出國報告(出國類別：其他)

參加「APEC 金融監理人員訓練倡議—科技運作與風險管理研討會」

(APEC Financial Regulators Training Initiative: Regional Seminar on Technology Operations and Risk Management)

服務機關：金融監督管理委員會銀行局

姓名職稱：副研究員劉婉芝

出國地點：菲律賓馬尼拉

出國期間：107 年 5 月 15 日至 18 日

報告日期：107 年 6 月

目錄

出席 APEC 相關會議簡要報告

會議名稱 (含英文縮寫)	APEC 金融監理人員訓練倡議—科技運作與風險管理研討會 (APEC Financial Regulators Training Initiative (FRTI): Regional Seminar on Technology Operations and Risk Management)
會議時間	107年5月15日至19日
所屬工作小組或次級論壇	APEC Financial Regulators Training Initiative (FRTI)
出席會議者姓名、單位、職銜	劉婉芝、金融監督管理委員會銀行局、副研究員
聯絡電話、e-mail	(02)8968-9755、irenel@banking.gov.tw
會議討論要點及 重要結論 (含主要會員體及 我方發言要點)	一、本次研討會旨在對金融機構監管人員，就日新月異科技下之金融機構的資訊風險提供各類風險之發生、風險管理及監管上預期情形。 二、課程主題：主要係介紹金融機構之資訊科技(IT)風險概念、風險管理和綜合監管之基本概念。其中，資訊科技風險主題包含雲端運算、網絡安全、行動銀行、金融科技、支付系統及作業等議題介紹。同時亦將針對資訊科技風險管理之資訊安全、資料管理、供應商管理及業務連續性、資訊科技稽核進行討論。 三、課程進行方式：以講師授課方式，輔以個案分組討論、風險發生情境之意見交流及經驗分享，並另由參訓學員分享所面臨之資訊科技之風險爭議或挑戰。 四、我方於研討會中，除上台分享我國於發展金融科技下之資安挑戰外，積極參與分組討論及進行意見交流。研討會休息時間，並積極與參訓學員相互交流支付系統作業環境，瞭解與會各國之支付系統之發展情形與監理作法。
後續辦理事項	無。
建議資深官員發言要點	(無建議可免填)
檢討與建議	本次研討會之建議事項如下： 一、為強化資訊科技之風險控管，建議於金融科

	技部(辦公室)下設立專門獨立之IT 風險監督管理組室。 二、因應未來金融科技趨勢，建議思考金融監理人員之科技應用等相關專業培訓課程。 三、建議我國可持續參加訓練倡議等相關APEC活動，且本會檢查局或各局處資訊室可視議題共同派員參加訓練倡議研討會，並可邀請其他相關周邊單位自行參酌與會。

壹、 研討會背景與目的

一、背景

1998 年 5 月，亞太經濟合作組織(Asia-Pacific Economic Cooperation; APEC)財長部長會議(Finance Ministers)決議成立「APEC 金融監理人員訓練倡議」(Financial Regulators Training Initiative；FRTI)，以增進區域間金融監管與監理機構之分析與監理能力，達成強化金融監管者有效因應新科技發展與新興議題及趨勢之目標。

此訓練倡議(APEC FRTI；以下稱訓練倡議)藉由下列方式，就受訓之議題，提供區域金融監管者間協調及交流之管道：

1. 提供初階及中階金融監管人員廣泛之訓練機會；
2. 藉由強化銀行與證券監督管理者之課程規劃，妥切因應新穎式監理環境之需求；
3. 提昇區域間及國際間相互合作之訓練課程；及
4. 促進區域間金融監督主管機關間之相互交流與合

作。

二、訓練倡議課程規劃：

為執行訓練倡議，位於菲律賓馬尼拉之亞洲開發銀行(Asian Development Bank；ADB)成立秘書單位，負責支援每日訓練倡議活動，而由 23 個銀行監理成員及 24 個證券監理成員組成之 2 個諮詢小組(Advisory Groups;AGs)，分別針對銀行業與證券業，提供及推動倡議訓練課程活動、透過成員與與會者之調查與評估，決定訓練課程規劃與內容。就銀行監理成員，主要課程包含：銀行分析、信用、銀行作業面、利率、流動性風險分析、銀行風險管理、及防制洗錢與打擊恐怖主義等議題。截至目前為止，訓練倡議已舉辦 150 場研討會，總計 6,332 位金融監理人員參訓，平均每場研討會約有 42 位參訓者。

三、本次訓練倡議主題與內容：

本次研討會在亞洲開發銀行(ADB)位於馬尼拉之總部舉辦，並由亞洲開發銀行、菲律賓中央銀行

及菲律賓存保公司合辦，計有 13 個國家 57 名金融監理者參訓。我國係 ADB 創始會員國及 APEC 會員經濟體，有權利及義務參加該倡議相關活動。

此次訓練倡議主題在「科技運作與風險管理」(Technology Operations and Risk Management)，主要係介紹金融機構之資訊科技(IT)風險概念、風險管理和監管之基本概念，其中，資訊科技風險主題包含雲端運算(cloud competing)、網絡安全(cybersecurity)、行動銀行(mobile banking)、金融科技(Fintech)、支付系統及作業(payment system and operation)等議題介紹。同時亦將針對資訊科技風險管理之資訊安全(information security)、資料管理(data governance)、供應商管理(vendor management)及業務連續性(business continuity)、資訊科技稽核(IT audit)進行討論。

四、 本次訓練倡議目的：

此次訓練倡議課程藉由二位美國講師授課為主，

輔以個案分組討論各相關議題、風險發生情境之意見交流及經驗分享，並由參訓學員分享各國所面臨之資訊科技之風險爭議或挑戰，期於完成訓練後，能達成以下之目的：

1. 深入瞭解主要資訊科技風險
2. 辨識資訊科技與業務風險間之關聯，並將此關聯納入整合監理方法。
3. 金融機構適當資訊科技稽核(IT audit)的監理期待，包含組織架構、策略規畫、及稽核作業。
4. 瞭解資訊科技風險影響金融機構之整體情形與風險管理上之解決建議。

貳、 研討會議程

一、 課程內容

(資訊科技下表簡稱 IT)

日期	主題	講師
5 月 15 日	IT 風險監理概論	Colin Gavin
	IT 風險與商業策略	Linda Jeng
	IT 風險議題：雲端運算	Colin Gavin
5 月 16 日	IT 風險議題：網絡安全	Linda Jeng
	IT 風險議題：行動銀行	Colin Gavin
	IT 風險議題：金融科技	Linda Jeng
	IT 風險議題：支付系統及作業	Linda Jeng
5 月 17 日	IT 風險管理：資訊安全	Colin Gavin
	IT 風險管理：資料管理	Colin Gavin
	IT 風險管理：供應商管理	Linda Jeng
	IT 風險管理：業務連續性與災害復原	Linda Jeng
5 月 18 日	IT 稽核	Colin Gavin
	IT 組織管理與治理	Linda Jeng
	整合監管	Colin Gavin
	審查練習	Colin Gavin
	總結與評估	Colin Gavin
	授予證書	ADB,BSP,PDIC

二、 講師簡介

(一) Colin Gavin

目前是芝加哥聯邦準備銀行監理法規部資深科技設計師。過去曾在 STREAM Lab 就參與聯邦準備體系、聯邦存款保險公司、農業信貸管理局、國家信用管理局、及貨幣監理官辦公室等提供資訊科技法規之指導。以所學之資訊科技為背景，目前主要專研於 IT 之銀行檢查。

(二) Linda Jeng

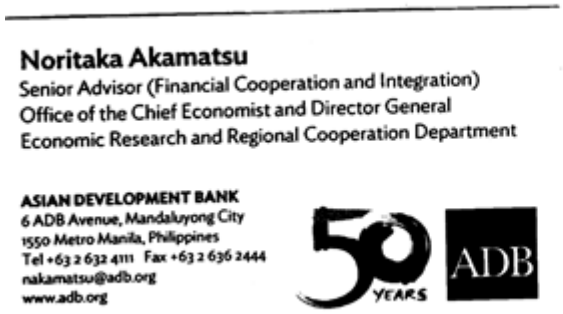
目前為聯邦儲備銀行監理部資深金融監理分析師。杜克大學、哥倫比亞法學院及法國吐魯斯大學畢業，擁有 17 年之金融法規經驗，包含 7 年於歐洲。曾草擬巴賽爾委員會之金融科技白皮書，並曾為參議員助理，參與多德-弗蘭克華爾街改革和消費者保護法（Dodd-Frank Wall Street Reform and Consumer Protection Act）。

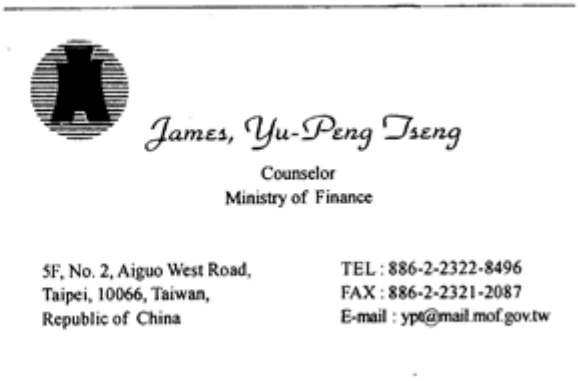
私下聊天得知 Linda Jeng(鄭)的父母皆為台灣人，Linda 雖自小移民美國，然在研討會場上，對台

灣十分友善，多次在國際會議上稱我方為「**Taiwan**」。

三、 ADB 資深顧問引言與我國駐 ADB 參事代表

本次研討會由 ADB 資深顧問 Noritaka Akamatsu 引言，並簡介訓練倡議之緣由及運作情形。我國財政部駐 ADB 代表曾參事，除負責參加 ADB 理事會年會與會務運作外，並積極協助各政府與民間團體與亞銀交流和提供東南亞地區需求，公務繁忙之際復撥冗前往研討會場關心我國受訓人員，於此深表感激之意。





參 、研討會重點摘要

一、 資訊科技(IT；以下簡稱 IT)風險

（一） 定義：什麼是資訊科技(IT)風險

1. 擴張性(Expansive)：電子自動化與科技日益發展，致 IT 風險與業務風險聯結。
2. 動態性(Dynamic)：創新不斷引入新風險，需有新策略。
3. 挑戰性(Challenging)：目前政策不易執行，應有靈活彈性的監理政策。

（二） IT 檢查之風險重點

IT 風險之檢查範圍分三層面：作業面、管理面、及環境面

1. 作業流程：包含存取與認證管理、網路與行動銀行、實體與遠端抓取(Branch and Remote Capture)、電訊傳輸(Wire Transfers)、自動提款機作業(ATM processing)、自動繳付循環帳項(ACH Origination)、虛擬與雲端(Virtualization/Cloud)、及作業模式(Models)。

2. 風險管理：包含資訊安全、網路安全、供應商(委外之第三人)風險管理、服務不中斷(業務連續性)與災害復原、應用程式存取控制、科技變革管理、資料管理及 IT 稽核。

3. 環境變革：更新作業系統、轉換作業系統、首次或更新資訊委外作業、重大產業趨勢變革、內部控制或風險管理越趨仰賴資訊科技、內部稽核或近期檢查報告之持續審查、及與應用網路和網路安全相關之相關議題。

（三） IT 檢查程序

1. 瞭解作業環境：IT 作業是否自行管理(In-House)、委外處理(Outsourced)、或併行兩項(Combination)管理，均會影響檢查程度。

2. 辨識 IT 與業務風險：分為管理程序(Management Process)、設備架構(Architecture)、統整性(Integrity)、安全性(Security)、可用性(Availability)。

3. 進行風險評估與總結：例如參考美國資訊科技統一評等制度(Uniform Rating System for

Information Technology, URSIT)頒布準則評估。IT 評等分 4 要素加 1 個綜合評等(composite rating)，與業務檢查的 CAMELS(1-5)相同。

4. 評等受檢機構：URSIT 之 5 要素分別為稽核(Audit)、管理(Management)、開發與購置(Development and Acquisition)、支援與傳輸(Support and Delivery) 等 4 項評估項目，加 1 項綜合評等(Composite)。
5. 評等檢查機構：包含稽核、管理、開發與購置及支援與傳輸等 4 個評估項目，加 1 項綜合評等。

（四） IT 與業務策略

金融業務策略與創新科技主要相關者有：雲端運算、網路安全、行動銀行、金融科技、及支付系統與銀行作業等。隨著科技不斷創新，雖然我們始終面臨監管趕不上日新月異的新穎科技之窘境，金融機構的策略規畫上仍應包含：

1.經營策略(董事會決策)是否注重 IT 議題與風險

2.更新 IT 設備之需求

3.引進 IT 變革以降低成本：意指應評估使用新 IT 技術之經營策略變化所產生之成本

4.引進 IT 變革以增益效益與成長:經營策略除應考量效益成長外，亦應同時考量潛在風險。

二、 IT 風險—雲端運算(Cloud Computing)

(一) 定義

下列機構分別就雲端運算定義如下表：

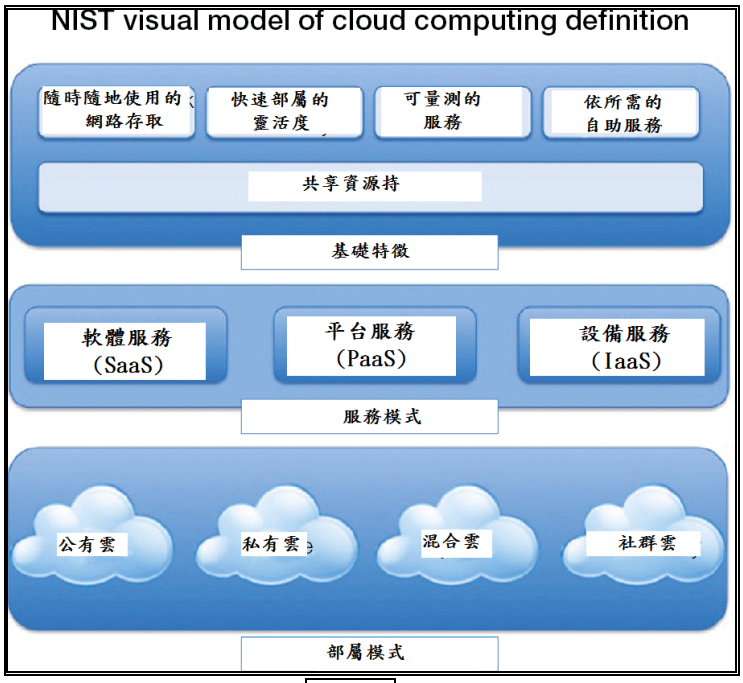
機構名稱	雲端運算定義
國家標準暨技術研究院 (NIST)	係一種可促使普遍存在、可轉換、並按所需之網路存取之共享可配置電腦資源,其可以快速提供並減少管理者負擔或服務提供者之介入的模式。
聯邦金融機構檢查委員會 (FFIEC)	係一種由自有資源轉至共享資源的運作模式,使用者可依所需自第三方服務提供者透過網路之雲端使用資訊科技服務。
維基百科 (Wikipedia)	係指使用透過傳送服務(通常為網路)所傳送之運算資源(軟體或硬體)。

附表 1

(資料來源：此次研討會簡報)

(二) 雲端運算之服務模式

NIST 就雲端運算提出標準定義，包含 5 個基礎特徵與模式如下：



附表 2

(資料來源：此次研討會簡報)

(三) 雲端運算之特徵

1. 不可控之 IT 管理如花費(Spending)
2. 日增月益的 IT 複雜性
3. 網路連接設備的暴增
4. 業務轉變之速度
5. 成本控制
6. 對新商業模式而增加 IT 需求

(四) 主要監理風險

1. 金融機構缺乏 IT 治理或不足
2. 法令遵循之挑戰
3. 供應商綁約限制

4. 雲端提供者之惡意內線(malicious insider)
5. 法律風險：例如司法傳訊(Subpoena)和電子證據發現程序(Discovery)
6. 資料保護風險
7. 隔離政策失效：如過於倚賴防火牆

三、 IT 風險—網路安全(Cybersecurity)

（一） 定義

目前只有廣泛定義而無共識的定義...

機構名稱	網路安全定義
國際結算銀行(Bank of International Settlements)	包含減少威脅、降低漏洞、嚇阻、國際間參與、災害回應、及恢復與復原活動與安全作業之策略、政策與標準。
國際電信聯盟(International Telecommunications Union)	用以保護網路環境、機構組織與使用者資產之一切工具、政策、安全防護、準則、風險管理方法、安全行動、訓練、科技方法等之統稱。
資訊科技協會(ISACA)	因應對資訊、儲存、與網路資訊系統傳輸之威脅所為之資訊資產保護。
國家標準暨技術研究院(NIST)	一切預防、偵測、回應攻擊之保護資訊之流程。

附表 3

(資料來源：此次研討會簡報)

（二） 網路風險之監管挑戰

1. 動態性質：網路威脅不斷。
2. 缺乏地域限制：網路風險無國界。
3. 專門檢查人員知識不足：檢查人員多為金融領域背景而缺乏科技背景，或科技領域背景之檢查人員則缺乏金融專業知識與經驗。
4. 當前監理之適用性：因網路日新月異，當前之監理政策不易判斷或無法完全適用。
5. 缺乏指導原則或標準規範。

（三） 金融機構對網路安全之回應

金融機構對網路之態度為主要影響網路安全之主要因素：

1. 企業文化上：多數金融機構多能接受網路風險可以管理，但認為絕對無法消除。
2. 財政上：財務成本為最重要之考量因素。報導預估顯示：**截至 2019，全美的網路犯罪將帶給企業超過美金$2 兆元**，因此，無論金融機構之規模與複雜性，均應花費更多財力物力於資訊安全或網路安全上。

3. 組織上：金融機構之組織亦應調整，於內部稽核下，除原有法律部門、法遵部門、人資行政部門外，應成立專門的資訊(網路)安全部門。

4. 實務上：網路安全不僅應考慮資訊安全或 IT 風險，而且應全面檢視策略目標裡潛藏的網路安全風險。根據 KPMG 於 2016 針對 100 家銀行之調查報告，過去 2 年約有 12%之機構未檢視其資訊安全而有遭受網路攻擊之可能。

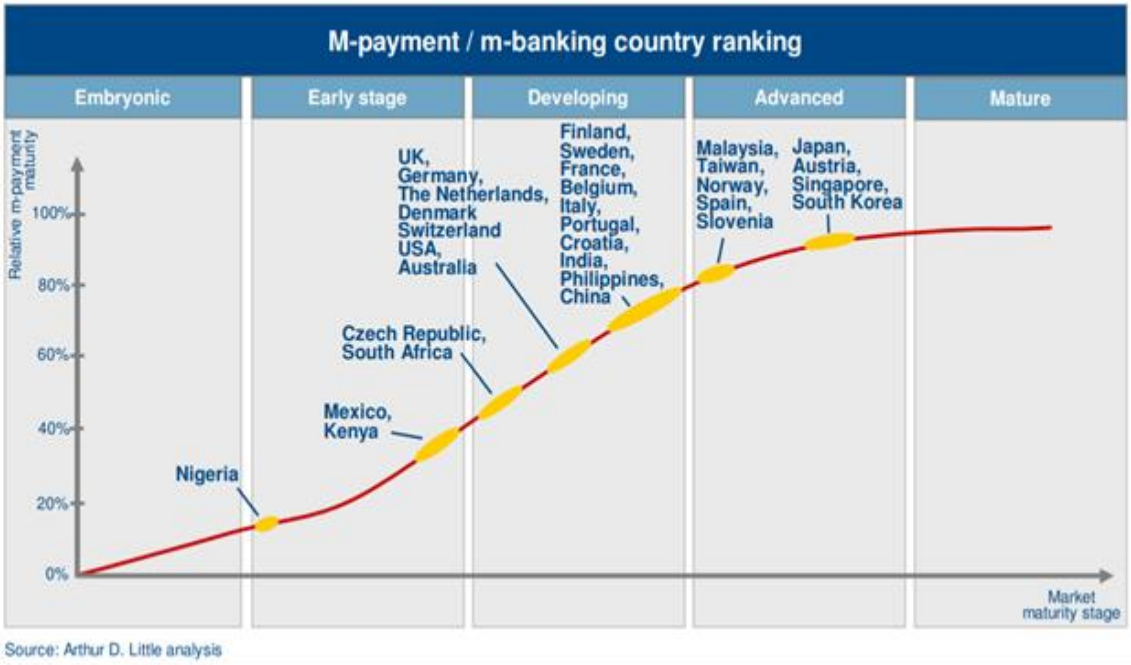
（四） 廣泛之監理考量

金融機構應持續辦理下列之網路安全事項：

1. 確定並管理突然(salient)之風險。
2. 維護作業與業務服務。
3. 保護消費者資訊、安全、穩健、及名聲。
4. 維持公眾信心。
5. 限制風險蔓延至其他領域：網路安全可能會波及到金融科技、行動支付、網際網路、雲端運算等。

四、 IT 風險—行動銀行與支付(Mobile Banking and Payments)

雖然目前美國的行動銀行或行動化支付在全球排名實屬後半段(參下表)，真實原因無人研究，惟研討會仍以美國為主說明行動銀行與行動支付之情形。



附表 4

(一) 現行與新興支付方式

發展中的支付商業類型有：由網路營運中心(如 Verizon 威訊無線)、銀行中心(Bank Centric)、及由可信賴之第三方(如 Google、Paypal、Square 等)等為主經營支付服務中心。

不過，現行支付類型有多元化之趨勢：行動網

路營運商、手機/SIM 卡製造商(Handset/SIM chip manufacturers)、銀行、卡片組織、支付網路(Payment Networks)、預付卡公司(Prepaid companies)、商家、網路搜尋和支付服務提供廠商、及專利支付系統供應商等紛紛加入支付服務市場。

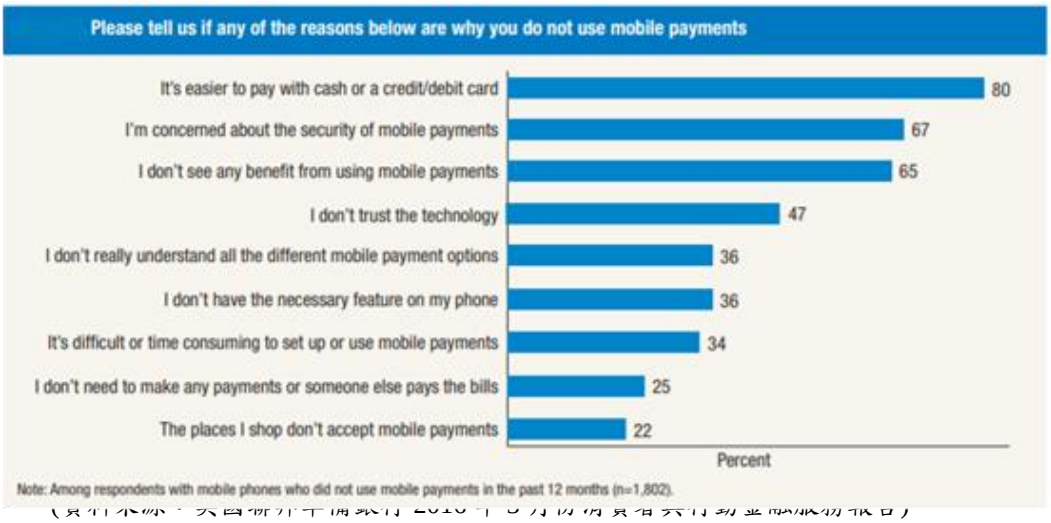
(二) 挑戰及風險

在美國，影響行動支付或行動銀行商業之因素計有：不確定監管法規因素；潛在非預期之事件如風險、詐欺、安全性等因素；資料治理及供應商管理；當創新產業或新創公司失敗時，對消費者不確定之影響性；對監理者及消費者保護性責任範圍之不確定；甚至行動支付成為未來泡沫化之可能因素，均是此產業可能面臨之挑戰與風險。

(三) 行動支付與消費者保護

美國聯邦準備銀行針對行動支付之市場調查所提出之報告，列出美國民眾之所以**不使用行動支付**之主要原因，除了多達 80%的受訪民眾認為使用卡片支付較為便捷外，多達 67%及 47%係不相信行動支付之安全性或不相信科技技術。因此，「安全性」

是推動行動支付發展之最主要考量因素。



（資料來源：美國聯邦準備銀行 2015 年 3 月份消費者與行動金融服務報告）

（四） 行動市場之主要政策內容

為了確保行動支付之安全性，首先應建制行動支付之安全性政策，而政策內容應考量下列因素：

1. 政策對業務發展及消費者經驗之影響
2. 資料儲存、資料分享與資料安全
3. 設備串接、設備驗證(Device Authentication)
4. 資料與設備之銷毀機制(Wipe Mechanisms)
5. 形態控制(Feature Controls)
6. 容許應用程式(Applications Allowed)

（五） 監管行動支付之考量因素

監管行動支付或行動銀行應考慮下列方向：

1. 行動產品發展之管控，如各電子產品間相互運用行動支付系統

2. 涉及第三方業者之管控，包含非銀行之第三方業者、網路業者、供應商或服務提供者(如RFP、SLAs)
3. 法規及遵法風險：例如資訊串接時，資料資料之擁有者、手機使用者之權利義務(如消費者使用不安全之 WIFI 造成交易資料外洩時)、洩密時之責任歸屬等。
4. 消費者曝露限制(Customer Exposure Limit)之執行，包含詐欺揭露與應對計畫
5. 消費者教育之要求及其安全性執行措施
6. 交易確認與驗證之操作

五、 IT 風險—金融科技(Fintech)

(一) 定義

金融科技(Fintech)係由使用科技創造金融系統、或促使金融服務更加有效之公司組成之產業。

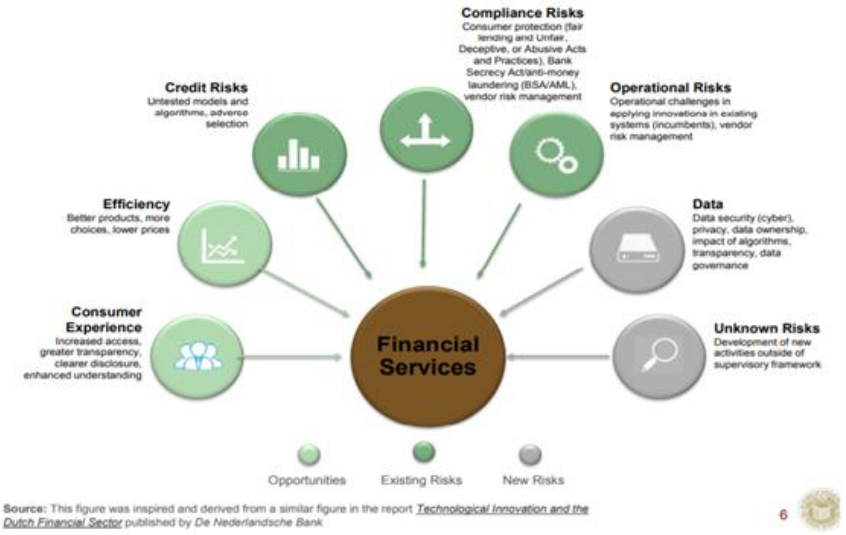
據概括統計，2015 年全球總計有約美金 190.1 億元投入金融科技公司，而美國則占有 130.8 億元。

(二)　金融科技與銀行業之結合方式

由於金融科技與銀行業以下列方式越趨多樣性結合，而與傳統銀行大相逕庭，而值得金融監理者留意：

1. 銀行投資金融科技公司
2. 銀行設立新創計畫以孵化金融科技公司 (incubate fintech companies)
3. 銀行與金融科技公司合作：包含如以借款予新創公司、為金融科技業募款等方式之合作。
4. 銀行併購金融科技公司
5. 銀行推行自己之金融科技方案

(三)　金融科技之機會與風險



附表 6

(資料來源：De Nederlandsche Bank 公布之 Technological Innovation and the Dutch Financial Sector 報告)

參詳上表，發展金融科技將面臨機會與風險，包含

消費者經驗與效率提升、信用風險、法遵風險、營運風險、及逾越監管之風險等，另外還有資料安全風險與未知之風險等。

(四) 美國近年監理主管機關對金融科技創新回應之表列如下：

1. 聯邦準備系統(Federal Reserve System; FRS)

(1) 2015 年由 Lael Brainard 擔任指導委員會主席，就聯邦儲備之支付系統全面研議

(2) 成立跨部門工作小組，優先研議金融科技新興議題

(3) 與巴賽爾委員會研議支付系統議題

(4) 研議銀行秘密法(BSL)、洗錢防制法(AML)、及分散式帳簿(DLT)議題

(5) 2016 年 12 月 2 日公布金融科技之機會與挑戰報告(The Opportunities and Challenges of Fintech)

2. 貨幣監理官辦公室(Office of the Comptroller of the Currency; OCC)

(1) 2016 年 3 月發布之「負責任的創新白皮書」

(Responsible Innovation Whitepaper)、6 月公布相關公開諮詢(public forum)。

(2) 考慮有限制目的之金融科技章程(Fintech Charter)及監管沙盒(regulatory sandbox)。

3. 美國聯邦存款保險公司(Federal Deposit Insurance Corporation; FDIC)

(1) 2015 年於理透視季刊有關網路借貸專文。

(2) 對與銀行合作之金融科技業者訂有限制之金融檢查。

(3) 更新提出第三方借貸指導原則

4. 美國財政部(U.S. Treasury)

(1) 2015 年完成網路借貸之公開意見徵詢

(2) 2016 年 5 月發布網路借貸白皮書

5. 消費者金融保護局(Consumer Financial Protection Bureau; CFPB)

(1) 2016 年 3 月發布有關網路借貸之消費者公告(Bulletin)。

(2) 受理消費者申訴網路借貸爭議。

(3) 促進政策規劃(Project catalyst)

6. 聯邦貿易委員會(Federal Trade Commission)

2016 年 6 月起舉辦一系列網路借貸論壇活動

(五) 聯邦準備銀行對金融科技產業之考量因素

面對金融科技業發展趨勢,聯邦準備銀行思考下列因素以因應未來之監管方向：

1. 瞭解金融機構著手或計畫之金融科技活動內容。
2. 除了創新外，思考金融科技可帶來之優劣，是否新產品、新服務可以達成過去未滿足之金融服務需求。
3. 試著從各式監理者角度獲取新的看法與民眾回應。
4. 在可允許金融科技之機會下，如何面對風險與挑戰。

六、 IT 風險—支付系統與銀行作業(Payment Systems and Operation)

支付系統分為零售支付與批發支付，零售係指於兩消費者間(C2C)、消費者與商家(C2B)、或商家與商家(B2B)間支付；而批發主要是國內與國際間商業活動之支付。本節主要討論為國內(指美國)之零售新支付工具。

(一) 零售支付工具(Retail Payment Instruments)

受到科技創新與消費者對快速支付之需求，美國之零售支付工具包含：

1. 媒體交換自動轉帳服務 ACH(Automated Clearing House)
2. 信用卡(Credit Card)
3. 簽帳卡(Debit Card)
4. 電子化工具(Electronic Instruments)，包含行動與網路

(二) 非銀行之第三方支付(Non Bank Third Parties)

非銀行之第三方參與者也紛紛加入支付服務行列，主要係受到下列因素影響：

1. 新創力量

2. 拉長交易鍊：意指由過去買賣雙方，增加中間之各式服務提供者。

3. 促進策略夥伴

4. 審慎檢查之要求

5. 必要之偵測詐欺進化

(三) 監理重點

針對支付系統引進新支付工具之監管檢查項目著重：

1. 系統部署

2. 清結算之執行

3. 銀行內部

4. 消費者之使用

5. 詐欺之偵測

為執行上述監理項目，監理流程可分為：

1.前端作業控制：包含辨識風險、預估風險

2.後端作業控制：包含保護、偵測、及對風險之回應

3.災害復原與金融服務不中斷：包含備援系統

七、 IT 風險管理—資訊安全與資料治理

（一） 資訊安全與網路安全區別

1. 資訊安全係綜合評估公司 IT 環境之主要參數。強調資訊的：可用性 (availability)、機敏性 (confidentiality)、完整性 (integrity)、確保性 (assurance)及可歸責性(accountability)。
2. 網路安全與資訊安全與科技基礎設施密切關聯，但被視為引發系統性且將影響深遠的風險。

（二） 存取與身分識別管理

1. 存取：應與工作內容及所需相對應，同時應建立一套自申請授權、審查監控與解消移除之存取流程。
2. 監控存取層級與活動時，尤應注意執掌員工的下列行為：詐欺、不當處理消費者資訊、故意或不慎查閱個人資料、內線人員之威脅。

（三） 資料治理(Data Governance)的重要性

資料安全的重要：在於如果發現一項錯誤時，表示整份資料都遭破壞(corrupt)。所有機構都高度仰賴系統產生之資料以進一步作決策制訂及法規函

報作業。管理階層或檢查人員一般均視機構所提供之資料是正確可信賴，然在此盲目的自信(blind confidence)下，當實際上資料有誤，卻無人知道該不知道的事(資料有誤)，恐將造成管理、稽核、系統及管理等全面嚴重性錯誤。

（四） 資料治理規劃：

應建立一套架構，確保資料完整性，可用合規報告、訂定標準流程、及其他供決策時之準確 MIS 資料。資料治理之規畫應包含下列項目：

1. 訂定政策與程序。
2. 報告及逐層上報程序
3. 建立工作流程檔案。
4. 執行資料可追蹤性實務作業。
5. 準確性與完整性之控管。

（五） 監管重點：

1. 管理階級及董事會層級之監督管理
2. 資料基礎設施與控管情形
3. 報告或資料之工作流程表
4. 內部稽核測試

八、 IT 風險管理—第三方風險與供應商管理

金融機構為優化其金融服務及提升競爭力，通常會將部分或全部 IT 作業委託第三方服務供應商處理，但同時增加各式供應商風險。

(一) 供應商風險之種類

1. 法遵風險：可能為國外供應商，而不熟悉當地法令、或商品服務不符合當地法規。
2. 集中性風險：如雲端供應商集中在少數幾家全球性供應商。
3. 名聲風險：供應商之錯誤可能連帶影響委外之金融機構聲譽。
4. 國家風險：外國供應商可能不受當地國司法管轄、或外國供應商所在國之政經不穩定等。
5. 作業風險：供應商內部作業或管理之缺失所帶來之風險。
6. 法律風險：一切因委外作業所造成之訴訟或糾紛等法律風險。

(二) 管理供應商/第三方風險之重點

1. 董事會及管理階層責任：

(1) 訂定委外供應商之政策與流程。

(2) 管理階層依委外政策訂定相關作業流程、盡責調查及評估程序，包含風險管理規劃。

(3) 服務供應商之風險管理規劃要點應包含：風險評估、盡職調查、委外契約條款、意外災害賠償辦法、監管控制服務供應商之辦法、服務不中斷及應變計畫。

2. 定期監控服務供應商遵循作業標準，及確實執行相關資料安全措施。監督管控應包含：適當專業人員、以風險為基礎之監控方式、供應商之經濟情形及內部控制、和上報監管活動。

3. 定期向董事會報告委外作業。

九、 IT 風險管理—災害復原與業務連續性 (Disaster Recovery and Business Continuity)

(一) 災害之定義

任何突發的災難而造成損害(damage)、損失(loss)、

或毀損(destruction)，廣義地說，就是一切突發或重大之變故(misfortune)或失敗(failure)。

(二) 復原規畫：

災害之復原規畫應包含：

1. 業務連續性計畫(Business Continuity Planning; BCP)：

(1) 採取整個企業體之廣泛方法，包含人員、作業流程、及供應商等。

(2) 應以業務影響分析(BIA)為基礎。

(3) 應遵循災害復原規劃(DR/DRP)。

2. 業務影響分析(Business Impact Analysis; BIA)：

(1) 分析受影響程度與(復原)優先順序

(2) 確認業務受損情形

(3) 確認法律與規範要求

(4) 評估最大允許之修復時間

(5) 評估修復時程目標(Recovery Time Objective; RTO)及修復點目標(Recovery Point Objective; RBO)

3. 災害之復原規劃(Disaster Recovery Plan; DR/

DRP)：災害之機構全面性復原作業規劃、迅速有效且無縫之修復回應，及恢復業務作業，包含系統面與實務作業面。

(三) 災害復原(DR-BCP-BIA)應考量因素：

1. 服務之準確性
2. 主要人員之風險
3. 修復能力
4. 人員流動與流失
5. 企業預期應與 IT 功能與服務聯結

(四) 監管重點

1. 復原規劃是否符合機構之業務模式
2. 董事會、管理階層及人員是否瞭解其在計畫中之角色與責任
3. 確保測試如期執行
4. 復原規畫除應反應目前之作業環境，同時所有新系統亦應一併考量，以確保 BCP 能配合營運環境與時俱進。

十、 IT 風險管理—IT 稽核

(一) 目的

資訊科技稽核的目地係提供以風險為重點之有效評估 IT 風險控管，透過風險管理評估、內部控制及政策遵循評估 IT 風險管理，以確保穩健之內部控制作業、及時之稽核缺失修補解決，並同時有效通知董事會以確實管理風險。

(二) 以風險為基礎之稽核規劃[第一道防線]

有效的稽核規劃應由上而下之風險評估，包含機構之全部主要活動，及依各單位之頻率與深度訂定稽核風險評估。

稽核風險規劃應經董事會及高階管理階層核准並確實執行，規劃內容包含：

1. 稽核政策：

(1) 由上而下之風險評估(Top-down Risk Assessment)

(2) 主要風險考量(Key Risks to Consider)

2. 執行稽核政策

(1) 瞭解並評估控管作業

(2) 蒐集證據

(3) 評估結果

(4) 監控完成

(三) 稽核管理[第二道防線]：

1. 執行經董事會核准之稽核政策

2. 監控稽核作業

3. 定期向董事會報告及溝通稽核政策、執行計畫與程序

4. 建立明確而層層分明之稽核與報告流程

5. 確保稽核之必要性、獨立性、專業性、及充足教育訓練與技能

(四) 內部管理與內部稽核人員[第三道防線]：

內部稽核管理應包含：內部控制風險評估、稽核計畫、稽核程序、稽核報告、監管稽核人員、提供稽核人員政策及流程、及確保足夠之獨立專業人員及資源以便確認固有風險並有效評估 IT 風險控管作業。

內部稽核人員應有之專業與責任(英文縮寫簡稱：IRMR)：辨識(Identify)弱點與風險、審查

(Review)弱點分析之管理計畫、監控(Monitor)解決方案、並定期向董事會或稽核委員會報告(Report)重大弱點。

(五) 外部稽核(External Auditors)：

1. 審查 IT 控管及控管評估作業
2. 確保管理作業之執行與符合目標

(六) 委外內部 IT 稽核

1. 委外契約：由金融機構與第三方 IT 稽核服務提供者簽訂。
2. 依機關大小及複雜度提供可行之執行計畫。
3. 可採行之各式稽核形式，包含就特定議題提供內部稽核人員專業知識、委外之內部稽核作業。
4. 董事會及高階管理階層仍應負所有責任。
5. 金融機構仍應執行適當之盡責調查。
6. 確保對委外內部稽核作業之充足監管。

(七) 評估資訊安全稽核

1. 董事(會)監督
2. 獨立性
3. 風險評估

4. 稽核計畫

5. 稽核範圍

6. 稽核作業報告

7. 監管及爭議之解決方案

8. 稽核報告品質

9. 有效向董事會及股東報告

肆、 與會心得與建議事項

一、 參與研討會心得

(一) 支持與鼓勵新南向政策：

政府推動新南向政策的主要目的，是在為臺灣的社會、經濟及文化的全面發展，找到新方向及新動能，藉此建立我國和東協、南亞及紐澳等國家有更廣泛的連結與對話，以及更緊密的合作，共同開創區域的繁榮發展。[1]

此次研討會多數參訓國家來自東協及南亞，包含印尼、汶萊、馬來西亞、柬埔寨、泰國及菲律賓等國家。參訓期間之交流與溝通中，瞭解當地之金融經濟起飛與發展，工商需求與人民知識水準大幅提升，台灣在西進受阻而與美國關係維持現狀之外，若不與東南國家合作，台灣的競爭力恐將在全球化互助互惠互利下漸漸削弱。

(二) 兼備金融科技之專業人才的缺乏

研討會中，無論是講師或與會人員均一致認為金融科技趨勢下，現階段兼具金融與科技專

[1] 參行政院重要施政成果: https://achievement.ey.gov.tw/cp.aspx?n=53E4AD5EA2AE7FA6

業知識之人微乎其微。二位講師也大方承認其一是所謂的 IT guy(資訊人員)，而另一位為法律金融人士，雙方相互對彼此之專業知識難謂熟稔專精，雙方係不斷透過溝通、討論、及交流下，始能達到目前程度，而其他與會國家亦有相同情形，參訓者若非單純資訊人員就是金融監理人員。足見，目前兼備金融與科技之專業人士仍屬缺乏與不足之情形。

(三)　與各國金融監理人員增加互動與交流

研討會期間，透過分組交流及餐敘時間，與各國參訓人員互動與交流，會後留影：

<table>
<tr><td rowspan="3">  </td><td colspan="2">與我國駐 ADB 代表曾參事及 2 位美國講師合影</td></tr>
<tr><td>與大陸銀監會、香港金管局人員合影</td><td>與各國監理人員訓後合影留念</td></tr>
<tr><td>上台分享我國經驗</td><td>受訓完成之證書</td></tr>
</table>

二、 建議事項

(一) 為強化資訊科技之風險控管，建議於金融科技部/辦公室下設立專門獨立 IT 風險監督管理組室

金融科技已是未來的金融發展趨勢，各國無不開始成立金融科技辦公室，如新加坡、香港，涵蓋支付、大資料分析、應用程式、平台及網絡安全，以便推動與促進金融科技發展，並確保金融科技下之交易安全與消費者保護。此次與會之中國在銀監會底下成立信科部，監管訊息科技風險，目前編制雖只有 7 人，但為獨立固定編組單位，仍可達到強化資訊科技之風險控管。

金管會已於今(107)年初，因應金融科技創新實驗條例通過，將金融科技辦公室擴編為「金融科技發展與創新中心」，由本會顧主委擔任創新中心主任，創新中心下分有 2 個組，「創新發展組」負責相關創新實驗條例所需研訂子法，及申請案件審查，目前已接受申請；「園區發展組」主要係設立園區以便金融科技新創業者進駐，園區預計於今年 9 月落成，媒體號稱「台版數碼港」，

預計 6 月中開始受理新創業者申請進駐，為鼓勵促進金融科技展開新的一頁。然而，考量未來之傳統金融業將與金融科技結合，屆時，金融科技之風險管理與監督將成為迫切之重要課題，建議應於現階段鼓勵與促進金融創新之同時，設有風險管理與監督組，打造一個負責任的創新之金融科技業。

(二) 因應未來金融科技趨勢，建議增加金融監理人員之科技應用等相關專業培訓課程

承上述可知，目前各國兼具金融與科技之專業人才是較缺乏與不足，而金融監督之經驗是不可取代的，因此，建議思考以增加相關科技應用培訓課程之方式，加強現有之金融監理人員之資訊科技應用知識，成為金融科技之專業監理人員。

(三) 建議我國可持續參加訓練倡議等相關 APEC 活動，且本會檢查局或各局處資訊室可視議題共同派員參加訓練倡議研討會，並可邀請其他相關周邊單位自行參酌與會

本次研討會課程內容涉及多項資訊科技(IT)

之電腦資訊設計方式與稽核檢查等實務及檢查執行面，多數國家與會代表同時有金融監理機關之IT部門人員或檢查人員、稽核人員共同參加(參附件二)。本會檢查局執掌金融檢查制度之建立及檢查，對於金融機構之檢查及資訊科技檢查經驗豐富，爰日後如有類似此跨領域之研討會，建議本會檢查局或各局處資訊室亦可視議題派員共同參訓，以利分享實務經驗與交流意見。

另外，各國參與人員亦不乏有存款保險公司(Deposit Insurance Corporation)參加，私下與渠等交流，知悉其等對所所握有之重要龐大資訊須有更高度之安全管理與風險控管，而從渠等分享實務之資安情境與困難挑戰，爰亦建議如有下次相關議題，可邀請周邊相關單位自費出席參訓。

伍、 附件

附件 1:研討會議程

附件 2:研討會參與者聯絡方式

附件 3：研討會資料