定義及不同風險程度之說明：將特定業務固有風險程度區分為高、中、低三級，其定義為 –

1.高固有風險：特定營業活動之暴險部位相較於該機構之整體規模及同業水準屬較大者，或交易量較大，或業務複雜度較其它業務為高，以致該業務易造成機構顯著損失或重大影響者。

2.中固有風險：特定營業活動之暴險部位相較於該機構之整體規模及同業水準屬平均水準，或交易量屬平均水準，業務性質屬傳統型，業務所造成之損失可由機構於日常營運中自行吸收。

3.低固有風險：依特定營業活動之暴險部位、交易量、業務性質判斷，即使該業務之內部控制有弱點，發生損失機率很低，或即使發生損失，對機構影響很低。

(五)風險管理之內涵與不同管理品質之說明：

1.評估機構風險管理能力時，品質以強、可及弱三級表示，須檢視下列四大項目：董事會與高階管理人員之積極監督、適足的管理政策與作業規範、適足的風險管理、監控及管理資訊系統、完整的內部控制與內部稽核制度。

3 級品質之定義為：

(1)強健：管理階層能有效辨識及控制所有主要風險；董事會及管理階層均積極參與風險管理作業且確保有適足的管理政策與作業規範;針對各項風險限額建置妥適監控、陳報及資訊管理機制；內部控制與內部稽核機制能配合業務及機構營運概況；以例外方式承作之案例很少且不致對機構造成損害。

(2)尚可：風險管理雖某些部分仍有欠缺，惟系統尚稱有效，能因應現有業務暴險及業務計畫之相關管理作業，管理階層對相關輕微管理弱點已能瞭解並予以因應，整體而研董事會及管理階層之監督、管理政策與作業規範、風險監控及資訊管理機制尚能有效運作，風險控制情形尚無須監理機關加強注意。

(3)弱：風險管理雖在某些重要部分有嚴重缺失，須要監理機關特別注意。內控機制可能有重大問題，例如持續有例外事件發生，相關缺失可能影響機構健全營運或導致財務報告無法正確表達，須採取積極導正措施。

此評估結果在分析三道防線加董事會與高階人員監督的整體管理架構、廣度及深度是否妥適，以評估機構內部控制與風險管理是否健全，以及可能造成未來損失之潛在風險所在，再配合重點項目之交易測試，以確認實際情形。

為有效評估機構風險管理能力，監理檢查人員須對各類型機構應具備之各類風險管理能力與管理運作方式有相當之認知，方可適當呈現不足之面向與內容，故此機制得以有效施行，首重建立監理檢查人員風險管理知能，以及對業者最佳運作

(Best Practices)之瞭解。

2.在判斷銀行風險管理能力時，對四大項目之評估重點如下：

(1)董事會及高階管理階層之積極監督

①董事會及高階管理階層對各類風險是否具專業知能，且能持續知悉機構暴險狀況、風險管理運作情形及業務動態。

②董事會是否訂定並定期檢視機構從事授信、投資、交易、信託及其他業務之風險管理政策及限額。

③董事會及管理階層是否透過正式陳報機制，充分瞭解機構主要暴險及其來源。

④董事會是否配合營運策略之調整，定期檢視及核准風險限額。

⑤管理階層是否就機構業務性質，聘僱適量具相當經驗、專業及品格之人員。

⑥各階層管理人員是否確實就機構日常營運採取適當監督。

⑦管理階層是否就外在環境改變有所因應。

⑧在從事新業務或新產品前，管理階層是否能辨識衍生之風險，並確保已建置相關風險管理及內部控制機制。

(2)妥適之政策、作業程序及限額

①機構之風險管理政策、作業程序及限額，是否足以對業務衍生之風險，進行適當之辨識、衡量、監督及控制。

②政策、作業程序及限額，是否與管理階層之經驗、金融機構之營運目標及財務能力相符。

③政策須能明確就機構所有業務之分層負責予以規範。

④新業務營運前須透過政策訂定以確保機構已建置相關風險辨識、監督及控制機制。

(3)適足的風險監督及管理資訊系統

①機構之風險監控及陳報機制應涵蓋所有重大風險。

②衡量風險之主要假設、資料來源及作業程序是否妥適、文件化、且經測試其可靠性。

③風險陳報機制須配合機構業務性質，並能比較預期及實際績效之差異。

④呈報董事會及管理階層之報告，須正確及時，且使決策者能夠辨識不利趨勢及妥適評估金融機構所面臨之風險。

(4)適當的內部控制及內部稽核

①須配合機構業務性質及風險態樣，建立適當內部控制制度。

②組織結構須建立明確分層負責機制，以有效監督政策、作業程序及限額之執行情形。

③內控的陳報系統須獨立於業務部門以外，且業務應有適當的牽制分工。

④機構之組織架構須真實反映營運情形。

⑤財務、營運及主管機關規定之報表，須可靠、正確及時，例外事件須註記並立即調查。

⑥是否有適當作業程序，以確保遵循法律及相關規定。

⑦內部稽核及內控檢視機制，須獨立客觀。

⑧內部控制及資訊系統須經妥適測試及檢視；對於稽核範圍、作業程序、稽核發現、改善回覆及檢驗測試等須適當文件化；及時注意重大缺失事項；管理階層對重大缺失之改善情形，須客觀驗證及檢視。

⑨稽核委員會及董事會須定期檢視稽核及內控有效性。

3.將 6 大固有風險之風險程度及風險管理品質評估結果分別填入二維矩陣後，即可得出其淨剩餘風險程度，另參考以往評估結果，可決定該風險之趨勢(增加、穩定或下降)，依據淨剩餘風險及趨勢的程度，決定該業務或作業是否納入檢查範圍。

二、檢查作業文件化項目

依據場外風險評估所得出的各種假設，決定實地檢查之範圍與項目，以進行實地驗證機構的風險水準，實地檢查作業之主要方式則包括抽查交易案件、評估風險模組、觀察實際營運及管理運作方式、與董事會、管理層級及作業層級人員面談、財務結果分析及風險管理品質分析。

介紹檢查流程中監理與檢查人員須完成之各類文件，包括-

(一)金融機構整體分析(Institutional Overview)

1.整體分析報告之內容包括：

(1)整體概況彙總：最近一次檢查等結果、場外評等結果、重要業務及風險管理變化與進展、重要組織架構或人員異動。

(2)風險概況：整體機構風險評估等級、趨勢及風險管理品質評估等級結果與理由，最近監理作業或實地檢查所發現主要風險管理問題。

(3)財務狀況分析：包括資產負債、獲利能力及資本適足性。

(4)重要財務指標之當年度預測值及前一年度數值比較。

(5)組織架構。

(6)主要業務與商品、新業務與商品、營運策略及市場競爭狀況。

(7)公司治理，包括董事結構、高階管理人員品質、管理資訊陳報機制、股東結構、市場指標反應。

(8)內部及外部稽核品質與結果。

(9)所處地區經濟狀況。

(10)未來展望及已採取監理措施。

2.相關所須資訊之來源包括：

(1)內部資訊：檢查報告、工作底稿、缺失回覆改善、與機構日常聯繫結果備忘錄、與機構管理人員會談紀錄(內外部經濟與市場狀況、機構營運狀況及未來發展)、預警及監控資料、監理報告、監理資訊系統、機構提供之業務營運分析報告等。

(2)外部資訊：評等機構報告、投資公司分析報告、報章、雜誌及產業期刊、經濟及會計研究資料及網路及報紙來源等。

(二)風險評估(Risk Assessment)

1.綜合風險評等：將 6 大固有風險之風險程度與風險管理品質評估結果，以及風險趨勢以風險矩陣完整表達後，彙總給予該機構一個綜合風險等級，並摘要說明理由。

2.機構主要風險問題。

3.信用風險：從信用組合、授信覆審、授信政策、損失準備提列、管理資訊系統、風險監控等項目說明風險程度及管理品質。

4.市場風險：從模組、資產負債管理委員會、風險監控等層面說明。

5.流動性風險：從整體風險管理、暴險部位、投資組合管理、風險監控等層面說明。

6.法律風險：從法令遵循、訴訟情形、風險監控等層面說明。

7.整體財務狀況分析。

8.第二道及第三道防線功能：分析風管、法遵及內稽的運作情形。

(三)監理計畫(Supervisory Plan)

1,每季規劃監理作業。

2.監理文件化要求。

3.監理目標及應執行作業。

4.所須監理資源。

(四)檢查計畫(Examination Program)

1.未來一年規劃實地檢查計畫：包括執行時間、檢查範圍、領隊、助檢人數及查核時間。

2.各次實地檢查之規劃情形與應注意事項。

(五)檢查範圍備忘錄(Scope Memorandum)：包括檢查目標、檢查流程摘要(董事會監督之查核重點等)、檢查結果之呈現方式、檢查人力之規劃。

(六)檢查通知信函(Entry Letter)

(七)重要檢查項目模組(Examination Modules)：包括工作計畫(Work Program)及三層檢查流程底稿(包括第一層之核心分析(Core Analysis)、第二層之擴大分析

(Expanded Analysis)、第三層之衝擊分析(Impact Analysis)。

(八)檢查報告(Reporting and Findings)

三、信用風險之風險評估與檢查技巧

(一)評估信用風險程度的流程：包括 3 個步驟：

1.定義風險內容：透過定義畫定應評估的範圍與事項，且以前瞻性（Forward Looking，如審核中放款、新貸放款、營運計劃所規劃新增業務及已推出之新產品等）及回顧性（Backward Looking，如逾期放款、轉銷呆帳、不良放款及投資組合等先前業務決策已產生的結果）。

2.找出風險的來源：可能來源包括業務活動（包括投資組合、產品組成、新產品、銷售通路、目標市場等）、營運策略（包括目標市場、購併、集中度及證券化業務等）、外在環境（包括經濟環境、產業狀況、市場競爭狀況、法規改變、技術進步等）。相關資訊可自機構內部管理性報告(投資組合分析、不良放款分析及收益分析等)、策略計畫、政策及作業規範及與管理階層會談等管道取得。

3.量化風險的程度：須考慮之因素包括

(1)信用組合：不同風險態樣之信用資產的比率及規模，如商業不動產放款、工商放款、房貸、汽車貸款等；各資產成長情形；申請獲准比率等。

(2)信用品質：問題資產之規模與趨勢（包括不良放款、逾期放款、問題資產、損失、加權平均風險評等、備抵呆帳的金額及趨勢）；放款業務量成長趨勢（包括表外融資業務、投資、付款、清算交割等業務）；借戶及交易對手之信用品質及及趨勢；放款定價、投資組合分析、損失預測及壓力測試；放款覆審及內部稽核之評等趨勢等。

(3)核貸品質：核貸標準的變化（包括信用評分、槓桿融資程度、政策、價格、期限、擔保品、保證、承諾及結構等）；借戶履約能力（依利息保障倍數、債務所得比率及信用紀錄進行評估）；例外案件數量及程度等。

(4)所須資訊之來源包括政策與規範、管理性報表(逾期報表、新貸放案件報表、審核中案件報表及問題放款報保)、相關委員會會議紀錄、與管理階層會談結果。

(5)評估風險程度可使用的量化指標：暴險額、問題資產規模與比率、投資等級資產與非投資等級資產比率、投資組合之加權平均風險等級、預期損失、歷史損失、例外案件比率等。

(二)高信用風險程度之特徵：

1.目前或未來暴險之損失對盈餘或資本有重大影響。

2.信用暴險反映出核貸或行銷作業很積極。

3.例外放款或違反核貸標準案件數量眾多。

4.信用暴險集中非投資等級放款，且借戶集中於波動較大之市場或產業。

5.信用暴險顯示放款高度集中。

6.因經濟、產業、競爭、法規及技術之惡化，將造成重大損失。

7.報酬與承受之風險不相當。

8.特定商品或產業之放款有高度成長。

9.問題放款量相較於資本偏高，需很長時間方能處理。

10.授信損失將嚴重降低現有備抵呆帳，導致大部分盈餘須用以提列備抵呆帳。

(三)信用風險管理品質之評估

1.董事會及高階管理階層之監督：包括僱用適當的高階管理人員；建立風險容忍度（Risk Tolerance）；決定機構策略計畫；機構之預算；建立獲利計畫及核准政策及規範等。

2.政策、作業程序及限額：包括信用風險政策須與銀行整體策略方向及風險容忍度限額一致；適當授信文化（credit culture）以平衡信用品質及市場行銷；授審作業之架構必須有效，並有妥適分層負責機制；對於政策、核貸標準、例外事項之記載及核准須有合理規範；定期審視風險限額及部位；信用政策須經董事會或適當的委員會核可；政策、作業程序及限額須有有效陳報管道。

3.衡量、監督及管理資訊系統：信用組合管理，有效辨識、衡量、監控信用結構及集中風險；信用組合壓力測試、信用評等定期更新、行為評等作業；定期辦理信用分析及履約情形監控；內部評等程序須正確、及時並適當紀錄；授信前後台作業系統須有效支援授信業務運作；管理報表須及時、正確且有用；資料正確性（須有確認、保護及驗證資料正確性之作業程序）。

4.內部控制及獨立驗證：

(1)授信核准：採有權人員核准或委員會核准；有權核可人員不得有授信及會計作業權限，且不能有撥貸、收息及解除擔保品抵押設定等作業權限；有權核可人員須為所貸案件負責，即從承作至貸款收回過程中所有可能發生之風險。

(2)授信管理：授信管理者主要職責包括貸放作業流程相關管理工作（例外事件之辨識及追蹤、授信文件保存、擔保品管理等）及政策之遵循、董事會所核准限額之控管等。

(3)會計制度：評估及維持放款備抵呆帳；遵守法律規定及會計規定；貸款核准、貸款處理及貸款資金作業(撥貸及收息)等功能之分工；貸款作業系統及帳務系統之安全。

(4)債權收回：評估金融機構問題債權回收策略之妥適性，須依機構規模及複雜性有不同處理方式，例如地區型機構，由授信人員負責；大型機構，則由專責部門負責。另對於債權收回，須由專門人員及實提供協助，如破產專員、律師、重整專家及信用顧問等。

(5)人力資源：在評估人力適足性時，須檢視專業及管理人力的適足性；績效管理及薪酬妥適性；管理階層對政策、作業程序、人事、控制系統等缺失改善之妥適性；重要職員之離職率；訓練之妥適性；管理人員推出新商品、服務及系統以因應業務調整、經濟及競爭狀況之能力；人員對董事會與高階管理所擬訂策略及風險容忍度之了解及遵循情形。

(6)內部稽核：內部稽核及貸款覆審之差異，在於貸款覆審之作業重點在維持資產品質，內部稽核則在確保遵循授信管理及會計流程。評估內部稽核品質時，須考慮其獨立性、稽核頻率及範圍以及是否有適格的內部稽核對機構作業有效性進行評估。

(7)貸款覆審：覆審係著重確認資產品質，主要功能在驗證內部評等系統之正確性。評估時需考慮其獨立性、覆審的頻率及範圍及是否有適格的覆審人員評估機構作業有效性。

(四)信用風險管理品質為弱者之特徵：

1.授信政策無法有效地定義風險容忍度及相關權，且無法有效地溝通及傳遞與相關人員。

2.授信文化（包括獲利計畫）相對於授信品質，過分強調行銷。

3.相較於所承受之風險，授信分析不夠充分。

4.風險衡量及監督機制未足以使管理階層因應資產品質及市場狀況之變化並採取適當因應措施。

5.相對於業務量及複雜度，資訊作業流程不妥當，管理資訊系統無法及時提供完整且充分資訊。

6.授信管理方法有瑕疵致無法充分降低固有風險造成之損失。

7.管理階層未能注意分散授信風，亦未辨識及有效管理投資組合風險，包括授信結構及集中度。

8.內部評等系統及曝險報告無法正確將投資組合進行分類。

9.相關人利缺乏專業及管理能力。

10.內部控制機制有弱點或為無效，另貸款覆審及內部稽核缺乏專業、品質及獨立性。

(五)信用風險模型及檢查技巧

1.董事會及高階管理階層之監督：

(1)對董事會及高階管理階層監督工作之評估，其實在進行場外監控及風險評估時，已大部份完成，實地檢查時，主要係透過與董事會（所屬各委員會）成員或高階管理階層面談，並審視董事會及各委員會所審議議案之附件內容，以評估其管理品質。

(2)與管理階層面談時可問下列問題，以確認其專業性：特定問題貸款、信用組合之策略管理、預算及預期成長、新任或離職員工、產品及工作流程改變及所衍生之風、管理階層是否意識到信用組合風險及貸放政策（特定貸放政策及限額、信用組合等）、是否注意到經濟的健全性（未來經濟發展、經濟狀況對預算盈餘之影響等）、董事會及高階管理人員是否取得足夠決策相關資訊、資訊是否有用、資訊是詳細或是彙總、書面分析資料、董事會及高階管理階層是否即時及有效回應稽核、貸款覆審及檢查發現等。

2.政策、作業流程及限額：

(1)場外監控時已確認機構之政策、作業流程及限額妥適性，風險評估時係著重於機構的風險容忍度，實地查核時則著重於測試政策、作業程序及限額等之遵循度及運作情形。

(2)查核授信個案時，重點包括是否遵守徵授信政策（例外案件及附帶條件核准案的情形）；是否依授信監控規定辦理（貸放條件之遵循及定期性分析）；內部評等系統之準確度與及時性；貸款分級的相關分析作業；問題貸款之辨識；放款備抵損失分析之妥適性；會計原則及規定之遵循；文件化作業（授信文件、擔保品及財務報表）；審核管理性報表的妥適性（銀行內部規範、法令規範及法定限額是否有相關報表進行控管）。

3.衡量、監督及管理資訊系統：

(1)傳統管理性報表：包括逾期放款、轉銷或損失、未計息、未履約及例外事項等。

(2)具前瞻性概念之管理性報表：包括新貸放案報表（包含數量、價格、授信品質等）、損失預估及洽談中案件報表。

(3)信用組合管理性報表：包括轉換矩陣(Transition Matrix，係將組合內不同信用評等案件，隨著時間過去，至下一期時信用評等的上下變動情形)、信用組合評等分配、經濟資本、信用評分報表（不同期間貸放案件之逾期情形分析(Vintage Analysis)、特徵分析及母體分析）、信用風險模型報告、產品線分析等。

(4)檢查管理性報表妥適性時，重點包括報表之及時性、正確性及有用性；資訊是否過舊；不正確之資料會產生導致錯誤決策；無用的報表容易遭經理人忽視或誤解（太多細節或不夠詳細、未標示（poor labeling）、易產生混淆的資訊）。

(5)管理性報表之產出方式（系統自動或手工產出，是否有明確政策或內規規範報表產出方式）；報表驗證程序與人員（特別是手工製作者）；辨識管理性報表資料來源（放款系統及其他資料來源，放款管理員及模型得來之資訊）；資料來源是否安全（是否被稽核及是否擷取正確的資訊）；評估各種報表是如何被使用的以及傳達何種資訊（提供越高層者使用之報表應越簡潔且涵蓋整體性）；必要時

是否檢附詳細的書面分析資料；彙總性報表須有詳細報表作附件以提供解釋；
(6)可提出的問題包括給不同管理層級的報表之內容是否妥適；誰決定報表內容之妥適性(是提出報表者或是審閱報表者)；新報表的需求是如何被提出的、如何研擬的及如何產出的。

4.模組的檢查方式

(1)機構於信用風險管理上，所使用之模型大致可分為二類，即企金貸款模型及消金貸款模型，企金貸款模型，包括違約機率(PD)模組、違約損失(LGD)模組及違約曝險(EAD)模型等，消金貸款模型，則包括違約(PD)模型、破產模型(Bankruptcy Model)、行為模型（Behavior Model）、違約損失模型、違約曝險模型等。

(2)企金貸款模型須嚴格定義那些要素係納入衡量信用風險，以及各要素之相關權重，模型所產出的信用風險衡量結果可以是相對性的(不同等級僅在表達相對性的風險高低)，也可以是絕對性的(不同等級的風險可表達絕對性的違約機率)。

(3)消金模組一般係依借戶的特徵為評估基礎，但不同模組會採用不同特徵。

(4)違約機率模型係對一組具有相同特性之借戶中，預測某一特定時間內（如：一年）發生違約的借戶數，檢視的重點在給借戶的額度有多少、借戶的穩定性及歷史違約率（違約率會受外在經濟環境的影響，因此須要每年以新的資料重新作評等）。

(5)破產模型係就相同特徵之借款者，預測未來一定期間（如一年）借款者發生破產之戶數，重點是借款者額度之金額及形式。

(6)行為模型則強調個別顧客之行為及金融機構本身對於顧客之收款及行銷之經驗，強調客戶支出之歷史及花費模式。

(7)消金與企金的 EAD 及 LGD 模組基本上是採相同的理論。

(8)違約損失模型則嘗試預測違約事件發生時之損失金額，模型之基礎係產品之特性（如：擔保品條款）。

(9)違約曝險模型則嘗試決定違約時曝險之金額，模型之基礎係建構於產品之特性、目的及借款者之行為。

(10)健全之模型驗證政策包括：獨立檢視對小機構而言可能不實用，但投入與產出仍應經常受到詳細檢定，可藉由將相關假設與潛在限制告知決策者代替檢視；定義批准之模型、相關假設條件、資料來源之驗証、新模型之實行及發現缺失之追蹤等相關責任；機構所使用的全部模型、各模型的使用程序、模型組成的說明、使用模型人員的責任及模型與資料喪失的緊急應變計畫模型等之相關書面文件；模型更改頻率限制、儘可能獨立檢視所有更改、追蹤更改預期及實際之效果、對所有模型與重要支援程式需設相關權限及適當的備援工作；內部稽核需評估政

策有效性的責任、遵守政策的責任、對於驗證工作，如：財務資料及確認相關假設條件已正確的輸入。金融機構可利用內部稽核、外部稽核及風險管理顧問等，對模型驗證。並可與其他指標模型比較，找出較適合之模型工具，同時進一步與實際結果進行比較。對於輸入資料之驗證，需核對總帳及內部資料、外部資料；相關假設條件應依據金融機構經驗，將假設條件與實際情形做比較。另對於資料之處理（processing）驗證，需將執行結果與指標模型做比較，並可要求供應商驗證並提供相關報告，所有技術處理程序須以非技術及財務用語表示及了解。金融機構之決策者應了解模型產出的意涵及限制，且高階經理階層對模型作業程序，其重要性應等同於所衡量之重大風險。輸入模型的資料應定期稽核，且模型驗證的責任必須被清楚劃分，模型之建立及驗證須分開獨立。

5.內部控制與稽核制度

(1)所有內部控制的控制點均應在作業規範中訂定，在作風險評估時應就內部控制之有效性提出一些假設，這些假設在實地檢查時即進行驗證。

(2)核貸作業內控之檢查著重驗證徵審作業是否遵循規定；例外案件之處理是否遵循相關流程；檢視進入授信系統與帳務系統的人員是否符合規定，且徵審的相關有權人員在授信及帳務系統並無經辦與主管權限，僅有閱讀之權限。

(3)授信前、後台作業是否妥適分工，包括驗証新貸款案之帳務處理、撥貸、手續費、費用及解除擔保品設定等作業之相關責任區分；確定資訊系統之資料更改處理，如：地址、貸款評等、利率等，是否遵循相關政策。另須確認貸款維護和處理擔保品文件人員之責任，包括對於遺失或過期文件是否有相關處理程序；確認對例外案件的追蹤和報告的程序(政策上的例外、文件資料和其他技術上的例外)等。

6.獨立驗證

(1)授信審查與內部稽核係扮演不同角色，有時二者界限並不清楚。

(2)授信覆審，主要在測試徵授信作業是否遵循徵審政策與規範，並評估授信決策與授信分析資料之完整性與妥適性，同時確認授信評等之正確性。

(3)內部稽核主要係測試內部控制的遵循情形(如：付款程序、授信撥貸、授信確認等)及信用管理之有效性，以保障銀行資產 (如：擔保品的完整性、書面資料及技術上的例外與解決方式)。

(4)檢查授信審查與內部稽核作業的重點包括，檢視相關報告；檢核其工作規劃並了解其工作範圍；是否依工作規劃進行；查核工作底稿以確認相關授信決策之妥適性；人員適格性；發現的問題是否有效傳達予應知悉人員並進行追蹤。

四、作業風險之風險評估與檢查技巧

(一)作業風險的來源

1.人員：檢視事項包括組織架構與陳報機制之妥適性；各部門間平行溝通之機制；分層負責及職務分工之清楚且妥適定義；員工及管理階層之適格性。
2.作業流程：檢視事項包括作業流程之妥適規劃；跨部門或涉及委外單位之作業流程妥善規劃；作業流程設計是否妥善考量商品性質、交易量及交易金額、風險控管點、流程順暢性、監控報表之產出及營運策略。
3.系統：檢視事項包括主要系統及相關設施（架構及軟硬體）、資訊部門網路架構、資料處理傳送流程、委外廠商、安全性及金融機構之應變計畫及業務單位及其他支援單位之繼續營業計劃等。
4.外在環境：主要來自天然災害與政治動盪產生之營運中斷。
(二)內部控制品質之指標：包括績效指標及風險指標。
1.績效指標：屬短期導向，一般使用損益表之獲利及損失數據，並供業務單位或功能別經理人使用。
2.風險指標：屬長期導向，一般使用資產負債表及資本數據，供高階管理階層及董事會使用，相對於績效指標，風險指標係供少數人使用且指標數較少。
(三)依據巴塞爾對作業損失之分類，各作業風險來源與損失之對照為：
1.人員：舞弊、員工作業及作業場所安全。
2.流程：執行、傳遞及作業流程管理。
3.系統：營運中斷及系統失靈；客戶、商品及業務作業之損失。
4.外部：實體資產之損失。
(四)各類作業風險來源之固有風險及剩餘風險指標：
1.人員：
(1)固有風險：離職率、空缺率、各業務及高階經理人年資、組織調整、相較業務規模之員工數、依賴主要職員及管理階層之程度。
(2)剩餘風險：系統錯誤使用情形、機密資料錯誤使用情形、職位空缺及空缺時間、內部舞弊、費用造假等。
2.流程：
(1)固有風險：複雜度、交易量（每筆金額或金額加總）、架構調整或成長率（考慮購併、整併或委外）、新商品或新流程、舞弊或作業損失、違反規定情形、例外事件、客戶滿意度、遠端作業等。
(2)剩餘風險：退匯率、退票比率、客戶或內部電話未接聽率、報表錯誤、截止日前完成對帳作業之帳戶、新貸案件作業完成率、新產品或流程之錯誤率等。
3.系統：
(1)固有風險：資訊策略明確性、依賴供應商程度、成熟及新興技術之比率、專案計畫之複雜度、系統作業表現、穩定性、負載整合度、緊急應變計畫、存取控

制及安全性等。

(2)剩餘風險：供應商經營績效、主架構及網路之可獲得性、負載之使用度（處理、儲存及資料傳遞）、災害復原反應時間、系統中斷次數及中斷時間、違反安全事件之次數及嚴重度與形態、系統反應時間等。

4.外部：

(1)固有風險：經濟狀況、競爭環境、法規（法律及行政命令）、國有化、外部或犯罪威脅、自然災害等。

(2)剩餘風險：重新建置資產負債及調整業務所需時間、保險理賠及可扣除金額、營運持續計畫之回復時間及目標等。

5.其它：

(1)固有風險：組織文化、組織架構、薪酬制度、系統（複雜度及成熟度、連外程度、集中式或分散式、自動化及整合程度）、是否有品質控管計畫與指標、是否建置遵法風險管理機制。

(2)剩餘風險：票據清算情形（處理及清算之數量及形態）、會計及財務報告驗證之流程、人力資源（雇用及訓練）。

(五)評估作業風險可使用之資訊來源：

1.一般資訊來源：資訊來源之管道包括財務報表、網站、面談、媒體報導、宣傳文件、管理報告、組織圖、稽核報告、檢查報告、競爭者及市場佔有率等；資訊的項目包括法律訴訟案件（依帳戶型態、曝險及原因分類）、帳戶數（依類形及成長率）、交易量（依帳戶形態、個別及總交易量）、舞弊損失（依帳戶型態及發生原因）、作業錯誤率（依帳戶型態及原因細分）、品質表現率、錯誤解決次數、政策及限額違反情形等。

2.特殊資料來源：管道包括資訊管理系統、監理機關出版品、經濟研究、產業研究等；資訊的項目包括人力資源（管理階層繼任計畫，訓練成本及領悟力）、技術（網路架構型態及資料流程）、貸款作業（付款作業例外事件、限額及規定例外比率、文件處理、問題帳戶解決）、存款作業（存款作業例外比率、編碼錯誤率、對帳單寄送作業、問題帳戶解決）等。

(六)高作業風險程度之特徵：

1.人員：作業人員不熟悉作業流程或未適當訓練；流動率過高無法有效填補空缺致影響業務運作；平均每名員工管理資產金額高於同業；重要業務倚賴少數員工或管理階層；員工數相較同業偏低，所從事作業較複雜或數量高；工作負擔重須長期加班。

2.流程：營業作業包含多個控制點且與許多其他業務有關聯性，以致人員須對流程控管有較高熟悉度；相較於設備負載能力，交易量偏高，或超過同業水準；個

別交易之金額超逾平均水準，或核心交易之金額均較高；作業流程須仰賴大量人工作業；機構正進行重要調整（合併，整併或系統轉換）；營運據點跨多個國家及城市；與同業相較，商品量較多。

3.系統：營運須依靠大量且複雜的基礎設備；因系統功能受限影響營運績效之提升；現有系統欠穩定、或已過時或外部供應商及內部員工無法有效提供援助；對內外部人員授予過大權限使其得接觸超逾職務範圍之重要資料;未考量機構規模及複雜性，而積極發展複雜系統或進行併購以致對業務運作產生負面影響；積極採用開發中之新技術，影響內部系統之作業。

4.外部：營運處所位於易受自然災害影響或基礎建設不佳之地區；營運處所位於易受戰爭或恐怖活動影響之地區；所營業務易涉及複雜法律規範；高度仰賴委外廠商之服務或系統;所處市場具高度競爭或其他機構進行商品或技術創新而增加競爭性；業務易受市場波動影響。

(七)作業風險管理品質之評估：

1.董事會及高階管理階層之監督：檢視項目包括對營運及技術之監督情形；董事會成員之多樣性、管理階層之經驗。評估資料來源包括組織圖、委員會會議紀錄，董事會會議及委員會相關附件資料等。

2.政策、作業流程及限額：檢視項目包括主要營運範圍之政策、作業流程及限額；遵循測試及相關執行情形。評估資料來源包括政策、作業流程及限額文件；法令遵循機制及例外報告等。

3.衡量、監督及管理資訊系統：檢視項目包括完整及適當的董事會、委員會及管理階層報告；報告之驗證作業。評估資料來源包括董事會及委員會相關附件資料、內部稽核報告等。

4.內部控制及內部稽核：檢視項目包括內控環境、稽核人員對作業風險及技術風險之瞭解。評估資料來源包括內部稽核風險評估及稽核計畫、內部稽核報告，外部稽核報告等。

(八)作業風險管理品質為弱之特徵：

1.董事會及高階管理階層之監督：董事會及高階管理階層未充分了解主要作業風險，且無法採取及時導正措施；缺失範圍大或嚴重性高，包括缺乏相關知識、風險管理不足、未利用管理報表或未能反映產業或法規的發展。

2.政策、作業流程及限額：缺乏正式書面信用風險管理規範，以規範風險之辨識、衡量、監控作業。作業風險管理架構缺少或無法適當辨識、評估、監控及控制主要風險；缺失範圍大或嚴重性高，政策無法隨金融機構之規模、複雜度及風險內涵而調整；從事新業務或開發新產品前，未訂定或調整政策與規範。

3.衡量、監督及管理資訊系統：缺乏全面性的作業風險辨識與衡量機制，且相關

假設有誤，或資料內容有誤，文件化不足或未經有效測試。缺失範圍大且嚴重性高，風險未被監控或依規定呈報；管理資訊系統未呈報至決策單位，致無法監控重大風險、或辨識不利發展趨勢及所面臨之風險。

4.內部控制及內部稽核：

(1)內部稽核功能不足；董事會未有效監督；稽核人員缺乏專業知識或獨立性；風險評估過程未有效辨識風險或對應機構之規模、複雜度及風險顯有不足；年度稽核計畫無法涵蓋主要業務單位；管理階層未因應業務市場及科技之變化，就內控提出調整；工作底稿未涵蓋內控測試；重要缺失繼續存在，反映管理單位未積極解決問題。

(2)內部控制長期有待改善之重大缺失；不實財務及管理報表影響健全經營；管理階層無法回應或怠慢於缺失更正；重要資產未妥善保管；利益衝突未被適當揭露及監控；授權及風險限額未有效實行；高風險或重要內控點之負責人員缺乏專業知能；調節表及驗證工作未定時實行；自行評估未完整。

(九)作業風險的檢查技巧

1.董事會及高階管理階層之監督

(1)董事會職責包括定義作業風險、了解主要業務作業風險、訂定風險容忍度及政策規範、監控作業風險及衡量績效等工作；高階管理階層職責包括依風險忍受度及政策訂定作業規範、建置有效內控機制、驗證內控有效性、辨識及監督作業風險及衡量績效等。

(2)建立全面控制及陳報系統、適足管理資訊系統及風險控管報表、健全會計與稽核作業、資訊技術及營運業務不中斷計畫、風險管理及法令遵循。

(3)重要缺失：董事會組成人員缺乏實務背景；董事會受到少數人操控；組織文化不強調控制、透明及品行操守；監督與企業文化不一致；缺乏全面性風險控制機制；董事會或高階管理委員會未將作業及技術作業之風險納入監控；人員分工不清或陳報系統欠明確；缺乏技術及作業策略計劃，或與營運計畫不一致；提報董事會之報告欠妥適，資訊管理系統未能辨識風險；內部稽核計畫未涵蓋主要業務，若未能動態調整、過度依賴外部稽核或外部檢查等。

2.政策、作業程序及限額

(1)須清楚劃分權責；須研擬風險管理及風險抵減策略；建立及維持風險衡量與監控系統，並能夠辨識、評估及核准新商品(服務或業務)之潛在風險；訂定風險管理政策、作業程序及風險容忍度，及相關例外報告。

(2)業務授權須有共通風險管理語言及架構，以確保風險辨識及評估具一致性。審查及核准重要或新業務時，須有風險評估流程，確保風險管理策略與實際施行之管理作業一致。風險管理工具須經有權人員核准，須建立質與量的風險限額，

且風險限額應清楚傳達，並由董事會核准且定期評估，此外，限額應與企業文化、複雜度及財務狀況相配合，且應與整體之衡量、管理及監控風險方法相一致，適合於機構之業務規模、多樣化、複雜度及所面臨之競爭環境等，另限額須考量正常及可預期之風險，及不常發生但重大之外部事件。

(3)重要缺失：超逾風險限額、缺乏文件化作業、涵蓋所有重要作業範圍；未建立風險限額；未定期修定政策與規範；未配合依調整重新檢視權責；缺乏訓練計畫或未確實辦理；政策及作業程序不完備；報告欠嚴謹或權責不清；對於法令遵循或例外報告及追蹤未規範作業程序等。

(十)內部稽核在企業風險管理的角色

為配合美國國會崔德威委員會（COSO）新發布的企業風險管理-綜合架構，內部稽核師協會針對內部稽核在企業的風險管理的角色，於 2004 年 9 月 29 日發出一份立場文件，其目的是協助稽核長 Chief Audit Executives (CAEs)，如何應對組織企業風險管理（ERM）問題。該文件建議內部稽核人員依國際內部稽核師協會的國際標準--內部稽核專業實務（標準）的要求，在提供保證和諮詢服務時，保持客觀性和獨立性。

內部稽核在企業風險管理方面的核心角色，是就企業風險管理活動的有效性，向董事會提供客觀確認，以幫助確保關鍵的經營風險妥善加以管理，及內部控制制度有效地運作。

稽核長在決定內部稽核在企業風險管理方面所應扮演的角色時，應考慮之關鍵因素為：

1.內部稽核的活動是否威脅內部稽核的獨立性和客觀性。

2.內部稽核能否改善組織的風險管理、控制和治理流程。

該機構強調，組織應充分認識到，管理階層仍然須負責風險管理。內部稽核人員應提供諮詢，或挑戰，支持管理階層對風險管的決策，而不是行使風險管理決策。內部稽核人員的責任，應記錄在稽核章程，由稽核委員會批准。

(十一)內部稽核在風險管理所扮演的角色

(1)核心角色：

1.確認風險管理流程之有效性。

2.確認風險評估之正確性。

3.評估風險管理過程。

4.評估主要風險及控制的相關報告。

5.覆核主要風險的管理包括控制的有效性及對風險的回應。

(2)與保障資產安全有關的合法的角色：

1 協助風險的辨識和評估。

2.指導對風險的應對與處理。

3.協調風險管理活動。

4.合併風險報告。

5.維持和發展企業風險管理架構。

6.倡導建立企業風險管理。

7.研發風險管理策略，提交委員會批准。

(3)內部稽核不應承擔的角色：

1.設定風險胃納。

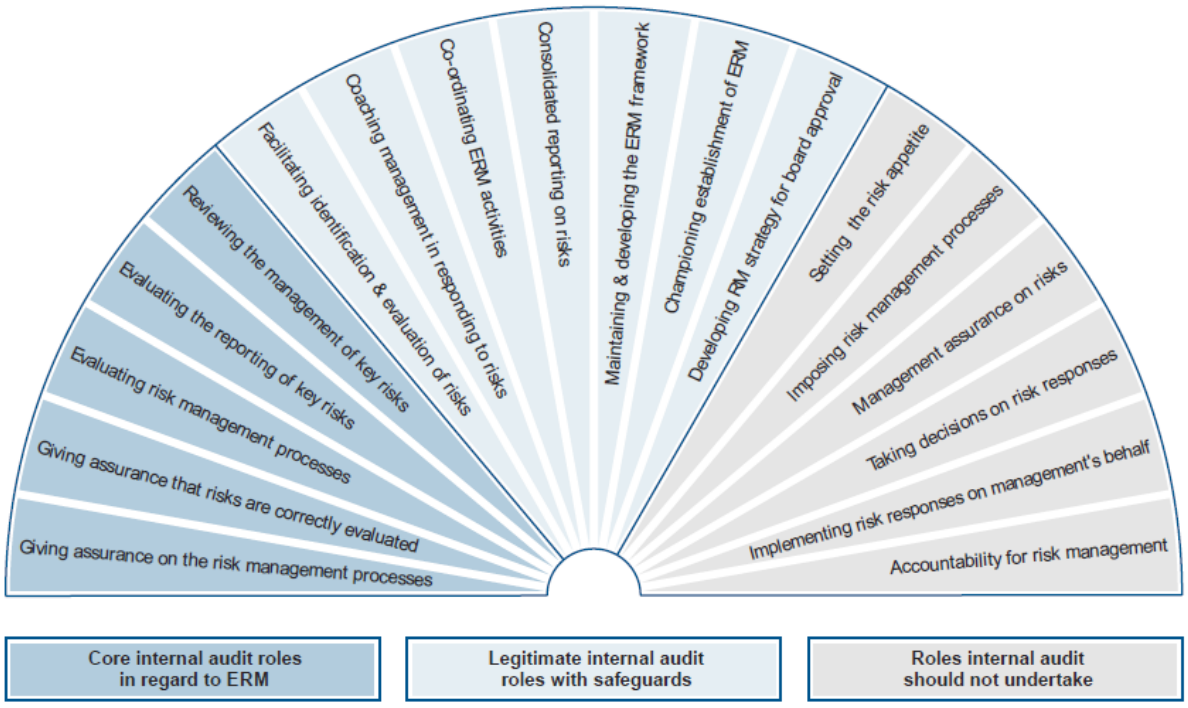
2.設計風險管理流程。

3.對風險之管理確認。

4.對風險回應的決策。

5.代管理階層執行風險回應。

6.承擔風險管理的責任。



資料來源：國際內部稽核師協會網站：http://www.theiia.org

附錄五：美國銀行秘密法遵循情形

資料來源：美國通貨監理署〈OCC〉

美國通貨監理署（OCC）於 2000 年 4 月 24 日發布銀行秘密法遵循計畫一對客戶非常態行為報告之必要條件，內容涵蓋一般銀行秘密法依循缺失。本文旨在介紹銀行內部控管應注意事項。根據美國聯邦規章彙編（CFR）第 12 議題銀行與銀行業務第 21.21 節規定，銀行本身應具備審慎嚴密內部控管、單獨偵測、負責人員、及符合銀行秘密法（Bank Secrecy Act）規定之在職訓練等。

若銀行未能建立並維持適當控管系統，除將遭受主管機關監理強制措施處分外，銀行亦將面臨法令遵循風險與信譽風險之考驗。OCC 已就銀行秘密法與洗錢防制方面常見法令遵循缺失部分，進行專案監理。銀行雖有良好貨幣交易報告（currency transaction reporting, CTR）計畫，但仍缺乏對客戶可疑行為報告之適當控管系統。

OCC 發現銀行具有下列疏失，導致若干可疑交易案件未能及時處理：1.未妥切記錄並評估新開立暨高風險之洗錢帳戶；2.未對高風險服務建立控制暨覆審程序；3. 未能察覺並監視高風險帳戶移作洗錢專用，致發生超逾帳戶正常交易水準行為；4.未適當測試可能被用以洗錢之高風險帳戶；5.未訓練職員偵測客戶可疑交易行為，如類似電匯交易（尤其是已知該交易係與毒品和洗錢有關）等高風險業務等；6.未從貨幣交易報告中，發現與洗錢有關之交易行為模式。監視期間所發現高風險服務，包括貨幣工具、跨國現金信袋、存款經紀人及跨國電匯交易等。高風險帳戶涵蓋通貨服務（moneyservices）業務、境外私人投資公司、非任意處置（non-discretionary）之私人銀行、及國際性往來銀行消費者等。對高風險帳戶進行覆審，係為良好銀行秘密法遵循計畫關鍵所繫。

CTR 覆審為偵測可疑現金交易行為，提供有效方法。對消費者非常態或超逾可理解範圍之現金交易，應考量其違法之可能。自動貨幣交易報告系統允許銀行有效率監管現金交易，以判定超過一萬美元現金交易者，是否以變相方式進行。

OCC 認為銀行應審慎判斷高風險帳戶與可疑交易行為。內部控管程序應防範洗錢用之高風險帳戶、產品與服務之風險，確保：1.內部控管：包括開戶與文件處理程序、管理資訊監視系統，適時偵測可疑交易行為；2.稽核程序：以風險考量為主；注意高風險帳戶與服務情形；單獨偵測銀行系統與控管、CTR、及可疑交易行為報告；3.在職訓練：強調銀行所有部門可能涉及客戶非常態交易部分，尤指高風險帳戶、產品、服務與區域等；4.CTR 覆審程序。（資料來源：OCC Advisory Letter, AL2000-3）

附錄六：銀行防制洗錢及打擊資助恐怖主義注意事項範本修正條文

金融監督管理委員會 102 年 8 月 30 日金管銀法字第 10200247510 號函准予備查
金融監督管理委員會 103 年 6 月 24 日金管銀法字第 10300160160 號函准予備查
金融監督管理委員會 104 年 5 月 11 日金管銀法字第 10400092790 號函准予備查
金融監督管理委員會 105 年 2 月 19 日金管銀法字第 10500029440 號函准予備查

第一條

本範本依「洗錢防制法」第六條規定、「金融機構對達一定金額以上通貨交易及疑似洗錢交易申報辦法」及「銀行業防制洗錢及打擊資助恐怖主義注意事項」訂定，以防制洗錢及打擊資助恐怖主義（以下簡稱防制洗錢及打擊資恐）為目的。

第二條

銀行依「金融控股公司及銀行業內部控制及稽核制度實施辦法」第三十五條規定建立之風險控管機制或內部控制制度，應包括下列事項：

一、依據「銀行評估洗錢及資助恐怖主義風險及訂定相關防制計畫指引」(附件)，訂定之洗錢及資恐風險辨識、評估、管理相關政策、程序，並依該指引及風險評估結果，訂定之防制洗錢及打擊資恐計畫。

二、洗錢防制法令遵循之標準作業程序，並納入自行查核及內部稽核項目。在台之外國金融機構集團分行或子行就前項第一款依據「銀行評估洗錢及資助恐怖主義風險及訂定相關防制計畫指引」訂定之洗錢及資恐風險辨識、評估、管理相關政策、程序，若母集團已建立不低於我國規定且不違反我國法規情形者，在台分行或子行得適用母集團之規定。

第三條

本範本用詞定義如下：

一、一定金額：指新台幣五十萬元（含等值外幣）。

二、通貨交易：單筆現金收或付（在會計處理上，凡以現金收支傳票記帳者皆屬之）或換鈔交易。

第四條

確認客戶身分措施，應依下列規定辦理：

一、 確認客戶身分時機：

（一）與客戶建立業務關係時。

（二）進行下列臨時性交易：

1、辦理達一定金額以上之通貨交易時。

2、辦理新台幣三萬元以上、未達一定金額之國內現金匯款時。

（三）辦理新台幣三萬元以上之國內轉帳匯款案件時。

（四）發現疑似洗錢或資恐交易，或自洗錢及資恐高風險國家或地區匯入款項之交易時，包括但不限於金融監督管理委員會函轉國際防制洗錢組織所公告防制洗錢及打擊資恐有嚴重缺失之國家或地區，及其他未遵循或未充分遵循國際防制洗錢組織建議之國家或地區。

（五）對於過去所取得客戶身分資料之真實性或妥適性有所懷疑時。

二、確認客戶身分方式，除金融監督管理委員會另有規定外，應依下列方式辦理：

（一）以可靠、獨立之原始文件、資料或資訊，辨別及驗證客戶身分，並保存該身分證明文件影本或予以記錄。

（二）對於由代理人辦理之開戶或交易，應確實查證代理之事實，並依前目方式確認代理人身分。

（三）採取辨識及確認客戶實際受益人之合理措施。

（四）確認客戶身分措施，應包括徵詢業務關係之目的與性質。

三、前款第三目規定於客戶為法人或信託之受託人時，應瞭解下列資訊以確認客戶之實際受益人：

（一）客戶為法人時：

1、具控制權之最終自然人身分（如姓名、出生日期、國籍及身分證明文件號碼等）。所稱具控制權係指持有該法人股份或資本超過百分之二十五者。

2、如未發現具控制權之自然人，或對具控制權自然人是否為實際受益人有所懷疑時，應徵詢有無透過其他方式對客戶行使控制權之自然人。必要時得取得客戶出具之聲明書確認實際受益人之身分。

3、如依前二小目規定均未發現具控制權之自然人時，銀行應採取合理措施，確認擔任高階管理職位（如董事或總經理或其他具相當或類似職務之人）之自然人身分。

（二）客戶為信託之受託人時：應確認委託人、受託人、信託監察人、受益人及其他可有效控制該信託帳戶之人。

（三）客戶或具控制權者為下列身分者，除有第九條第一項但書情形者外，得不適用上開應辨識及確認實際受益人身分之規定：

1、我國政府機關。

2、我國公營事業機構。

3、外國政府機關。

4、我國公開發行公司或其子公司。

5、於國外掛牌並依掛牌所在地規定，應揭露其主要股東之股票上市、上櫃

公司，或其子公司。

6、受我國監理之金融機構及其管理之投資工具。

7、設立於我國境外，且所受監理規範與防制洗錢金融行動工作組織（FATF）所定防制洗錢及打擊資恐標準一致之金融機構，及該金融機構管理之投資工具。銀行對前開金融機構及投資工具需留存相關文件證明（如公開資訊查核紀錄、該金融機構防制洗錢作業規章、負面資訊查詢紀錄、金融機構聲明書等）。

8、我國公務人員退休撫卹基金、勞工保險基金、勞工退休基金及郵政儲金。

四、確認客戶身分應遵循之事項：

（一）銀行在與客戶建立業務關係時或與臨時性客戶進行金融交易超過一定金額時或懷疑客戶資料不足以確認身分時，應從政府核發或其他辨認文件確認客戶身分並加以記錄。

（二）應對委託帳戶、由專業中間人代為處理交易，要特別加強確認客戶身分之作為。

（三）應特別留意非居民型之客戶，瞭解這些客戶選擇在國外開設帳戶之原因。

（四）應加強審查私人理財金融業務客戶。

（五）應加強審查被其他銀行拒絕金融業務往來之客戶。

（六）對非「面對面」之客戶，應施以具相同效果之確認客戶程序，且必須有特別和足夠之措施，以降低風險。

（七）在不違反相關法令情形下，銀行如果得知或必須假定客戶往來資金來源自貪瀆或濫用公共資產時，應不予接受或斷絕業務往來關係。

五、有以下情形應予以婉拒開戶或交易：

（一）疑似使用假名、人頭、虛設行號或虛設法人團體開設帳戶者。

（二）客戶拒絕提供審核客戶身分措施相關文件者，但經確實查證身分屬實者不在此限。

（三）對於得採委託、授權之開戶者，若查證委託、授權之事實及身分資料有困難者。

（四）持用偽、變造身分證明文件或出示之身分證明文件均為影本者。

（五）提供文件資料可疑、模糊不清，不願提供其他佐證資料或提供之文件資料無法進行查證者。

（六）客戶不尋常拖延應補充之身分證明文件者。

（七）受理開戶時，有其他異常情形，客戶無法提出合理說明者。

（八）辦理開戶對象為受經濟制裁、外國政府，或國際洗錢防制組織認定或追查之恐怖分子或團體者。

六、有以下情形得依契約約定為下列之處理：

（一）對於前款第八目情形，銀行得拒絕業務往來或逕行關戶。

（二）對於不配合審視、拒絕提供實際受益人或對客戶行使控制權之人等資訊、對交易之性質與目的或資金來源不願配合說明等客戶，銀行得暫時停止交易，或暫時停止或終止業務關係。

第五條

以臨櫃方式開戶應注意事項：

一、行員受理開戶時（包括個人戶及非個人戶），應實施雙重身分證明文件查核及留存第一身分證明文件影本，另有關身分證及登記證照外之第二身分證明文件應具辨識力。

二、若屬個人開戶，除身分證外，並應徵提其他可資證明身分之文件，如健保卡、護照、駕照、學生證、戶口名簿或戶籍謄本等，機關學校團體之清冊，如可確認客戶身分，亦可當作第二身分證明文件。另應利用銀行自行建置之資料庫或外部之資訊來源查詢是否為外國擔任重要政治職務人士，如是，應採取較高之風險管理措施並定期檢討。

三、非個人戶部分，應提供登記證照、公文或相關證明文件，並應徵提董事會議紀錄、公司章程或財務報表等，始可辦理開戶。繳稅證明不能作為開戶之唯一依據，但如已徵提公司設立等登記證照，得作為該非個人戶代表人（負責人）之第二身分證明文件。另如公司戶開戶，已徵提登記證照，並由銀行辦理經濟部網站查詢並留存公司登記資料，得免再徵提其他董事會議紀錄等文件。

以網路方式開立帳戶者，應依本會所訂並經主管機關備查之相關作業範本辦理。

對採委託授權開戶或開戶後始發現有存疑之客戶應以電話、書面或實地查訪等方式確認。

採函件方式辦理開戶者，應於開戶手續辦妥後以掛號函復，以便證實。

其他開戶應注意事項悉應依銀行內部作業規定辦理。

第六條

帳戶及交易之持續監控應注意事項：

一、應對客戶業務關係進行持續性審查，及對其交易過程進行詳細審視，以確保所進行之交易與客戶及其業務、風險相符，必要時並應瞭解其資金來源。

二、 應定期檢視其辨識客戶及實際受益人身分所取得之資訊是否足夠，並確保該等資訊之更新，特別是高風險客戶。

三、 對客戶身分辨識與驗證程序，得以過去執行與保存資料為依據，無須於客戶每次從事交易時，一再辨識及確認客戶之身分。但銀行對客戶資訊之真實

性有所懷疑，如發現該客戶涉及疑似洗錢或資恐交易，或客戶帳戶之運作方式出現與該客戶業務特性不符之重大變動時，應對客戶身分再次確認。

第七條

對達一定金額以上之通貨交易申報：

一、應確認客戶身分並留存交易紀錄憑證。

二、銀行確認客戶身分措施，應依第四條第一項第二款辦理。

三、除本條第二項及第三項之情形外，應於交易完成後五個營業日內以媒體申報方式（檔案格式如附表一），向法務部調查局申報。無法以媒體方式申報而有正當理由者，得報經法務部調查局同意後，以書面（格式如附表二）申報之。

對下列達一定金額以上之通貨交易，得免向法務部調查局申報，但仍應確認客戶身分及留存交易紀錄憑證：

一、與政府機關、公營事業機構、行使公權力機構（於受委託範圍內）、公私立學校、公用事業及政府依法設立之基金，因法令規定或契約關係所生之交易應收應付款項。

二、金融機構間之交易及資金調度。但金融同業之客戶透過金融同業間之同業存款帳戶所生之應付款項，如兌現同業所開立之支票，同一客戶現金交易達一定金額以上者，仍應依規定辦理。

三、公益彩券經銷商申購彩券款項。

四、代收款項交易（不包括存入股款代收專戶之交易），其繳款通知書已明確記載交易對象之姓名、身分證明文件號碼（含代號可追查交易對象之身分者）、交易種類及金額者。但應以繳款通知書副聯作為交易紀錄憑證留存。

非個人帳戶基於業務需要經常或例行性須存入現金達一定金額以上之百貨公司、量販店、連鎖超商、加油站、醫療院所、交通運輸業及餐飲旅館業等，經銀行確認有事實需要者，得將名單轉送法務部調查局核備，如法務部調查局於十日內無反對意見，其後該帳戶得免逐次確認與申報。銀行每年至少應審視交易對象一次。如與交易對象已無本項往來關係，應報法務部調查局備查。

對於前二項交易，如發現有疑似洗錢或資恐交易之情形時，仍應依洗錢防制法第八條規定辦理。

第八條

客戶有關交易如有下列情形之一者，應特別注意，如認為有疑似洗錢或資恐之交易，除應確認客戶身分並留存交易紀錄憑證外，應自發現疑似洗錢或資恐交易之日起十個營業日內依本範本規定程序向法務部調查局辦理申報：

一、同一帳戶於同一營業日之現金存、提款交易，分別累計達一定金額以上，且該交易與客戶身分、收入顯不相當或與本身營業性質無關者。

二、同一客戶於同一櫃檯一次辦理多筆現金存、提款交易，分別累計達一定金額以上，且該交易與客戶身分、收入顯不相當或與本身營業性質無關者。

三、同一客戶於同一櫃檯一次以現金分多筆匯出、或要求開立票據（如本行支票、存放同業支票、匯票）、申請可轉讓定期存單、旅行支票、受益憑證及其他有價證券，其合計金額達一定金額以上，而無法敘明合理用途者。

四、同一客戶於不同櫃檯以每筆未逾（或逾）疑似洗錢或資恐交易申報門檻之現金辦理存、提款，累計達一定金額以上，且該交易與客戶身分、收入顯不相當或與本身營業性質無關者。

五、客戶突有不尋常之大額存款（如將多張本票、支票存入同一帳戶），且與其身分、收入顯不相當或與本身營業性質無關者。

六、久未往來之帳戶突然有大額現金出入（如存入大額票據要求通融抵用），且又迅速移轉者。

七、開戶後立即有與其身分、收入顯不相當或與本身營業性質無關之大額款項存、匯入，且又迅速移轉者。

八、存款帳戶密集存入多筆小額款項，並立即以大額、分散方式提領，僅留下象徵性餘額，其款項與客戶之身分、收入顯不相當或本身營業性質無關者。

九、客戶經常於相關帳戶間移轉大額資金，或以現金方式（提現為名，轉帳為實）處理有關交易流程者。

十、每筆存、提金額相當相距時間不久。

十一、自洗錢或資恐高風險國家或地區匯入之交易款項，且該交易與客戶身分、收入顯不相當或與本身營業性質無關者。本款所述之國家或地區，將依據金融監督管理委員會函轉國際防制洗錢組織所公告防制洗錢及打擊資恐有嚴重缺失之國家或地區、及其他未遵循或未充分遵循國際防制洗錢組織建議之國家或地區。

十二、對結購大額外匯、旅行支票、外幣匯票或其他無記名金融工具，但其用途及資金來源交代不清或其身份業務不符者。

十三、經常性地將小額鈔票兌換成大額鈔票，或反之。

十四、經常替代他人或由不同之第三人存提大筆款項出入特定帳戶。

十五、同一帳戶或同一客戶透過不同帳戶分散交易，並經常有多筆略低於必須申報之金額存入帳戶或自帳戶提出者。

十六、突然償還大額問題放款，而無法釋明合理之還款來源。

十七、其他明顯不正常之交易行為，如大量出售金融債券卻要求支付現金之交易、或頻繁利用旅行支票或外幣支票之大額交易而無正當原因、或大額開發信用狀交易而數量與價格無法提供合理資訊之交易或以巨額（數千萬）金融同業支

票開戶但疑似洗錢或資恐交易者。

十八、交易最終受益人或交易人為金融監督管理委員會函轉外國政府所提供之恐怖分子或團體者；或國際洗錢防制組織認定或追查之恐怖組織；或交易資金疑似或有合理理由懷疑與恐怖活動、恐怖組織或資恐有關聯者。

十九、電視、報章雜誌或網際網路等媒體報導之特殊重大案件，該涉案人在銀行從事之存款、提款或匯款等交易。

二十、數人夥同至銀行辦理存款、提款或匯款等交易者。

銀行對前項以外之其他經認定有疑似洗錢或資恐交易情形者(含現金及轉帳交易)，不論交易金額多寡，應向法務部調查局申報。 前兩項交易未完成者，銀行亦應向法務部調查局申報。

第九條

第四條第一項第二款及第六條規定之確認客戶身分措施及持續監控機制，應以風險為基礎之方法決定其執行強度，對於高風險情形，應加強確認客戶身分或持續監控措施，對於低風險情形，得採取簡化措施。但有下列情形者，不得採取簡化確認客戶身分措施：

一、 客戶來自未採取有效防制洗錢或打擊資恐之高風險國家或地區，包括但不限於金融監督管理委員會函轉國際防制洗錢組織所公告防制洗錢及打擊資恐有嚴重缺失之國家或地區，及其他未遵循或未充分遵循國際防制洗錢組織建議之國家或地區。

二、 足資懷疑該客戶或交易涉及洗錢或資恐者。

銀行得採行之簡化確認客戶身分措施如下：

一、 降低客戶身分資訊更新之頻率。

二、 降低持續性監控之等級，並以合理的金額門檻作為審查交易之基礎。

三、 從交易類型或已建立業務往來關係可推斷其目的及性質者，得無須再蒐集特定資訊或執行特別措施以瞭解業務往來關係之目的及其性質。

銀行應依重要性及風險程度，對現有客戶進行客戶審查，並於考量前次執行客戶審查之時點及所獲得資料之適足性後，在適當時機對已存在之往來關係進行審查。

第十條

對於保存與客戶往來相關文件及交易之紀錄憑證，應依下列規定辦理：

一、 對國內外交易之所有必要紀錄之保存至少保存五年，且確保能夠迅速遵循權責機關對相關資訊之請求，並足以重建個別交易，及作為犯罪行為之起訴證據。前述必要紀錄包括：

（一）進行交易的各方姓名或帳號或識別號碼。

（二）交易日期。

（三）貨幣種類及金額。

（四）存入或提取資金的方式，如以現金、支票等。

（五）資金的目的地。

（六）指示或授權的方式。

二、對達一定金額以上大額通貨交易，其確認紀錄及交易憑證，以原本方式至少保存五年。確認客戶程序之紀錄方法，由銀行依本身考量，根據全行一致性做法之原則，選擇一種紀錄方式。

三、對疑似洗錢或資恐交易之申報，其申報紀錄及交易憑證，以原本方式至少保存五年。

四、下列資料應留存與客戶業務關係結束後或臨時性交易結束後至少五年：

（一）確認客戶身分所取得之所有紀錄，如護照、身分證、駕照或類似之官方身分證明文件影本或紀錄。

（二）帳戶檔案。

（三）業務往來資訊，包括對複雜、異常交易進行詢問所取得之背景或目的資訊與分析資料。

第十一條

防制洗錢及打擊資恐風險控管機制或內部管制程序：

一、帳戶及交易持續之監控：

（一）銀行應逐步利用資訊系統，輔助發現可疑交易。

（二）對較高風險帳戶加強監控。

（三）銀行應特別注意沒有明顯經濟目的或合法目的之所有複雜、不尋常大額交易或所有不尋常型態交易；銀行應儘可能審視上述交易之背景及目的，並將所發現建立資料。

二、客戶有下列情形應婉拒服務，並報告直接主管：

（一）當被告知依法必須提供相關資料確認身份時，堅不提供相關資料。

（二)任何個人或團體強迫或意圖強迫銀行行員不得將交易紀錄或申報表格建檔。

（三）意圖說服行員免去完成該交易應填報之資料。

（四）探詢逃避申報之可能性。

（五）急欲說明資金來源清白或非進行洗錢。

（六）堅持交易必須馬上完成，且無合理解釋。

（七）客戶之描述與交易本身顯不吻合。

（八）意圖提供利益於行員，以達到銀行提供服務之目的。

三、銀行應建立審慎適當之員工遴選程序，包括檢視擬僱用員工具備廉正品格，及執行其職責所需之專業知識，特別是負責執行防制洗錢及打擊資恐控管之員工。另並應注意員工與其防制洗錢及打擊資恐職責間有無潛在利害衝突。

四、行員有下列情形之一者，應對其經辦事務予以抽查，必要時可洽請稽核單位協助：

（一）行員奢侈之生活方式與其薪資所得顯不相當。

（二）行員依規定應休假而無故不願意休假。

（三）行員無法合理解釋其自有帳戶之大額資金進出。

五、專責人員及相關申報流程：

（一）銀行應指派副總經理（或相當職位以上人員）擔任專責人員，以協調監督本範本之執行，並應指定一級單位為事務單位；該副總經理應曾參加洗錢防制法訓練課程，新到任者應於六個月內參加該類訓練課程。

（二）各分支營業單位應指定資深主管人員專責督導該項工作。

（三）疑似洗錢或資恐交易申報程序：

1、各單位承辦人員發現異常交易，應立即陳報專責督導主管。

2、專責督導主管應儘速裁決是否確屬應行申報事項。

3、如裁定應行申報，應立即交由原承辦人員依附表三格式填寫申報書。

4、將申報書呈經單位主管核定後轉送總行（總公司）。

5、由銀行主管單位簽報專責人員核定後，立即向法務部調查局申報。

（四）如屬明顯重大緊急之疑似洗錢或資恐交易案件之申報，應立即以傳真或其他可行方式儘速向法務部調查局申報，並立即補辦書面資料，若經法務部調查局以傳真資料確認回條（格式如附表四）確認收件者，無需補辦申報書。銀行並應留存傳真資料確認回條。

六、防止申報資料及消息洩漏之保密規定：

（一）依第八條規定申報事項，各級人員應保守秘密，不得任意洩漏。

（二）本申報事項有關之文書，均應以機密文件處理，如有洩密案件應依有關規定處理。

（三）洗錢防制專責人員、法令遵循主管人員或稽核單位人員為執行職務需要，應得及時取得客戶資料與交易紀錄，惟仍應遵循保密之規定。

七、對內部管制措施，是否足以防制洗錢之定期檢討規定：

（一）銀行應就所訂防制洗錢範本定期檢討。

（二）分支機構較多且分佈較廣者，得召集有關人員分區舉辦防制洗錢作業檢討會，以收集思廣益之效。

八、稽核單位對本項工作之職責：

（一）應依據所訂內部管制措施暨有關規定訂定查核事項，定期辦理查核，並測試防制洗錢及打擊資恐計畫之有效性及銀行營運、部門與分支機構之風險管理品質。

（二）發現執行該項管理措施之疏失事項，應定期簽報專責副總經理或相當職位人員陳閱，並提供行員在職訓練之參考。

（三）查獲故意隱匿重大違規事項而不予揭露者，應由總行權責單位適當處理。

（四）得設立專責人員對各單位之大額交易抽查，並瞭解其交易之正當性。

九、銀行兼營其他業務時，該兼營部門亦應適用與該業務有關之防制洗錢及打擊資恐注意事項範本，如銀行兼營票券業務，該票券部門即應適用票券商防制洗錢及打擊資恐注意事項範本。

十、對具有跨國通匯往來銀行業務（cross-border correspondent banking）及其他類似關係之金融機構，應訂有一定政策及程序，至少包括：

（一）蒐集足夠之可得公開資訊，以充分瞭解該通匯往來銀行之業務性質，並評斷其商譽及管理品質，包括是否遵循防制洗錢及打擊資恐之規範。

（二)評鑑該通匯往來銀行對防制洗錢及打擊資恐具備相當之控管政策及執行效力。

（三）銀行在與其它銀行建立通匯往來關係前，應先取得內部業務主管層級人員核准後始得辦理。

（四）以文件證明各自對防制洗錢及打擊資恐之責任作為。

（五）當通匯往來銀行業務涉及過渡帳戶（payable–through accounts）時，須確認該通匯往來之銀行確實已執行確認客戶身份等措施，必要時並能提供客戶確認之相關資料。

（六）不得與空殼銀行（Shell banks）或與允許空殼銀行使用其帳戶之外國金融機構建立通匯往來關係。

十一、銀行在外國當地法規許可之情形下，應確保其國外分行及子公司遵循與國內同樣嚴謹之防制洗錢及打擊資恐（AML/CFT）作為，當總機構及分支機構所在國之最低要求不同時，分支機構應就兩地選擇較高標準者作為遵循依據，惟就標準高低之認定有疑義時，以銀行母公司所在國之主管機關之認定為依據；倘因外國法規禁止，致無法採行與總機構相同標準時，應向金融監督管理委員會銀行局陳報。

第十二條

定期舉辦或參加防制洗錢及打擊資恐之在職訓練：

一、職前訓練：新進行員訓練班至少應安排若干小時以上有關洗錢防制法令

及金融從業人員法律責任訓練課程，使新進行員瞭解相關規定及責任。

二、在職訓練：

（一）初期之法令宣導：於洗錢防制法施行或修正後，應於最短期間內對行員實施法令宣導，介紹洗錢防制法及其有關法令，並講解銀行之相關配合因應措施，有關事宜由負責督導洗錢防制作業之權責單位負責規劃後，交由行員訓練單位負責辦理。

（二）平時之在職訓練：

1、行員訓練部門應每年定期舉辦有關之訓練課程提供行員研習，以加強行員之判斷力，落實防制洗錢及打擊資恐之功能，並避免行員違法，本訓練得於其他專業訓練班中安排適當之有關課程。

2、有關訓練課程除由銀行培訓之講師擔任外，並得視實際需要延聘學者專家擔綱。

3、訓練課程除介紹相關法令之外，並應輔以實際案例，使行員充分瞭解洗錢及資恐之特徵及可疑交易之類型，俾助於發覺「疑似洗錢及資恐之交易」。

4、規劃或督導行員訓練之權責部門應定期瞭解行員參加訓練之情形，對於未曾參加者，應視實際需要督促其參加有關之訓練。

5、除行內之在職訓練外，銀行亦得選派行員參加行外訓練機構所舉辦之訓練課程。

（三）專題演講：為更充實行員對洗錢防制法令之認識，銀行得舉辦專題講座，邀請學者專家蒞行演講。

第十三條

行員有下列對防制洗錢或打擊資恐有功之具體事蹟者，應給予適當獎勵：

一、行員發現有疑似洗錢或資恐案件，並依據洗錢防制相關規定申報，對檢警單位防範或偵破犯

二、行員參加國內外防制洗錢或打擊資恐相關業務講習，成績優良或蒐集國外法令研提對銀行防制洗錢或打擊資恐活動具有價值之資料者。

第十四條

本範本經銀行董事會（或分層授權之權責單位）通過後實施，並呈報金融監督管理委員會備查；並應每年檢討。修改時亦同。

附錄七：銀行評估洗錢及資助恐怖主義風險及訂定相關防制計畫指引

資料來源：金管會

一、本指引依「銀行業防制洗錢及打擊資助恐怖主義注意事項」訂定，以防制洗錢及打擊資助恐怖主義（以下簡稱防制洗錢及打擊資恐）為目的，內容涵括我國銀行如何辨識、評估各項業務之洗錢及資恐風險，以及制訂防制洗錢及打擊資恐計畫等面向，作為執行之依據。

二、銀行之風險控管機制或內部控制制度，應包括針對洗錢及資恐風險進行辨識、評估、管理與相關書面政策、程序之訂定，以及依據風險評估結果而訂定之防制洗錢及打擊資恐計畫，並定期檢討。

以風險為基礎之方法（risk-based approach）旨在協助發展與洗錢及資恐風險相當之防制與抵減措施，以利銀行決定其防制洗錢及打擊資恐資源之配置、建置其內部控制制度、以及訂定和執行防制洗錢及打擊資恐計畫應有之政策、程序及控管措施。

銀行業務具多樣性，如消費金融業務、企業金融業務、投資服務（或財富管理）及跨國通匯代理銀行業務等，不同業務伴隨之洗錢及資恐風險亦有所不同。銀行於評估與抵減其洗錢及資恐曝險時，應將上開業務差異性納入考量。

本指引所舉例之各項說明與附錄並非強制性規範，銀行之風險評估機制應與其業務性質及規模相當。對較小型或業務較單純之銀行，簡單之風險評估即足夠；惟對於產品與服務較複雜之銀行、有多家分支機構提供廣泛多樣之產品、或其客戶群較多元者，則需進行較高度的風險評估程序。

三、銀行應採取合宜措施以識別、評估其洗錢及資恐風險，並依據所辨識之風險訂定具體的風險評估項目，以進一步管控、降低或預防該風險。

具體的風險評估項目應至少包括地域、客戶與產品三類指標，並應進一步分析各風險項目，以訂定細部的風險因素。

（一）地域風險：

1、銀行應識別具較高洗錢及資恐風險的區域。

2、於訂定高洗錢及資恐風險之區域名單時，銀行得依據其各分支機構的實務經驗或參照附錄，並考量個別需求，以選擇適用之參考依據。

（二）客戶風險：

1、銀行應綜合考量個別客戶背景、職業與社會經濟活動特性、地域、以及非自然人客戶之組織型態與架構等，以識別該客戶洗錢及資恐風險。

2、於識別個別客戶風險並決定其風險等級時，銀行得依據以下風險因素為

評估依據：

（1）客戶之地域風險：依據銀行所定義之洗錢及資恐風險的區域名單，決定客戶國籍與居住國家的風險評分。

（2）客戶職業與行業之洗錢風險：依據銀行所定義之各職業與行業的洗錢風險，決定客戶職業與行業的風險評分。高風險行業如從事密集性現金交易業務、或屬易被運用於持有個人資產之公司或信託等。

（3）客戶開戶與建立業務關係之管道。

（4）客戶開戶與建立業務關係之金額。

（5）帳戶預期的交易金額。

（6）客戶是否有其他高洗錢及資恐風險之表徵，如客戶留存地址與分行相距過遠而無法提出合理說明者、客戶為具隱名股東之公司或可發行無記名股票之公司、法人客戶之股權複雜度，如股權架構是否明顯異常或相對其業務性質過度複雜等。

（三）產品風險：

1、銀行應依據個別產品或服務的性質，識別可能會為其帶來較高的洗錢及資恐風險者。

2、銀行應於新產品或新服務上線前，進行全面洗錢風險評估，並按照風險控制原則，建立相應風險管理措施。

3、個別產品或服務之風險因素舉例如下：

（1）與現金之關聯程度。

（2）建立業務關係或交易之管道，包括是否為面對面交易及是否為電子銀行等新型態支付工具等。

（3）是否為高金額之金錢或價值移轉業務。

四、銀行應建立不同之客戶風險等級與分級規則

就客戶之風險等級，至少應有兩級（含）以上之風險級數，即「高風險」與「一般風險」兩種風險等級，作為加強客戶審查措施及持續監控機制執行強度之依據。若僅採行兩級風險級數之銀行，因「一般風險」等級仍高於本指引第五點與第七點所指之「低風險」等級，故不得對「一般風險」等級之客戶採取簡化措施。銀行不得向客戶或與執行防制洗錢義務無關者，透露客戶之風險等級資訊。

五、除外國擔任重要政治職務人士與受經濟制裁、外國政府或國際洗錢防制組織認定或追查之恐怖分子或團體直接視為高風險客戶外，銀行得依自身之業務型態及考量相關風險因素，訂定應直接視為高風險客戶之類型。

銀行得依據完整之書面風險分析結果，自行定義可直接視為低風險客戶之類型，而書面風險分析結果須能充分說明此類型客戶與較低之風險因素相稱。

六、對新建立業務關係的客戶，銀行應在建立業務關係時，確定其風險等級

對於已確定風險等級之既有客戶，銀行應依據其風險評估政策及程序，重新進行客戶風險評估。

雖然銀行在建立業務關係時已對客戶進行風險評估，但就某些客戶而言，必須待客戶透過帳戶進行交易，其全面風險狀況才會變得明確，故於得知客戶身分與背景資訊有重大變動、或察覺客戶交易模式變更時，應適時調整客戶風險等級。

針對重新進行客戶風險評估之時點，舉例說明如下：

（一）客戶加開帳戶或新增業務往來關係時。

（二）依據客戶風險等級進行定期客戶審查時。

（三）經申報疑似洗錢交易等，可能導致客戶風險狀況發生實質性變化的事件發生時。

七、銀行應依據已識別之風險，建立相對應的管控措施，以降低或預防該洗錢風險；銀行應依據客戶的風險程度，決定不同風險等級客戶所適用的管控措施

對於風險之管控措施，應由銀行依據其風險防制政策、監控及程序，針對各類型之高風險客戶採取不同的管控措施，以有效管理和降低已知風險，舉例說明如下：

（一）進行加強客戶審查措施(Enhanced Due Diligence)，例如：

1、取得開戶與往來目的之相關資料：如帳戶用途、預期的客戶交易活動等資料。

2、進行客戶資產評估：取得客戶財富來源、往來資金來源、資產種類與數量以對客戶進行資產評估。

3、取得客戶進一步之商業資訊：瞭解客戶最新商業活動與業務往來資訊。

4、取得將進行或已完成交易之說明與資訊。

5、依據客戶型態進行實地或電話訪查，以確認客戶之實際營運情形。

（二）取得較高管理階層之核准。

（三）增加進行客戶審查之頻率。

（四）加強之監控機制。

銀行對於風險等級為最高之客戶，應至少每二年進行一次客戶審查。

對於低風險情形，得由銀行依據其風險防制政策、監控及程序，採取簡化措施。簡化確認客戶身分措施得採行如下：

（一）降低客戶身分資訊更新之頻率。

（二）降低持續性監控之等級，並以合理的金額門檻作為審查交易之基礎。

（三）從交易類型或已建立業務往來關係可推斷其目的及性質者，得無須再

對瞭解業務往來關係之目的及性質，蒐集特定資訊或執行特別措施。

但依據本範本第四條第一項及第六條規定之確認客戶身分及持續監控時，遇有下列情形者，不得採取簡化確認客戶身分措施：

（一）客戶來自未採取有效防制洗錢或打擊資助恐怖主義之高風險地區或國家，包括但不限於金融監督管理委員會函轉國際防制洗錢組織所公告防制洗錢與打擊資助恐怖主義有嚴重缺失之國家或地區，及其他未遵循或未充分遵循國際防制洗錢組織建議之國家或地區。

（二）足資懷疑該客戶或交易涉及洗錢或資助恐怖主義者。

八、銀行應建立定期之全面性洗錢及資恐風險評估作業，使管理階層得以適時且有效地瞭解銀行所面對之整體洗錢與資恐風險、決定應建立之機制及發展合宜之抵減措施。

銀行應依據下列指標，建立定期且全面性之洗錢及資恐風險評估作業：

（一）業務之性質、規模、多元性及複雜度。

（二）目標市場。

（三）銀行交易數量與規模：考量銀行一般交易活動與其客戶之特性等。

（四）高風險相關之管理數據與報告：如高風險客戶之數目與比例；高風險產品、服務或交易之金額、數量或比例；客戶之國籍、註冊地或營業地、或交易涉及高風險地域之金額或比例等。

（五）業務與產品，包含提供業務與產品予客戶之管道及方式、執行客戶審查措施之方式，如資訊系統使用程度及是否委託第三人執行審查。

（六）內部稽核與監理機關之檢查結果。

銀行於進行前項之全面性洗錢及資恐風險評估作業時，除考量上開指標外，建議輔以其他內部與外部來源取得之資訊，如：

（一）銀行內部管理階層(如事業單位主管、客戶關係經理等)所提供的管理報告。

（二）國際組織與他國所發布之防制洗錢及打擊資恐相關報告。

（三）主管機關發布之洗錢及資恐風險資訊。

銀行之全面性洗錢及資恐風險評估結果應做為發展防制洗錢及打擊資恐計畫之基礎；銀行應依據風險評估結果分配適當人力與資源，採取有效的反制措施，以預防或降低風險。

銀行有重大改變，如發生重大事件、管理及營運上有重大發展、或有相關新威脅產生時，應重新進行評估作業。

九、銀行應依其洗錢與資恐風險及業務規模，訂定、執行防制洗錢及打擊資恐計畫，內容除應涵蓋確認客戶身分、紀錄保存與申報一定金額以上通貨交易及

疑似洗錢交易等內部政策、程序及控管外，並應包括指定管理階層人員協調督導防制洗錢及打擊資恐之執行、建立審慎適當之員工遴選程序、實施持續性之員工訓練計畫及測試銀行防制洗錢及打擊資恐系統有效性之獨立稽核功能等內部政策、程序及控管，銀行得依本範本相關規定辦理。

十、銀行依據本指引訂定之政策應經董事會（或分層授權之權責單位）通過後實施，並與其「防制洗錢及打擊資助恐怖主義注意事項」陳報金融監督管理委員會備查；並應定期檢討。修改時亦同。

附錄八：銀行業防制洗錢及打擊資助恐怖主義注意事項

105.12.02 金管銀法字第 10510005200 號

一、為強化我國防制洗錢與打擊資恐機制，並健全銀行業內部控制及稽核制度，訂定本注意事項。

二、銀行業防制洗錢及打擊資恐等事宜，除應遵循洗錢防制法、資恐防制法、金融機構對達一定金額以上通貨交易及疑似洗錢交易申報辦法、存款帳戶及其疑似不法或顯屬異常交易管理辦法及金融機構辦理國內匯款作業確認客戶身分原則等規定外，並應依本注意事項所定事項辦理。

三、本注意事項所稱銀行業包括銀行、信用合作社、辦理儲金匯兌之郵政機構、票券金融公司、信用卡公司及信託業。

四、銀行業確認客戶身分措施，應依下列規定辦理：

（一）銀行業不得接受客戶以匿名或使用假名開立帳戶。

（二）銀行業於下列情形時，應確認客戶身分：

1.與客戶建立業務關係時。

2.進行臨時性交易：

（1）辦理新台幣五十萬元（含等值外幣）以上之單筆現金收或付（在會計處理上，凡以現金收支傳票記帳者皆屬之）或換鈔交易時。

（2）辦理新台幣三萬元（含等值外幣）以上之跨境匯款時。

3.發現疑似洗錢或資恐交易時。

4.對於過去所取得客戶身分資料之真實性或妥適性有所懷疑時。

（三）銀行業確認客戶身分應採取下列方式：

1.以可靠、獨立之原始文件、資料或資訊，辨識及驗證客戶身分，並保存該身分證明文件影本或予以記錄。

2.對於由代理人辦理之開戶或交易，應確實查證代理之事實，並以可靠、獨立之原始文件、資料或資訊，辨識及驗證代理人身分，並保存該身分證明文件影本或予以記錄。

3.採取辨識及驗證客戶實際受益人之合理措施。

4.確認客戶身分措施，應包括徵詢業務關係之目的與性質。

（四）前款規定於客戶為法人或信託之受託人時，應瞭解客戶或信託（包括類似信託之法律協議）之業務性質、所有權與控制權結構，並至少取得客戶或信託之下列資訊，辨識及驗證其身分：

1.客戶或信託之名稱、法律形式及存在證明。

2.規範及約束法人或信託之章程或類似之權力文件，及在法人或信託之受託

人中擔任高階管理職位人員之姓名。

3.法人或信託之受託人註冊登記之辦公室地址，及其主要之營業處所地址。

（五）客戶為法人時，應瞭解其是否可發行無記名股票，並對已發行無記名股票之客戶採取適當措施以確保其實際受益人之更新。

（六）第三款第三目規定於客戶為法人或信託之受託人時，應瞭解下列資訊，辨識客戶之實際受益人，並採取合理措施驗證：

1.客戶為法人時：

（1）具控制權之最終自然人身分。所稱具控制權係指持有該法人股份或資本超過百分之二十五者。

（2）如未發現具控制權之自然人，或對具控制權自然人是否為實際受益人有所懷疑時，應辨識有無透過其他方式對客戶行使控制權之自然人。

（3）如依前二小目規定均未發現具控制權之自然人時，銀行業應辨識擔任高階管理職位之自然人身分。

2.客戶為信託之受託人時：應確認委託人、受託人、信託監察人、受益人及其他可有效控制該信託帳戶之人，或與上述人員具相當或類似職務者之身分。

3.客戶或具控制權者為下列身分者，除有第七點第二款但書情形者外，得不適用上開應辨識及驗證公司股東或實際受益人身分之規定。

（1）我國政府機關。

（2）我國公營事業機構。

（3）外國政府機關。

（4）我國公開發行公司或其子公司。

（5）於國外掛牌並依掛牌所在地規定，應揭露其主要股東之股票上市、上櫃公司，或其子公司。

（6）受我國監理之金融機構及其管理之投資工具。

（7）設立於我國境外，且所受監理規範與金融行動工作組織（FATF）所定防制洗錢及打擊資助恐怖主義標準一致之金融機構，及該金融機構管理之投資工具。

（8）我國公務人員退休撫卹基金、勞工保險基金、勞工退休基金及郵政儲金。

（七）銀行業完成確認客戶身分措施前，不得與該客戶建立業務關係或進行臨時性交易。但符合下列各目情形者，得先取得辨識客戶及實際受益人身分之資料，並於建立業務關係後，再完成驗證：

1.洗錢及資恐風險受到有效管理。包括應針對客戶可能利用交易完成後才驗

證身分之情形，採取風險管控措施。

2.為避免對客戶業務之正常運作造成干擾所必須。

3.會在合理可行之情形下儘速完成客戶及實際受益人之身分驗證。如未能在合理可行之時限內完成客戶及實際受益人之身分驗證，須終止該業務關係，並應事先告知客戶。

（八）銀行業對於無法完成確認客戶身分相關規定程序者，應考量申報與該客戶有關之可疑交易。

（九）銀行業懷疑某客戶或交易可能涉及洗錢或資恐，且合理相信執行確認客戶身分程序可能對客戶洩露訊息時，得不執行該等程序，而改以申報可疑交易。

五、銀行業確認客戶身分時，有以下情形之一者，應予以婉拒建立業務關係或交易：

（一）疑似使用假名、人頭、虛設行號或虛設法人團體開設帳戶。

（二）客戶拒絕提供審核客戶身分措施相關文件。

（三）對於得採委託、授權之開戶者，若查證委託、授權之事實及身分資料有困難。

（四）持用偽、變造身分證明文件或出示之身分證明文件均為影本。

（五）提供文件資料可疑、模糊不清，不願提供其他佐證資料或提供之文件資料無法進行查證。

（六）客戶不尋常拖延應補充之身分證明文件。

（七）建立業務關係時，有其他異常情形，客戶無法提出合理說明。

（八）建立業務關係對象為資恐防制法指定制裁之個人、法人或團體，以及外國政府或國際洗錢防制組織認定或追查之恐怖分子或團體。

六、客戶身分之持續審查：

（一）銀行業應依重要性及風險程度，對現有客戶身分資料進行審查，並於考量前次執行審查之時點及所獲得資料之適足性後，在適當時機對已存在之往來關係進行審查。上開適當時機至少應包括：

1.客戶加開帳戶或新增業務往來關係時。

2.依據客戶之重要性及風險程度所定之定期審查時點。

3.得知客戶身分與背景資訊有重大變動時。

（二）銀行業應對客戶業務關係中之交易過程進行詳細審視，以確保所進行之交易與客戶及其業務、風險相符，必要時並應瞭解其資金來源。

（三）銀行業應定期檢視其辨識客戶及實際受益人身分所取得之資訊是否足夠，並確保該等資訊之更新，特別是高風險客戶，銀行業應至少每年

檢視一次。

（四）銀行業對客戶身分辨識與驗證程序，得以過去執行與保存資料為依據，無須於客戶每次從事交易時，一再辨識及驗證客戶之身分。但銀行業對客戶資訊之真實性有所懷疑，如發現該客戶涉及疑似洗錢交易，或客戶帳戶之運作方式出現與該客戶業務特性不符之重大變動時，應依第四點規定對客戶身分再次確認。

七、第四點第三款與前點規定之確認客戶身分措施及持續審查機制，應以風險基礎方法決定其執行強度：

（一）對於高風險情形，應加強確認客戶身分或持續審查措施，其中至少應額外採取下列強化措施：

1.在建立或新增業務往來關係前，應取得高階管理層級同意。

2.應採取合理措施以瞭解客戶財富及資金來源。其中資金來源如為存款，應進一步瞭解該存款之來源。

3.對於業務往來關係應採取強化之持續監督。

（二）對於較低風險情形，得採取簡化措施，該簡化措施應與其較低風險因素相當。但有下列情形者，不得採取簡化確認客戶身分措施：

1.客戶來自未採取有效防制洗錢或打擊資恐之高風險地區或國家，包括但不限於金融監督管理委員會（以下簡稱本會）函轉國際防制洗錢組織所公告防制洗錢與打擊資恐有嚴重缺失之國家或地區，及其他未遵循或未充分遵循國際防制洗錢組織建議之國家或地區。

2.足資懷疑該客戶或交易涉及洗錢或資恐。

八、客戶及交易有關對象之姓名及名稱檢核政策及程序：

（一）銀行業應依據風險基礎方法，建立客戶及交易有關對象之姓名及名稱檢核政策及程序，以偵測、比對、篩檢客戶或交易有關對象是否為資恐防制法指定制裁之個人、法人或團體，以及外國政府或國際洗錢防制組織認定或追查之恐怖分子或團體者，並依資恐防制法第七條等規定辦理。

（二）銀行業之客戶及交易有關對象之姓名及名稱檢核政策及程序，至少應包括比對與篩檢邏輯、檢核作業之執行程序，以及檢視標準，並將其書面化。

（三）銀行業執行姓名及名稱檢核情形應予紀錄，並依第十點規定之期限進行保存。

九、帳戶及交易之持續監控：

（一）銀行業應逐步以資訊系統整合全公司（社）客戶之基本資料及交易資

料，供總分支機構進行基於防制洗錢及打擊資恐目的之查詢，以強化其帳戶及交易監控能力。對於各單位調取及查詢客戶之資料，應建立內部控制程序，並注意資料之保密性。

（二）銀行業應依據以風險為基礎之方法，建立帳戶及交易監控政策與程序，並利用資訊系統，輔助發現可疑交易。

（三）銀行業應依據防制洗錢與打擊資恐法令規範、其客戶性質、業務規模及複雜度、內部與外部來源取得之洗錢與資恐相關趨勢與資訊、銀行業內部風險評估結果等，檢討其帳戶及交易監控政策及程序，並定期更新之。

（四）銀行業之帳戶及交易監控政策及程序，至少應包括完整的監控型態、參數設定、金額門檻、預警案件與監控作業之執行程序與監控案件的檢視程序及申報標準，並將其書面化。

（五）前款完整之監控型態應包括各同業公會所發布之態樣，並應參照銀行業本身之洗錢及資恐風險評估或日常交易資訊，增列相關之監控態樣。監控態樣例示如下：

1.同一帳戶於同一營業日之現金存、提款交易，分別累計達新台幣五十萬元（含等值外幣）以上，且該交易與客戶身分、收入顯不相當，或與其營業性質無關者。

2.同一客戶於同一櫃檯一次辦理多筆現金存、提款交易，分別累計達新台幣五十萬元（含等值外幣）以上，且該交易與客戶身分、收入顯不相當，或與其營業性質無關者。

3.同一客戶於同一櫃檯一次以現金分多筆匯出、或要求開立票據（如本行支票、存放同業支票、匯票）、申購可轉讓定期存單、旅行支票及其他有價證券，其合計金額達新台幣五十萬元（含等值外幣）以上，而無法敘明合理用途者。

4.涉及洗錢或資恐高風險國家或地區之交易，且與客戶身分、收入顯不相當，或與其營業性質無關者。

5.交易最終受益人或交易人為金融監督管理委員會函轉外國政府所提供之恐怖分子或團體；或國際洗錢防制組織認定或追查之恐怖組織；或交易資金疑似或有合理理由懷疑與恐怖活動、恐怖組織或資助恐怖主義有關聯者。

6.交易金額超過銀行業所設一定門檻，且與帳戶平均餘額顯不相當。

7.短期內密集使用電子交易功能，且一定期間累計交易金額超過銀行業所設一定門檻。

（六）銀行業執行帳戶及交易持續監控之情形應予紀錄，並依第十點規定之期限進行保存。

十、銀行業應保存與客戶往來及交易之紀錄憑證，並依下列規定辦理：

（一）銀行業對國內外交易之所有必要紀錄，應至少保存五年。

（二）銀行業對下列資料，應保存至與客戶業務關係結束後或臨時性交易結束後，至少五年：

1.確認客戶身分所取得之所有紀錄，如護照、身分證、駕照或類似之官方身分證明文件影本或紀錄。

2.帳戶檔案。

3.業務往來資訊，包括對複雜、異常交易進行詢問所取得之背景或目的資訊與分析資料。

（三）銀行業保存之交易紀錄應足以重建個別交易，以備作為認定不法活動之證據。

（四）銀行業對權責機關依適當授權要求提供交易紀錄及確認客戶身分等相關資訊時，應確保能夠迅速提供。

十一、銀行業於確認客戶身分時，應利用銀行自行建置之資料庫或外部之資訊來源查詢客戶或其實際受益人是否為現任或曾任國外政府或國際組織之重要政治性職務人士：

（一）客戶或其實際受益人若為現任國外政府之重要政治性職務人士，應將該客戶直接視為高風險客戶，並採取第七點第一款各目之強化確認客戶身分措施。

（二）客戶或其實際受益人若為現任國際組織之重要政治性職務人士，應於與該客戶建立業務關係時，審視其風險，嗣後並應每年重新審視。對於經銀行業認定屬高風險業務關係者，應對該客戶採取第七點第一款各目之強化確認客戶身分措施。

（三）前二款規定於重要政治職務人士之家庭成員及有密切關係之人時，亦適用之。

（四）對於非現任國外政府或國際組織之重要政治性職務人士，銀行業得依該人士之影響力、擔任重要政治性職務之年資等因素，審視其風險，如決定其仍應列為重要政治性職務人士，應適用前三款之規定。

十二、銀行業辦理通匯往來銀行業務及其他類似業務，應定有一定政策及程序，至少包括：

（一）蒐集足夠之可得公開資訊，以充分瞭解該委託銀行之業務性質，並評斷其商譽及管理品質，包括是否遵循防制洗錢及打擊資恐之規範。

（二）評估該委託銀行對防制洗錢及打擊資恐具備相當之控管政策及執行效力。

（三）在與委託銀行建立通匯往來關係前，應先取得高階主管層級人員核准後始得辦理。

（四）以文件證明各自對防制洗錢及打擊資恐之責任作為。

（五）當通匯往來銀行業務涉及過渡帳戶時，須確認該委託銀行確實已執行確認客戶身份等措施，必要時並能提供確認客戶身分之相關資料。

（六）不得與空殼銀行或與允許空殼銀行使用其帳戶之委託銀行建立通匯往來關係。

（七）委託銀行為銀行業本身之國外分支機構時，亦適用上開規定。

十三、銀行業於推出新產品或服務或辦理新種業務（包括新支付機制、運用新科技於現有或全新之產品或業務）前，應進行產品之洗錢或資恐風險評估，建立相應之風險管理措施以降低所辨識之風險。

十四、匯款相關規定：

（一）銀行業辦理外匯境內及跨境之一般匯出及匯入匯款業務，應依「銀行業辦理外匯業務作業規範」辦理。

（二）銀行業辦理新台幣境內匯款業務，應依下列規定辦理：

1.境內電匯之匯款金融機構應採下列方式之一提供匯款人及受款人資訊：

（1）隨匯款交易提供匯款人及受款人資訊。

（2）隨匯款交易提供匯款人及受款人之帳戶號碼或可供追蹤之交易碼，並於收到受款金融機構或權責機關請求時，於三個營業日內提供匯款人及受款人資訊。

2.匯款金融機構應保存所有有關匯款人及受款人資訊。

3.上開匯款人資訊應包括：匯款人姓名、扣款帳戶號碼（如無，則提供可供追蹤的交易碼）；及匯款人地址或身分證號或出生日期及出生地。

4.上開受款人資訊應包括：收款人姓名、受款帳戶號碼（如無，則提供可供追蹤的交易碼）。

十五、內部控制制度：

（一）銀行業依「金融控股公司及銀行業內部控制及稽核制度實施辦法」第八條規定、「郵政儲金匯兌業務內部控制及稽核制度實施辦法」第五條規定或「信用卡業務機構管理辦法」第三十三條規定建立之內部控制制度，應包括下列事項：

1.就洗錢與資恐風險進行辨識、評估、管理之相關政策及程序。

2.依據洗錢及資恐風險、業務規模，訂定防制洗錢及打擊資恐計畫，以管理

及降低已辨識出之風險，並對其中之較高風險，採取強化控管措施。

3.監督控管防制洗錢及打擊資恐法令遵循及防制洗錢及打擊資恐計畫執行之標準作業程序，並納入自行查核及內部稽核項目，且於必要時予以強化。

（二）前款第一目洗錢及資恐風險之辨識、評估與管理，應依下列規定辦理：

1.應將風險評估內容書面化。

2.應考量所有風險因素，並至少涵蓋客戶、地域、產品及服務、交易或支付管道等面向，以決定整體風險等級，及降低風險之適當措施。

3.應訂定更新風險評估之機制，以確保風險資料之更新。

（三）第一款第二目之防制洗錢及打擊資恐計畫，應包括下列政策、程序及控管機制：

1.確認客戶身分。

2.客戶及交易有關對象之姓名及名稱檢核。

3.帳戶及交易之持續監控。

4.通匯往來銀行業務。

5.紀錄保存。

6.一定金額以上通貨交易申報。

7.可疑交易申報。

8.指定防制洗錢及打擊資恐專責主管負責遵循事宜。

9.員工遴選及任用程序。

10.持續性員工訓練計畫。

11.測試防制洗錢及打擊資恐系統有效性之獨立稽核功能。

12.其他依防制洗錢及打擊資恐相關法令及主管機關規定之事項。

（四）具國外分支機構之銀行業，應訂定集團層次之防制洗錢與打擊資助恐怖主義計畫，除包括前款政策、程序及控管機制外，另應在符合我國及國外分支機構所在地資料保密規定之情形下，訂定下列事項：

1.為確認客戶身分與洗錢及資恐風險管理目的所需之集團內資訊分享政策及程序。

2.為防制洗錢及打擊資恐目的，國外分支機構須建置符合集團之遵循及稽核規定，並提供有關客戶、帳戶及交易資訊。

3.對運用被交換資訊及其保密之安全防護。

（五）銀行業應確保其國外分支機構，在符合當地法令情形下，實施與母公司一致之防制洗錢及打擊資恐措施。當總機構及分支機構所在國之最低要求不同時，分支機構應就兩地選擇較高標準者作為遵循依據，惟就標準高低之認定有疑義時，以銀行業母公司所在國之主管機關之認

定為依據；倘因外國法規禁止，致無法採行與總機構相同標準時，應採取合宜之額外措施，以管理洗錢及資恐風險，並向主管機關陳報。

（六）銀行業之董事會及高階管理人員應瞭解其洗錢及資恐風險，及防制洗錢及打擊資恐計畫之運作，並採取措施以塑造重視防制洗錢及打擊資恐之文化。

十六、專責單位及專責主管：

（一）銀行業應於總經理、總機構法令遵循單位或風險控管單位下設置獨立之防制洗錢及打擊資恐專責單位，該單位不得兼辦防制洗錢及打擊資恐以外之其他業務，且應依其規模、風險等配置適足人力及資源，並由董事會指派高階主管一人擔任專責主管，賦予執行防制洗錢及打擊資恐之充分職權，至少每半年向董（理）事會及監察人（監事、監事會）或審計委員會報告，如發現有重大違反法令時，應即時向董（理）事會及監察人（監事、監事會）或審計委員會報告。但本國銀行以外之銀行業，得不設置專責單位，惟仍應依其規模、風險等配置適足之防制洗錢及打擊資恐人員，由董事會指派一人為專責主管，並確保該等人員及主管無與其防制洗錢及打擊資恐職責有利益衝突之兼職。

（二）前項專責單位或專責主管掌理下列事務：

1.督導洗錢及資恐風險之辨識、評估及監控政策及程序之規劃與執行。

2.協調督導全面性洗錢及資恐風險辨識及評估之執行。

3.監控與洗錢及資恐有關之風險。

4.發展防制洗錢及打擊資恐計畫。

5.協調督導防制洗錢及打擊資恐計畫之執行。

6.確認防制洗錢及打擊資恐相關法令之遵循，包括所屬金融同業公會所定並經本會准予備查之相關範本或自律規範。

7.督導向法務部調查局進行可疑交易申報及資恐防制法指定對象之財物或財產上利益及其所在地之申報事宜。

（三）銀行業國外營業單位應綜合考量在當地之分行家數、業務規模及風險等，設置適足之防制洗錢及打擊資恐人員，並指派一人為主管，負責執行防制洗錢及打擊資恐法令遵循事宜。

（四）銀行業國外營業單位防制洗錢及打擊資恐主管之設置應符合當地法令規定及當地主管機關之要求，並應具備執行防制洗錢及打擊資恐之充分職權，包括可直接向第一款專責主管報告，且除兼任法令遵循主管外，應為專任，如兼任其他職務，應與當地主管機關溝通，以確認其兼任方式無利益衝突之虞，並報主管機關備查。

十七、防制洗錢及打擊資恐內部控制制度之執行及聲明：

（一）銀行業國內外營業單位應指派資深管理人員擔任督導主管，負責督導所屬營業單位執行防制洗錢及打擊資恐相關事宜，並依「金融控股公司及銀行業內部控制及稽核制度實施辦法」相關規定辦理自行查核。

（二）銀行業內部稽核單位應依「金融控股公司及銀行業內部控制及稽核制度實施辦法」規定辦理下列事項之查核，並提具查核意見：

1.洗錢及資恐風險評估與防制洗錢及打擊資恐計畫是否符合法規要求並落實執行。

2.防制洗錢及打擊資恐計畫之有效性。

（三）銀行業總經理應督導各單位審慎評估及檢討防制洗錢及打擊資恐內部控制制度執行情形，由董（理）事長（主席）、總經理、總稽核、防制洗錢及打擊資恐專責主管聯名出具防制洗錢及打擊資恐之內部控制制度聲明書（附表），並提報董（理）事會通過，於每會計年度終了後三個月內將該內部控制制度聲明書內容揭露於銀行業網站，並於主管機關指定網站辦理公告申報。

十八、員工任用及訓練：

（一）銀行業應建立審慎適當之員工遴選及任用程序，包括檢視員工是否具備廉正品格，及執行其職責所需之專業知識。

（二）銀行業之防制洗錢及打擊資恐專責主管、專責單位人員及國內營業單位督導主管應具下列資格條件之一：

1.曾擔任專責之法令遵循或防制洗錢及打擊資恐人員三年以上者。

2.參加主管機關認定機構所舉辦二十四小時以上課程，並經考試及格且取得結業證書。但中華民國一百零六年六月三十日前充任者，專責主管及專責單位人員得於充任後半年內取得證書，國內營業單位督導主管得於充任後一年內取得證書者。

3.取得主管機關認定機構舉辦之國內或國際防制洗錢及打擊資恐專業人員證照者。

（三）銀行業之防制洗錢及打擊資恐專責主管、專責單位人員及國內營業單位督導主管，每年應至少參加主管機關認定機構所舉辦或所屬金融控股公司（含子公司）或銀行業（含母公司）自行舉辦十二小時之教育訓練，訓練內容應至少包括新修正法令、洗錢及資恐風險趨勢及態樣。當年度取得主管機關認定機構舉辦之國內或國際防制洗錢及打擊資恐專業人員證照者，得抵免當年度之訓練時數。

（四）國外營業單位之督導主管與防制洗錢及打擊資恐主管、人員，應至少

參加由國外主管機關或相關單位舉辦之防制洗錢及打擊資恐教育訓練課程十二小時，如國外主管機關或相關單位未舉辦防制洗錢及打擊資恐教育訓練課程，得參加主管機關認定機構所舉辦或所屬金融控股公司（含子公司）或銀行業（含母公司）自行舉辦之教育訓練課程。

（五）銀行業法令遵循人員、內部稽核人員及業務人員，應依其業務性質，安排適當內容及時數之防制洗錢及打擊資恐職前訓練及在職訓練，以使其瞭解所承擔之防制洗錢及打擊資恐職責，及具備執行該職責應有之專業。

十九、銀行業違反本注意事項所定事項者，本會將視其情節之輕重，依銀行法第六十一條之一、第一百二十九條規定及洗錢防制法等相關法令處分。

【訂定高洗錢及資恐風險區域名單之參考依據】

金融監督管理委員會函轉國際防制洗錢組織所公告防制洗錢與打擊資助恐怖份子有嚴重缺失之國家或地區、及其他未遵循或未充分遵循國際防制洗錢組織建議之國家或地區。受聯合國、美國或歐盟經濟制裁或採取其他類似措施的國家或地區。國際貨幣基金組織(International Monetary Fund)所公布之境外金融中心的國家或地區。

美國財政部愛國者法案 Section 311 (USA PATRIOT Act’s Section 311) 指定有重大洗錢疑慮之國家或地區(Special Measures for Jurisdictions, Financial Institutions, or International Transactions of Primary Money Laundering Concern.)。國際透明組織之貪腐印象指數所列具相當貪瀆程度之國家或地區(Transparency International's Corruption Perceptions Index.)。提供資金或支持恐怖主義(如美國國務院發布之 State Sponsors of Terrorism)或有被列名之恐怖分子團體活動之國家或地區。

為防制洗錢，打擊犯罪，自民國 104 年 1 月 1 日起，代理親友辦理現金交易。若不是到被代理人開戶銀行，須提供：1.被代理人身分證明文件、2.代理事實證明及代理人身分證明文件、3.出資超過 25%以上自然人身分證明文件、4.代理事實證明及代理人身分證明文件建議民眾至被代理人開戶銀行辦理交易，省時省麻煩。代理法人辦理現金交易，則須提供：1.法人登記證明文件、2.出資證明文件。

附錄九：金融科技國際發展與國內現況

資料來源：金融科技發展策略白皮書

金融科技的概念及應用已存在六十多個年頭。1950 年代美國加洲的富蘭克林國民銀行首先發行了信用卡，讓人們出外購物時，不再需要以實體貨幣的形式支付。1960 年代，英國倫敦北部的巴克萊銀行出現第一台自動提款的 ATM ，取代銀行櫃台和分行的角色。隨後的十幾年，Charles Schwab 成了第一個擁抱新的交易規則的證券交易商。這個新規定廢除了固定佣金。在此之前，數以百萬計家戶的投資機會是受到限制的。遊戲規則在 1975 年被改變，當證券交易商對於佣金的限制被 SEC 打破。

1990 年代，網路和電子商務發展日新月異，且線上股票交易改變佣金的形式。很多公司被包含在這波線上交易行動的浪潮。例如 1994 年的八月，K. Aufhauser & Company 成為第一家透過自身的 WealthWEB 提供線上交易的券商，或者像 Datek 是一家在 1970 年建立的證券經紀商，並在 1996 年提供了線上零售交易的服務。

當 PayPal 在 1998 年 12 月成立，意味著第一個給網路客戶的銀行品牌成立。當時大家沒有辦法把這概念和科技做連結，因為「金融科技」這概念當時尚未被提及。PayPal 並沒有受到如同銀行的管制，但它是和線上銀行最接近的一種形式。一開始以 Confinity 的名稱成立，接著才和 X.com 合併。這是一個非常遠大的目標-透過 email 寄送現金，並且這家公司藉由 eBay 的買賣雙方找到了利基市場。PayPal 在 2002 年 IPO，接著變成 eBay 完全持有的子公司。

「網路 2.0」從 2004 年開始變成一個非常受歡迎的階段，用來描述網路的第二次崛起。千禧年的第一個十年，P2P 借貸模式、機器人顧問、比特幣、支付等金融科技的崛起，搭配 iPhone 的推出，代表了一種所有產業很會就會被科技打亂的前奏。智慧型手機在這個階段允許所有產業的創新可以百花齊放。人們隨身攜帶智慧型手機，如同個人電腦可以隨時連接到網路。

目前金融科技公司（例如：LendingClub 、OnDeck ）逐漸踏上 IPO 的階段。相信金融科技的創新還會再延續到未來，創造出更多的改變。

一、國際發展

經濟學人雜誌（The Economists）2015 年 5 月 9 日特別報導「Slings and Arrows」，描繪金融科技對銀行業所帶來的挑戰；世界經濟論壇（World Economic Forum, WEF）2015 年 6 月研究報告「The Future of Financial Services」，分析金融服務業的未來，破壞性創新如何重塑金融服務業結構、供應及消費；銀行家雜誌（The Banker）2015 年 8 月封面故事「Wealth Manager Robot」，探討無需面對客

戶藉由線上投資平台機器人理財顧問，提供個人化投資管理及建議的現象。面對科技業者積極投入研發創新各項金融服務應用，當前金融機構面臨的經營環境變化及競爭壓力更甚以往。

金融服務在創新應用上有其特殊性，從小處著手，縝密分析設計，提升客戶體驗，解決顧客問題，藉由網路各種服務平台與大數據資料來源，以小額資本即可開業提供服務，銀行業最先受到衝擊，美國有線電視新聞網（CNN）2015 年 7 月報導 1，由於消費者轉向使用行動服務，美國銀行（Bank of America）在過去兩年縮減 10%的分行數，員工數減少 15%，ATM 數量刪減 2%，其他如摩根大通（J.P. Morgan）、花旗等大銀行也在縮減分行規模。美國銀行關閉實體分行與刪減人力的同時，透過增加網路銀行業務留住客戶。2015 年起我國也有銀行開始裁撤分行，形勢之嚴峻可見一斑。因金融科技創新而產生勞動力節省幅度相當龐大，可以預見擁有最多從業人員的保險業者，將會受到最大的衝擊。

國際機構調查顯示，2014 年全球金融科技投資額為 67 億美元，2015 年成長 2 倍之多高達 138 億美元，其中美國投資額 73.9 億美元占比超過 5 成，歐洲 14.8 億美元，亞洲為 45.2 億美元。目前全球金融科技前 3 大發展聚落城市分別為矽谷、紐約及倫敦。此外，包括中國大陸、新加坡、韓國、澳洲、以色列台拉維夫及香港等地亦是發展重鎮，亞太地區的發展更不容小覷，金融科技研發與投資已蔚為趨勢。其快速發展之關鍵因素可歸納為政府政策支持、創投資金挹注、豐沛技術人才與成熟商業環境等，綜整各國在推動金融創新概況，說明如次：

（一）美國

美國金融環境競爭激烈，金融業為突破現有法規如賦稅、經營業務及地點限制，以及滿足客戶多變需求，而推出可能挑戰現行法令之創新商品，再遊說監理機關放寬規定或立法管理。美國以新創業者為創新驅動之核心，主管機關多為被動因應金融業者創新行為，雖未訂有專法或專區鼓勵金融創新，卻能成為金融科技之發展重鎮，在於其擁有世界金融中心紐約華爾街的環境，矽谷高科技人才，與資本雄厚的創投基金等優異條件。

（二）英國

英國金融行為監理總署（Financial Conduct Authority, FCA）於 2014 年公布創新計畫（Project Innovate），支持與鼓勵業者提出更多的創新，具體作法成立育成中心（Incubator）與創新樞紐（Innovation Hub）等 2 個單位，提供新創事業輔導與諮詢，協助與主管機關溝通，但不降低對新創業者之許可標準。創新樞紐所投注之資源，必須是真正創新、有利於消費者及具商業上可行性之企業。

（三）新加坡

新加坡推動智慧國家計畫，打造智慧金融中心，首要之務為持續加強產業的

網路安全，對培植創新及採用新技術的監管採取三種形式：金融機構自行的創新、沙箱（Sandbox）中的創新、金管局與業界共同合作的創新。除營造有利創新又不致忽略監管的適宜環境外，並與業界合作制定智慧金融中心發展策略，措施包括「金融領域科技和創新計劃」（Financial Sector Technology & Innovation Scheme, FSTI），預估未來 5 年將投入 2 億 2,500 萬新幣，以支持創造有活力的創新產業生態，另外亦將發展便捷安全數位及行動支付系統、技術支持的監管報告系統及智慧監控系統、支持 FinTech 產業生態以及人才培育。新加坡政府宣布 3 在 2016 年 5 月 3 日成立金融科技辦公室（FinTech Office），作為新加坡金融科技樞紐，提供一站式服務。

（四）韓國

韓國於 2014 年 8 月推出「Creative Finance」行動計畫，政策著重科技與金融發展，消除非必要法規，重點有二，第一調和科技與金融業，草擬無實體網路銀行，設立金融科技支援系統以提供法規及財務諮詢，其二為強化金融業之競爭力，將修訂電子金融交易法、拓展新商業領域、促進國際競爭力；另外挹注資金至新創產業。

（五）澳洲

澳洲政府 2014 年 12 月發布「金融系統調查」（Financial System Inquiry, FSI）最終報告，對於未來 10 年金融體系藍圖提出 44 項建議，包括復原力及競爭力、創新、退休金、消費者成果、法規系統等 5 個面向。鑑於科技驅動之創新已轉變金融系統，建議 7 項鼓勵創新重點，包括公私部門合作、發展澳洲電子認證架構、強化零售支付相關法規、交換系統費用及客戶附加費用、群眾募資、資料取得與使用、綜合信用報告等。2016 年 2 月 24 日由首相及財政部長成立金融科技諮詢顧問團 4（FinTech advisory group）以加速推動金融科技創新服務。

（六）中國大陸

2015 年 7 月由中國人民銀行等 10 部委發布「關於促進互聯網金融健康發展的指導意見」，按照「鼓勵創新、防範風險、趨利避害、健康發展」的總體要求，積極鼓勵互聯網金融平台、產品和服務創新，鼓勵從業機構相互合作，拓寬從業機構融資管道，推動信用基礎設施建設和配套服務體系建設。按照「依法監管、適度監管、分類監管、協同監管、創新監管」的原則，確立互聯網支付、網路借貸、股權眾籌融資、互聯網基金銷售、互聯網保險、互聯網信託和互聯網消費金融等互聯網金融主要業態的監管職責分工。大陸國務院 2015 年 8 月 31 日亦發布「促進大數據發展行動綱要」，將數據視為國家基礎性戰略資源，運用大數據推動經濟發展、完善社會治理、提升政府服務和監管能力。

為跟上市場與技術變化的步伐，提供金融新創事業的發展環境，培養創新與

分析能力，加強跨業合作，綜整各國在推動金融科技方面的作法，可歸納如次：

（一）法規調適

英國（創新計畫）、新加坡（成立金融科技和創新部門）、韓國（放寬 IT 與金融相關法規、修法促進創投）、澳洲（強化零售支付相關法規）、美國（金融總會提升金融法規制訂透明度）。

（二）成立相關諮詢協調單位或機構

英國（育成中心及創新樞紐）、香港（金融科技督導小組）、新加坡（金融科技辦公室）、韓國（金融科技支援系統）、澳洲（金融科技諮詢顧問團）、美國（金融總會－銀行科技部門）。

（三）設置相關研發單位

新加坡（金融科技創新實驗室）。

（四）提供租稅、補助、擔保融資

新加坡（提供新創公司前 3 年的免稅優惠、若能提升產業水準，則可享 15 年優惠）、韓國（科技擔保借款、創投資本）、以色列（天使投資減免租稅）。

二、國內現況

現今金融業所面臨之挑戰，不僅是國內同業的激烈競爭，更要適應行動網路時代興起，科技創新快速發展，全球商業模式變革引進的非金融業者進入市場。故金管會自 2014 年起積極打造數位化金融環境，協助金融服務業引入科技創新思維以支援產業發展。

（一）擴大線上金融服務

1.銀行業：已開放銀行得於線上提供存款、授信、信用卡、財富管理及共同行銷等 12 項服務及線上開戶，民眾可透過線上申辦開戶、結清銷戶、信用貸款、增貸房貸車貸、信用卡、信託開戶及同意共同行銷等。對於銀行辦理低風險交易之電子銀行業務，簡化作業程序，由其法遵部門、稽核部門及資訊部門確認相關作業方式符合金融機構辦理電子銀行業務安全控管作業基準、相關定型化契約等相關法令規定後即可開辦。

2.證券業：2015 年 6 月放寬證券商得委由往來銀行確認身分等方式，開放新客戶可採非當面開戶，2015 年 1 至 12 月電子下單筆數平均比重為 48.3%（電子式下單金額平均比重為 44.1%），未來電子下單比重可望逐步提升。

3.保險業：在開放網路投保方面，自 2014 年 8 月 26 日開辦迄今已完成 4 階段開放措施，包括進一步擴大開放網路投保之險種、提高投保額度、增加網路保險服務，以及放寬要保人、被保險人不同人可以自然人憑證投保等，同時要求保險業應強化資訊安全。

（二）普及行動支付服務

為鼓勵金融機構推展多元行動支付服務，截至 2015 年 12 月底止，金管會已同意 24 家銀行或機構辦理手機信用卡、18 家辦理行動金融卡、1 家辦理行動 X 卡、20 家辦理 QR Code 行動支付，及 9 家辦理 mPOS 行動收單業務。2015 年 8 月再開放電子票證發行機構可委託信用卡收單機構辦理收單業務之推廣，便利來台旅客及民眾小額消費付款，加快商家結帳速度、減少現金管理風險。

（三）開放電子支付機構業務，協助電子商務發展

電子支付機構管理條例已於 2015 年 5 月 3 日施行，參採國外相關法規之運作機制，賦予原則性與開放性之內涵，並保留主管機關未來開放其他業務項目之空間，以鼓勵業者積極創新與發展新型態支付服務，規範電子支付機構業務範圍，除立法前原即得辦理之代理收付實質交易款項外，新增開放收受儲值款項（含外幣儲值）及無實質交易基礎之資金移轉（電子支付帳戶間款項移轉）服務。

本條例施行後，預估將可增加個人及網路商店家數成長，帶動整體電子商務產業產值，對於扶植我國電子商務產業發展、國內支付服務創新，以及協助青年創業與保護消費者權益，均具重大效益。

（四）推動金融大數據分析應用

運用大數據分析業已成為產業發展的重要趨勢，金管會於 2015 年度共推動 12 項大數據應用案，同時亦針對民眾需求及協助產業發展考量，積極公開相關金融資料，截至 2015 年底前達成開放 1,032 項以上資料集。

（五）開放金融業轉投資金融科技業

已開放金融控股公司、銀行、證券期貨業及保險業可 100%轉投資從事與金融機構業務密切相關之金融科技事業，包括大數據資料分析應用、雲端科技、機器學習、生物辨識、自動化投資理財顧問、區塊鏈技術等。

（六）成立金融科技辦公室

金管會於 2015 年 9 月成立金融科技辦公室，並已召開 3 次金融科技諮詢委員會會議，啟動國內電子支付倍增計畫，並積極推動銀行、證券、保險及生物辨識等金融科技應用。

附錄十：Money Laundering Control Act of 1986

TITLE 18 > PART I > CHAPTER 95 > § 1956

§ 1956. Laundering of monetary instruments

(a)

(1) Whoever, knowing that the property involved in a financial transaction represents the proceeds of some form of unlawful activity, conducts or attempts to conduct such a financial transaction which in fact involves the proceeds of specified unlawful activity—

(A)

(i) with the intent to promote the carrying on of specified unlawful activity; or

(ii) with intent to engage in conduct constituting a violation of section 7201 or 7206 of the Internal Revenue Code of 1986; or

(B) knowing that the transaction is designed in whole or in part—

(i) to conceal or disguise the nature, the location, the source, the ownership, or the control of the proceeds of specified unlawful activity; or

(ii) to avoid a transaction reporting requirement under State or Federal law,shall be sentenced to a fine of not more than $500,000 or twice the value of the property involved in the transaction, whichever is greater, or imprisonment for not more than twenty years, or both.

(2) Whoever transports, transmits, or transfers, or attempts to transport, transmit, or transfer a monetary instrument or funds from a place in the United States to or through a place outside the United States or to a place in the United States from or through a place outside the United States—

(A) with the intent to promote the carrying on of specified unlawful activity; or

(B) knowing that the monetary instrument or funds involved in the transportation, transmission, or transfer represent the proceeds of some form of unlawful activity and knowing that such transportation, transmission, or transfer is designed in whole or in part—

(i) to conceal or disguise the nature, the location, the source, the ownership, or the control of the proceeds of specified unlawful activity; or

(ii) to avoid a transaction reporting requirement under State or Federal law, shall be sentenced to a fine of not more than $500,000 or twice the value of the monetary instrument or funds involved in the transportation, transmission, or transfer, whichever is greater, or imprisonment for not more than twenty years, or both. For the purpose of the offense described in subparagraph (B), the defendant’s knowledge may be established by proof that a law enforcement officer represented the matter specified in

subparagraph (B) as true, and the defendant's subsequent statements or actions indicate that the defendant believed such representations to be true.

(3) Whoever, with the intent—

(A) to promote the carrying on of specified unlawful activity;

(B) to conceal or disguise the nature, location, source, ownership, or control of property believed to be the proceeds of specified unlawful activity; or

(C) to avoid a transaction reporting requirement under State or Federal law, conducts or attempts to conduct a financial transaction involving property represented to be the proceeds of specified unlawful activity, or property used to conduct or facilitate specified unlawful activity, shall be fined under this title or imprisoned for not more than 20 years, or both. For purposes of this paragraph and paragraph (2), the term "represented" means any representation made by a law enforcement officer or by another person at the direction of, or with the approval of, a Federal official authorized to investigate or prosecute violations of this section.

(b) Penalties.—

(1) In general.— Whoever conducts or attempts to conduct a transaction described in subsection (a)(1) or (a)(3), or section 1957, or a transportation, transmission, or transfer described in subsection (a)(2), is liable to the United States for a civil penalty of not more than the greater of—

(A) the value of the property, funds, or monetary instruments involved in the transaction; or

(B) $10,000.

(2) Jurisdiction over foreign persons.— For purposes of adjudicating an action filed or enforcing a penalty ordered under this section, the district courts shall have jurisdiction over any foreign person, including any financial institution authorized under the laws of a foreign country, against whom the action is brought, if service of process upon the foreign person is made under the Federal Rules of Civil Procedure or the laws of the country in which the foreign person is found, and—

(A) the foreign person commits an offense under subsection (a) involving a financial transaction that occurs in whole or in part in the United States;

(B) the foreign person converts, to his or her own use, property in which the United States has an ownership interest by virtue of the entry of an order of forfeiture by a court of the United States; or

(C) the foreign person is a financial institution that maintains a bank account at a financial institution in the United States.

(3) Court authority over assets.— A court described in paragraph (2) may issue a pretrial restraining order or take any other action necessary to ensure that any bank

account or other property held by the defendant in the United States is available to satisfy a judgment under this section.

(4) Federal receiver.—

(A) In general.— A court described in paragraph (2) may appoint a Federal Receiver, in accordance with subparagraph (B) of this paragraph, to collect, marshal, and take custody, control, and possession of all assets of the defendant, wherever located, to satisfy a civil judgment under this subsection, a forfeiture judgment under section 981 or 982, or a criminal sentence under section 1957 or subsection (a) of this section, including an order of restitution to any victim of a specified unlawful activity.

(B) Appointment and authority.— A Federal Receiver described in subparagraph (A)—

(i) may be appointed upon application of a Federal prosecutor or a Federal or State regulator, by the court having jurisdiction over the defendant in the case;

(ii) shall be an officer of the court, and the powers of the Federal Receiver shall include the powers set out in section 754 of title 28, United States Code; and

(iii) shall have standing equivalent to that of a Federal prosecutor for the purpose of submitting requests to obtain information regarding the assets of the defendant—

(I) from the Financial Crimes Enforcement Network of the Department of the Treasury; or

(II) from a foreign country pursuant to a mutual legal assistance treaty, multilateral agreement, or other arrangement for international law enforcement assistance, provided that such requests are in accordance with the policies and procedures of the Attorney General.

(c) As used in this section—

(1) the term "knowing that the property involved in a financial transaction represents the proceeds of some form of unlawful activity" means that the person knew the property involved in the transaction represented proceeds from some form, though not necessarily which form, of activity that constitutes a felony under State, Federal, or foreign law, regardless of whether or not such activity is specified in paragraph (7);

(2) the term "conducts" includes initiating, concluding, or participating in initiating, or concluding a transaction;

(3) the term "transaction" includes a purchase, sale, loan, pledge, gift, transfer, delivery, or other disposition, and with respect to a financial institution includes a

deposit, withdrawal, transfer between accounts, exchange of currency, loan, extension of credit, purchase or sale of any stock, bond, certificate of deposit, or other monetary instrument, use of a safe deposit box, or any other payment, transfer, or delivery by, through, or to a financial institution, by whatever means effected;

(4) the term "financial transaction" means

(A) a transaction which in any way or degree affects interstate or foreign commerce

(i) involving the movement of funds by wire or other means or

(ii) involving one or more monetary instruments, or

(iii) involving the transfer of title to any real property, vehicle, vessel, or aircraft, or

(B) a transaction involving the use of a financial institution which is engaged in, or the activities of which affect, interstate or foreign commerce in any way or degree;

(5) the term "monetary instruments" means

(i) coin or currency of the United States or of any other country, travelers' checks, personal checks, bank checks, and money orders, or

(ii) investment securities or negotiable instruments, in bearer form or otherwise in such form that title thereto passes upon delivery;

(6) the term "financial institution" includes—

(A) any financial institution, as defined in section 5312 (a)(2) of title 31, United States Code, or the regulations promulgated thereunder; and

(B) any foreign bank, as defined in section 1 of the International Banking Act of 1978 (12 U.S.C. 3101);

(7) the term "specified unlawful activity" means—

(A) any act or activity constituting an offense listed in section 1961 (1) of this title except an act which is indictable under subchapter II of chapter 53 of title 31;

(B) with respect to a financial transaction occurring in whole or in part in the United States, an offense against a foreign nation involving—

(i) the manufacture, importation, sale, or distribution of a controlled substance (as such term is defined for the purposes of the Controlled Substances Act);

(ii) murder, kidnapping, robbery, extortion, destruction of property by means of explosive or fire, or a crime of violence (as defined in section 16);

(iii) fraud, or any scheme or attempt to defraud, by or against a foreign bank (as defined in paragraph 7 of section 1(b) of the International Banking Act of 1978));

(iv) bribery of a public official, or the misappropriation, theft, or embezzlement

of public funds by or for the benefit of a public official;

(v) smuggling or export control violations involving—

(I) an item controlled on the United States Munitions List established under section 38 of the Arms Export Control Act (22 U.S.C. 2778); or

(II) an item controlled under regulations under the Export Administration Regulations (15 C.F.R. Parts 730–774); or

(vi) an offense with respect to which the United States would be obligated by a multilateral treaty, either to extradite the alleged offender or to submit the case for prosecution, if the offender were found within the territory of the United States;

(C) any act or acts constituting a continuing criminal enterprise, as that term is defined in section 408 of the Controlled Substances Act (21 U.S.C. 848);

(D) an offense under section 32 (relating to the destruction of aircraft), section 37 (relating to violence at international airports), section 115 (relating to influencing, impeding, or retaliating against a Federal official by threatening or injuring a family member), section 152 (relating to concealment of assets; false oaths and claims; bribery), section 215 (relating to commissions or gifts for procuring loans), section 351 (relating to congressional or Cabinet officer assassination), any of sections 500 through 503 (relating to certain counterfeiting offenses), section 513 (relating to securities of States and private entities), section 541 (relating to goods falsely classified), section 542 (relating to entry of goods by means of false statements), section 545 (relating to smuggling goods into the United States), section 549 (relating to removing goods from Customs custody), section 641 (relating to public money, property, or records), section 656 (relating to theft, embezzlement, or misapplication by bank officer or employee), section 657 (relating to lending, credit, and insurance institutions), section 658 (relating to property mortgaged or pledged to farm credit agencies), section 666 (relating to theft or bribery concerning programs receiving Federal funds), section 793, 794, or 798 (relating to espionage), section 831 (relating to prohibited transactions involving nuclear materials), section 844 (f) or (i) (relating to destruction by explosives or fire of Government property or property affecting interstate or foreign commerce), section 875 (relating to interstate communications), section 922 (l) (relating to the unlawful importation of firearms), section 924 (n) (relating to firearms trafficking), section 956 (relating to conspiracy to kill, kidnap, maim, or injure certain property in a foreign country), section 1005 (relating to fraudulent bank entries), 1006 (relating to fraudulent Federal credit institution entries), 1007 [2] (relating to

Federal Deposit Insurance transactions), 1014 (relating to fraudulent loan or credit applications), section 1030 (relating to computer fraud and abuse), 1032 [2] (relating to concealment of assets from conservator, receiver, or liquidating agent of financial institution), section 1111 (relating to murder), section 1114 (relating to murder of United States law enforcement officials), section 1116 (relating to murder of foreign officials, official guests, or internationally protected persons), section 1201 (relating to kidnapping), section 1203 (relating to hostage taking), section 1361 (relating to willful injury of Government property), section 1363 (relating to destruction of property within the special maritime and territorial jurisdiction), section 1708 (theft from the mail), section 1751 (relating to Presidential assassination), section 2113 or 2114 (relating to bank and postal robbery and theft), section 2280 (relating to violence against maritime navigation), section 2281 (relating to violence against maritime fixed platforms), section 2319 (relating to copyright infringement), section 2320 (relating to trafficking in counterfeit goods and services), section 2332 (relating to terrorist acts abroad against United States nationals), section 2332a (relating to use of weapons of mass destruction), section 2332b (relating to international terrorist acts transcending national boundaries), or section 2339A or 2339B (relating to providing material support to terrorists) of this title, section 46502 of title 49, United States Code, a felony violation of the Chemical Diversion and Trafficking Act of 1988 (relating to precursor and essential chemicals), section 590 of the Tariff Act of 1930 (19 U.S.C. 1590) (relating to aviation smuggling), section 422 of the Controlled Substances Act (relating to transportation of drug paraphernalia), section 38 (c) (relating to criminal violations) of the Arms Export Control Act, section 11 (relating to violations) of the Export Administration Act of 1979, section 206 (relating to penalties) of the International Emergency Economic Powers Act, section 16 (relating to offenses and punishment) of the Trading with the Enemy Act, any felony violation of section 15 of the Food Stamp Act of 1977 (relating to food stamp fraud) involving a quantity of coupons having a value of not less than $5,000, any violation of section 543(a)(1) of the Housing Act of 1949 (relating to equity skimming), any felony violation of the Foreign Agents Registration Act of 1938, or any felony violation of the Foreign Corrupt Practices Act; environmental crimes

(E) a felony violation of the Federal Water Pollution Control Act (33 U.S.C. 1251 et seq.), the Ocean Dumping Act (33 U.S.C. 1401 et seq.), the Act to Prevent Pollution from Ships (33 U.S.C. 1901 et seq.), the Safe Drinking

Water Act (42 U.S.C. 300f et seq.), or the Resources Conservation and Recovery Act (42 U.S.C. 6901 et seq.); or

(F) any act or activity constituting an offense involving a Federal health care offense;

(8) the term "State" includes a State of the United States, the District of Columbia, and any commonwealth, territory, or possession of the United States.

(d) Nothing in this section shall supersede any provision of Federal, State, or other law imposing criminal penalties or affording civil remedies in addition to those provided for in this section.

(e) Violations of this section may be investigated by such components of the Department of Justice as the Attorney General may direct, and by such components of the Department of the Treasury as the Secretary of the Treasury may direct, as appropriate and, with respect to offenses over which the United States Postal Service has jurisdiction, by the Postal Service. Such authority of the Secretary of the Treasury and the Postal Service shall be exercised in accordance with an agreement which shall be entered into by the Secretary of the Treasury, the Postal Service, and the Attorney General. Violations of this section involving offenses described in paragraph (c)(7)(E) may be investigated by such components of the Department of Justice as the Attorney General may direct, and the National Enforcement Investigations Center of the Environmental Protection Agency.

(f) There is extraterritorial jurisdiction over the conduct prohibited by this section if—

(1) the conduct is by a United States citizen or, in the case of a non-United States citizen, the conduct occurs in part in the United States; and

(2) the transaction or series of related transactions involves funds or monetary instruments of a value exceeding $10,000.

(g) Notice of Conviction of Financial Institutions.— If any financial institution or any officer, director, or employee of any financial institution has been found guilty of an offense under this section, section 1957 or 1960 of this title, or section 5322 or 5324 of title 31, the Attorney General shall provide written notice of such fact to the appropriate regulatory agency for the financial institution.

(h) Any person who conspires to commit any offense defined in this section or section 1957 shall be subject to the same penalties as those prescribed for the offense the commission of which was the object of the conspiracy.

(i) Venue.—

(1) Except as provided in paragraph (2), a prosecution for an offense under this section or section 1957 may be brought in—

(A) any district in which the financial or monetary transaction is conducted; or

(B) any district where a prosecution for the underlying specified unlawful

activity could be brought, if the defendant participated in the transfer of the proceeds of the specified unlawful activity from that district to the district where the financial or monetary transaction is conducted.

(2) A prosecution for an attempt or conspiracy offense under this section or section 1957 may be brought in the district where venue would lie for the completed offense under paragraph (1), or in any other district where an act in furtherance of the attempt or conspiracy took place.

(3) For purposes of this section, a transfer of funds from 1 place to another, by wire or any other means, shall constitute a single, continuing transaction. Any person who conducts (as that term is defined in subsection (c)(2)) any portion of the transaction may be charged in any district in which the transaction takes place.

附錄十一：國外金融業蒐集風險資料相關實務議題

資料來源：金融聯合徵信中心研究資料(金融聯合徵信雙月刊第九期)

自從巴塞爾銀行監理委員會將作業風險資本計提明文規範於 Basel Ⅱ後，相關議題所受到的重視程度與過去大為不同，但部分資料蒐集相關議題雖於條文中提及，卻未給予明確定義或評估標準，這一方面代表委員會給予各國主管機關裁量的彈性，另一方面亦代表金融機構對於相同的作業風險事件處理方式可能不一致，於在商言商的遊戲規則下，自行發展的處理原則很自然地以自身利益考量為依歸，並影響作業風險資本計提結果；這樣的結果或許不是各國主管機關或巴塞爾委員會所樂見，但亦不應因此苛責這些機構，因相對於其他在作業風險管理領域剛起步的同業，這些機構已經投注大量資源研究，並且在內部建立完整的架構與遵循程序。

由於作業風險管理發展的高度彈性，導致實務作法的發展多變，因此巴塞爾委員會於 2008 年中號召銀行進行損失資料的試行報送，內容涵蓋進階衡量法計算資本計提所需的四大類資料－內部損失資料、外部損失資料、情境分析、企業環境與內部控制因子（business environment and internal control factors, BEICFs)，期望能透過本次調查提供金融業界有別於一般國際性與區域性的資料蒐集與 AMA 實行標竿。

就現況而言，業界在作業風險議題所面臨的主要挑戰包括：資料蒐集、內部管理、模型量化三個層面，而資料議題是整個架構的基礎，唯有充分、高品質的資訊方能協助引導正確的內部管理決策，並進行關鍵風險指標與資本計提模型的發展；本文摘錄巴塞爾銀行監理委員會之研究，挑選其中較特殊之內容與國內金融同業分享。

國際作業風險資料之實務處理

作業風險資料的性質與品質不光是影響銀行的量化分析，同時也影響內部管理之決策，依資料類型與來源可分為 BEICFs 四類，在此著重於內部損失資料議題的國外實務介紹。

內部損失事件發生日

一般而言，損失事件被發現通常都在發生後一段時間，則其發生日應如何決定？新資本協定的規範中，雖指出需記錄損失事件相關日期，但卻未指導那些時間點是應該被記錄的，因此導致了銀行間實務做法的差異以及資本計算上的不同，尤其是重大損失事件的記錄影響更為廣泛，將衝擊該時間點及後續期間銀行作業風險概觀的評估以及資本計提結果。

銀行在此的處理方式受到會計與提存實務的強烈影響，因此其所採用的發生日期可能與實際日期不一致，而且也可能不具有直覺。訴訟的案例在此議題上就提供很好的說明，因為訴訟通常花費超過一年的時間，如果銀行在當年度的結帳

日就認列這筆損失，並用於計算作業風險資本計提，則一方面必須對相關的業務別增加資本配置，另一方面因為認列的金額是預估值，則日後還需用實際損失數再做調整，這樣的做法將對資本配置架構造成額外的負擔，並可能因頻繁的調整而讓其資本計提之可信度遭受質疑；此外，銀行在損失事件發生後，均會盡快研擬相關的改進措施，在這樣的情況下，採用會計入帳日以迅速將損失事件反映在資本計提上的意義也相對減弱。

實務上，國外銀行通常會由事件發生日、事件發現日、會計入帳日三個日期，擇一作為損失事件的時間點，而銀行通常較偏好採用事件發生日或事件發現日，因事件發生或發現日期之採用，並不需對外公開內部之預估損失，但若需於會計帳上揭露則不同；另一個原因則是因為在某些法律管轄區域，指導這些費用認列的會計準則有確定性的要求，且考量提早公開認列這些潛在損失將影響法律裁罰的可能性與金額；我國外部損失資料庫目前只規劃蒐集事件發生日與事件發現日兩個時間點，且對於損失事件蒐集範圍以是否實際產生支付金額或資產減損為準，而不論該事件是否列入損益表，故會計入帳日當初在規劃上即未納入考量。

內部損失之評估方法

內部損失毛額（gross loss）之金額在一般的認知上應該是個確切的數字，但實際上將受到對損失評估方法之影響。主要可分為對實體資產之損害估計（主要有帳面價值與市場價值兩種）或重置成本估計，而另外是否包含將損失情況復原所耗用的資源（如加班費），則是另一個影響損失毛額的因素。新資本協定中並未明確定義損失毛額，而在重大的實體資產減損事件上，不同的實務做法將可能在同樣的事件產生重大差異。

由於被損傷的實體資產必須被修理或重置，因此有主張認為損失毛額應能反應資產經濟價值減損的程度，在這樣的情況下重置成本或市場價值的使用較為恰當，然而，重置成本或市場價值常常可能無法被客觀估計，同時，在現行會計準則的限制下，帳面價值則有與經濟價值脫軌的問題存在，銀行對方法之選擇將影響後續驗證損失金額與主管機關的覆核程序，在這樣的考量下，採用帳面價值作為資本計提目的將可使驗證簡單明確。但必須注意的是，不論採用何種方法，在AMA 架構下對實質資產減損的資本處置方式，仍必需考量該行在新資本協定架構中，於信用風險部分對同樣資產的處理方式。

實務上，國外銀行通常於以下三種方法，擇一評估作業風險管理之實體資產減損議題：帳面價值、市場價值、重置成本。目前銀行使用這三種方法的比例相當，且可能會納入機會成本的概念，如加班等修復損害額外所用資源，並用於作業風險的管理與衡量；我國外部損失資料庫對於上述資產減損之評估方式並無限制，主因在於國內各銀行之會計制度與認列方式不同，在一致性上存有困難，且並無證據顯示何者為最佳之處理方式，故一般認為並無強制規定之必要；關於損失事件機會成本的評估，我國資料庫在衡量上已要求各報送單位排除，主因在於國內資料蒐集處於剛起步的階段，大部分的報送單位應無足夠能力進行評估，且

機會成本之認定，在評估的一致性基礎上存在困難，如此對於資料庫的品質並無助益，國外之外部損失資料庫就目前所見，也未蒐集機會成本相關資訊，故現階段在損失金額評估納入機會成本的概念，其使用上均侷限於銀行內部評估，有興趣的銀行建議可在行內嘗試估計。

在損失金額的驗證上，採帳面價值方式者，係透過與會計總帳比對的方式驗證損失金額，而其他銀行則運用風險控管或查核功能來驗證這些損失金額。

隨時間實現之內部損失

某些個別作業風險事件在發生一段時間後，許多隱藏性的損失才逐漸實現，或著在事件發生一段時間後，又因為相同的原因而再度發生，這裡所衍生的議題是銀行在風險衡量上應如何看待這些損失，以及應如何將這樣的事件反應於內部損失資料庫。

在某些案例中，隨時間逐步實現的損失將對資本計算造成重大影響。其中一個例子是一連串個別損失都肇因於相同的作業風險事件，但個別損失的金額低於資料蒐集門檻（threshold），若加總則超過，因個別損失未被記錄，則這個事件將不會被納入模型進行資本計算，在這種情況下，資料蒐集的門檻越
高，此類型事件的潛在影響也越大。

另一個例子是某段時間內一連串的損失事件肇因於相同原因，如果這些損失事件彼此間的關聯性未能反應於資料庫中，將可能造成低估銀行實際面臨的風險。銀行可能於內部損失資料庫中，運用以下類別對具關聯性的事件加以記錄，如相同的違法者、相同的損失類別、法定罰緩之成因、在定義的期間內對實體資產
之減損等，許多銀行用這些標準來辨識單一事件的所有相關損失，以用於內部管理與量化分析；國內外部損失資料庫對於單一事件之認定亦採相同態度，建議報送機構於判斷上可考量事件之風險成因，資料庫對於單一事件認定採取彈性處理的主因在於貼近銀行內部管理實務，避免採強硬的一致性規定致破壞實務上的合理認定，進而造成銀行管理上的困擾。

內部資料面向－機會成本與近乎造成損失事件

在作業風險資料蒐集的設計與實行過程，銀行必須決定所蒐集的內部損失資料在目的性方面之廣度，因為某些類型的資料需視銀行內部的運用方式才能決定其價值，例如機會成本與近乎造成損失事件，這些資料可能未包含於作業風險損失或事件中，且並未明確被納入新資本協定規範的內部損失資料範疇。機會成本的蒐集與否主要在損失衡量層面的不同，而近乎造成損失事件則因作業風險損失資料的缺乏而展現其價值，這兩種資訊提供管理決策參考，將有助於管理人更清楚了解銀行之作業風險暴險及其潛在影響，且可提供內部稽核討論作業流程改善的問題。然而，這類型的資料在衡量、運用與驗證上面具有相當難度，且需花費較高的成本在資料蒐集上。

在國外銀行實務上，這個領域的做法分歧，但相較而言，蒐集近乎造成損失事件資料者較蒐集機會成本者為多。許多蒐集近乎造成損失事件者，將其定義為可能導因於作業失敗的直接或間接損失，但最後被避免的，其中某些銀行當潛在損失超過資料蒐集門檻時，才記錄這類型的案例。這類型資料通常用於判斷作業風險趨勢以及其他作業流程或風險管理用途，因為並非實際損失案例，所以通常不會使用在量化分析，但可能會用於進行情境分析之發展。

此外必須注意到，內部資料蒐集的第一步在於辨識損失事件，然後判斷是否為作業風險事件，但近乎造成損失事件在定義或實際上並未真的發生損失，因此在資料辨識與蒐集的持續性上，具有相當難度，且業務端對於此類型事件潛在的不願報送，更增加資料蒐集的困難。

風險類型劃分－作業風險與信用、市場、其他風險之區分

損失事件風險類型的劃分常是內部資料庫所面臨的難題之一，有些事件很明確，但其他的可能模稜兩可，或者應該按比例分攤至各個風險類別較為恰當。新資本協定中規定，損失事件若同時與作業風險及市場風險相關時歸類為作業風險事件，並依此進行資本計提，但作業風險事件若與信用風險相關，其所適用的規範就變得模糊，Basel Ⅱ規定損失事件過去若被歸類為信用風險，則依信用風險相關規定進行資本計提，但對於過去未歸類為信用風險的事件則未加以說明；此外，作業風險的定義中排除聲譽與策略風險，但 Basel Ⅱ中對這兩種風險類型也沒有加以定義，於是在這些模糊地帶中問題也隨之而生，並導致後續風險分析與資本計提的落差。

新資本協定對各個風險類型採用不同的資本計提規範，因此風險分類對於資本計提結果的影響重大，而資本計提上的利差導致銀行有誘因去調整損失事件分類，使銀行在類似事件上的分類不同，這樣的情況導致納入作業風險評估的範圍與實情不符，進而對作業風險暴險之衡量產生偏誤。例如 AMA 銀行同時於信用風險上採用 FIRB 法者，可能將作業風險的重大損失事件改列為信用風險事件，因為 FIRB 法的銀行其 LGD 是固定的，則可能減少資本計提。相反的，標準法銀行於信用風險上採用 AIRB 法者，則可能將重大的信用風險事件轉列為作業風險，以降低對資本計提的影響。而作業風險與策略、聲譽風險間的界線不明，也讓銀行有空間操縱此分界，並在資本計算上刻意排除部分損失。

就目前國外實務來看，風險類型的定義與區隔之差異似乎還無法避免，或者實務的做法與一般通行的定義仍有落差，比如說授信程序不完整雖屬於作業風險事件，但外國銀行通常將其歸為信用風險並套用於信用風險資本計算上，雖然這類的案例並未真正被當作信用風險事件，而且也不符合前面所提的傳統上被歸類為信用風險的作業風險事件。另以英國銀行公會之全球作業損失資料庫為例（Global Operational Loss Database），至目前雖已成立六年但仍按月與會員銀行討論相關事件分類與風險歸類，即可知這部分工作的複雜程度，且因金融業

務之與時俱進，導致規劃永遠趕不上變化。為了解決這樣的問題，國外部份銀行採用決策樹（decision trees）的方式，減少對事件的人為判斷，另外有些銀行則對內部需覆核檢視分類的損失事件設定一個較高的門檻，以減少需評估的事件數。

國內資料庫面對此一問題，雖設置與其他風險關聯性之選項，但因風險定義困難以及目前新資本協定規範主要專注於信用風險、市場風險、作業風險三個領域，故在選項設計上也只涵蓋信用與市場兩區塊，且因上述之金額分攤問題複雜，所以現階段只蒐集損失事件之總損失金額，而不另外再作分攤，但未來在進階衡量法發展上，仍需思考適當的切分方式或邏輯。

內部損失蒐集門檻

新資本協定對損失事件的蒐集門檻規範中說明，可依業務別或銀行而有不同標準，但資料若有共享機制，則應該要有較為一致的規範，因為在門檻設定不同的情況下，將使資料庫蒐集的輕微損失事件之分配產生偏誤（因門檻較高之銀行均不報送輕微事件）。損失門檻的選擇主要影響預期損失的計算，並對損失分配與非預期損失的估計有一定的重要性，在其他條件一致的情況下，蒐集越多的損失資料，一般來說可有效的降低預期損失估計上的誤差，然而，蒐集微小的損失事件可能不符合成本效益，因此必須取得一個平衡點。

實務上，絕大多數銀行依賴專家判斷來決定報送門檻，而非運用實證的方式來決定，主要的原因在於開始蒐集資料的時間點，並沒有足夠的資料量去進行實證研究，同樣的國內資料庫所設的報送門檻—新台幣 10 萬元，也是會議討論下的產物。

在國外實務上，銀行可能直接選擇已被其他機構使用一段時間的門檻標準，而業務部門經理人與風險量化專家也可能基於對業務以及量化分析影響的瞭解，提供個人的看法來設定或調整門檻。目前大多數銀行對不同的業務別採用相同的報送門檻，但也有部份銀行開始依業務別導入不同的門檻。此外，有些銀行雖已

建立門檻，但仍繼續蒐集門檻以下的資料，這些資料主要是用來分析預期損失的估計，以及驗證門檻值的設定是否恰當。

內部損失資料驗證

驗證包含覆核與評估資料蒐集流程及資料內涵，包括資料的真實性、資料內涵的廣度，並檢視銀行如何處理不完全的資料與來自結束營業之業務線的資料等議題，對內部資料定期驗證是提升風險管理決策的必要條件，並能確保量化分析結果是有意義且可信賴的，但因為銀行開始蒐集內部損失資料的時間不長，驗證內部損失資料的方法仍處於發展階段，且目前同業間也沒有較一致的實務做法。目前較為常見的驗證方法有以下五種：

一、確認損失與會計帳之一致；

二、風險管理人員覆核，包含檢查各種內部報
表間之一致性；
三、內、外部稽核人員複查；
四、檢查損失資料在業務單位與總行是否有不
一致；
五、損失資料蒐集系統的特性，例如決策樹與
使用者指南。

當銀行判斷其內部損失資料不足以進行風險衡量時，多數銀行仰賴外部資料或情境分析的協助，但這兩種來源均需要另外進行驗證的工作。

銀行在處理來自於退出的業務線之損失事件態度差異很大，有些銀行仍保存業務線過去內部損失資料，作為未來參考之用。有些銀行則認為不會再有事件發生於退出的業務線，而將這類的損失資料排除於分析或資本計提的計算上。

結語

由於新資本協定給予各機構發展作業風險管理的高度自由，導致國際實務上對於相同的資料議題均有數種不同的做法，國內各銀行現有之內部損失資料庫的架構也是如此，因為經營業務特性或專家判斷的不同，而發展出不同的資料蒐集與判斷流程。在這樣的情況下，金融機構自然會希望能有一致性的做法，然而因資料長度不足、資料蒐集廣度的限制或資料基礎不同的問題，導致尚未出現有效的實證研究來指導最佳的資料判讀邏輯。

在目前各機構對作業損失資料判讀邏輯不同的情況下，外部損失資料庫的建置可以說是統一規格的方法之一，但必須注意的是，內部損失資料庫與外部損失資料庫在運用以及資料蒐集精細程度上有所不同，比如說，文中所提及的近乎造成損失事件，其運用就主要侷限在事件發生銀行，因此銀行需注意在行內的資料蒐集不應僅侷限於外部損失資料庫的規格，可以更進一步去蒐集範圍外的資料，比如改變門檻、進行風險相關金額分攤或更多的回收來源等。

現行國內外作業風險資料庫架構的規劃一般均缺乏實證研究支持且高度依賴專家判斷，而不同專家的見解可能完全不同，如損失事件之辨識是否需以列入損益表為依據或是否進行損失金額風險相關性的分攤等，但現階段在資料不足以進行實證與進階衡量法研究下，並無法證明何種作法較佳，因此作業風險外部損失資料庫報送機制的啟動只是一個開端，未來仍有必要持續檢討欄位定義、資料必要性、報送門檻妥適性等，以修正資料庫架構供本國銀行使用；本文介紹國外損失資料蒐集與判讀邏輯的目的，即是希望銀行在資料蒐集上，除外部損失資料庫欄位之最低要求外，能嘗試蒐集其他資訊，則對未來資料庫擴充上將可能有所助益，並希望藉由這樣的方式去思考所蒐集的資料背後隱含的意義，以及瞭解對後續分析結果的影響，並由此印證國內外部損失資料庫之架構。

附錄十二：金融實務與管理專家論壇-「銀行經營的風險導向思維：反洗錢(AML)、金融科技(FinTech)、監理科技(RegTech)及資訊安全(Information Security)」研討會

一、主辦單位：台灣金融研訓院

二、協辦單位：台灣銀行家雜誌

三、舉辦時間：105年12月21日(星期三)下午2：30至5：30

四、舉辦地點：台灣金融研訓院菁華講堂(台北市羅斯福路3段62號6樓)

五、會議議程：

時　　間	議 程 內 容	洽 邀 講 座
14:00-14:30	報到	
14:30-14:40	開場致詞	盧陽正(台灣金融研訓院副院長)
14:40-15:10	專題演講一： 風險導向內部稽核之發展現況及趨勢	李潤之(資誠企業管理顧問公司執行董事)
15:10-15:40	專題演講二： 反洗錢及金融科技風險內部稽核實務應用	張晉瑞(資誠企業管理顧問公司執行董事)
15:40-16:10	專題演講三： 銀行業導入風險導向內部稽核制度的做法	林維琪(資誠聯合會計師事務所副總經理)
16:10-16:30	Coffee Break	

時　　間	議 程 內 容	洽 邀 講 座
16:30-17:00	專題演講四： 銀行資訊安全內部控制、實務應用	洪偉淦(趨勢科技臺灣暨香港區總經理)
17:00-17:30	綜合座談	主持人： 盧陽正 (台灣金融研訓院副院長) 與談人： 1. 李潤之執行董事 (資誠企業管理顧問公司) 2. 林維琪副總經理 (資誠聯合會計師事務所) 3. 洪偉淦總經理 (趨勢科技臺灣暨香港區) 4. 張晉瑞執行董事 (資誠企業管理顧問公司) **＊與談人謹依姓紙筆劃順序排序**