行政院及所屬各機關因公出國人員報告書

（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屆顧問小組會議及網路資安科技風險監理研討會」

# (APEC Financial Regulators Training Initiative 22st Advisory Group Meeting and the APEC FRTI Regional Seminar on Cybersecurity / Technology Risk Supervision)

## 摘要與心得報告


服務機關：金融監督管理委員會檢查局

姓名職稱：李偉旭　專員


派赴國家：庫克群島

出國期間：106 年　6 月 5 日 至 9 日

報告日期：106 年　6 月 30 日

# 參加「APEC 金融監理人員訓練倡議-第 22 屆顧問小組會議及網路資安科技風險監理研討會」

## 摘要

「亞太經濟合作金融監理官訓練行動計畫」(Asia-Pacific Economic Cooperation Financial Regulators Training Initiative，簡稱 APEC FRTI)之目的為藉由持續舉辦金融監理訓練，提升銀行業與證券業監理人員的分析與監理技能。訓練行動計畫包含顧問小組會議(Advisory Group Meeting)及主題研討會，顧問小組會議討論訓練執行及合作事宜，而主題研討會則就會員經濟體之監理課程調查需求，舉辦相關研討主題，達成監理資訊交流及合作。

本屆會議為 APEC 金融監理官訓練行動計畫第 22 屆顧問小組會議，由 APEC 金融監理人員訓練倡議秘書處及亞洲開發銀行舉辦，本次主辦國為庫克群島金融監督管理委員會（the Financial Supervisory Commission of Cook Islands），於 2017 年 6 月 5 日在庫克群島之拉羅湯加之 Edgewater Resort and Spa 會議室召開，顧問小組會議主要討論明(2018) 年度倡議之執行及合作事宜，並檢討 2016－2017 年度之執行成效。

會議討論重點包括（一）檢討 2016-2017 年已舉辦的金融監理人員訓練成果；（二）簡報訓練需求之調查結果；（三）研議是否繼續辦理該訓練倡議（四）規劃 2018 年之訓練計畫及徵詢各會員代表擔任主辦國之意願。另本屆上開討論重點之會議結論包含熱門優先訓練主題及 FRTI 工作小組經費來源籌措方案，如會議結論摘要所示。

金融業面臨網路科技發展與金融創新應用的趨勢，非金融業運用金融科技與傳統金融業競爭，促使金融業改變原有經營思維，開始大力研究發展金融科技，使用金融科技以擴大交易與服務之競爭力，惟伴隨金融科技而來的是資訊安全與網路安全等相關風險議題。

對資訊安全與網路安全等風險議題迫切需求，反應在 APEC FRTI 最新調查，該調查顯示會員經濟體訓練需求，金融科技（含網路風險）仍為穩居前三名最熱門的訓練項目，因此為增進各國金融監理檢查人員對網路安全監理重點之瞭解及交流檢查經驗，APEC FRTI 於 106 年 6 月 6 日至 9 日在庫克群島拉羅湯加主辦「Cybersecurity / Technology Risk Supervision」研討會，邀請美國理察蒙德聯邦準備銀行資深檢查人員 Ms. Gwynne Williams 擔任講師，與學員一起研討 Cybersecurity / Technology Risk 監理及檢查技術，並從技術發展趨勢中掌握辨識、評估、管理和監控資訊安全及網路安全之科技風險監理能力。

研討會課程採互動討論方式，上課主軸議題為網路風險與資訊科技(IT)風險包括網路安全、雲端運算、行動銀行、金融科技及支付系統和作業處理，此外課程並討論資訊安全、資料治理、委外作業管理、災害復原計畫及 IT 稽核等，由講師介紹及講授各項網路資安科技風險主題，並適時請各國金融監理人員個案討論及分組報告，引導學員相互交流分享監理實務經驗。

本次研討會由庫克群島為舉辦國，參與之國家包括來自庫克群島、印度、馬來西亞、尼泊爾、紐西蘭、巴布亞紐幾內亞、索羅門群島、斯里蘭卡、泰國、坦桑尼亞及我國等 11 個國家 25 位金融監理人員。研討會計為 4 天研討課程，學員分別來自各國之證券、保險及銀行之監理機關，及中央銀行與存款保險公司等機構。

本會此次派員赴庫克群島參加研討會，一方面增進檢查人員對網路風險與資訊科技(IT)風險之檢查專業知識，另一方面希冀藉由參加此類國際研討會，加強與會各國金融監理人員交流分享檢查經驗，借鏡國際監理檢查實務經驗，針對本局現行對金融機構資訊業務實地檢查措施提出強化且具體有效之建議。

# 目　次

## 壹、APEC 金融監理官訓練行動計畫第 22 屆顧問小組會議目的及過程

鑑於當今金融環境監理之複雜性，「亞太經濟合作金融監理官訓練行動計畫」(Asia-Pacific Economic Cooperation Financial Regulators Training Initiative,簡稱 APEC FRTI)係 1998 年 5 月在 APEC 各國為強化亞太區域的金融監理工作，藉由每年持續舉辦金融監理訓練，來提升銀行業與證券業監理人員的專業監理技術職能，

亞洲開發銀行 (Asian Development Bank, ADB)成立秘書單位以執行 APEC FRTI，負責訓練課程規劃、 講座遴選及各項訓練活動的執行，並設置顧問小組（Advisory Group,簡稱 AG）為其決策單位並督導行動計畫的執行。

本屆會議為 APEC 金融監理官訓練行動計畫第 22 屆顧問小組會議係由 APEC 金融監理人員訓練倡議秘書處及亞洲開發銀行所舉辦，本次主辦國為庫克群島金融監督管理委員會（the Financial Supervisory Commission of Cook Islands），於 2017 年 6 月 5 日在庫克群島之拉羅湯加之旅館 Edgewater Resort and Spa 會議室召開。

顧問小組會議主要討論明(2018) 年度倡議之執行及合作事宜，並檢討 2016－2017 年度之執行成效。下午第一場時間 13:00-16:00 為證券監理官場次，下午第二場時間 15:00-18:00 為銀行監理官場次；其中 15:00-16:00 之重疊時間（Overlap）為聯合開放討論(Joint Session with Securities Regulators)，銀行監理官可依意願自由參加證券監理官開放討論場次（附件，顧問小組會議議程）。。

會議討論重點包括（一）檢討 2016-2017 年已舉辦的金融監理人員訓練成果；（二）簡報訓練需求之調查結果；（三）研議是否繼續辦理該訓練倡議（四）規劃 2018 年之訓練計畫及徵詢各會員代表擔任主辦國之意願。

## 貳、APEC 金融監理官訓練行動計畫第 22 屆顧問小組會議內容

### 一、各國列席參加人員

**(一)顧問小組會議－證券監理官場次（時間 13:00-16:00）**

參與會員包括亞洲開發銀行秘書處、澳洲證管會(以電話方式參與)、孟加拉證管會、韓國金融監督院、馬來西亞證管會(以電話方式參與)及本會，合計有 5 國經濟體代表參與討論，會議議程如附件一，各國參加人員名單如下：

Ms. Marian KLJAKOVIC (via telephone conference)
Australian Securities and Investments Commission

Mr. Md Helal Uddin NIZAMI
Bangladesh Securities and Exchange Commission

Ms. Jae Woo KIM
Financial Supervisory Service

Mr. Weihsu Li
Financial Supervisory Commission,Taiwan

Ms. Ida KAMARIA (via telephone conference)
Ms. Syahrizatul Iza ISMAIL (via telephone conference)
Securities Commission Malaysia

Mr. Noritaka AKAMATSU
Mr. Woohyun KIM
Ms. Sue JEFFERY
Ms. Chona P. GUATLO
Asian Development Bank

(二)顧問小組會議－銀行監理官場次（時間 15:00-18:00）

參與會員包括亞洲開發銀行秘書處、庫克群島金管會、韓國金融監督院、馬來西亞中央銀行及存款保險公司(以電話方式參與)、菲律賓中央銀行、泰國中央銀行、印尼中央銀行、美國聯邦儲備委員會、本會，合計有 8 國經濟體代表參與討論，會議議程如附件二，各國參加人員名單如下：

Ms. Louise WITTWER
Cook Islands Financial Supervisory Commission

Mr. UNTORO
Mr. Yusuf Wicaksono HASCARYOTOMO
Bank Indonesia

Mr. Jae Woo KIM
Financial Supervisory Service

Ms. Cindy Siah Hooi HOON (via telephone conference)
Mr. Shahril Nizam Mohd RAZALI (via telephone conference)
Bank Negara Malaysia

Ms. Hoh Li YUN
Malaysia Deposit Insurance Corporation

Mr. Restituto C. CRUZ
Bangko Sentral ng Pilipinas

Mr. Jen-Chun HSIEH
The Central Bank of the Republic of China

Ms. Sunadda PARIPUNNA (via telephone conference)
Bank of Thailand

Mr. Amol VAIDYA
Board of Governors of the Federal Reserve

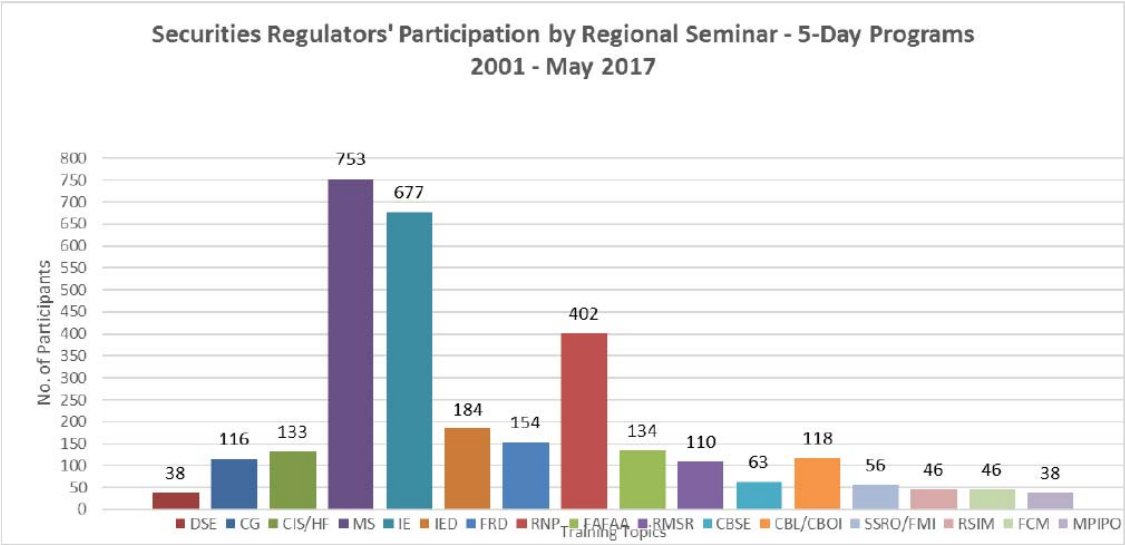
Mr. Noritaka AKAMATSU
Mr. Woohyun KIM
Ms. Sue JEFFERY
Ms. Chona P. GUATLO
Asian Development Bank

## 二、簡報及討論重點

### (一) 證券監理官之會議情形摘要

1.證券監理官參與區域研討會各項主題之 2001 年至 2017 年 5 月之參與人數統計資料如下圖，可知市場監理(Market Supervision)、調查與執法（Investigation & Enforcement）及財務分析和鑑識會計與稽核(Financial Analysis,Forensic Accounting & Auditing)為為參與人數最

多之前三名主題。




FAFAA – Financial Analysis, Forensic Accounting & Auditing
I&E/IE – Investigation & Enforcement
RNP –Regulation of New Products
RMSR – Risk Management for Securities Regulators
Mkt Super/MS – Market Supervision
ECB – Enforcement including Cross Border
CBL/CBOI – Cross Border Listing/Cross Border Offering & Investment
BEP – Building Education Programs for Investors & Market Intermediaries
CG/CGC – Corporate Governance & Compliance
CIS/HF – Collective Investment Schemes/Hedge Funds
DMP – Derivatives including HFT & use of new Trading Technologies
RSIF – Regulation & Supervision of Investment Funds
FCM – Fintech in Capital Markets
MPIPO – Mechanisms for promoting IPOs & SMEs

DSP – Derivatives including Structured Products
CBSE –Cross Border Supervision & Enforcement
RSDM – Regulation & Supervision of Derivatives Markets
MSDM – Market Surveillance of Derivatives Markets
SSMI – Supervision & Surveillance of Market Intermediaries
IED – Investor Education & Financial Literacy
UGFMP – Understanding Global Financial Markets & Products
ENF – Enforcement – Assessing, Planning & Interviewing
FRD – Financial Reporting & Disclosure
DSE – Demutualisation of Stock Exchanges
SSRO – Supervision of Self-Regulatory Organisations & Financial Market Infrastructures
RSIM – Regulation & Supervision of Interconnected Markets

17

2. 會員經濟體訓練需求調查結果

最近調查顯示會員經濟體訓練需求如下圖，前三名依序為包含網路風險之資本市場之金融科技（Fintech in Capital Markets including cyber risks）、市場及市場中介商之監理及監控（Supervision & Surveillance of Market, Market Intermediaries）及金融素養和投資人及市場中介商之教育（Financial Literacy, Investor & Market Intermediary Education，可見近年來由於金融科技之進步，使得金融科技仍為最熱門的訓練項目。

# Review of Recent Survey


3. 2016 年 9 月迄今之重要成果包括：

(1)荷蘭金融監管機構(AFM)第一次提供講師資源參與金融監理人員訓練倡議。

(2)從各金融業中所而擔任研討會講師人數增加。

(3)從證券業所選而擔任研討會講師人數增加。

(4)參與研討會的人數增加。

(5)在舉辦的 4 次研討會中，有 2 個主題是 APEC FRTI 研討會主題中的新主題。

(6)柬埔寨，印尼和越南第一次選任人員擔任講師。

4. 2016 年 8 月至 2016 年 7 月共舉辦 6 場研討會，成果如下：

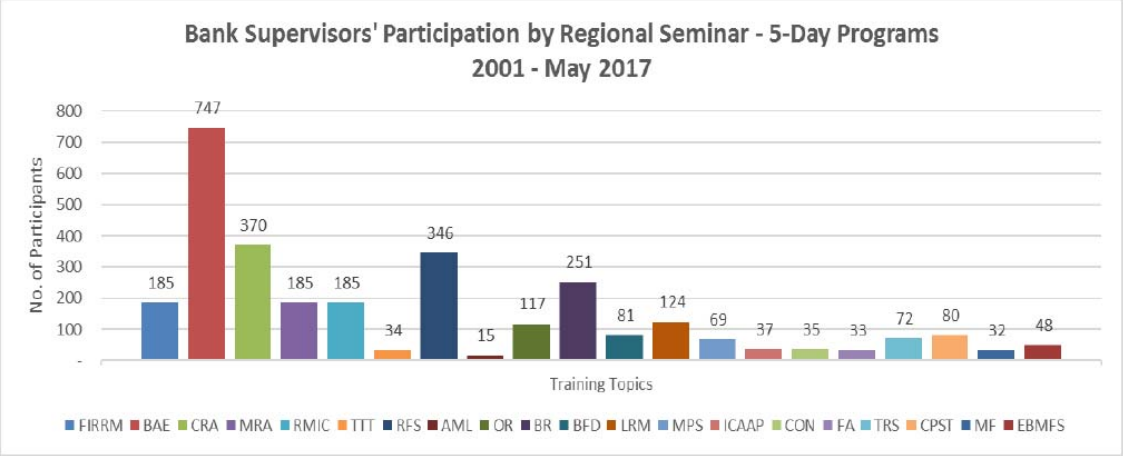
| | | | | |
|---|---|---|---|---|
| 舉辦時間 | 2016.8 | 2016.10 | 2016.１１ | 2017.4 |
| 舉辦地點 | 泰國<br>曼谷 | 馬爾地夫<br>馬利 | 馬來西亞<br>吉隆坡 | 柬埔寨<br>暹粒市 |

| 訓練題目 | 資本市場之金融科技 | 跨國投資 | 市場中介商之監理 | 中小企業上市融資之機制 |
|---|---|---|---|---|
| 參與學員人數 | 46 | 35 | 75 | 38 |
| 各經濟體之參與數 | 12 | 12 | 20 | 10 |
| 學員評價*(%) | 83 ~90.23 | 95.01 ~98.73 | 87.61 ~93.41 | 81.78 ~94.33 |

*評價指標包括：有無符合學習目標、課程內容有無符合需求、對主講者之評分

## (二) 銀行監理官之會議情形摘要

1. 銀行監理官參與區域研討會各項主題之2001年至2017年5月之參與人數統計資料如下圖，可知銀行分析監理與檢查研討(Bank Analysis Supervision/Examination School)、信用風險分析（Credit Risk Analysis）及風險導向監理(Risk Focused Supervision)為參與人數最多之前三名主題。




RFS – Risk Focused Supervision
Ops Risk – Operational Risk Management
FIRRM – Fundamentals of Interest Rate Risk Management
Mkt Risk – Market Risk Management
BASS/BAES – Bank Analysis Supervision/Examination School
Adv Cr Risk – Advanced Credit Risk
Bank Reh – Bank Rehabilitation
PALM – Principles of Asset & Liability Management
Fin Prod – Financial Markets & Products
DPB – Dealing with Problem Banks
CRA – Credit Risk Analysis
CPST – Capital Planning & Stress Testing
EBMFS – Electronic Banking & Mobile Financial Services

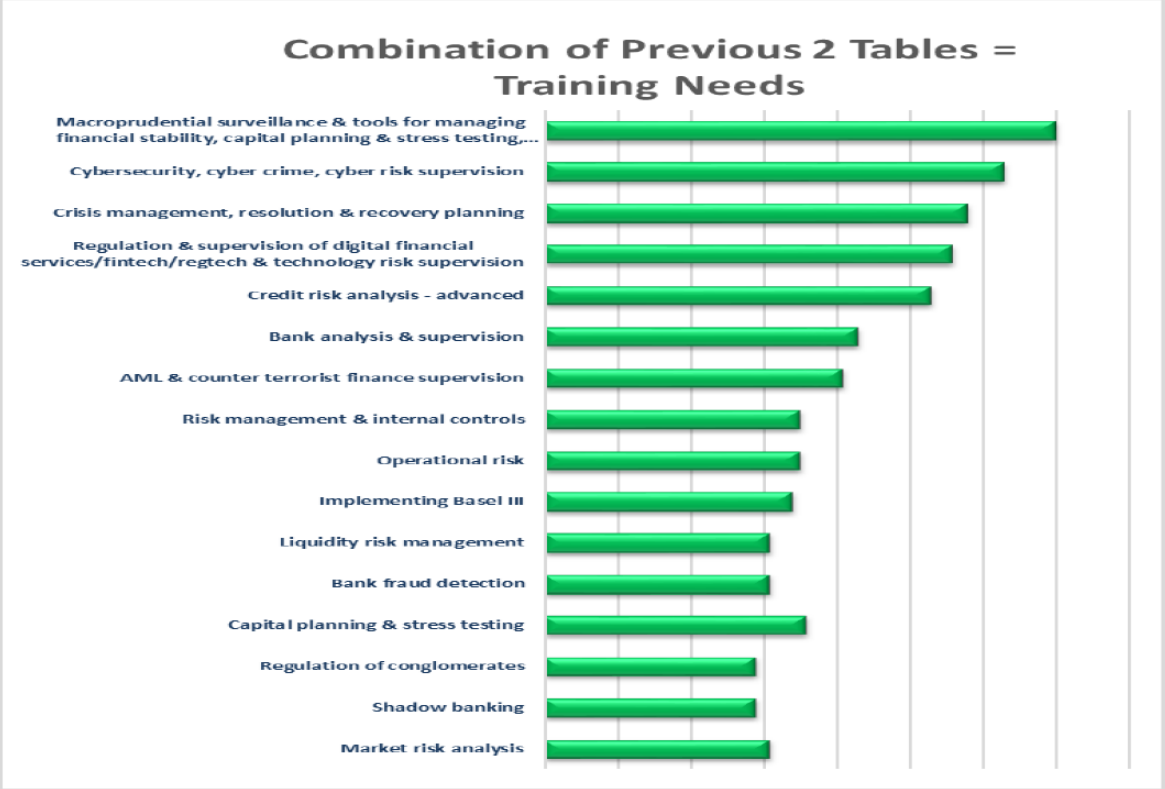
LRM – Liquidity Risk Management
RMIC – Risk Management & Internal Controls
EWT – Early Warning Tests
MPS – Macroprudential Supervision
ICAAP – Internal Capital Adequacy Assessment
Con Sup –Consolidated Supervision
ALM – Asset & Liability Management
FA – Forensic Accounting
RMOR – Risk Management & Operational Risk
CPBR –Crisis Preparedness for Bank Regulators
TRS – Technology Risk Supervision
MF – Microfinance Activity

18

2. 會員經濟體訓練需求調查結果

最近調查顯示會員經濟體訓練需求如下圖，前三名依序為金融穩定和資本計畫與壓力測試等總體審慎監控工具(Macroprudential surveillance & tools for managing financial stability、capital planning & stress testing…)、網路安全或網路犯罪或網路風險監理（Cyber Security, cyber crime, cyber risk supervision）及危機管理與清理及復原計畫(Crisis Management, resolution & recovery planning)，會員經濟體訓練需求調查結果，對證券監理官或銀行監理官調查結果皆顯示可見的將來金融科技（含網路風險）仍為最熱門的訓練項目。

# Review of Recent Survey




3. 2016 年 9 月迄今之重要成果包括：

(1) SEACEN 第一次參與派任講師。

(2)香港第一次參與派任講師。

(3)參與研討會的人數增加

(4)從亞太經合組織經濟體(APEC)參與研討會的人數增加。

(5)記錄曾擔任研討會之講師，作為講師資源。

4. 2016 年 9 月迄今之重要成果包括：

| | | | |
|---|---|---|---|
| 舉辦時間 | 2017.2 | 2017.3 | 2017.5 |
| 舉辦地點 | 印尼<br>巴厘島 | 香港 | 菲律賓<br>馬尼拉 |

| 訓練題目 | 以總體審慎方式下的危機管理 | 流動性風險管理 | 銀行詐欺偵測 |
|---|---|---|---|
| 參與學員人數 | 67 | 38 | 42 |
| 各經濟體之參與數 | 9 | 12 | 8 |
| 學員評價*(%) | 88.75 ~94.36 | 89.91 ~99.55 | 89.6 ~94.03 |

## 三、會議結論

### (一) 2018 年證券監理官訓練之舉辦

孟加拉證管會出席本次會議，當場發言同意舉辦訓練，至於時間及訓練議題目前尚待確認。另會中 ADB 資深顧問 Mr. Woohyun KIM 於中場休息時間，於私下場合聊天時，建議台灣可舉辦一場訓練，惟我國於問卷已表達無舉辦訓練之意願，因是私下場合，職於是委婉表示依問卷結果，我國尚無舉辦訓練之意願。

### (二) 2018 年銀行監理官訓練之舉辦

部分會員經濟體，如：孟加拉、庫克群島、印尼及泰國等 4 個會員表達願意承辦 2018 年 AG 諮詢小組會議及研討會，惟須視各項技術援助(technical assistance, TA)專案及預算情形，來決定是否獲准繼續辦理而定，至於時間及訓練議題目前亦尚待確認。

## (三)熱門優先訓練主題

1.對證券監理官或銀行監理官調查結果皆顯示可見的將來金融科技監理（含網路風險）仍為本年度調查最熱門的訓練項目，會議討論結果亦再次將金融科技監理排定為 2018 年度優先訓練主題，如以下 2(2) 網路安全風險監理及 2(4) 數位金融或金融科技監理。

2.經會議討論結果所排定之熱門優先訓練主題

(1)金融穩定和資本計畫與壓力測試等總體審慎監控工具(Macroprudential surveillance & tools for managing financial stability、capital planning & stress testing…)

(2)網路安全、網路犯罪或網路風險監理（Cyber Security,cyber crime, cyber risk supervision）

(3)危機管理與清理及復原計畫(Crisis Management, resolution & recovery planning )

(4)數位金融或金融科技監理(Digital Finance Supervision or Fintech Supervision )

(5)信用風險分析(Credit Risk Analysis)

## (四) FRTI 工作小組因經費不足，研議是否繼續辦理訓練倡議

1. ADB 因應開發中會員經濟體龐大之基礎建設融資需要，在籌覓營運資金來源方面臨相當挑戰，故 ADB 為有效運用資金於開發貸款項目，近幾年已著手檢討各項技術援助(technical assistance, TA)專案(包括預算)是否與其開發貸款目的相連結，進而影響 FRTI 訓練倡議之經費來源。

2.自 1998 年運作迄今，ADB 計核准 FRTI 工作小組 8 項 TA 專案，每項 TA 專案運作期間約 2 至 3 年，共計支出約 7.4 百萬美元。

3.目前 ADB 協助 FRTI 之 TA 專案將於本(106)年 7 月最後一場由韓國金融監督院(Financial Supervisory Service, FSS)主辦之「金融科技在資本市場之運用」研討會結束後屆滿，FRTI 工作小組刻在研擬新 TA 專案，若獲 ADB 核准即可繼續協助辦理訓練倡議。

4. FRTI 另須籌覓訓練財源，計有如下方案：

(1)尋求外部捐助資金，例如韓國提供捐助 55 萬美元供 2013-2014 年舉辦之研討會使用。

(2)會員經濟體攤付費用成立基金之可行性，惟銀行監理官會議中，所有會員經濟體均意願不高。

(3)在無法確定 TA 是否會獲准情況下，FRTI 工作小組目前考慮包括尋求 FRTI 會員經濟體捐助設立特別信託基金及外部捐助資金。

# 參、網路資安科技風險監理研討會目的及課程設計

## 一、研討會目的及課程設計

### (一)研討會之參與對象

此次研討會是為具有廣泛職責之資深監理人員所設計之介紹性課程，以有助於上開資深監理人員希望能更多地了解資訊科技(Information Technology, 以下簡稱 IT)風險及其監理運作。研討會適合想要了解金融機構存在的 IT 風險及能夠討論 IT 相關的風險管理計畫和監理期望之檢查人員。

### (二)課程綱要

研討會旨在提供對檢查金融機構 IT 業務人員之監理培訓，包括統合性整體監理概念和 IT 與業務風險之間關聯所產生之綜合風險。

### (三)課程目標

課程介紹 IT 風險、風險管理和監理之基本概念。 IT 風險主題將包括網路安全、雲端運算、行動銀行、金融科技及支付系統和作業處理，課程並討論資訊安全、資料治理、委外作業管理、災害復原計畫及 IT 稽核等風險管理期望成效。參與本研討會後，參與者應該能夠：

1.認識和了解主要 IT 風險，並對當今金融機構的 IT 重大課題有更深入的了解。

2.確認 IT 與業務風險之間的關連點，以確保可以併入全面性整體監理方法。

3.討論 IT 風險管理成效期望，包括資訊安全、資料治理、委外作業管理、

災害復原計畫之關鍵要素及目的。

4.認識到對適當 IT 治理之監理期望，包括組織架構、策略規劃和 IT 稽核。

5.向金融機構管理階層提供有關 IT 風險及其對整體組織更廣泛衝擊影響之相關建議。

**(四)課程之效益**

參與網路安全科技風險監理研討會之後，參與者將能在實地 IT 業務檢查中，藉由課堂所學習的增強檢查能力，包括下列檢查能力：

1.在較為資深 IT 檢查人員之協助下，完成非複雜性金融機構之 IT 環境風險評估。

2.準備或協助編撰有關金融機構技術風險的檢查報告

3.與銀行管理階層就 IT 檢查結果進行討論

**(五)研討會課程設計**

研討會課程設計之課表如下圖所示，資訊安全、雲端運算、行動銀行、金融科技、資料治理、委外作業管理、災害復原計畫、IT 風險管理組織架構、策略規劃及 IT 稽核等課程模組。

**APEC FRTI Regional Seminar on**
**Cybersecurity / Technology Risk Supervision**
6–9 June 2017, Rarotonga, Cook Islands
Presented by U.S. Federal Reserve
Hosted by Cook Islands Financial Supervisory Commission (FSC)

| Time | Tuesday, June 6 | Wednesday, June 7 | Thursday, June 8 | Friday, June 9 |
|---|---|---|---|---|
| 8:30 to 12:00 | **Participant Registrations**<br>(8:00 – 8:30)<br>**Welcome Remarks**<br>Louise Wittwer, Commissioner, FSC<br>**Opening Remarks**<br>Noritaka Akamatsu, Senior Advisor, ADB<br>Amol Vaidya, Program Manager, US FED<br>**Group Photo**<br>(8:30 – 9:00)<br>IT Risk Supervision Overview<br>(9:00 – 10:15)<br>Gwynne Williams | IT Risk Topics:<br>Cybersecurity<br>(8:30 – 10:15)<br><br>Gwynne Williams | IT Risk Management:<br>Information Security<br>(8:30 – 10:15)<br><br>Gwynne Williams | IT Audit<br>(8:30 – 10:15)<br><br>Gwynne Williams |
| | **Break (10:15 – 10:30)** | **Break (10:15 – 10:30)** | **Break (10:15 -10:30)** | **Break (10:15 – 10:30)** |
| | IT Risk Supervision Overview (cont.)<br>(10:30 – 12:15)<br><br>Gwynne Williams | IT Risk Topics:<br>Mobile Banking<br>(10:30 – 12:15)<br>Gwynne Williams | IT Risk Management:<br>Data Governance<br>(10:30 – 12:15)<br>Gwynne Williams | IT Management Organization and Governance<br>(10:30 – 12:15)<br>Gwynne Williams |
| 12:15 to 1:15 | **LUNCH** | **LUNCH** | **LUNCH** | **LUNCH** |
| 1:15 | IT Risk and Business Strategies<br>(1:15 – 2:45)<br>Gwynne Williams | IT Risk Topics: FinTech<br>(1:15 – 2:45)<br>Gwynne Williams | IT Risk Management: Vendor Management<br>(1:15 – 2:45)<br>Gwynne Williams | Integrated Supervision<br>(1:15 – 2:45)<br>Gwynne Williams |
| | **Break (2:45 – 3:00)** | **Break (2:45 – 3:00)** | **Break (2:45 – 3:00)** | **Break (2:45 – 3:00)** |
| to 4:30 | IT Risk Topics: Cloud Computing<br>(3:00 – 4:30)<br><br>Gwynne Williams | IT Risk: Payment Systems and Operations<br>(3:00 – 4:30)<br><br>Gwynne Williams | IT Risk Management:<br>Business Continuity and Disaster Recovery<br>(3:00 – 4:30)<br><br>Gwynne Williams | Examination Practices and Wrap Up<br>Gwynne Williams<br><br>**Closing Remarks**<br>Louise Wittwer, FSC<br>**Certificate Presentation**<br>Louise Wittwer, FSC<br>Woohyun Kim, ADB<br>(3:00 – 4:30) |

## 二、講師簡介及各國列席參加人員

本次研討會課程由美國聯邦準備銀行之 1 位資深檢查人員擔任全程之講師，講師 Ms. Gwynne Williams 係屬理查蒙德聯邦準備銀行(Federal Reserve Bank of Richmond)監督與監理部門 (Department of Supervision and Regulation)之大型銀行資深檢查人員(Large Bank Sr. Examiner II)，主要職務尚包括在隸屬於國家監理學習辦公室 (National Supervision Learning Office)擔任聯邦準備銀行在職專業學習計畫負責人（the Federal Reserve System's Continuing Professional Development Learning Program's Lead)。

Gwynne 具有拉斐特大學電腦科學學士學位和經濟與商業學士學位、弗吉尼亞州立大學資訊管理碩士學位，亦畢業賓夕法尼亞大學華頓商學院之銀行與之領導力發展計畫研究所。 Gwynne 亦取得並繼續保持她的國際資訊系統稽核師證照，於 2004 年成為聯邦銀行的 IT 檢查人員，通過檢查更複雜的大型金融機構及其服務委外作業廠商，逐漸建立其 IT 檢查之專業知識。 然後，Gwynne 亦擴大了她的監理視野，包括專注於市場和流動性風險、作業風險管理與測量、數位化策略管理、內部稽核、委外作業管理及資訊科技(Information Technology, IT)等。擔任聯邦準備銀行在職專業學習計畫負責人之前， 她也曾負責企業風險管理和激勵補償計畫項目負責人。

本次研討會地點位於庫克群島拉羅湯加，由庫克群島為舉辦國，參與之國家包括來自庫克群島、印度、馬來西亞、尼泊爾、紐西蘭、巴布亞紐幾內亞、索羅門群島、斯里蘭卡、泰國、坦桑尼亞及我國等 11 個國家 25 位金融監理人員（附件，研討會參與者名單與聯絡方式）。

研討會計為 4 天研討課程，學員分別來自各國之證券、保險及銀行之監理機關，及中央銀行與存款保險公司等機構，課程採互動討論方式，由講師介紹及講授各項網路資安科技風險主題，並適時請各國金融監理人員分享監理經驗及引導個案討論及分組報告，讓學員相互交流表達監理上之觀點與看法。

。

## 肆、網路資安科技風險監理研討會內容

### 一、資訊科技風險監理總論（IT Risk Supervision Overview）

新興金融科技(Fintech)之發展，使資訊作業角色改變，資訊作業從過去較為被動與後勤支援之配合角色，逐步成為引領業務創新之主角，且伴隨可能產生新的資訊及網路風險議題，必須由資訊、法令遵循、業務與管理等各部門之聯繫合作來防護資訊安全及網路安全。

#### (一)資訊科技風險（IT Risk）之獨特性

1.擴展性

因自動化和科技進步而逐漸擴展連接到業務風險。

2.動態

創新帶來新風險，及 IT 發展之動態策略。

3.具有挑戰性

科技進步而使金融機構難以一直維持現行 IT 策略及政策，故監理須有彈性。

#### **(二)IT 風險管理及風險聚焦檢查範圍**

1.從業務作業角度觀之

IT 風險管理及風險聚焦檢查，從業務作業角度觀之，聚集在如下範圍：

(1)應用系統存取和身分識別管理(Access and Identity Management)

(2)網路銀行和行動銀行(Internet and Mobile Banking)

(3)分行和遠端管理(Branch and Remote Capture)

(4)電匯(Wire Transfers)

(5)自動櫃員機作業處理（ATM Processing）

(6)虛擬化/雲端運算( Virtualization / Cloud)

(8)其他作業模型（Models）

2.從技術作業角度觀之

此外 IT 風險管理及風險聚焦檢查，若從技術作業角度觀之，則會聚集在如下範圍：

(1)資訊安全(Information Security)

(2)網路安全(Cybersecurity)

(3)委外作業廠商風險管理(Vendor Risk Management)

(4)業務連續性/災難恢復(Business Continuity / Disaster Recovery)

(5)業務應用系統存取控制(Application Access Controls)

(6)變更管理 (Change Management)

(7)資料治理(Data Governance)

(8)IT 稽核覆蓋範圍(IT Audit Coverage)

(三)IT 風險與業務風險

金融機構發展業務時，其業務策略往往伴隨著提高 IT 風險，業務策略當前趨勢與 IT 風險對應連結如下：

1.作業風險管理和 IT 風險(Enterprise/Operational Risk Management and IT Risk)

2.財務報告和資料治理(Financial Reporting and Data Governance)

3.支付系統風險和網路安全(Payment Systems Risk and Cybersecurity)

4.併購和系統整合(Mergers/Acquisitions and System Integration)

5.資訊作業委外風險管理和共享服務(Third Party Risk Management and Shared Services）

6.FinTech 和 IT 策略（FinTech and IT Strategy）

7.大資料/資料分析和雲端運算（Big Data/Data Analytics and Cloud Computing）

**(四)金融機構發展業務策略中之主要 IT 計畫(Major IT Initiatives in Business Strategies)**

1.Cloud Computing（雲端運算）

2.Cybersecurity(網路安全)

3.Mobile Banking(行動銀行)

4.金融科技(Financial Technology, FinTech)

5.支付系統和銀行作業（Payment Systems and Bank Operations）

**(五)各國監理交流討論**

1.尼泊爾學員提問:應用系統委外開發，金融機構及委外廠商，誰應擁有原始程式碼?

講師回答: 若為客製化，則金融機構應擁有原始程式碼，但若為國際知名廠商開發則應視契約約定而定。

2.印度學員提問:如何克服IT檢查人員與一般業務檢查人員在IT檢查上的差距，目前的情況，雙方都是各管各的，不願涉入對方的檢查領域？

講師回答:這個問題在美國也一樣，IT 檢查人員不足，IT 檢查人員與一般業務檢查人員也是因專業上的差距，不願涉入對方的檢查領域，這需要文化的改變及兩者都需要訓練。

3.庫克群島學員提問: IT 檢查人員與一般業務檢查人員可否一起檢查 IT?

講師回答: 應該可一起檢查，但主要還是看檢查的業務所遇到的作業問題，檢查人員如果能同時具有檢查 IT 及一般業務的專長是更佳。

台灣學員檢查經驗分享：台灣 IT 檢查人員有特別成立一個電腦稽核科專

門檢查 IT，且台灣足足花了兩年對銀行之資訊作業作了完整的專案檢查，這是台灣引以為傲的，與各位學員國家最大的不同。至於 IT 檢查人員與一般業務檢查人員各查各的業務之問題,台灣會在檢查期程內同時派兩隊檢查人員，IT 檢查人員與一般業務檢查人員，交流 IT 與一般業務檢查資訊，台灣在這方面雖然也不是做到很成功，很完美，但至少是一個好的開始及努力的方向。

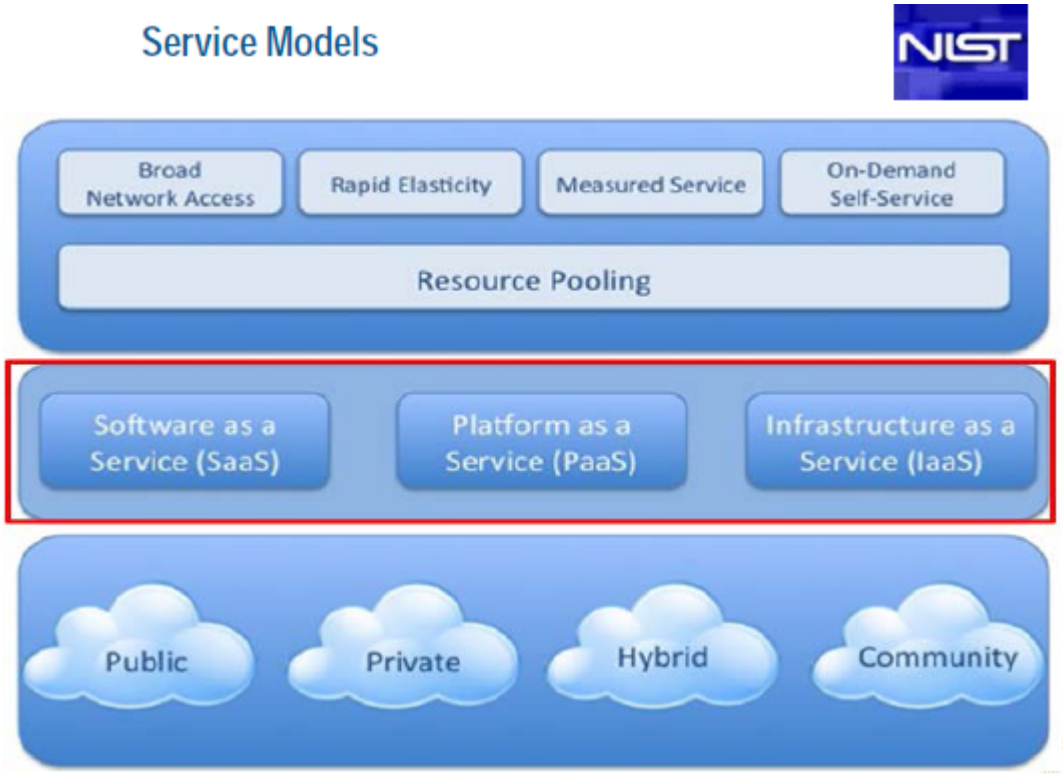
4.台灣學員檢查經驗分享：2016 年 7 月台灣第一銀行的 41 台 ATM 被國際犯罪集團植入惡意程式吐鈔模組，被盜領約新台幣 8,000 萬元現金，歹徒在未操作 ATM 的情形下，利用吐鈔模組繞過應用系統直接讓 ATM 大量吐鈔後提領，這是支付系統風險和網路安全連繫的絕佳案例，也是上開資訊科技風險（IT Risk）具有擴展性、動態及挑戰性之最佳例證，台灣已將 ATM 系統及 SWIFT 兩大支付系統，列為檢查項目。

## 二、雲端運算(Cloud Computing)

### (一)雲端運算定義、服務模式及部署模式

雲端運算係指一項將持有之硬體或軟體資源整合為分享資源,客戶端使用者得透過委外作業廠商所提供之網路（稱之「雲端」）軟硬體設備，依需求取得資訊科技之服務。

雲端運算服務模式如下圖所示,計有軟體即服務(Software as a Service, SaaS)、平台即服務(Platform as a Service, PaaS)、基礎架構即服務(Infrastructure as a Service, IaaS)三種服務模式。若依雲端運算部署模式則可分為公用雲(Public Cloud)、私有雲(Private Cloud)、社區雲(Community Cloud)及混合雲(Hybrid Cloud)，其中混合雲係結合公用雲及私有雲。




**(二)雲端運算之資安風險**

雲端運算服務提供金融機構委外彈性運用資源，可節省 IT 成本與相關處理技術，惟金融機構面臨如下之風險：

1.資產成為廣泛分佈(Assets becomes widely public and distributed)

2.若雲端運算服務無法提供預期結果，反造成資源受限

3.客戶資料無預警遭更改

4.資訊/資料被重複儲存在其他地方，委外作業廠商未予通知

5.雲端運算服務被中斷一段期間

6.委外作業廠商可能不了解或未符合監理要求

**(三)雲端運算服務之資料安全管理**

雲端運算之資訊安全機制必須兼顧產業特性、法令規範、內部控制及技術解決方案等，才能有效降低潛在的資訊安全風險，金融機構之資料安

全管理必須查核下項目：

1.決定使用雲端運算服務之前，應有法務人員參與以確保契約條款與服務等級協議可以滿足法規與內部稽核的要求，避免資安風險導致金融機構及金融消費者權益受損。

2.雲端運算服務委外作業廠商蒐集那些種類資料、對於這些資料擁有的存取權限及委外作業廠商保護資料之方式。

3.雲端運算服務委外作業廠商則是否有適當安全措施與分析資安相關之軌跡資料，包括網路層的防火牆、入侵偵測／防護系統、路由器流量、主機層的主機系統紀錄檔、應用層的應用程式紀錄及金融機構之憑證資訊等。

4.雲端運算服務契約或服務水準協議（SLA）中有關業務持續運作的流程與要求，包括業務持續運作計畫、災變復原程序及演練紀錄。

**(四)雲端運算服務檢查重點**

1.失去治理(Loss of Governance)

包括委外廠商作業權責不分、SLA 條款與不同的利益相關方有抵觸及跨雲應用程序隱藏依賴關係，檢查重點為金融機構是否有成熟的廠商管理計畫，包含有清楚明確的契約和 SLA 條款規範廠商績效。

2.法令遵循之挑戰(Compliance Challenge)

包括金融機構及監理機關無稽核權、缺乏標準技術和解決方案、未符合或取得雲端基礎架構認證及使用條件缺乏完整性和透明度，檢查重點為金融機構是否有全面的盡職調查流程（Comprehensive due diligence process）及契約是否明訂涉及法律、法遵及獨立審核/認證之條款。

3.委外作業廠商鎖定(Vendor Lock-in)

包括缺乏標準技術和解決方案、長期協議/契約、缺乏備援之第二委

外作業廠商及使用條件缺乏完整性和透明度,檢查重點為金融機構是否有全面的盡職調查、簽訂短期協議/契約、定期廠商審查及正式之退出策略和轉換計畫。

4.惡意之雲端運算服務委外作業廠商 (Cloud Provider Malicious Insider)

包括權責不清、職責執行不力、實體安全程序不足、未以加密形式處理資料及弱點漏洞修補管理不足等,檢查重點為金融機構是否有對雲端運算服務委外作業廠商執行背景查核、存取管理、實地檢查、資料分類及加密等。

5.監理管轄問題

包括 IT 軟硬體資源隔離不足、在多個國家監理管轄區儲存資料及缺乏有關上開國家監理管轄區的資訊,檢查重點為金融機構是否有法律部門參與雲端管理計畫和異常事件通報程序、非共享性之雲資產及資料處理和歸檔架構。

6.資料保護風險(Data Protection Risks)

包括 SLA 條款缺乏符合客戶之資訊安全要求、缺乏關於國家監理管轄區之資訊、在多個國家監理管轄區儲存資料缺乏透明度、未及時發現事故並通知及全雲環境（full cloud environment）之未知風險等，檢查重點為金融機構是否有清楚的 SLA，法律及資訊安全之盡職調查、異常事件通報處理計畫和資料加密。

7.資源隔離失敗(Isolation Failure)

包括虛擬機管理程序、漏洞、IT 軟硬體資源隔離不足、可能發生內部(雲)網路探測等,檢查重點為金融機構是否有靈活的雲架構、安全性、資源共享和雲端運算服務能力審查。

雲端運算服務仍持續演進與成長,金融機構採用雲端運算後,資訊作業從向來內部自行管理,轉變成委外作業廠商提供金融機構外部甚至跨國

之運算服務，可預見將來面對所衍生的資訊安全及網路安全問題，雲端運算服務如何符合法令法規與內部規範對內部控制及資訊安全稽核之要求，為監理重點。

**(五)雲端運算服務之網路監理資源（Additional Resources）**

金融機構須對雲端之及資訊安全建立管理機制，管理機制可以參考 ISO 27017、ISO 27018 與 ISO 29100 等國際標準之相關實務規範，包括雲端運算服務委外作業廠商人員之職責區隔、虛擬環境之隔離、系統管理者之作業安全、雲端運算服務之監控機制等。對雲端運算個人資料管理及保護則須綜合考量組織、程序及技術等層面，建立安全保護之系統管理架構，下列為可參考之其他網路監理資源（Additional Resources）：

1. Amazon Web Services Security and Compliance Center

http://aws.amazon.com/security/

2. Cloud Security Alliance

https://cloudsecurityalliance.org/

3. Cloud Standards Organization

http://cloud-standards.org/ wiki/index.php?title=Main_Page

4. FFIEC Cloud Computing Standards

http://ithandbook.ffiec.gov/media/153119/06-28-12_-_external_cloud_computing_-_public_statement.pdf.

**(六)各國監理交流討論**

印度學員提問:若新的金融商品在雲端運算服務發展出來，而所委外之雲端運算服務為全球性公司，如何對其執行 IT 檢查？

講師回答:雲端運算服務因為資料之存取地點與實體儲存資料與運算

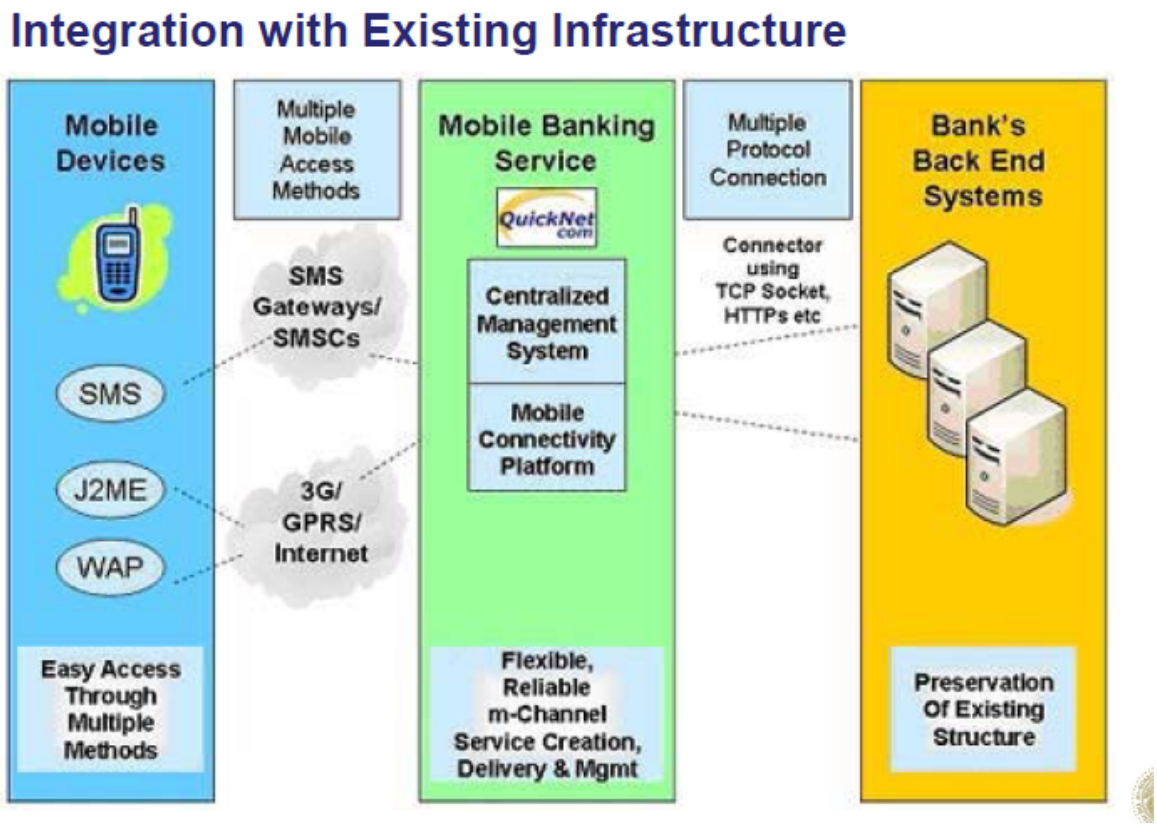
之主機之存放地點可能分屬不同國際地理區域,究竟應屬於那個區域的行政監理機關管轄是一個議題,基本上契約要有稽核權,而國家間相互要有監理備忘錄（MOU）。

## 三、行動支付（Mobile Payments）系統

### (一)行動支付系統與業務發展趨勢

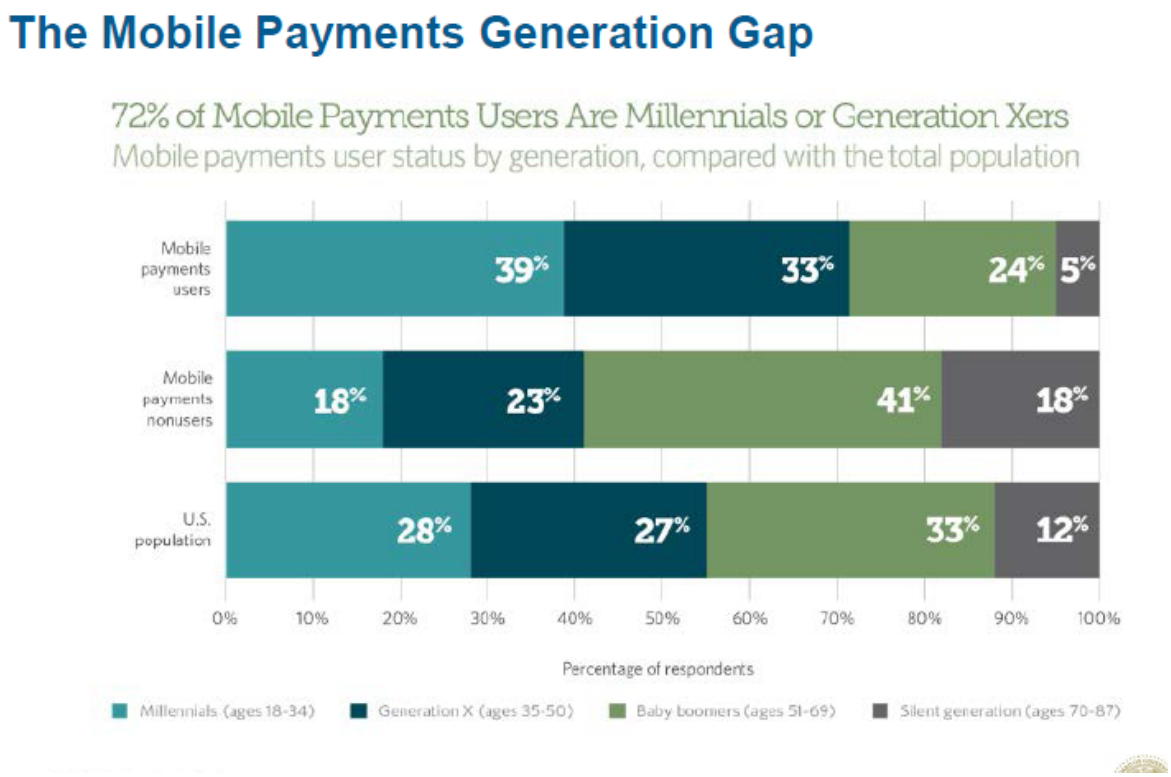
1.行動支付系統

行動支付系統如下圖所示,行動銀行或行動支付系統可整合至銀行之電子交易後台系統，除傳統銀行、電信公司及 IT 公司等，尚有第三方支付公司，如:Apple, Google 及 Samsung 等，民眾及企業可使用移動設備來啟動對個人或企業付款。




2.年輕族群對行動支付的接受度很高

隨著社會大眾普遍資訊素養的提昇及 3C 產品的普及，尤其是年輕族群對行動支付的接受度很高，下圖所示為美國行動支付使用者年齡分布與美國總人口分布比較圖，年輕世代如：千禧年世代(18 - 34 歲)及 X 世代(35 - 50 歲)，占比例高達 72%。

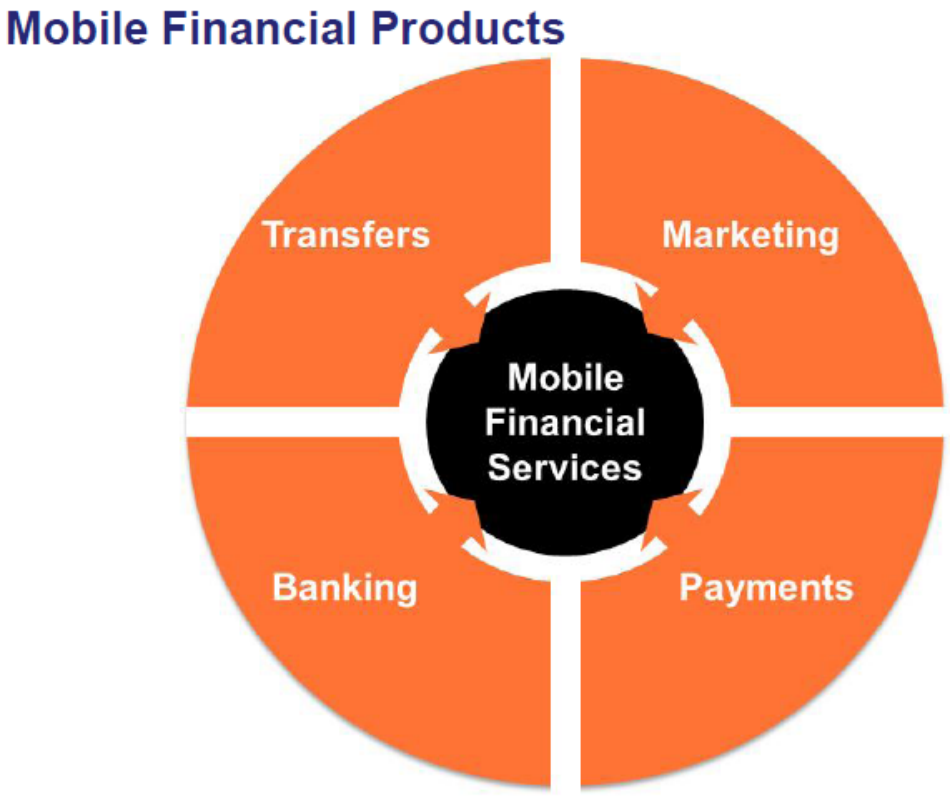



3. 行動支付業務發展市場成熟度排名

行動支付業務發展市場成熟度依 Arthur D. Little M-Payment Report 排名如下圖所示，中國已是發展中進步極快的國家，而在亞洲向來是我國的競爭對手如：日本、韓國及新加坡業務發展市場成熟度已超過 80%，值得作為借鏡。


4.行動金融商品是監理機關所須面對之新的議題

由於行動裝置之便利與普及，行動金融商品如下圖所示，包含行動行銷、行動支付、行動銀行及行動轉帳等，行動商品之發展技術有別於傳統網路銀行，是目前監理機關所須面對之新議題。




**(二)行動支付系統之資安風險**

行動支付系統之資安風險須防範如下資安風險：

1.行動應用程式發布安全性

2.資料敏感性與資料保護

3.付費資源控管安全

4.身分認證授權與連線管理安全

5.行動應用程式碼安全性

**(三)行動應用程式（App） 的風險與威脅**

App 的風險與威脅，可參考開放網路應用程式安全計畫（Open Web Application Security Project，簡稱 OWASP)。開放網路軟體安全計畫，簡稱 OWASP（Open Web APPlication Security Project)，是一個開放社群之非營利性組織，主要目標是研議協助解決網路軟體安全之標準、工具

與技術文件，針對不同的軟體安全問題進行討論與研究。OWASP 在美國發表關於行動式裝置的十大弱點風險，由技術角度透視目前所面臨的風險：

1.平台使用不當（Improper Platform Usage)。

2.不安全之資料儲存（Insecure DataStorage)。

3.不安全之通訊（Insecure Communication)。

4.不安全之認證（Insecure Authentication)。

5.不足之加密方式（Insufficient Cryptography)。

6.不安全的授權（Insecure Authorization)。

7.用戶端程式碼的品質（Client Code  Quality)。

8.程式碼竄改（Code Tampering)。

9.逆向工程（Reverse Engineering)。

10.有安全疑慮的功能(Extraneous Functionality)。

**(四)各國監理交流討論**

群組討論－台灣檢查經驗分享：

行動應用程式發布安全性、身分認證授權與連線管理安全、防止軟體竄改的防護、軟體系統環境偵測、金鑰等敏感性資料的儲存等為金融檢查重點，另須要求對行動支付軟體的黑箱、白箱及滲透測試（Penetration Test)做完整的檢測，依台灣之檢查經驗有如下重點：

1.行動應用程式發布安全性

2.行動支付系統需要多因素驗證，特別是行動銀行系統，多因素驗證包含需制訂並落實密碼政策。

3.行動支付系統之行動裝置是否有越獄或 root、感染病毒、遺失位置及異常使用行為。

4.身分驗證產生稽核日誌，包含不尋常的登入活動及入侵檢測。

5.在一個持續的基礎，評估新的風險，驗證機制須進行適當更新

6.針對金融機構自行開發或委外廠商開發之行動應用程式，要求弱點掃描與源碼檢測活動。

7.防止軟體竄改的防護

## 四、金融科技(Fintech)

### (一)金融科技 (FinTech)已成為全球金融發展趨勢

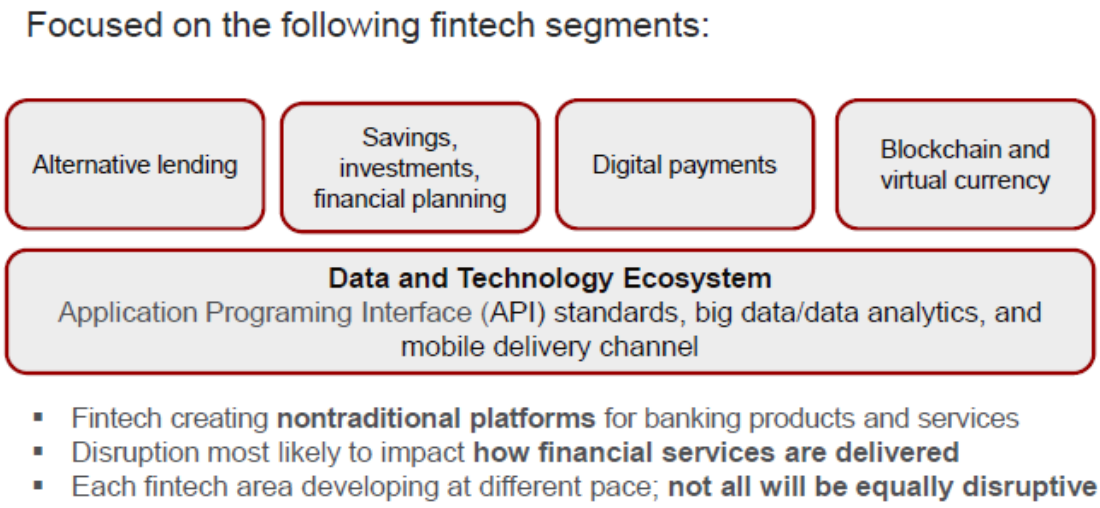
金融科技 (FinTech)已成為全球金融發展趨勢並對金融產業將產生巨大影響，金融科技可由金融業增加科技的應用以擴大服務範圍，或是由科技業跨界提供金融服務， FinTech 發展如下圖所示，目前集中焦點在下列金融業務：

1.替代性借款

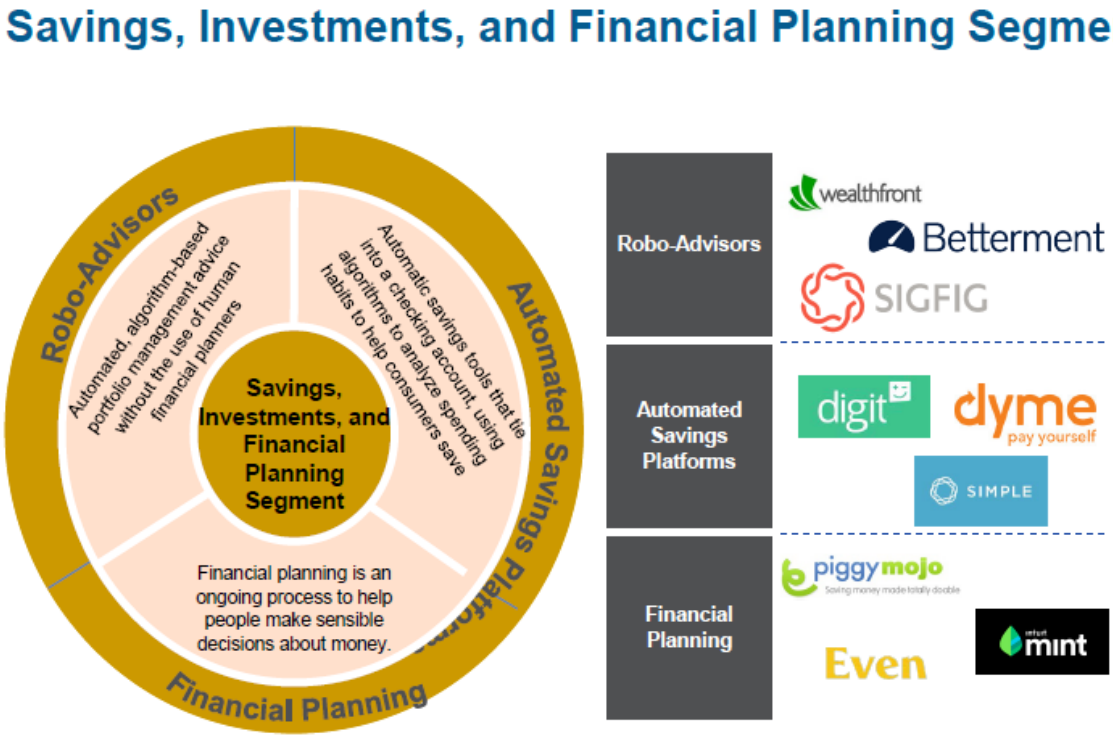
2.存款、投資及財務規畫

3. 數位支付

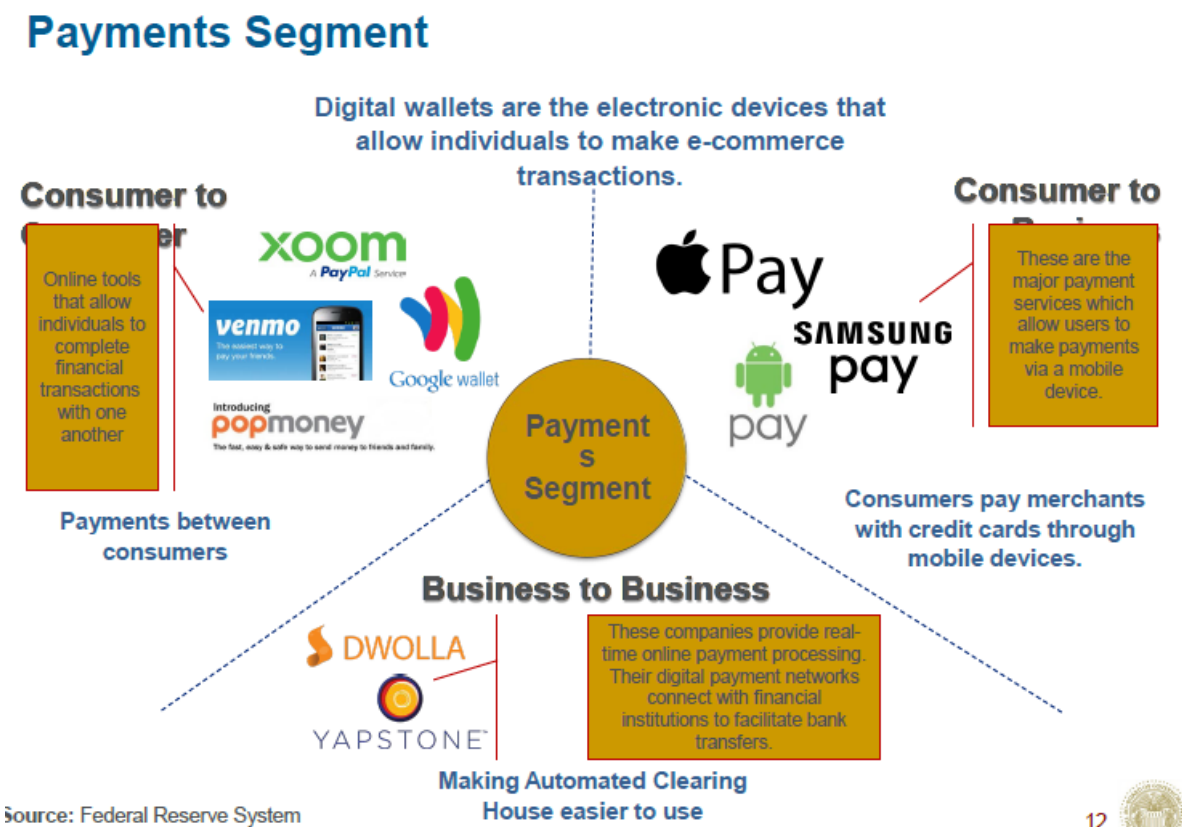
4. 區塊鏈及虛擬貨幣



FinTech 相關之存款、投資及財務規畫業務，在美國有下列新創公司如下圖所示，新創公司發展如機器人理財顧問、自動存款平台及財務規畫公司。




FinTech 相關之數位支付業務，國際及國內服務業者皆能支付及清算，如下圖所示，如 Google 電子錢包、Apple Pay 、Samsung Pay 及 Android Pay 等國際行動支付業者，國際行動支付業者與其他支付工具，如： 如金融卡、電子票證及第三方支付等業者合作。

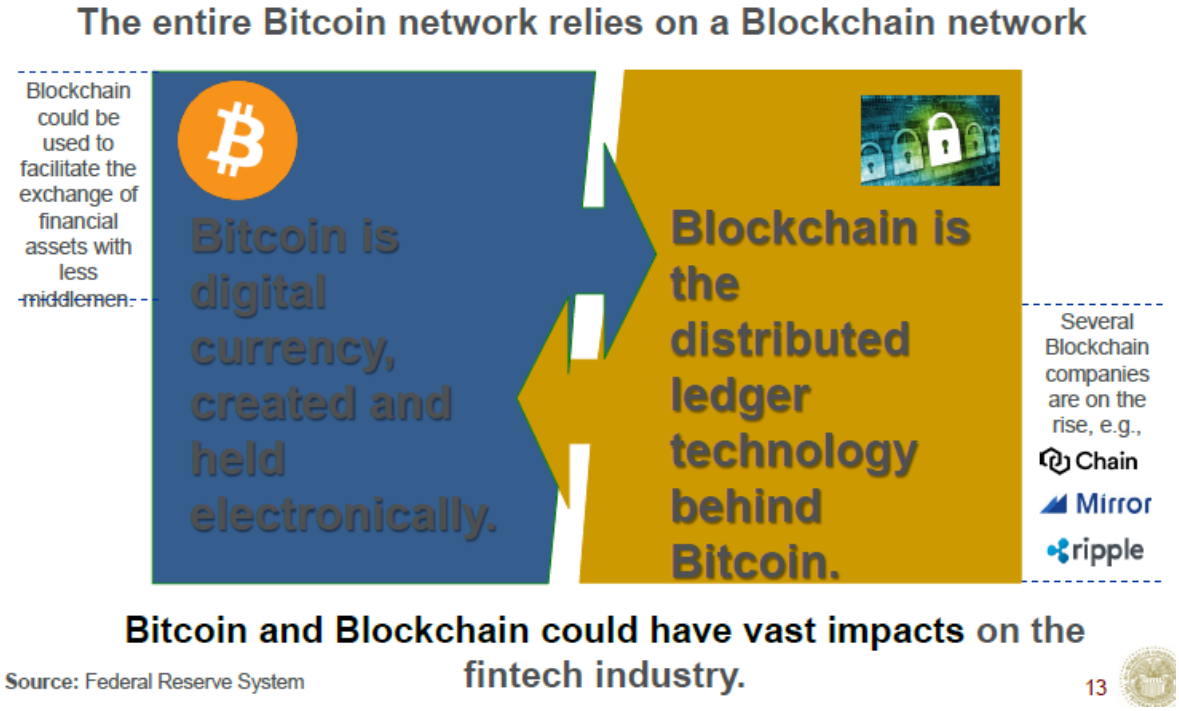



Fintech 可滲透生活中每一項服務及功能，包括金融服務、大數據分析、社群平台、店家資源及生活服務等，整合各種訊息而提升交易量與交易成功率，達成行銷效益。

## Fintech Innovations are Transforming Financial Services for Consumers and Businesses


區塊鏈技術可廣泛應用於各種金融與支付業務之金流，目前最知名的應用就是虛擬貨幣比特幣。

## Blockchain Segment



**(二) Fintech 衝擊所帶來機會與風險**

Fintech 衝擊帶來之機會，如：效率(更好的產品、更多的選擇及更低的價格)及消費者體驗（增加使用金融服務商品、更佳之揭露透明度及增強了解金融服務商品），惟 Fintech 衝擊亦帶來如下相關風險：

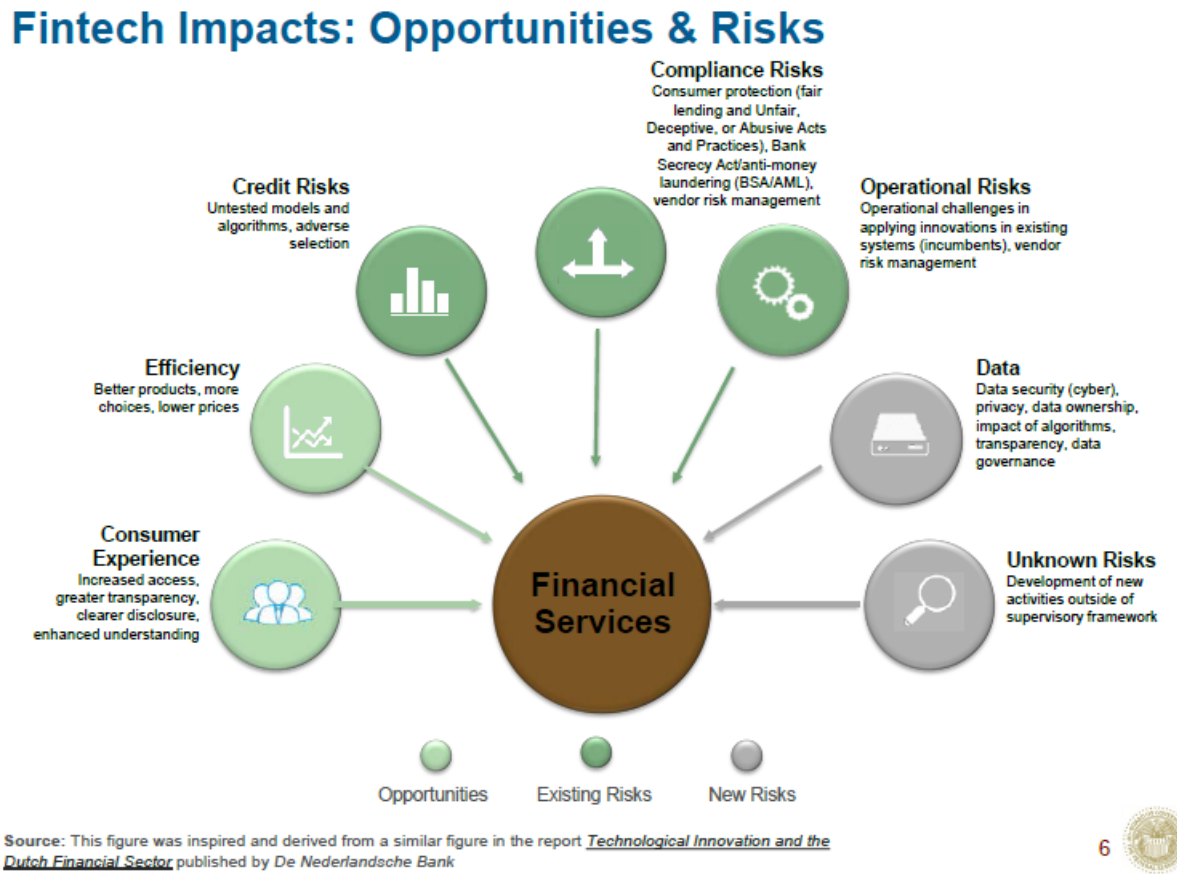
(1)信用風險：未經測試之模型和演算法及逆選擇

(2)法令遵循風險：消費者保護（不公平貸款、欺騙、濫用行為及做法）、銀行保密法/反洗錢（BSA / AML）及委外作業廠商風險管理

(3)作業風險：現有系統應用創新科技之操作風險挑戰及委外作業廠商風險管理

(4)資料風險：網路安全、資料所有權、演算法之影響、透明度、資料治理

(5)未知風險：超出監理架構之外新的交易活動。



**(三)監理及檢查關注重點**

Fintech 和銀行以多種方式進行連接：

1.銀行直接投資 Fintech 公司

2.銀行建立 Fintech 啟動計畫，孵化創立 Fintech 公司

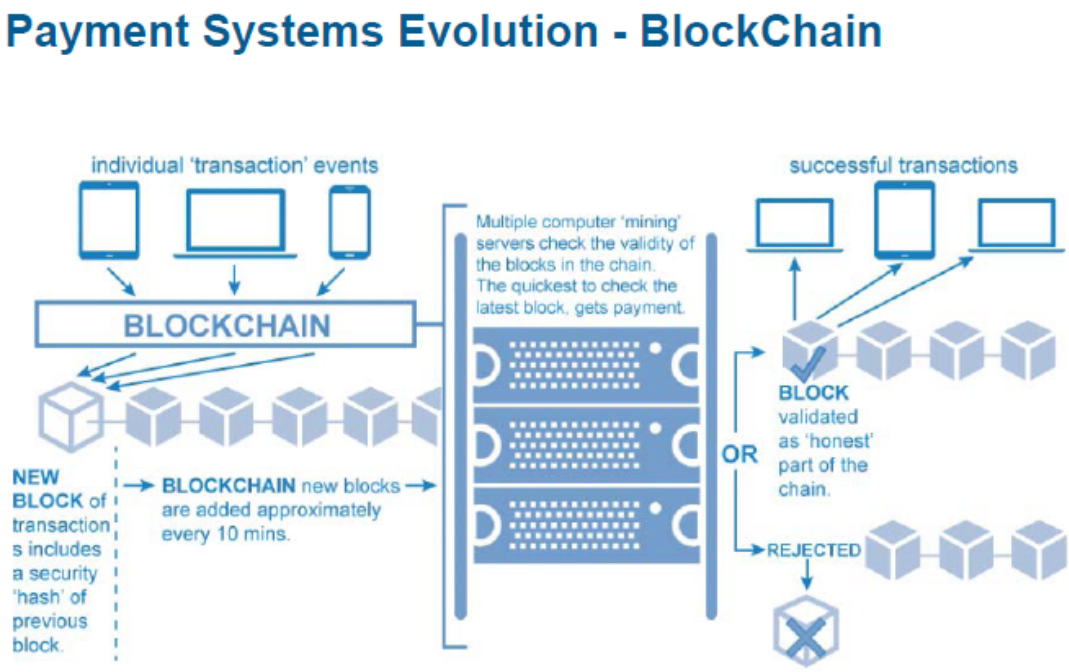
3.銀行與 Fintech 公司業務合作，如：來源於 Fintech 借款公司之貸款及轉介費用

4.銀行收購 Fintech 公司

5.銀行發起自己的 Fintech 解決方案(solutions)

**(四)金融科技(Fintech)－以區塊鏈為例**

區塊鏈技術如下圖所示，是以一串使用密碼學方法關聯產生的資料區塊 (block)，每一個區塊包含數位網路交易的資訊，區塊鏈可以將整個金融網路的所有交易資訊發布至每一個區塊鏈使用者，並確保每個人只能修改自己的財產，區塊鏈技術利用複雜的公鑰 (Public key) 及私鑰 (Private key) 運算機制，故可防偽驗證交易資訊之有效性及產生下一個區塊，因而區塊鏈技術可廣泛應用於各種金融與支付業務之金流。




區塊鏈核心技術已成為各國監理機關及金融機構之研究課題，全球金融機構已進行協議共同開發區塊鏈技術，建立一致的管理標準與協定。區塊鏈技術實現了去中心化的新金融體系進行自動化交易，區塊鏈交易可透明、公開地被追蹤與監督，故提供可靠的數位交易紀錄，亦提供稽核及監理，金融業者可透過實驗尋找區塊鏈有價值的應用機會。

**(五)各國監理討論及交流**

講師提問: 如何保護虛擬貨幣之價值?如何監理其風險?

講師回答:

1.監理之重點為防範駭客破壞區塊鏈之信任機制。

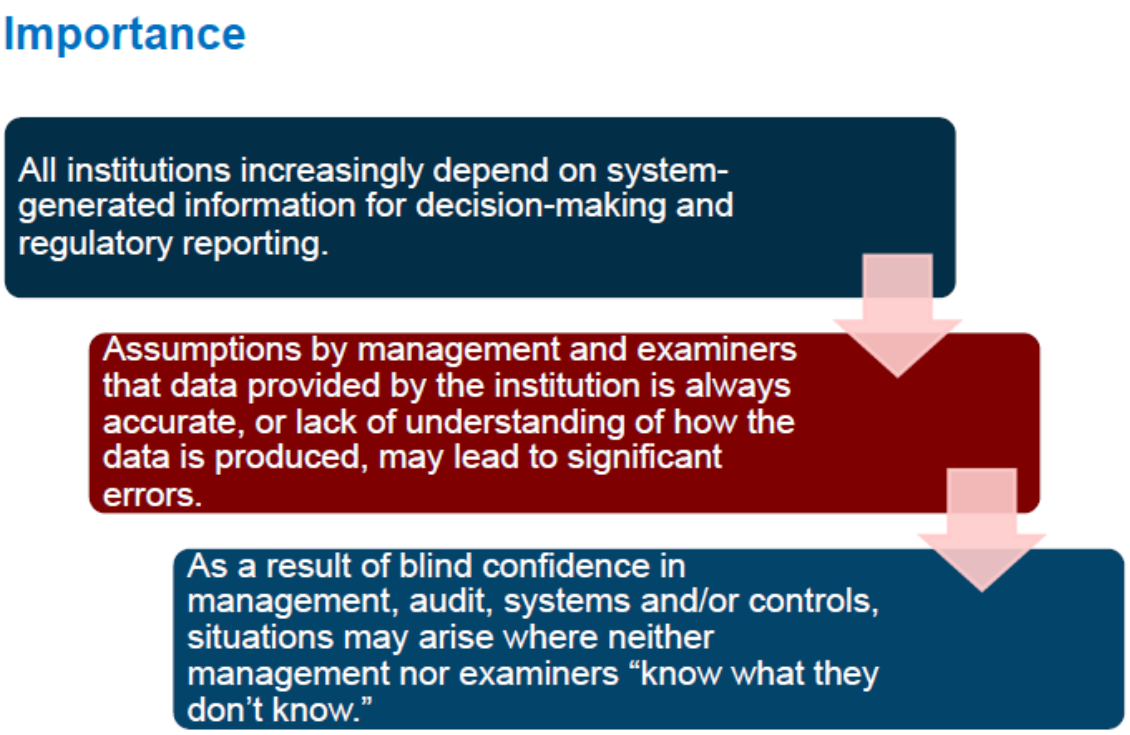
2.若傳統銀行的角色消失，由誰來負責商品交易之最終責任值得深思。

## 五、資料治理(Data Governance)及資訊作業委外風險/委外作業廠商管理(Vendor Management)

### (一)資料治理(Data Governance)

1.資料治理之重要性與效益

資料治理之重要性如下圖所示,金融機構越來越依賴系統產生的資訊進行決策和陳報監理報表,而金融機構管理階層和檢查人員卻假設機構提供的資料總是準確的，或者對金融機構資料的產生過程缺乏了解，則可能會導致重大錯誤。由於對管理、稽核、系統或控制之盲目信心，金融機構管理階層和檢查人員都忽略資料治理的重要性。




資料治理是一套確保重要資料資產之管理流程，修復和預防資料問題，確保資料可信賴，金融機構可利用大數據管理，以資料治理為基礎，進行資料整合而產生效益，如：資料倉儲作為海量資料蒐集與即時分析，分析資料及產生報表以確認事件發生根因並採取因應措施，並預測未來再發生機率及同步監控正在發生之事件。

2.資料治理計畫

金融機應建立架構，確保陳報之監理報表和業務決策及其他 MIS 系統資訊之完整性。這些方案應考慮：

(1)政策和程序

(2)工作流程文件

(3)資料可追蹤性之實務

(4)準確性和完整性控制

3.檢查人員對資料治理應關注之重點

(1)金融機構是否建立資料治理機制?

(2)允許及禁用之資料權限為何?

(3)資料治理如何確保資料完整性（Integrity），是否訂定資料變更管理政策?

(4)風險管理架構是否評估資料治理相關風險?

(5)資料治理政策是否考量其他國家或地區之法規遵循情形?

(6)資料治理對資安事件之回應機制?

**(二)資訊作業委外風險/委外作業管理 (Third Party Risk/Vendor Management)**

隨著資訊科技的快速發展,金融機構仰賴資訊委外作業建置先進的技術，透過有效的委外作業，金融機構使核心業務(core processing)更專業化,取得較佳的資訊作業方式,資訊委外作業亦有助金融機構強化其特定金融商品服務的機會。惟資訊委外作業風險趨勢日益升高,如：第三方廠商惡意未通知他們在資訊安全事件或其他網路安全漏洞事件、金融機構資訊安全需求須由第三方委外廠商提供解決方案而無法自主、委外廠商未揭露其最低限度的資訊安全措拖等,使金融機構曝露在第三方委外廠商之作業風險中。

1.委外契約條款訂定及注意事項(Contract Provisions and Considerations)

金融機構委外契約條款訂定應包括但不限於之重點如下，為資訊委外作業檢查重點：

(1)服務範圍

(2)成本和賠償

(3)金融機構及主管機關之稽核權力

(4)保密和資訊安全

(5)違約和契約終止

(6)業務恢復和應急應變計畫之服務委外作業廠商

(7)複委託

2.委外作業風險

資訊作業委外作業風險主要來自下列幾類：

(1)法遵風險

委外廠商（受託機構）的服務、產品或活動，未遵守我國法規。

(2)集中度風險

由於委外廠商有限，提供的委外服務或產品僅集中在有限少數幾家。

(3)聲譽風險

委外廠商的業績不佳或形象不佳，亦導致公眾形成了對金融機構(委託機構)的負面形象。

(4)國家風險

金融機構資訊委外作業是外國服務提供商，該機構所位於之國家可能經濟、社會和政治條件皆處於不穩定狀態。

(5)作業風險

當委外廠商由於不當或失敗的內部控制程序、系統或外部事件和人為錯誤虧損，因而出現作業風險。

(6)法律風險

當委外廠商的服務提供出現異常，使金融機構面臨訴訟的法律風險。

3.委外作業風險管理程序及監理實務要點

資訊委外作業所衍生的風險管理相當重要，管理階層及監理人員須嚴格監督金融機構是否謹慎分析及管理資訊委外作業所附隨的風險,包括瞭解相關作業的風險、透過謹慎程序遴選受託機構、績效評量及服務品質下降或停止營運時的緊急應變計畫，並建置對受託機構持續監督之計畫。其風險管理原則如下：

(1)考慮是否進行資訊委外作業，董事會及管理階層應針對銀行整體的經營策略及目標,確認委外作業所要扮演的角色,方能完全整合至公司的策略目標

(2)委外作業前，金融機構必須確認其策略目標、效益、相關法規及成本，並包括作業委外相關風險,管理階層對委外作業應建立一套完整及實用的全盤式的評估確認程序。

(3)風險評估項目應包效益、內部控制 、服務水準的報告及契約是否符合法規，資訊人員、內部稽核人員、法規遵循人員與法務應一起分析委外作業的相關風險 ，建立必要的控制及報告架構 。

(4)金融機構必須有效確認受託機構是否有足夠資訊安全措施保護客戶資料。

(5)金融機構依策略計畫與風險評估項目，須建立評估資訊委外作業的標準，就委外作業終止，亦應建立適當的策略及緊急應變計畫。

(6)管理階層應指派專人擔任監督資訊委外作業，從事評估與管理委外作業及其與受託機構的關係 ，提供必要的資源以監督及衡量受託機構對委外作業的執行成效，並定期向董事會提出報告之責。

4.監理交流討論

馬來西亞學員提問:若資訊作業委外至海外公司，特別是使用當地的IT 系統，請問如何檢查?

講師:需要了解委外公司之風險並與金融機構聯合檢查，如： VISA 公司及亞馬遜公司(Amazon)公司。

## 六、資訊安全與網路安全、資訊治理(IT Governance)及統合監理(integrated supervision)

### (一)資訊安全（Information security）與檢查關注重點

資訊安全之重點在於資訊可用性（availability）、保密性（confidentiality）、完整性（integrity）、正確性（assurance）和可靠性(accountability)。資訊安全檢查關注重點如下：

1.系統存取權限和身分識別管理

(1)系統存取權限須與工作責任和業務需求相符

(2)建立、審查和刪除系統系統存取權限之程序

(3)限制及監控重要存取權限級別和活動，如：舞弊、惡意或過失查詢客戶資料及內部消息走漏。

2.異常事件通報與管理

(1)異常事件通報計畫

(2)如果發生異常事件，應通知、溝通和適時回應處理

(3)金融機構需有一個行動計畫來應變解決客戶資料洩露

(4)事件通報計畫應說明如何保存鑑識證據及如何確認攻擊已經結束及系統或網路已經回復安全

(5)進行應變測試演練並確保員工了解其角色和職責

(6)應納入委外作業發生之異常事件

### (二)網路安全(Cybersecurity) 與檢查關注重點

1. 網路安全定義及其挑戰性(Challenging)

網路安全(Cybersecurity)為一個廣泛的概念，目前並沒有一致的定義，依 ISACA 之定義，網路安全(Cybersecurity)為解決網際網路資訊系統之威脅，包括從資訊處理、儲存和傳送過程中對資訊安全之防護，來保護資訊資產。網路風險相較於其他之 IT 監理風險有如下特點：

(1)動態:不斷變化的網際網路資訊系統之威脅

(2)無地理障礙，遍及全世界

(3)與網路駭客之專業知識上之差距

(4)無適用於現行做法之指導或防護標準

2.網路攻擊之類型

網路風險的主要挑戰之一是不斷變化，須不斷的監控和因應網路攻擊，如下圖所示，網路威脅在網路裏無所不在，網路攻擊之類型如下：

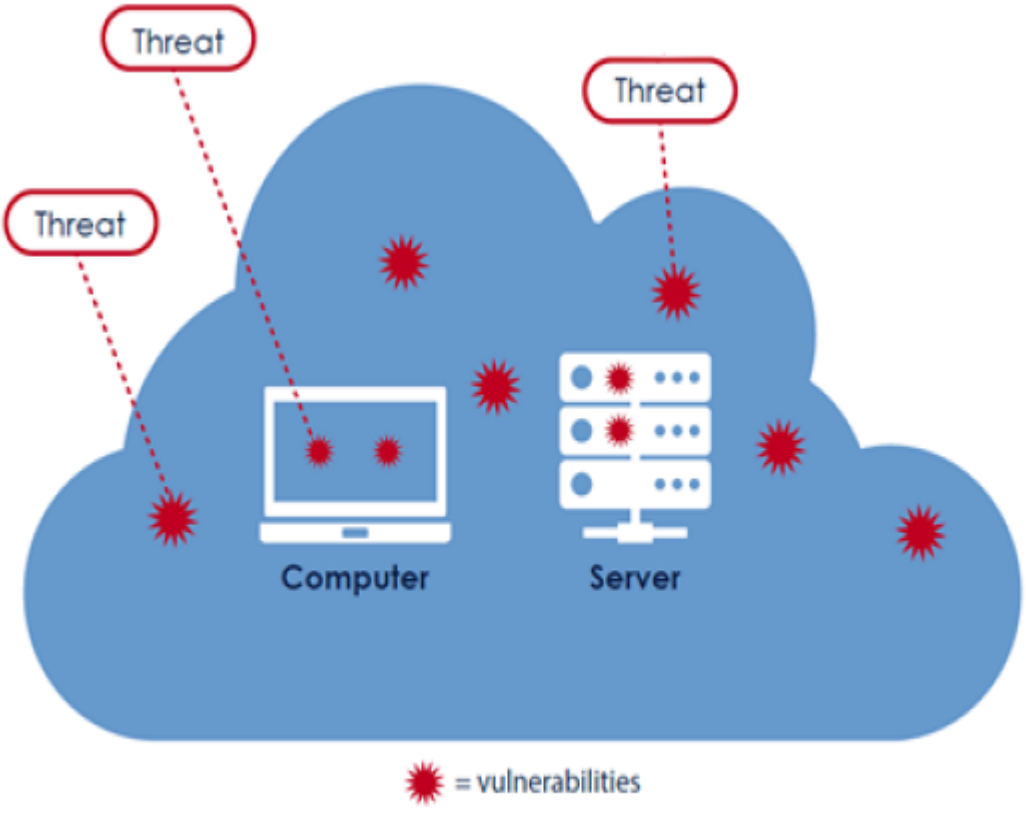



**Image:** Threats often take advantage of internal and external vulnerabilities.

(1)分佈式拒絕服務攻擊（DDoS）

分佈式拒絕服務攻擊（DDoS）時，網站擁有的流量超過了處理流量的網站，那麼網站的服務器就會超載，網站將無法將其內容提供給正在嘗試存取之用戶，癱瘓流量以便關閉所有用戶。這些 DDoS 攻擊是由許多電腦同時執行的，由於攻擊者同時出現在世界各地的許多不同的 IP 地址，使網路管理員對確認攻擊來源更加困難。

(2)惡意軟體或程式

惡意軟體是指各種形式的有害程式，如：病毒和勒索軟體， 一旦電腦中出現惡意軟體，它可能會導致各種破壞，包含控制電腦，監控操作和按鍵，將各種機密資料從電腦或網路發送給攻擊者。攻擊者使用各種方法將惡意軟體導入電腦，包括點擊連結下載文件，或打開可能看起來無害的附件（如 Word 文檔或 PDF 附件），但實際上隱藏了惡意軟體安裝程式。

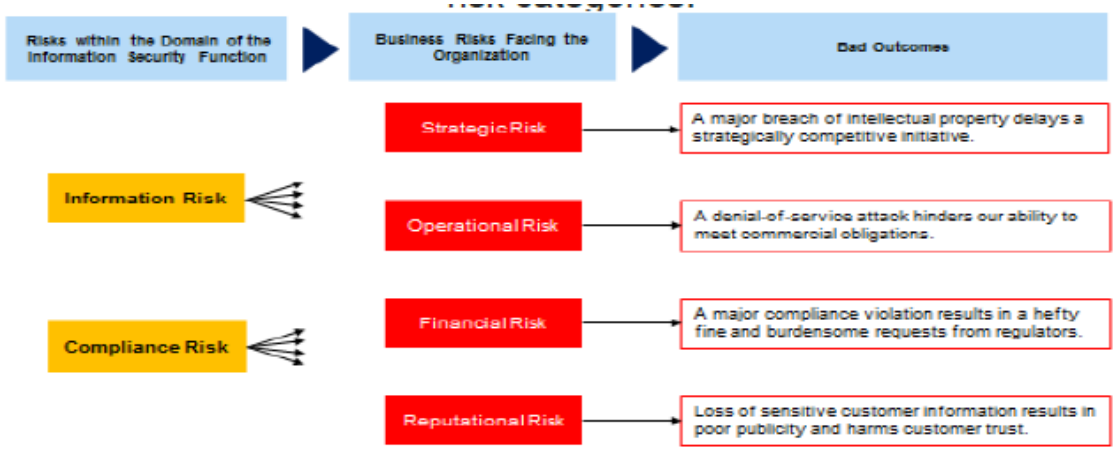
(3)網路釣魚（社交工程）

攻擊者使用網路釣魚，假裝成為某人或某些其他方法，讓您採取通常不會採取的行動。在網路釣魚攻擊中，點擊電子郵件連結它可能會發送到一個合法的網站，要求登錄，用於在您嘗試登錄時捕獲您的憑據，故了解驗證電子郵件發件人和附件/連結十分重要。

3.重大網路安全漏洞事件

迄 2016 年止，一些重大網路安全漏洞事件報告，在各企業部門詐欺使用之個人資訊，知名的公司及機構，如：Yahoo、Dropbox 及 UC Berkeley 等皆蒙受帳戶資料被盜。


網路風險不僅從資訊安全或 IT 風險角度考慮，而且還受到其他主要風險類別的影響，如下圖所示，包含策略、作業、財務及商譽等風險。




4.網路安全監理工具及檢查重點

(1)NIST 網路安全架構

- 著重理解、管理和減少網路安全風險的架構。
- 提供一個廣泛的架構，可以為來自任何行業的商業部門和組織所採用
- 該架構鼓勵企業領導者和 IT 職能之間更好的溝通和意識。

(2)FFIEC 網路安全評估工具（最適合本局檢查銀行業參考使用）

美國聯邦金融機構檢查委員會 (Federal Financial Institutions Examination Council， FFIEC) 為管理金融機構之網路安全，就網路安全威脅不斷增加的風險，發展出一套網路安全評估工具(Cybersecurity Assessment Tool) 提供可以重複衡量網路安全防護之評估工具，如：網路安全風險管理、威脅情資管理、資訊安全控管、委外關係管理、資安事件管理與回應等面向，協助金融機構辨識其網路安全風險，並採行對應之防範措施：

- 適用於所有規模金融機構的自我評估工具
- 旨在幫助評估網路風險並確定組織的準備狀況
- 提供可重複和可衡量的流程，以確認金融機構對風險狀況是否實施了適當控制和風險管理並納入了 NIST 網路安全架構的關鍵概念

(3)金融市場基礎設施網路回復指導原則(Guidance on Cyber Resilience for Financial Market Infrastructures)－最適合本局檢查證券業參考使用

由支付和市場基礎設施委員會（Committee on Payments and Market Infrastructures ,CPMI）和國際證券委員會組織（IOSCO）制訂：

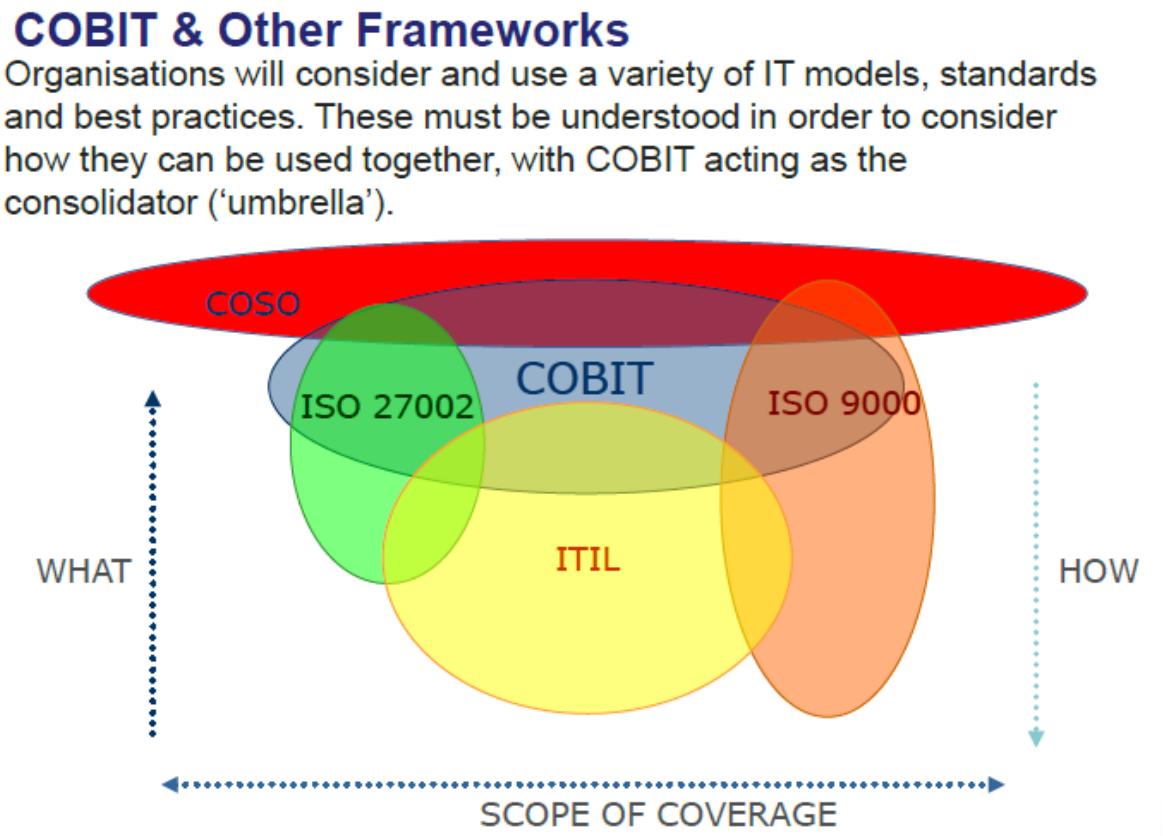
- 第一份有關金融業網路安全之國際指導原則
- 為金融業正在進行的網路安全灌輸國際一致性，以提高金融業預防網路攻擊的能力，迅速有效地因應，並實現更快更安全之恢復營運目標
- 旨在提供更多的準備工作的細節和因應措施，以提高網路回復能力，以盡量減少不斷上升之網路威脅，回復金融穩定。

**(三)資訊治理(IT Governance)與統合監理**

1.資訊治理之理念與架構

資訊治理是資訊系統稽核和內部控制領域中的一個相當新的理念，資訊治理是公司治理的一部分，用於描述企業或政府是否採用有效的機制，使得 IT 的應用能夠完成組織賦予它的使命，適當管理業務與資訊科技的風險，確保實現組織的策略目標實現所提供的治理結構。

金融機構之資訊治理可考慮並使用各種IT模型標準和實務做法。其中 COBIT 可整合與其他的 IT 標準和實務（如 COSO 、ITIL 、 ISO 27002 及 ISO 9000）共同使用，可用下圖以整體（'傘'）狀來說明，COBIT 作為這些不同模型標準和實務的整合者，係將較佳實務模式與治理和業務需求聯繫起來而成為一個架構。




金融機構使用 COBIT 架構可以有效執行資訊管理、提高業務靈活性、降低成本，同時更好地遵守內部資訊作業管理規定，也有助於確保遵守監理法規。

COBIT 通過將 IT 分為四個領域之監控評估模型，分別為計畫，構

建，運行，並監控，如下圖所示，**架構組件包括：**

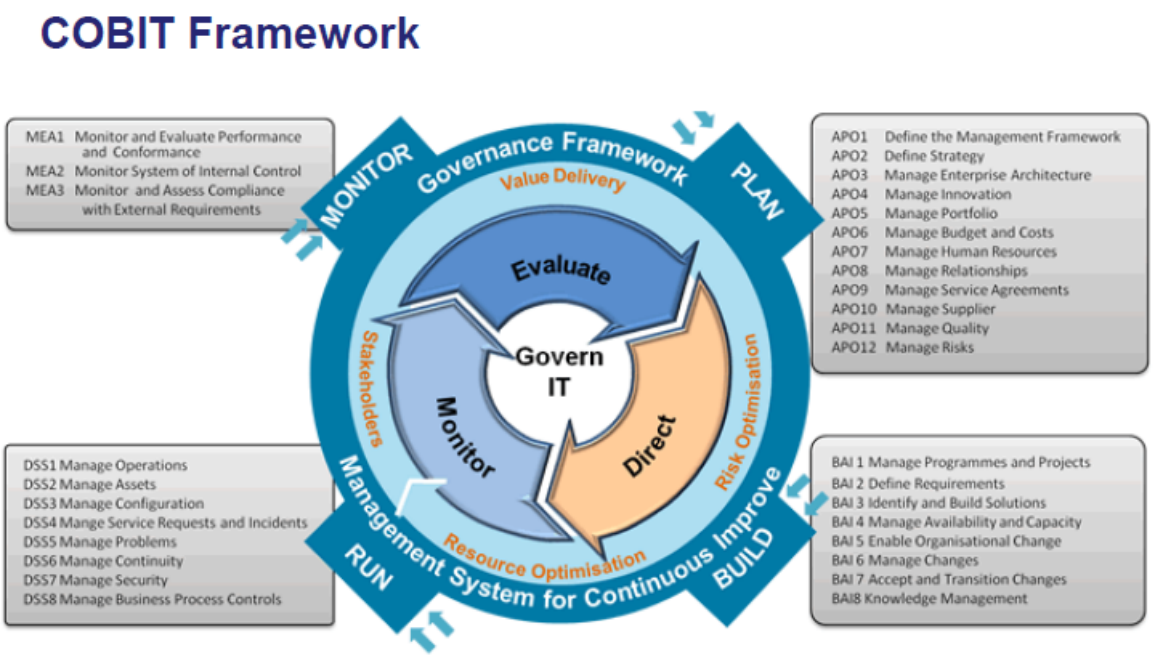
(1)架構：通過 IT 領域和流程組織 IT 治理目標和做法，並與業務需求聯繫。

(2)流程：組織中之參考流程模型和語言，對應計畫、構置、運行和監控之相關責任領域。

(3)控制：提供管理階層如何有效控制 IT 流程。

(4)管理：說明與其他流程的相互關係，分配責任及衡量績效。

(5)成熟度：評估每個過程的成熟度，解決差距。




2.檢查人員使用 COBIT 架構對董事會提問資訊治理問題

(1)金融機構策略規畫過程是否納入資訊長(CIO)或其他資深 IT 成員？

(2)目前影響組織的重要項目有多少涉及 IT 的重大變化？

(3)IT 項目未完成而未執行之預算？

(4)金融機構 IT 組織為反應性還是主動性（幫助各項業務改進）？

(5)IT 相關的問題列在議程上，由 CIO 解決或 IT 資深代表？

(6)業務部門是否將所屬之 IT 相關風險之傳達給董事會？

(7)董事會是否獲得 IT 風險被有效管理之獨立保證？

(8)金融機構和 IT 目標是否符合？

**(四)統合監理(Integrated Supervision)**

1. IT風險可能會影響金融機構之整體安全和健全

作業風險是 IT 風險普遍被接受的領域,但目前監理趨勢認為 IT 風險與法律及法遵，甚至流動性、信用和市場風險之間的關係是重要的， IT 風險可能會影響金融機構之整體安全和健全：

(1)IT 風險亦對美國監理指引 SR 16-11 所列金融機構經營之風險因素，如：信用、作業、市場及流動性／法遵等有所影響

(2)影響監理機構對金融機構風險與經營管理之評等

2.當前的 IT 監理之主要議題

影響金融服務之當前 IT 議題如下：

(1)資訊安全尤其是網路安全

(2)資訊治理與風險管理

(3)委外作業廠商風險管理

(4)IT 基礎設施

(5)業務方面特別是零售支付業務

3.IT 風險對金融機評等之影響

(1)美國監理機構目前對金融機構評等體系中，將 IT 風險主要納入風險管理評級、經營管理評級及綜合評級予以考量評等。

(2)網路安全、資訊作業委外風險管理、資料治理和支付創新是提高 IT 風險在評等中考慮的主要驅動因素。

**(五)各國監理交流**

1.印度學員提問:是否認為董事會成員應有具 IT 背景之董事加入?

講師回答:美國目前是有在考慮研議中，目前在場各位有法規規定 IT 背景之董事嗎?無人舉手，應該是沒有。

印度學員分享：雖然印度沒有法規規定須具有 IT 背景之董事加入董事會，但董事會底下，我們有要求要成立一個 IT 稽核委員會( IT audit Committee)。另外我們認為銀行的高階管理人員應該接受教育訓練 IT 的相關風險，以有助於主管機關對 IT 之風險監理。

2.台灣央行學員提問：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？

講師回答：依美國聯邦準備體系(Federal Reserve System, 下稱 Fed)之監理用詞，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(或單位)全體業務與財務之監督。

# 伍、結論與建議

## 一、結論

行動支付商品發展越來越普及，技術創新更有別於傳統網路銀行，其資訊安全是目前監理機關所須重視及面對之新議題，透過本次研討會與各國學員交流，顯示我國對行動支付系統之檢查經驗符合國際對行動支付日趨重視之監理潮流，爰我國得以現有規範及檢查模式為基礎，包括行動應用程式發布安全性、身分認證授權與連線管理安全、防止軟體竄改及金鑰等敏感性資料之儲存，並要求定期辦理行動支付系統滲透測試等，持續關注相關風險，輔以透過國際研討會與各國互相交流。

## 二、建議

### (一)強化金融機構雲端運算服務委外廠商之認證要求

考量金融機構推出雲端運算服務逐漸朝向將相關資訊作業委外處理，相關作業及服務已轉移至機構外部甚至跨境，建議就其衍生之網路安全、資料儲存及實體設備安全問題，納入雲端運算服務之檢查重點，並進一步要求委外廠商宜通過 ISO 等國際標準認證。

### (二)視金融機構自組區塊鏈平台之發展，適時參與其管理標準之訂定

區塊鏈技術應用於跨領域及跨國之金融交易日益成熟，同時亦成為惡意軟體及駭客攻擊勒索之標的，為強化金融機構洗錢防制及消費者保護作業，建議密切關注金融機構自組區塊鏈平台之發展，適時參與金融機構對區塊鏈技術之管理標準與協定制定，要求納入消費者保護及洗錢防制之稽核及監理檢查相關資訊。

### (三)研議推動金融機構成立資訊安全委員會，強化金融機構 IT 風險管理

依現行規定上市上櫃公司董事會為健全監督功能及強化管理機能，得考量董事會規模及獨董人數，設置審計、報酬或其他各類功能性委員會，

考量數位金融已成趨勢，營運風險逐漸轉向網路安全，又資訊治理屬公司治理一部分，建議參酌本次國外(印度)作法，研議推動金融機構成立資訊安全委員會，以強化其 IT 風險管理。

## 陸、附件

顧問小組會議議程及研討會參與者名單與聯絡方式。

# APEC Financial Regulators Training Initiative
# 22nd Advisory Group Meeting – Securities Regulators

## Rarotonga, Cook Islands
## 5 June 2017

## AGENDA

**Welcome and Opening Remarks**

13:00 – 13:05 Asian Development Bank (ADB)
13:05 – 13:10 Opening Remarks - Chair

**Session I- Review of the FRTI Activities in 2016-2017**

13:10 – 13:15 **Confirm Minutes of 21st AG Meeting 2016**
13:15 – 13:25 **Review of the Action Items from 21st AG Meeting 2016**
Open Discussion

13:25 - 13:45 **Report on Seminars Conducted**
*FRTI Secretariat*
Open Discussion

13:45 – 14:05 **Report on Survey Results**
*FRTI Secretariat*
Open Discussion

**Session II- Select Seminar Programs, Hosts and Dates for 2018**

14:05 – 14:25 **Open Discussion to Select Seminar Programs, Hosts and Dates for 2018**
*Chair*
*Moderator: ADB*

14:25 – 14:45 **Open Discussion for other Agenda items**
- Review of APEC FRTI Charter
- AG Meeting in 2018 – Host and Date

**Closing Remarks**

14:45 – 14:50 Closing Remarks - Chair

15:00 - 16:00 **Open Discussion on APEC FRTI (Joint session with Bank Supervisors)**
*FRTI Secretariat*

# APEC Financial Regulators Training Initiative
# 22nd Advisory Group Meeting – Bank Supervisors

## Rarotonga, Cook Islands
## 5 June 2017

## AGENDA

| | | | |
|---|---|---|---|
| 15.00 | – | 16.00 | **Open Discussion on APEC FRTI (Joint session with Securities Regulators)** |
| | | | **Welcome and Opening Remarks** |
| 16.10 | – | 16.15 | Asian Development Bank (ADB) |
| 16.15 | – | 16.20 | Opening Remarks - Chair (Ms. Louise Wittwer, FSC) |
| | | | **Session I- Review of the FRTI Activities in 2016-2017** |
| 16.20 | – | 16.25 | **Confirm Minutes of 21st AG Meeting 2016** |
| 16.25 | – | 16.30 | **Review of the Action Items from 21st AG Meeting 2016**<br>Open Discussion |
| 16.30 | – | 16.50 | **Report on the Seminars Conducted**<br>*FRTI Secretariat*<br>Open Discussion |
| 16.50 | – | 17.10 | **Report on Survey Results**<br>*FRTI Secretariat*<br>Open Discussion |
| | | | **Session II- Select Seminar Programs, Hosts and Dates for 2018** |
| 17.10 | – | 17.30 | **Open Discussion to Select Seminar Programs, Hosts and Dates for 2018**<br>*Chair: FSC*<br>*Moderator: ADB* |
| 17.30 | – | 17.50 | **Open Discussion for other Agenda items**<br>• Review of APEC FRTI Charter<br>• AG Meeting in 2018 – Host and Date |
| | | | **Closing Remarks** |
| 17.50 | – | 18.00 | Closing Remarks - Chair (Ms. Louise Wittwer, FSC) |

**APEC FINANCIAL REGULATORS TRAINING INITIATIVE**
**Regional Seminar on Cybersecurity / Technology Risk Supervision**
**6–9 June 2017, Rarotonga, Cook Islands**
**Hosted by Cook Islands Financial Supervisory Commission**

**PARTICIPANTS**

| ECONOMY | NAME | | CONTACT DETAILS |
|---|---|---|---|
| BANGLADESH | 1 | Mr. Gour Chand SARKER | Assistant Director<br>Management Information System<br>Bangladesh Securities and Exchange Commission<br>Tel +880-2-55007112<br>Fax +880-2-55007106<br>Email gour@sec.gov.bd |
| BANGLADESH | 2 | Mr. Md Ziaul KARIM | Chief Technology Officer<br>Information and Communication Technology<br>Dhaka Stock Exchange Limited<br>Tel 88029551935<br>Fax +8802956727<br>Email cto@dse.com.bd |
| COOK ISLANDS | 3 | Mr. James CARGILL | Finance and IT Administrator<br>Finance Department<br>Financial Supervisory Commission |
| COOK ISLANDS | 4 | Ms. Emilie PIERCE | Supervisory Analyst<br>Supervision Department<br>Financial Supervisory Commission<br>Tel +682 20798<br>Fax +682 21798<br>Email emilie.pierce@fsc.gov.ck |
| COOK ISLANDS | 5 | Mrs. Munokoa PUREA | Supervisory Analyst<br>Supervision Department<br>Financial Supervisory Commission<br>Tel (682) 20798<br>Email Munokoa.Purea@fsc.gov.ck |
| COOK ISLANDS | 6 | Mrs. Margaret TANGIMETUA | Senior Supervisor<br>Supervision Department<br>Financial Supervisory Commission<br>Tel +68220798<br>Email Margaret.Tangimetua@fsc.gov.ck |
| COOK ISLANDS | 7 | Mr. Cedric TORU | Compliance Officer<br>Compliance Department<br>Financial Supervisory Commission<br>Tel 0068220798<br>Fax 0068229182<br>Email cedric@cifiu.gov.ck |

**APEC FINANCIAL REGULATORS TRAINING INITIATIVE**
**Regional Seminar on Cybersecurity / Technology Risk Supervision**
**6–9 June 2017, Rarotonga, Cook Islands**
**Hosted by Cook Islands Financial Supervisory Commission**

**PARTICIPANTS**

| ECONOMY | NAME | | CONTACT DETAILS |
|---|---|---|---|
| COOK ISLANDS | 8 | Ms. Amanda TUATAI | Supervisory Analyst<br>Supervision Department<br>Financial Supervisory Commission<br>Tel +682 20798<br>Email Amanda.Tuatai@fsc.gov.ck |
| INDIA | 9 | Mr. Dhiraj RAMTEKE | Assistant General Manager<br>Department of Banking Supervision<br>Reserve Bank of India<br>Tel 02222189131-39 ext 342<br>Fax 02222180157<br>Email dhirajbramteke@rbi.org.in |
| INDIA | 10 | Mr. Sunil KUMAR | Assistant General Manager<br>Market Intermediaries Regulation and Supervision Department<br>Securities and Exchange Board of India<br>Tel 26449723<br>Fax 26449031<br>Email SUNILKU@SEBI.GOV.IN |
| INDIA | 11 | Mr. Virendra KUMAR | Assistant General Manager<br>Information Technology<br>Securities and Exchange Board of India<br>Tel +912226449592<br>Fax +912226449020<br>Email VIRENDRAK@SEBI.GOV.IN |
| MALAYSIA | 12 | Mr. Wan Muhd Rasimi WAN NGAH | Senior Supervisor<br>Financial Conglomerates Supervision Department<br>Central Bank of Malaysia<br>Tel 60326988044 ext 8157<br>Fax 60326914585<br>Email rasimi@bnm.gov.my |
| MALAYSIA | 13 | Ms. Li Yun HOH | Senior Manager<br>Policy and International Division<br>Malaysia Deposit Insurance Corporation<br>Tel +603 2173 7436<br>Fax +603 2173 7533<br>Email liyun@pidm.gov.my |
| NEPAL | 14 | Mr. Ram Briksh PANDIT | Deputy Director<br>Information Technology<br>Nepal Rastra Bank<br>Tel +97715012530<br>Fax +97714428202<br>Email rbpandit@nrb.org.np |

**APEC FINANCIAL REGULATORS TRAINING INITIATIVE**
**Regional Seminar on Cybersecurity / Technology Risk Supervision**
**6–9 June 2017, Rarotonga, Cook Islands**
**Hosted by Cook Islands Financial Supervisory Commission**

**PARTICIPANTS**

| ECONOMY | NAME | | CONTACT DETAILS |
|---|---|---|---|
| NEPAL | 15 | Mr. Tej Narayan THAKUR | Deputy Director<br>Information Technology<br>Nepal Rastra Bank<br>Tel +977 1 5012530<br>Fax +977 1 4428202<br>Email tejnarayanthakur@gmail.com |
| NEW ZEALAND | 16 | Ms. Paula HONTALBA | Analyst<br>Prudential Supervision<br>Reserve Bank of New Zealand<br>Tel +64 471 3623<br>Fax +64 4 471 3995<br>Email paula.hontalba@rbnz.govt.nz |
| PAPUA NEW GUINEA | 17 | Mrs. Bernadette CALEB | ICT Security Officer<br>Information and Communication Technology<br>Bank of Papua New Guinea<br>Tel 3227562<br>Fax 3211617<br>Email BCaleb@bankpng.gov.pg |
| PAPUA NEW GUINEA | 18 | Mr. Matthew DOREA | Analyst<br>Superannuation and Life Insurance Department<br>Bank of Papua New Guinea<br>Tel 675-3227132<br>Fax 675-3214548<br>Email MDorea@bankpng.gov.pg |
| PAPUA NEW GUINEA | 19 | Mr. Justin WOHUINANGU | Senior IT Auditor<br>Internal Audit Department<br>Bank of Papua New Guinea |
| SOLOMON ISLANDS | 20 | Mr. Glen BUKA | IT Network and Support<br>Information Technology Department<br>Central Bank of Solomon Islands<br>Tel (+677) 21791<br>Fax (+677) 23513<br>Email gbuka@cbsi.com.sb |
| SRI LANKA | 21 | Mrs. Chaya WATHAWANA VITHANAWASAM | Director<br>Finance and Administration<br>Insurance Board of Sri Lanka<br>Tel +94112396193<br>Fax +94112396190<br>Email chaya@ibsl.gov.lk |

**APEC FINANCIAL REGULATORS TRAINING INITIATIVE**
**Regional Seminar on Cybersecurity / Technology Risk Supervision**
**6–9 June 2017, Rarotonga, Cook Islands**
**Hosted by Cook Islands Financial Supervisory Commission**

**PARTICIPANTS**

| ECONOMY | NAME | | CONTACT DETAILS |
|---|---|---|---|
| TAIWAN,R.O.C | 22 | Mr. Jen-Chun HSIEH | Chief<br>Financial Inspection<br>Central Bank of the Republic of China |
| TAIWAN,R.O.C | 23 | Mr. WEIHSU LI | Inspector<br>Financial Examination Bureau<br>Financial Supervisory Commission<br>Tel 886-2-8968-0899<br>Fax 886-2-8969-1215<br>Email vincent@feb.gov.tw |
| TANZANIA | 24 | Ms. Witness GOWELLE | Financial Analyst<br>Market Supervision and Market Development<br>Capital Markets and Securities Authority<br>Tel +255222114959<br>Fax +255222113846<br>Email wheyg@yahoo.com |
| THAILAND | 25 | Ms. Napada AIKEAMWORAKUL | Senior Officer<br>Intermediaries supervision Department<br>Securities and Exchange Commission<br>Tel (66)2-033-9547<br>Fax (66)2-033-9547<br>Email napada@sec.or.th |