

行政院及所屬各機關出國報告
(出國類別：出席國際會議及其他)

參加「APEC 金融監理人員訓練倡議-
第 22 次諮詢小組會議」及「網路安全
暨科技風險監理研討會」報告

服務機關：中央銀行
姓名職稱：謝人俊 科長
派赴國家：庫克群島
出國期間：106 年 6 月 3 日至 13 日
報告日期：106 年 8 月 24 日

摘要

自 1998 年 5 月「亞太經濟合作」組織財長會議決議成立「金融監理人員訓練倡議」起，亞洲開發銀行即接受委託，設立工作小組，並提供行政支援，協助舉辦該倡議項下之諮詢小組會議及訓練活動。本次小組會議旨在討論訓練倡議課程計畫及檢討執行成效；另「網路安全暨科技風險監理研討會」，則以金融科技風險監理近期發展所面臨之挑戰為主題，由美國聯邦準備體系講師授課，並進行分組討論。

參加會議及研討會心得：(一)依據會員經濟體訓練需求之調查結果，各國重視總體審慎及金融科技監理；(二)金融科技生態系統持續蛻變，金融科技須動態監管，並調和「產業發展、公平競爭、安全穩健及消費權益」監理目標；(三)先進經濟體央行(例如美國聯邦準備體系)或監理機關為增進對金融科技實務之瞭解，已陸續在機關內部設立研究小組，著手研議新興議題，俾即時掌握實務發展對其主管業務之影響，以利決策。

本報告彙整研討會資料及近期國際文獻，就金融科技監理提出建議：(一)主管機關應督促金融機構強化資訊科技之風險控管；(二)主管機關應掌握金融數位化發展態勢；(三)主管機關宜持續關注監理科技之應用。

目次

	頁次
摘要	
目次.....	i
壹、參加目的及與會人員.....	1
一、目的.....	2
二、與會人員.....	2
貳、參加過程.....	3
一、AG會議.....	3
二、網路安全暨科技風險監理研討會.....	5
參、網路安全暨科技風險監理.....	9
一、金融科技發展階段.....	9
二、資訊科技風險監理概論.....	10
三、網路安全.....	12
四、雲端運算.....	14
五、行動銀行與行動支付.....	17
六、金融科技.....	20
七、資料治理.....	22
八、委外處理.....	23
九、統合監理.....	24
肆、國際組織對金融科技風險監理之觀點.....	26
一、國際貨幣基金.....	26
二、國際清算銀行.....	27
三、金融穩定理事會.....	28
四、防制洗錢金融行動工作組織.....	29
五、歐洲聯盟.....	30
伍、心得及建議事項.....	32
一、研討心得.....	32
二、建議事項.....	33
參考資料	

表 次

	頁次
表 3.1 雲端運算之定義	14
表 3.2 美國主管機關對金融科技之因應措施	21
表 3.3 當前資訊科技主要監理議題	25

圖 次

圖 2.1 資訊科技監理之重要領域	6
圖 3.1 金融科技發展之重要時期	9
圖 3.2 雲端運算之特徵與模式	15
圖 3.3 雲端運算應用平台基礎設施	16
圖 3.4 行動金融服務涉及之 4 大面向	18

參加「APEC 金融監理人員訓練倡議-第 22 次諮詢小組會議」 及「網路安全暨科技風險監理研討會」報告

壹、參加目的及與會人員

1998 年 5 月「亞太經濟合作」(Asia-Pacific Economic Cooperation, APEC)組織財政部長會議決議成立「APEC 金融監理人員訓練倡議(Financial Regulators Training Initiative, FRTI)」，其目的係藉舉辦訓練活動，提昇會員經濟體銀行與證券監理人員之分析與專業能力，俾強化金融監理。

該倡議下設 FRTI 諮詢小組(Advisory Groups, AG)，負責指導及推動該倡議活動，小組成員則由 APEC 會員經濟體銀行與證券監理機關組成。迄至本(2017)年 5 月底止，銀行監理小組成員計有 18 經濟體 23 機關；證券監理小組則有 22 經濟體 23 機關。相關行政作業則委託亞洲開發銀行(Asian Development Bank, ADB)設立工作小組，並提供行政支援。AG 每年定期集會，討論區域訓練課程相關計畫及檢討該倡議執行成效。

本行自 AG 小組成立之初即派員與會，金管會則自 95 年起亦逐年派員參加會議，均有利我國在區域金融監理領域之聯繫與合作，以及提升金融監理能力。本次小組會議為第 22 次舉辦，援例在一天內上、下午分別召開證券監理人員及銀行監理人員會議。

除諮詢小組會議外，隸屬於 ADB 之 FRTI 工作小組通常會在會議當週，另外安排一場銀行或證券監理議題之研討

會。本次在小組會議後接續辦理之研討會係以「網路安全暨科技風險監理」為主題，由美國聯邦準備體系(Fed)講師授課，探討資訊業務檢查重點及金融科技風險監理近期發展所面臨之挑戰。

一、目的

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。參加本次會議目的：

- (一)實質參與 ADB 與 APEC 國際金融活動。
- (二)就近蒐集國際金融監理資訊與他國監理實務做法，供本行審慎監理業務參考。

二、與會人員

(一)AG 會議(6 月 5 日)

除 ADB 負責辦理 FRTI 之工作小組 4 名成員外，另有庫克群島、印尼、韓國、馬來西亞、菲律賓、泰國、美國及我國等 8 會員國(經濟體)11 人，共計 15 人參加，主要為負責銀行或存保監理訓練業務人員，我國金管會亦派乙名人員參加。

(二)網路安全暨科技風險監理研討會(6 月 6 日至 9 日)

計有孟加拉、庫克群島、印度、馬來西亞、尼泊爾、紐西蘭、巴布亞紐機內亞、所羅門群島、斯里蘭卡、坦尚尼亞及我國等 11 國(經濟體)央行及金融監理機關(構)人員共 38 人參加。研討會由聯邦準備體系理事會(Board of Governors of the Federal Reserve System)銀行監理處資深經理引言與引導分組討論；里奇蒙聯邦準備銀行資深檢查人員主講。

貳、參加過程

一、AG 會議

由庫克群島金管會主委 Louise Wittwer 主持，ADB 資深顧問 Noritaka Akamatsu 引言及簡報有關協辦 FRTI 情形。會議旨在討論 FRTI 項下之財務資源運用、訓練課程計畫及檢討該倡議執行成效。

(一)議程

- 1.討論 ADB 對 FRTI 提供之技術協助(TA)專案。
- 2.檢討 2016-2017 年訓練活動辦理情形。
- 3.確認上(第 21)次 AG 會議紀錄。
- 4.討論訓練需求調查結果。
- 5.檢視 APEC FRTI 章程。
- 6.商議下(2018)年訓練計畫之主辦國(機關)及舉辦日期。

(二)討論內容摘要

1.銀行監理參訓人數統計

FRTI 訓練課程以區域研討會形式舉辦，自 2001 年至 2017 年 5 月止，歷年參訓學員總數達 6,200 名來自 53 經濟體，平均每場研討會計有 42 名來自 11 經濟體。參訓人數前三名之課程主題為(1)銀行分析監理與檢查、(2)信用風險分析及(3)風險導向監理。

2.工作小組已著手研議下年 FRTI 預算計畫

(1)自 FRTI 開始運作迄今，ADB 前後已核准 8 期 TA 專案(包括預算編列)，共支出約 7.4 百萬美元，每年訓練活動約支出 30 萬美元。

(2)因應開發中會員經濟體龐大之基礎建設融資需要，ADB

在籌集營運資金方面臨相當挑戰。為有效運用資金於開發貸款項目，ADB 已啟動檢討 TA 專案是否與其開發貸款目的結合。

- (3)最近一期 TA 專案即將於本年 7 月屆期，工作小組刻在研擬新 TA 專案，若獲 ADB 核准，即可繼續協助 APEC 辦理訓練倡議活動。惟在無法確定 ADB 是否核准情況下，工作小組考慮下列 3 種可能因應作法：
- a.洽尋 FRTI 會員經濟體捐助並設立特別信託基金。
 - b.尋覓外部捐助資金。
 - c.若無法獲得上述捐助資金，則擬報請停止協助 FRTI。

3.Fed 出席人員建議

- (1)Fed 循例指派講座支持 FRTI 活動。
- (2)若工作小組擬以問卷調查會員經濟體對 FRTI 之支持意願，建請該小組詳細說明最近 5 年 FRTI 運作及經費支出情形。

4.會員經濟體訓練需求調查結果

- (1)優先訓練主題
 - a.總體審慎監視(包括金融穩定與壓力測試等相關議題)。
 - b.網路安全或科技風險監理。
 - c.危機處理與清理及復原計畫。
 - d.數位金融或金融科技監理。
 - e.信用風險分析。
- (2)部分會員經濟體表達承辦下年 AG 會議及研討會之意願(例如孟加拉、柬埔寨、庫克群島、印尼及泰國)，惟須視目前研擬中之 TA 專案是否獲准繼續辦理而定。

二、網路安全暨科技風險監理研討會

自資訊作業檢查觀點，探討銀行運用不同資訊科技 (information technology, IT) 所涉特殊風險，以及以統合監理方法對 IT 與業務風險關聯性進行風險管理。

(一) 探討議題

1. 資訊科技風險與當前金融機構浮現之主要議題。
2. 資訊科技與業務風險連結點納入統合監理之方法。
3. 資訊科技風險管理之預期事項，包括資訊安全、資料治理、系統供應商管理與營業不中斷計畫等。
4. 對資訊科技適當管控之監理期望，包括組織架構、策略規劃及稽核作業。
5. 對金融機構管理層提供有關資訊科技風險與其對整體機構影響之建議。

上述議題涵蓋網路安全、雲端運算、行動銀行與行動支付、金融科技、資料治理(data governance)、委外處理及統合監理等 7 項重要監理領域(圖 2.1)，與檢查作業有關者尚包括災害復原計畫、IT 風險管理組織架構、策略規劃及 IT 稽核等資訊管理作業等。

圖 2.1 資訊科技監理之重要領域



資料來源：(1)網路安全與資訊科技風險監理研討會簡報資料；(2)作者繪製。

(二)主要提問與講座答復摘要

- 1.簡報以專節介紹「統合監理」 (integrated supervision)，其與「合併監理」 (consolidated supervision)之字義有無區別？

講座回答：

依 Fed 監理用詞，統合監理係應用於 IT 監理與檢查作業，旨在描述檢查人員須將 IT 風險納入整體業務風險(信用、市場、流動性、作業及法律等風險)作綜合評估；合併監理則指對金融集團母公司與其旗下海內、外分支機構全體業務與財務之監管。

- 2.Fed 檢查人員可否要求受檢單位提供專用稽核識別帳號與密碼，允許其進入受檢單位電腦系統搜尋與調閱資料？

講座回答：

Fed 檢查作業係採「不碰觸原則」(no-touch principle)，不會要求銀行提供稽核識別帳號與密碼，所有檢查均透過受檢單位提供書面資料查核。若發現有異常或重大缺失涉及刑事犯罪，則移請檢調機關辦理。

3. 美國眾議院共和黨議員 Patrick McHenry 已於上(2016)年 9 月 22 日與另一議員 Kevin McCarthy 聯署提出「金融服務創新法」(Financial Services Innovation Act of 2016)草案，目前該法案審議進度及要旨為何？

講座回答：

1. 該法草案目前仍在眾議員相關委員會(包括金融服務、農業及商品交易、能源暨信用等委員會)中審議，眾議院通過後，尚須送請參議院覆議。鑒於冗長之審議程序，短期內似無法完成立法。
2. 草案旨在創設類似英國金融行為監理署(Financial Conduct Authority, FCA)或澳大利亞證券投資委員會(Australian Securities and Investments Commission, ASIC)所推動的「金融監理沙盒」機制，主要方法有二
(1) 在相關政府部門建立金融科技監督機制，例如要求聯邦金融權責機關，包括財政部金融管理局、證管會及聯準會等，在機關內部設置「金融服務創新辦公室」(Financial Services Innovation Offices, FSIOs)，以利協助金融科技業者測試新種金融商品或業務，相關權責機關主管並組成「金融服務創新聯繫委員會」(FSIO Liaison Committee)，以促進跨機關間之協調合作事宜。
(2) 採法規豁免制度，權責機關得針對金融科技業者所提出之創新計畫，核定可據以執行之法遵方案。
4. 國際性支付系統開發公司 Ripple，已利用分散式總帳技

術，研發即時清算、貨幣兌換及跨國匯款系統，Fed 對其監管立場為何？

講座回答：

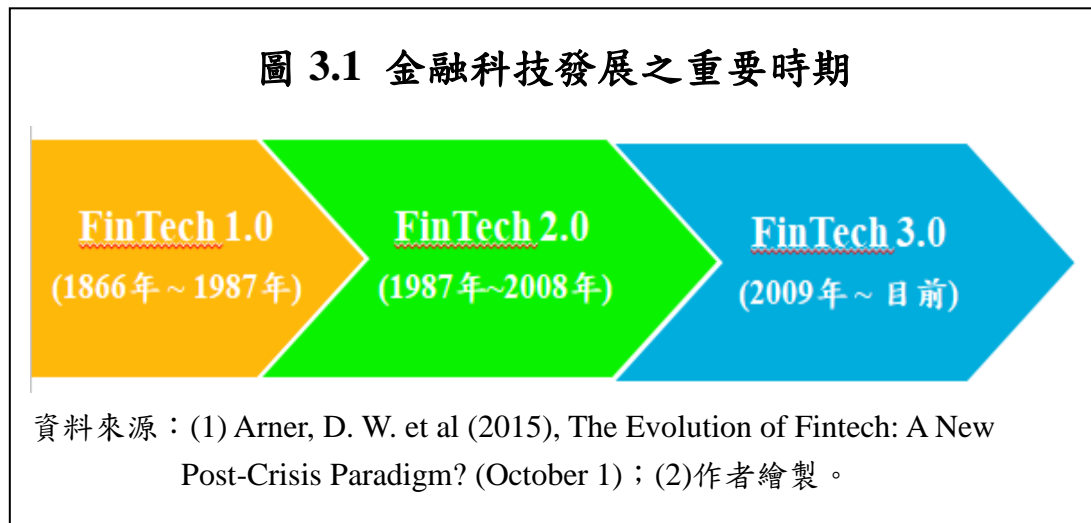
Ripple 或其他金融科技業者所研發之區塊鏈或分散式總帳技術可能改變現行結算與清算系統，牽涉層面廣泛，Fed 目前對其仍持審慎態度，並將密切關注其發展動向。

參、網路安全暨科技風險監理

本章先鋪陳金融科技之發展階段作為背景，接續就研討會簡報所提及之 IT 風險管理與監理，以及其應用不同新技術所浮現之特殊風險監理議題，摘述討論要點。

一、金融科技發展階段

依據 Arner, Douglas W. 等人研究¹，全球金融科技發展歷經 3 個重要時期(圖 3.1)。



第一代(所謂 FinTech 1.0)可溯自 1866 年迄至 1987 年，藉初期發展之科技基礎設施，透過橫跨大西洋間之傳輸電報，促成金融國際化。在此時期，1967 年計算機與自動提款機的問世開啟了金融服務現代化先河，並為金融全球化之發展奠立基礎，其中以 1987 年美國股市崩盤喚起全球共思解決經濟金融難題，作為該時期結束之重要事件。

¹ 詳參 Arner, D. W., J. Barberis, and R. P. Buckley (2015), The Evolution of Fintech: A New Post-Crisis Paradigm? (October 1). University of Hong Kong Faculty of Law Research Paper No. 2015/047; UNSW Law Research Paper No. 2016-62. Available at SSRN: <https://ssrn.com/abstract=2676553>

第二代(FinTech 2.0)始自 1987 年迄至 2008 年，在此時期，金融業逐步推出傳統數位化金融服務，電子交易處理及電腦化風險管理作業日漸風行。其中，以美國富國銀行(Wells Fargo)於 1995 年利用網際網路提供客戶連線查詢帳戶服務；2001 年美國及其他主要國家銀行已普遍應用網路作為金融服務工具；2005 年第一家無實體銀行出現在英國等，最為著例。

第三代(FinTech 3.0)則自 2009 年起迄至目前為止，金融科技在已開發及開發中國家蓬勃興起之新時代，其發展背景與全球金融危機發生後，民眾對金融業觀感欠佳、監理尺度趨嚴、主要國家金融政策及經濟發展情況等因素有關。本時期並非以金融業提供之金融商品或服務為特徵，而係以誰提供金融商品服務為判定標準。特別是，西方先進國家與亞非地區國家在此時期之發展動機分歧，前者係金融危機發生後科技業者所推動之創新作為；後者則為追求經濟發展所驅動之現象(尤其是中國大陸)，Arner, Douglas W.等人將亞非二地區之金融科技發展之特殊性稱為 FinTech 3.5。

二、資訊科技風險監理概論

主要包括 IT 風險特性、風險結合下之管理與監督，以及風險聚焦之檢查作業。

(一)IT 風險特性

- 1.擴張性—金融業務倚賴資訊系統處理程度日益加深，導致科技風險與業務風險聯結。
- 2.動態性—金融科技不斷創新，引進新風險。
- 3.挑戰性—不易執行與時俱進、靈活應對之監理政策。

(二)IT 風險與業務風險結合下之管理

- 1.當前銀行業務策略與 IT 有關者主要有網路安全、雲端運算、行動銀行、金融科技，以及支付系統等 5 大領域，大幅超越傳統銀行電子資料處理 (electronic data processing, EDP) 範疇，並衍生特殊態樣風險。
- 2.監理機關之檢查人員宜採行「由上而下方法」(top-down approach)，檢視銀行經營策略(董事會決策)是否改變、有無計畫引進與 IT 有關之新種營銷商品、業務(或服務)、配合更新 IT 設備(或工具)，並審慎評估經營策略變化所產生之成本、效益及潛在風險²。

(三)風險聚焦之檢查作業

1.風險聚焦檢查

除原有金融業務風險外，尚須視 IT 功能特性找出作業盲點與潛在風險，檢查範圍包括下列二大層面：

- (1)業務操作：包括存取登錄與認證管理、網路與行動銀行、實體分行與遠端抓取(remote capture)、電訊傳輸、自動提款機作業、媒體交換自動轉帳之結(清)算作業、虛擬平台與雲端，以及營運模式等。
- (2)風險管理：包括資訊安全、網路安全、資訊服務供應商(委外作業)風險管理、營運不中斷與災害復原、傳輸媒介應用程式存取控制、科技變革管理、資料管控及電腦

² 相關風控與稽核作業可參美國資訊系統稽核與控制協會(Information Systems Audit and Control Association, ISACA)於 1996 年發布之「資訊與相關技術的控制目標」(Control Objectives for Information & Related Technology, 簡稱 COBIT)，該文件提供企業管理人員、稽核人員及 IT 人員有關 IT 管理與治理之最佳實務準則，目前已成為國際公認的 IT 管理與控制標準。現有版本 COBIT 5 已於 2012 年 6 月更新發布。

稽核作業等。

2. 檢查程序

- (1) 瞭解資訊作業環境：IT 系統之委外處理、自主管理或兩者併行運用，均會影響風險管控程度。
- (2) 辨識科技與業務風險：包括管理程序、資訊設備、監督周延性、安全性及可用性。
- (3) 進行風險評估：依據 Fed 監理函令(supervisory letter, SR) 第 99-8 號(有關 IT 檢查評等)、第 99-17 號(銀行監理評等)及第 00-3 號(IT 檢查頻率)，以及聯邦金融機構檢查委員會 (Federal Financial Institutions Examination Council, FFIEC) 資訊科技統一評等制度(Uniform Rating System for Information Technology, URSIT) 等規定辦理。IT 檢查之 5 級評等與一般業務檢查 CAMELS³ 評等制度所採分級相同。
- (4) 賦予受檢機構 IT 檢查評等：包括內部稽核、管理監督、開發與購置、支援與傳輸等 4 項評估項目。

三、網路安全(cybersecurity)

溯自 1969 年 10 月，美國加州大學洛杉磯分校(UCLA) 與史丹佛研究院(Stanford Research Institute, SRI) 兩個實驗室的電腦第一次試連成功後，隨著遠程終端模擬(Telnet)、檔案傳輸(File Transfer Protocol, FTP)及通訊協定(Transmission Control Protocol/Internet Protocol)等技術標準陸續制定，網際網路之應用發展方興未艾。惟自 1988 年 11 月全球首次出現網路蠕蟲(病毒)，癱瘓數千部電腦事件⁴之後，網路安全已成

³ CAMELS 係指資本適足性(C)、資產品質(A)、管理能力(M)、獲利能力(E)、流動性(L)，以及市場風險敏感性(S)等 6 個要素。

⁴ 詳參「Internet 的發展史」

為資訊科技應用之重要議題⁵。主要國家近年亦制定相關法規，例如美國 2015 年 12 月之「網路安全法」(Cybersecurity Act of 2015)及歐盟上(2016)年 7 月之「網路安全指令」(EU Directive on Cyber-security)。

(一)與資訊安全之差異

資訊安全強調資訊本身之可利用性、機敏性、完整性、信賴性及可歸責性，且為綜合評估銀行 IT 環境良窳之重要因素。網路安全雖與資訊安全及科技基礎設施密切相關，惟被視為可能造成系統性癱瘓、影響深遠的風險。

(二)風險源起

銀行內部或外部因素所產生的作業弱點，分為下列 4 面向：

- 1.科技面：包括軟(硬)體、連結網絡、系統等缺陷。
- 2.組織面：員工對風險認知不足、異常事件處置不當及資訊系統管理不到位等。
- 3.人為面：員工好奇、舞弊或背信等不當行為。

(<http://web.ntnu.edu.tw/~499700326/Internethistory.htm>)、The Day the Infant Internet Uttered its First Words, UCLA Professor Leonard Kleinrock Homepage, (https://www.lk.cs.ucla.edu/internet_first_words.html)及維基百科「Morris worm」。

⁵ 網路威脅型態包括惡意軟體(Malware)、病毒(Virus)、蠕蟲(Worm)、木馬(Trojan Horse)、垃圾郵件(Spam)、網路釣魚(Phishing)、網址嫁接(Pharming)、間諜軟體(Spyware)、廣告軟體(Adware)、殭屍電腦與殭屍網路(Bot and Botnet)及勒索軟體(Ransomware)等 11 類惡意軟體，這些程式會在未經他人許可或知情下，安裝到其電腦上，透過網站來散播、隱藏、更動及竊取資料，並相互結合進行犯罪行為。資料來源：(1)趨勢科技全球技術支援與研發中心，<https://blog.trendmicro.com.tw/?p=5795>；李樹民「淺析企業網路安全的潛在風險」，行政院主計總處，<http://www.stat.gov.tw/public/Data/7951125871.pdf>；以及(3)劉先覺(2017)，「網路資安風險與因應之道」，工商時報，2月8日。

4.設備面：例如傳輸媒介或行動載具遭受病毒感染等。

(三) 監理挑戰

- 1.威脅不斷變化之動態特性。
- 2.風險來源不受地理疆界限制。
- 3.檢查人員科技專業知識不足。
- 4.不易判定當前監理實務之適用性。
- 5.欠缺指導原則及標準規範。

四、雲端運算(cloud computing)

雲端運算看似一種抽象概念⁶，惟本質上屬於分散式電腦運算的架構，亦即資訊服務供應商整合各項軟硬體配備，建立結構化資訊匯集之共享平台，可由不同電腦同時進行運算、互相存取及溝通。其實務運作係以網路傳輸為基礎，資料全部建置於平台，使用者本身不放置資料，亦得隨時隨地視需要自該平台存取。不同機關(構)之定義如表 3.1。

表 3.1 雲端運算之定義

機關(構)	定 義
美國商務部國家標準與科技研究院	係指透過結構化運算資源(例如連結網路、伺服器、資料儲存、應用程式及相關服務)，使資料使用者可在任何時間、地點，方便迅速存取共用資

⁶ 雲端運算一詞最早在 1997 年由南加州大學教授 Ramnath K. Chellappa 所提出，該教授以抽象、簡單的方式比喻複雜的電腦網路架構。因在電腦流程圖中，網際網路常以一個雲狀圖來表示，故業界遂以該圖象類比為雲端運算，亦稱為「網路運算」。詳參郭斯彥(2010)，「雲端運算—資訊科技成熟下的委外產物」，臺大校友雙月刊，第 72 期雙月刊，11 月 15 日，以及維基百科。

	料池，並減輕使用者資料管理負擔及服務提供者介入互動至最低的一種服務模式。
美國聯邦金融機構檢查委員會	係指顧客使用者自第三方服務提供者所建置之網路平台，按顧客需要得隨時接收資訊科技服務之方式，此種從使用自有資源轉移至利用共享資源的運作模式，謂之。
維基百科	係指使用網際網路所傳送各項運算資源(軟硬體)的服務

資料來源：網路安全暨科技風險監理研討會簡報「Cloud Computing」，投影片 3。

雲端運算具有 5 項重要特徵、3 種服務模式(service modes)及 4 類部署模式(deployment models)(圖 3.2)；其應用平台基礎設施如圖 3.3。

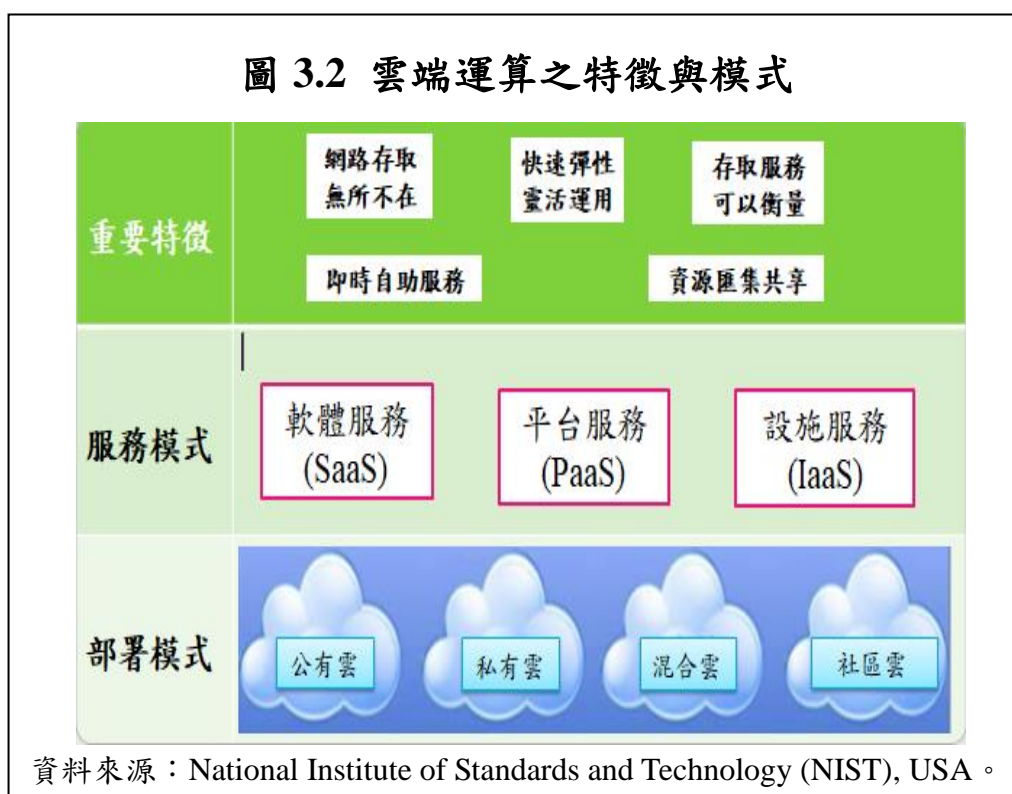
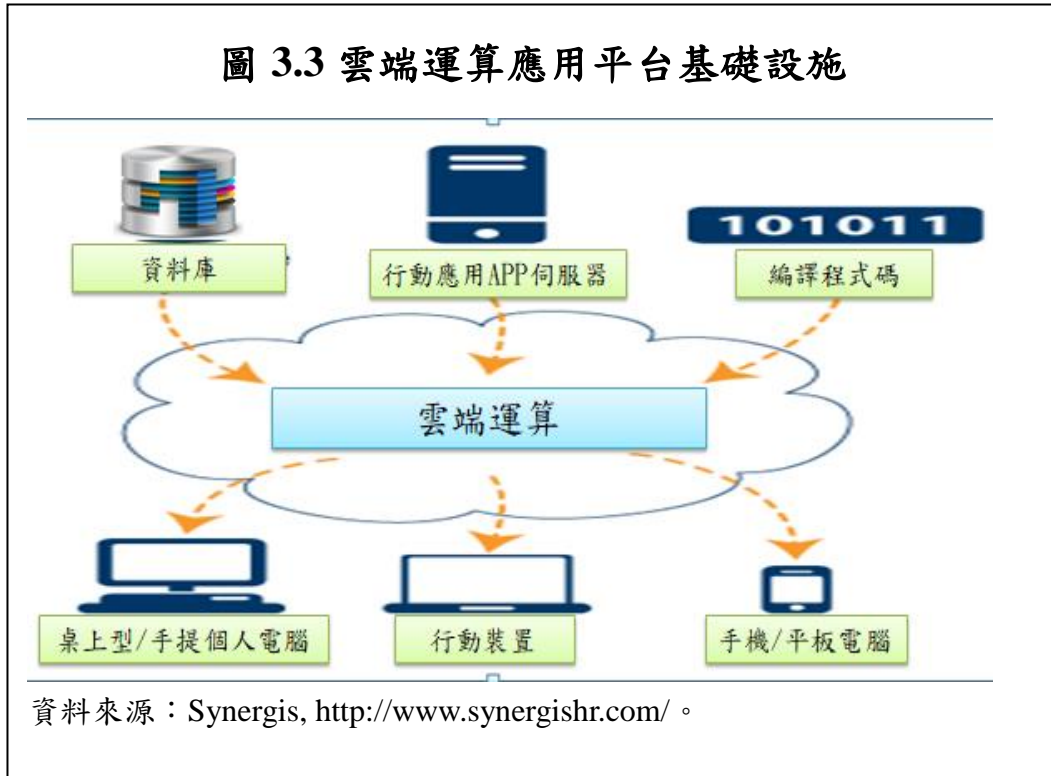


圖 3.3 雲端運算應用平台基礎設施



(一)特殊風險

- 1.內部資料透過雲端存取，易滋對外散布流通問題。
- 2.雲端平台無法提供預期服務時，變通運用的其他支援有限。
- 3.平台資訊(或資料)無預期變更。
- 4.平台資產(或資料)可能重複，或未經通知而儲存他處。
- 5.平台服務或資料可能暫時中斷。
- 6.銀行業務無預期大幅波動所須承擔的變動成本。
- 7.平台提供者可能不瞭解或不受使用者業務要求或法規規範。

(二) 監理考量⁷

1. 銀行管控鬆弛或不當。
2. 法規遵循挑戰。
3. 平台綁約限制。
4. 平台提供者之惡意內線行為(malicious insider)。
5. 法律風險，起因於跨國存取資料所衍生之司法傳訊或用於訴訟或調查的電子資料搜索(electronic discovery 或 E-discovery)。
6. 資料保護欠嚴謹。
7. 防火牆隔離失敗。

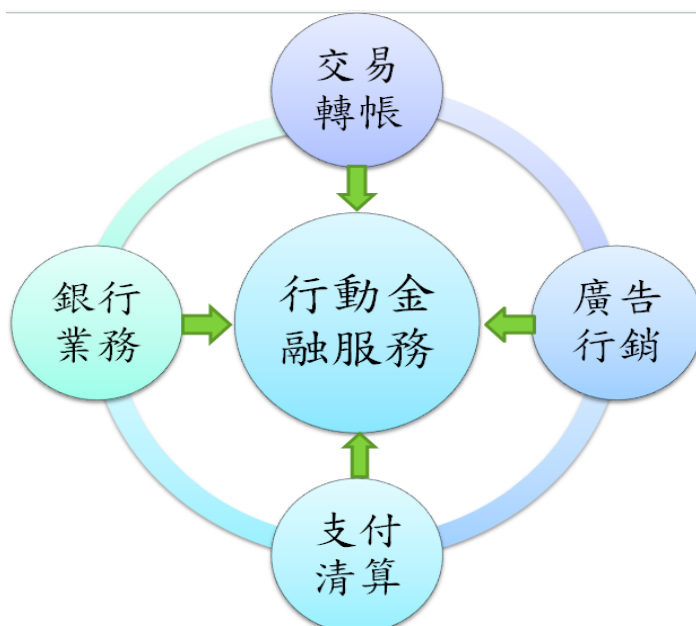
五、行動銀行與行動支付

(一) 行動金融服務涉及之 4 大面向

行動金融服務係金融機構利用行動裝置或載具，以連線(on-line)或離線(off-line)方式，提供金融商品或服務。該服務涉及之營運層面包括廣告行銷、銀行業務、交易款項轉帳及支付清算，與透過營業廳面對面交易、款項撥轉支付及跨行結(清)算之傳統經營方式明顯不同(圖 3.4)。

⁷ 歐洲銀行監理委員會(European Banking Authority, EBA)本年 5 月公布一份「雲端運算委外處理建議」(Draft recommendations on outsourcing to cloud service providers)諮詢報告，該報告旨在補充歐洲銀行監理委員會(Committee of European Banking Supervisors, CEBS)前於 2006 年 12 月所發布之一般性資訊作業委外處理準則。該報告建議銀行業審慎管理雲端運算委外處理所可能產生之風險，包括委外契約簽訂、組織架構安排、相關業務在不同服務供應商間之轉移、緊急應變計畫、契約終止或退出策略、資料處理與儲存地點等要項，並建議依「比例原則」(principle of proportionality)，視組織架構、營運環境、業務規模、特性及複雜度等因素，執行適當管理措施。

圖 3.4 行動金融服務涉及之 4 大面向



資料來源：(1)網路安全暨科技風險監理研討會簡報「Mobile Banking and Payments」，投影片 3；(2)作者繪製。

(二)行動銀行(mobile banking)特殊風險

- 1.部分國家欠缺明確法規。
- 2.可能產生非預期的不利結果，例如風險、舞弊及資安問題。
- 3.資料管控與銷售供應商作業不良問題。
- 4.金融創新或創新失敗對消費者衝擊不明。
- 5.法規監督或消費者保護責任未釐清。
- 6.共用平台可能有營運失靈匯聚的風險。

(三)作業規章須納入之重要監控項目

- 1.資料儲存流程。
- 2.資料分享程序。
- 3.行動載具連線作業。

- 4.資料處理與刷卡載具機制。
- 5.服務或商品特性之控管。
- 6.應用設備或程式之核准。

(四)監理考量

- 1.監控行動服務或商品，包括複雜支付系統間之相互操作性(interoperability)。
- 2.監控第三方機構，包括與非銀行之合作廠商、聯繫網絡、銷售供應商及服務提供者所簽訂之契約。
- 3.檢查範圍應涵蓋法律風險與法遵風險。
- 4.檢視客戶暴險限制(含舞弊偵測及應對計畫)。
- 5.落實資訊安全、網路安全及教育客戶要求。
- 6.檢視交易驗證及授權作業。

(五)行動支付系統與銀行作業

1.新支付工具之管理構面

支付系統有零售及批發二種類型，其管理重心在防範系統運作中斷，造成金融體系流動性，甚至系統性危機。

檢查項目包括：

- (1)系統部署與設備配置。
- (2)結(清)算執行程序。
- (3)銀行內部作業及客戶使用情形。
- (4)舞弊或犯罪行為之偵測。

2.監理重點

- (1)前端交易控制。
- (2)後端作業控制。
- (3)災害復原與營業不中斷。

- (4)資訊安全。
- (5)銷售供應商管理。
- (6)新商品風險評估。
- (7)稽核計畫及執行結果。
- (8)風險報告頻率與內容。
- (9)網路安全威脅程度。

六、金融科技(financial technology, FinTech)

(一)特殊風險

- 1.信用風險：統計模型不精確及金融行為逆選擇等問題。
- 2.法遵風險：違反有關公平借貸、消費者保護、洗錢防制及銷售供應商管理等規定。
- 3.作業風險：引進創新科技對現行作業系統之衝擊與融合問題。
- 4.資安疑慮：客戶個資及交易資料之遺失或遭竄改等風險。
- 5.未知風險：科技創新帶來之新風險，未及時納入監理範疇。

(二)監理考量

FinTech 涉及多種商品與服務，且其態樣正在不斷變化當中，監理人員宜掌握金融實務發展：

- 1.瞭解金融機構對從事 FinTech 業務是否做好準備。
- 2.對 FinTech 持開放態度，不宜僅看待其風險面，尚須觀察其對消費者或市場發展之利益。
- 3.瞭解不同監理機關對 FinTech 新興議題之政策或看法。
- 4.在允許 FinTech 發展機會同時，適當兼顧其帶來之風險疑慮。

(三)美國聯邦金融權責機關對 FinTech 創新之因應措施

鑒於金融科技應用所衍生之交易糾紛及對金融發展與金融穩定造成之潛在風險，美國聯邦金融監理機關近年已著手採行下列因應措施(表 3.2)，期掌握金融科技趨勢及其對金融政策與貨幣政策之影響。

表 3.2 美國主管機關對金融科技之因應措施

主管機關	因應措施
財政部	<ul style="list-style-type: none">• 上年 5 月發布「網路借貸白皮書」
金融管理局	<ul style="list-style-type: none">• 上年 3 月發布「負責任創新白皮書」，並於同年 6 月舉辦相關之公開論壇活動。• 研議核發限制目的之金融科技營業執照及採行金融監理沙盒機制。
聯邦準備體系理事會	<ul style="list-style-type: none">• 2015 年 7 月宣布成立指導委員會，由理事 Lael Brainard 擔任主席，並邀集業者參加建言，全面檢討支付系統業務。• 內部成立研究小組，研議金融科技新興議題。• 與巴塞爾委員會共同研議有關支付系統議題。• 研議有關洗錢防制/打擊資恐及分散式總帳技術 (distributed ledger technology, DLT) 議題。
聯邦存款保險公司	<ul style="list-style-type: none">• 2015 年 12 月發布「監理透視季刊」有關網路借貸專文。• 對與銀行合作之金融科技業者，辦理有限

	<p>度之金融檢查。</p> <ul style="list-style-type: none"> • 上年 7 月提出第三方貸款指導原則草案。
消費者金融保護局	<ul style="list-style-type: none"> • 上年 3 月發布有關網路借貸之消費者保護政策聲明。 • 受理消費者投訴網路借貸糾紛。 • 上年 10 月發布有關金融創新維護消費者利益及促進市場發展之政策報告。
聯邦貿易委員會	<ul style="list-style-type: none"> • 自上年 6 月起，舉辦一系列之網路借貸論壇活動，作為檢討法規參考。

資料來源：網路安全暨科技風險監理研討會簡報「FinTech」。

七、資料治理

(一) 意義

資料治理係指組織處理資料的政策與程序，以確保內部重要資料正確且值得信賴的一系列活動。執行資料治理能將錯誤資料自資料流程與業務流程中及早篩選出來，建立可靠資訊以供決策使用，並可降低企業整體風險⁸。

(二) 目標

資料治理不論是採委員會或工作小組形式，其重要性皆不及於建立系統性方法，且能提供一貫的作業程序、使用規則、支援技術及結果紀錄。資料治理須賴組織內之員工、作業流程(環境)及資訊科技(軟硬體設備)等三大元素，共同建立組織內部資料管控制度，其執行目標主要包括：

1. 增進組織決策之一致性與可信度。

⁸ 詳參維基百科「Data governance」。

- 2.確保資訊安全及系統順暢運作。
- 3.達成資料產出效益之極大化。
- 4.降低違規處分風險。

(三)計畫項目

- 1.訂定政策與程序。
- 2.建立工作流程檔案。
- 3.執行資料可追蹤性實務作業。
- 4.確保準確性與完整性之控管。

(四)檢查重點

- 1.受檢單位是否建立資料治理機制。
- 2.准許及禁止存取資料權限。
- 3.有無訂定資料管理政策規章。
- 4.風險管理架構是否納入資料治理風險評估作業。
- 5.資料治理政策是否考量其他國家或地區之法遵情形。
- 6.資料治理對資安事件之因應機制。

八、委外處理

銀行為強化其核心業務之專業性及競爭力，通常會將部分作業委託第三方服務供應商處理，若該供應商操作管理不當，可能造成銀行之潛在風險。

(一)委外風險

- 1.法遵風險：委外之商品或服務不符我國法規。
- 2.集中風險：委外契約集中於少數幾家供應商。
- 3.國家風險：外國服務供應商所在國家處於政治、經濟或社會不穩定之情況。

- 4.聲譽風險：委外廠商業績或形象欠佳之連帶影響。
- 5.作業風險：委外廠商因內部管理與控制欠佳、人為作業疏失及外部衝擊事件等所產生之風險。
- 6.法律風險：因委外服務異常所面臨訴訟之風險。

(二)檢查重點

- 1.董事會是否訂定委外處理之策略及目標。
- 2.管理階層是否依上述策略目標訂定相關作業規範、風險管控及效益評估程序。
- 3.風險評估項目包括委外契約之法規遵循、內部控制、服務水準、處理效益及報告機制等，並由資訊、法遵、法務人員及內部稽核共同分析檢視及評估。
- 4.有效確認受託機構是否有足夠資安措施保護客戶資料。
- 5.依策略計劃與風險評估項目建立委外作業標準程序，並就委外作業終止，建立緊急應變計畫。
- 6.指派專人監督委外作業，並定期向董事會報告。

九、統合監理

(一)監理考量

- 1.資訊科技之作業疏失會影響個別銀行之安全穩健，甚至透過網路傳遞，衝擊整體金融體系。
- 2.銀行業務由人工與電腦共同處理，其風險本質相同，包括信用、作業、市場、法律(或聲譽)、流動性及守法性等6大類型。
- 3.資訊科技風險評估項目包括對資訊系統影響性之管理(所謂 impact management)及賦予檢查評級，並納入受檢單位整體檢查評級作綜合評估。

(二)當前資訊科技之主要監理議題

在資訊環境快速變遷環境下，監理人員對資訊科技應用之關切重點包括治理與風險管理、資訊安全、服務供應商風險管理及資訊科技基礎設施等4大項(表3.3)，亦為銀行業面對科技創新環境須審慎應對之問題。

表 3.3 當前資訊科技主要監理議題

治理與風險管理	資訊安全
• 資料品質	• 資料存取管理
• 資訊化對盈餘產生之壓力	• 網路安全
• 社群網路	• 應用軟體安全
	• 行動裝置使用
服務供應商風險管理	資訊科技基礎設施
• 持續對服務供應商之管理	• 雲端運算
• 全球服務供應商之管理	• 虛擬化
• 安全服務供應商之管理	• 營業不中斷計畫

資料來源：網路安全暨科技風險監理研討會簡報「Integration Supervision」。

肆、國際組織對金融科技風險監理之觀點

近期國際金融組織對金融科技創新所帶來之機會與風險，陸續提出相關研究報告、作業準則或監理架構。本報告彙整相關研究報告重點，期就總體監理原則與個體金融檢查相互為濟角度，提出補充說明。

一、國際貨幣基金(International Monetary Fund, IMF)

IMF 本年 6 月公布一份名為「金融科技與金融服務初探」之討論報告⁹，著重探討跨境支付對金融穩定所帶來之影響。該報告發現，數位科技之快速發展已改變金融服務樣態：

- (一)金融中介機構、金融市場及新服務提供者間之界線日益模糊。
- (二)進入障礙正在改變，有些情況是障礙降低，惟其他情況卻有提高現象，特別是在大型封閉式金融服務網路的出現，降低(或排擠)其他業者參與競爭機會。
- (三)即使大眾對傳統金融中介機構之倚賴性降低、更多金融服務網路及新型態服務提供者出現，信任(trust)仍是金融交易之必要元素。
- (四)科技可改善跨境支付作業，提供更有效率與較廉價服務，並可降低防制洗錢(AML)及打擊資恐(CFT)之法遵成本。

該報告建議金融監理機關宜在鼓勵金融創新與維持金

⁹ He, D, R. Leckow, V. Haksar, T. Mancini-Griffoli, N. Jenkinson, M. Kashima, T. Khiaonarong, C. Rochon, and H. Tourpe (2017), “Fintech and Financial Services : Initial Considerations,” International Monetary Fund, IMF discussion note SDN/17/05.

融穩定間取得適當平衡：

- (一) 監理機關須加強關注不同型態業者及市場平台所提供之金融性服務。
- (二) 制定法規與業務標準，要求業者強化公司治理，俾確保資料與演算法(algorithm)之正確性，以及交易平台的誠信經營。
- (三) 支持開放性之金融服務網路，並納入政策考量。
- (四) 明定立法原則，以釐清相關參與者在全球新金融生態下的權利與義務。

二、國際清算銀行(Bank for International Settlements, BIS)

BIS 貨幣經濟處本年 8 月公布一份名為「金融科技機會」之研究報告¹⁰，內容旨在評估金融科技對金融業之潛在影響。作者闡述金融科技業者的出現係因為金融服務價格昂貴，故有吸引其參與金融領域的誘因。

目前各國對金融科技之監管方式受政治經濟運作與行政作業程序框架的影響，難免產生極大的協調成本，短期內似乎不易作結構性改變。惟順應金融科技之市場需求與創新環境，管理重心似宜作較大幅度之調整，並建立業者有正當誘因之經營環境。該報告提出 4 項監管指導原則：

- (一) 鼓勵業者加入經營，並關注要求公平競爭的嚴格管理方法可能抑制金融創新與金融改革的副作用。
- (二) 逐步推動創新服務，例如行動支付、即時支付及數位貨幣發行。

¹⁰ Philippon T. (2017), “The FinTech Opportunity,” BIS Working Papers No 655, Bank for International Settlements, Monetary and Economic Department, August.

(三)監視金融科技業者之資本規模及併購行為，避免對金融穩定產生負面影響。

(四)持續關注並即時研議應對創新業務所產生的監理議題，例如自動化投資顧問服務(Robo-Advisor)衍生之法律、作業及消費者保護等議題。

三、金融穩定理事會(Financial Stability Board, FSB)

金融科技快速發展為金融業務帶來創新機會，相對地亦對金融穩定造成潛在風險。基於多數創新方法尚未經歷一個完整金融循環期間的檢驗，值此金融科技發展初期(或快速成長期)所作之監理決策，可能為日後類似案件立下重要先例，為達興利除弊目的，20 國集團(G20)輪值國德國建議 FSB 建立監控方法，並自金融穩定角度，辨識相關監理議題。

FSB 爰於本年 6 月發布一份名為「金融科技對金融穩定之涵義：主管機關須注意之監管議題」報告¹¹，列舉 10 大建議作為各國監理機關持續監控與評估金融科技風險之參考，包括 3 項國際合作之優先領域及 7 項主管機關須注意之監管議題：

(一)國際合作之優先領域

- 1.管理第三方服務提供者可能產生之作業風險。
- 2.管理網路風險，防範網路攻擊事件，並確保網路安全。
- 3.管理總體金融(macrofinancial)風險，評估資訊揭露不足之金融科技業務對系統重要性及順循環之潛在影響。

¹¹ Financial Stability Board (2017), “Financial Stability Implications from FinTech: Supervisory and regulatory issues that merit authorities’ attention,” 27 June.

(二)主管機關須注意之監管議題

1. 研議跨國法律與監管安排之調和議題，例如智能合約及分散式總帳技術(distributed ledger technology, DLT)之跨國應用。
2. 檢視大數據分析之治理與資訊揭露規範架構。
3. 及時檢討修訂金融業務法規，以因應市場發展需要。
4. 與私部門不同金融科技業者保持溝通聯繫，並相互學習，俾找出新的適當監管模式。
5. 相關主管機關間宜進一步建立有關金融科技監理之溝通管道。
6. 提升監理人員有關金融科技新領域之專業知識與技能。
7. 研究數位貨幣對本國金融體系及全球貨幣架構之影響及相關規範架構(例如利用虛擬貨幣所為之非法活動及網路攻擊等)。

四、防制洗錢金融行動工作組織(Financial Action Task Force on Money Laundering, FATF)

FATF 本年 5 月於美國加州聖荷西舉辦「2017 金融科技與監理科技論壇」¹²，旨在提供監理機關與金融科技業者等各界人士討論平台，探討有關支持金融業務創新、洗錢與資恐潛在風險，以及新興科技對監理挑戰等議題。

上述論壇提出下列 5 項指導原則(稱為「聖荷西原則」(The San Jose Principles)：

(一)打擊資恐與洗錢仍為金融科技發展之共同目標。

¹² Chairman's Summary of the FATF FinTech and RegTech Forum 2017, San Jose, California, United States, 25-26 May 2017.

- (二)鼓勵公私部門參與，增進雙方對金融科技發展、潛在風險及關切議題之瞭解。
- (三)追求正向與負責任之創新，強化防制洗錢與打擊資恐之有效性。
- (四)設定清晰之監理期望與制定靈活應變的法規，以減低風險及鼓勵創新。
- (五)調和國內與國際間相關法規管理之公平性與一致性。

五、歐洲聯盟(European Union, EU)

EU(簡稱歐盟)定期召開會員國之「金融中心圓桌會議」，探討有關該經濟區內之金融發展與監理議題，並於上年1月公布一份名為「歐盟金融科技法規管理架構」報告¹³，旨在提供會員國監理機關檢視、評估及訂定各該國有關法規之準據。整體而言，金融監理機關通常採行即時應對(re-active)與積極主動(pro-active)之監理方法，執行下列4項重要之法定職責：

- (一)金融穩定。
- (二)審慎監理。
- (三)誠信經營。
- (四)公平競爭。

歐洲銀行監理機關(EBA)復於本年8月公布一份金融科技監管方法之諮詢報告¹⁴，說明該機關對會員國監理法規檢視比對成果，並建議後續之研議工作：

- (一)營業許可與監理沙盒機制。

¹³ EU Financial Centres Roundtable (2016), “EU FinTech Regulatory Framework,” 22 January.

¹⁴ European Banking Authority (2017), EBA Discussion Paper on Fintech, 4 August.

- (二)信用機構、支付機構及電子貨幣機構之業務風險。
- (三)金融科技對上述3類機構營運模式之影響。
- (四)消費者保護與消費金融業務議題。
- (五)金融科技對問題金融機構清理之影響。
- (六)金融科技對防制洗錢及打擊資恐之影響。

伍、心得及建議事項

金融科技有助於創新經營模式、改善作業效率、提升客戶體驗滿意度，以及促進數位普惠金融。惟銀行應用日益精密複雜之高科技，其伴隨產生之負作用，輕則作業中斷、資訊外洩、財物遭竊；重則支付清算失序、市場信心動搖、甚至造成金融恐慌，其對金融體系之潛在風險不容小覷。

目前全球金融科技發展處於快速成長期，依據媒體報導與研究文獻，主要國家相當重視消費者保護、業者健全經營、公平競爭與產業競爭力，以及金融穩定等問題。特別是在重大資安事件發生後，主管機關即會啟動檢討改革措施，無論在管理制度、機制建立或業務規範等方面，以收亡羊補牢之效。基於金融科技風險難以掌控，國際準則制定機構頻頻呼籲各國監理機關，務須提高警覺、持續監視金融科技業務活動，並建議採行適度監理措施，以在鼓勵創新與維持穩定間取得適當平衡。

一、研討心得

他山之石，可以攻錯，任何自國際會議所習得之經驗及啟示，均有助於改進現行監理作業。研習心得如次：

(一)各國重視總體審慎及金融科技監理

依據 FRTI 訓練需求調查結果，前 5 項優先訓練主題中，有關總體審慎與金融科技監理主題即占 3 項，與本處填答之訓練需求項目大致類同，足資印證亞太區域國家央行與銀行監理機關均重視培訓職員，提升其對上述議題之專業能力。

(二)金融科技須「動態監管」

金融科技生態系統持續蛻變，金融監理宜以宏觀角度思考，調和「產業發展、公平競爭、安全穩健及消費權益」的監理目標。對於創新之金融商品、服務及商業模式，監理機關宜視環境變遷需要及行業發展成熟度，參酌國際監理實務，適時採行與時俱進之監管方法。

(三)增進同仁對金融科技實務之瞭解

美國 Fed 內部已成立研究小組，分別研議金融科技新興議題，俾即時掌握實務發展趨勢對其主管業務之影響，以利決策。本行亦於上年 2 月成立跨局處室之「數位金融研究小組」，透過研究討論與參與委外研究計畫，並就新生議題舉辦研討會，邀請金融科技專家分享實務經驗，該做法有助增進本行同仁對金融科技應用之專業知識。

二、建議事項

本報告彙整研討會資料及近期國際文獻，就金融科技監理提出建議：

(一)主管機關應督促金融機構強化資訊科技之風險控管

金融科技日趨複雜，未來發展樣態難以預期。在網際網路、無線傳輸及虛擬雲端之科技環境下，金融部門參與者均暴露在跨商品、跨市場、跨機構、跨地域之風險中。主管機關除透過政策聲明、提升金融從業人員對網路安全與資訊安全之風險意識外，允宜檢討修訂法規、作業規範及檢查手冊，督促業者強化風險控管機制，並視監

理需要，要求金融機構定期舉辦演練測試，俾確保個別機構之安全穩健及金融市場基礎設施之順暢運作。

(二)主管機關應掌握金融數位化發展態勢

金融機構在資訊科技業者加入競爭之壓力下，亟思改變傳統經營策略，以符合市場需要與時代潮流。除電子化(e化)作業外，期利用不同的數位科技方法，創新營運模式，拓展行銷通路，俾擴大交易服務層面及提升競爭力。準此，電子/網路/行動銀行逐漸對傳統金融機構所提供之實體分行服務造成衝擊，金融主管機關宜掌握該發展趨勢，以利對金融機構與金融業務之管理。

(三)主管機關宜持續關注監理科技之應用

現行各國金融監理與檢查實務多透過申報資料或調卷方式進行書面審核(或查核)。在金融科技盛行之下，未來監理科技(regulatory technology, RegTech)可望改變傳統書面審核作業，逐步採行線上檢核，將成為監理主流方法。金融主管機關宜檢視金融機構申報資料及審核作業，著手因應數位化時代的到來。

參考資料

一、會議資料

編號	講座	資料名稱
1		Agenda: 22 nd Advisory Group Meeting- Bank Supervisors
2	Noritaka Akamatsu	APEC Financial Regulators Training Initiative (FRTI)
3	Sue Jeffery	Training Program Review
4	Sue Jeffery	Review of Recent Survey (Bank Supervisors)
5	Noritaka Akamatsu	Asia-Pacific Economic Cooperation Financial Regulators Training Initiative Charter
6		Agenda: Regional Seminar on Cybersecurity/Technology Risk Supervision
7	Gwynne Williams Amol Vaidya	IT Risk Supervision
8	Gwynne Williams	IT and Business Risk
9	Gwynne Williams	IT Risk: Cloud Computing
10	Gwynne Williams	IT Risk: Cybersecurity
11	Gwynne Williams	IT Risk: Mobile Banking and Payments
12	Gwynne Williams	IT Risk: FinTech
13	Gwynne Williams	IT Risk: Payment Systems and Operations
14	Gwynne Williams	IT Risk Management: Information Security
15	Gwynne Williams	IT Risk Management: Data Governance
16	Gwynne Williams	IT Risk Management: Third Party Risk/Vendor Management
17	Gwynne Williams	IT Risk Management: Disaster Recovery and Business Continuity
18	Gwynne Williams	IT Risk Management: IT Audit
19	Gwynne Williams	IT Governance

20	Gwynne Williams Amol Vaidya	Integrated Supervision
----	--------------------------------	------------------------

二、相關文獻

1. Arner, D. W., J. N. Barberis and R. P. Buckley (2015), The Evolution of Fintech: A New Post-Crisis Paradigm? University of Hong Kong Faculty of Law Research Paper No. 2015/047; UNSW Law Research Paper No. 2016-62, October 1. Available at SSRN: <https://ssrn.com/abstract=2676553>
2. Bailey, T., J. M. Kaplan and C. Rezek (2015), “Book Excerpt: Repelling the cyberattackers,” McKinsey Quarterly, July.
3. Bianchi L. (2017), “FinTech Regulation (2.0): An Overview on the Proposed Three Element Solution,” Swiss Capital Markets Law, 7 February.
4. Chairman’s Summary of the FATF FinTech and RegTech Forum 2017, San Jose, California, United States, 25-26 May 2017.
5. EU Financial Centres Roundtable (2016), “EU FinTech Regulatory Framework,” 22 January.
6. European Banking Authority (2017), EBA Discussion Paper on Fintech, 4 August.
7. Financial Stability Board (2017), “Financial Stability Implications from FinTech: Supervisory and regulatory issues that merit authorities’ attention,” 27 June.
8. He, D., R. Leckow, V. Haksar, T. Mancini-Griffoli, N. Jenkinson, M. Kashima, T. Khiaonarong, C. Rochon, and H. Tourpe (2017), “Fintech and Financial Services : Initial Considerations,” International Monetary Fund, IMF discussion note SDN/17/05
9. Philippon T. (2017), “The FinTech Opportunity,” BIS Working Papers No 655, Bank for International Settlements, Monetary and Economic Department, August.