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—電子銀行與行動金融服務研討會 APEC Financial Regulators Training Initiative (FRTI)—Regional Seminar on Electronic Banking and Mobile Financial Services
會議時間	105 年 6 月 20 日至 24 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	朱衛華、金融監督管理委員會銀行局、科長
聯絡電話、e-mail	(02)8968-9813、whchu@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、本次研討會主要探討電子銀行(e-banking)及行動金融服務(mobile financial services)相關議題，內容包括 e-banking、e-money、mobile financial services 成功案例及成功要素、支援該等服務之 IT 基礎設施與雲端服務平臺、IT 基礎設施與雲端服務平臺之管理與風險控管、網路安全之評估、業務持續運作及災害復原計畫、洗錢防制及反恐與消費者保護等議題。 二、課程內容主要為講師講授，並輔以個案研討、小組討論與報告之型式進行；另由參訓學員分享在相關議題上之金融監理實務經驗。 二、我方於研討會中，除主動提問以瞭解授課內容、積極參與討論及分享我國金融監理之作法外，亦與參訓學員相互交流，瞭解與會各國金融監理之作法。
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	隨著資通訊科技之發展，金融服務之網路化與行

	動化是大勢所趨，本次研討會兼具理論與實際個案之研析，使筆者獲益良多，謹研提下列心得與建議： 一、本次課程所探討相關議題，有助於未來金融監理之需。 二、由於各國發展 e-banking、e-money 或 mobile financial services 之程度不一，相關業務發展之內容及監理資訊亦非完全公開或透過網路而可完整得知，藉由本次課程可掌握最新資訊、國際發展趨勢與相關監理重點。 三、課程設計採個案研討、小組討論與報告之型式，可藉由與會學員間之腦力激盪，研議因應措施，亦可透過互動溝通，瞭解不同國家之金融監理實務。 四、建議我國應積極參與此類研討會，增廣見聞、互相交流，且分享我國金融監理之作法，提昇區域金融之發展。

目　錄

壹、研討會目的

1998 年 5 月，亞太經濟合作組織(Asia-Pacific Economic Cooperation, APEC)財長會議同意成立 APEC 金融監理人員訓練倡議(Financial Regulators Training Initiative, FRTI)，以增進亞太地區銀行監理機構及證券監理機構之分析與技術能力。APEC FRTI 每年分別就銀行業及證券業重要之監理議題舉辦研討會，提供各國監理機關交換意見及交流之管道。

有鑒於資通訊科技之發展，銀行未來必須將行銷管道與網路、行動裝置等整合，而科技加速變革也推進電子錢包之使用和商品創新，如：電子貨幣(e-money)、行動銀行(mobile banking)、行動金融服務(mobile financial services)、電子或行動錢包或優惠券(electronic or mobile wallet or vouchers)，行動貨幣(mobile money)及儲值(stored value)。此類創新商品之運作模式，所運用之 IT 架構與平臺，及可能衍生之風險，對於監理機關有必要瞭解並採行相關因應措施，因此亞洲開發銀行(Asian Development Bank，ADB)與泰國中央銀行(Bank of Thailand)共同舉辦本次研討會，就相關議題進行探討。課程進行方式除由講師講授外，並以個案研討、小組討論及報告之形式進行，進而由參訓學員分享其金融監理實務經驗。

本次研討會出席人員包括孟加拉、中國、韓國、印尼、寮國、澳門、馬來西亞、尼泊爾、巴布亞紐幾內亞、菲律賓、所羅門群島、斯里蘭卡、泰國及我國等 14 國家之中央銀行、金融監理機關、證券監理機關及存款保險公司等單位，合計 48 位代表參訓，互相交流並分享監理經驗。

貳、研討會議程

一、課程安排

日期	主題	講師
6/20 (一)	什麼是電子貨幣	David Kleiman
	電子銀行與行動金融服務之發展趨勢	Jane Winn
	數位金融服務之模式及成功因素	Jane Winn
	行動金融服務－個案研討	David Kleiman
6/21 (二)	行動銀行支付與風險	David Kleiman
	數位金融服務產品比較(個案研討)	David Kleiman
	資訊科技治理和風險管理	Melchor Plabasan
	對雲端運算供應商之管理	Melchor Plabasan
6/22 (三)	電子管道之風險－自動提款機(ATM)與刷卡設備(POS)	David Kleiman
	數位金融服務之監理架構	Jane Winn
	常見之漏洞與威脅－電子銀行及行動金融服務常見之漏洞與風險	Melchor Plabasan
	網路安全評估架構	Melchor Plabasan
6/23 (四)	業務持續運作及災害復原計畫	David Kleiman
	防制洗錢個案研討	David Kleiman Jane Winn Melchor Plabasan
	消費者保護	Jane Winn
	行動金融服務與消費者保護之監理作業	Dhanasite Suphachotiwatana
6/24 (五)	透過雲端提供行動銀行服務－個案研討	Jonathan Rault & Ben Potter

二、講師簡介

(一) David Kleiman：

David 是數位金融服務(Digital Financial Service, DFS)專家，對於創新電信服務與行動金融服務有 18 年經驗，目前任職於 PHB Development 公司資深顧問，除了與寮國央行合作發展 DFS 之監理機制、推動該國第 1 家網路銀行外，也在柬埔寨推動電子貨幣，並與柬埔寨央行合作，核發該國第 1 家第三方支付業者之營業執照。

(二) Jane Winn：

Jane 現任美國華盛頓大學法學院教授、查爾斯斯通講席教授及浙江大學互聯網金融研究院研究員，她專精於全球化與科技創新對商事法之影響，目前主要研究美國、歐盟、中國及印度電子商務法之發展及電子支付之創新與競爭對監理規範之影響。

(三) Melchor T. Plabasan：

任職於菲律賓中央銀行，負責銀行資訊安全及支付系統之監理與檢查。他的專業領域包含科技風險、網路安全、雲端計算、行動支付及支付系統監理。

(四) Dhanasite Suphachotiwatana

畢業於美國匹茲堡大學，取得雙學位(MBA 及 MS) ，目前任職於泰國央行資訊系統檢查與風險管理部。他在泰國央行服務達 27 年，主要經歷為資訊系統檢查及銀行、特殊金融機構及非銀行支付服務業者之監理，也是目前泰國電子支付服務發展之推手，在進入泰國央行前，曾任職多家銀行及國營事業單位。

(五) Ben Potter

Ben 在科技產業有 15 年經驗，目前擔任亞馬遜網路服務(Amazon Web Services, AWS)團隊之網路安全顧問。

(六) Jonathan Rault

Jonathan 專精於雲端安全、風險管理，曾服務於美國、法國及亞太區之多家銀行、保險公司，負責建構網路安全機制。目前服務於 AWS，許多大型企業都借重他的專業來改進他們使用雲端技術之安全策略。

參、研討會內容摘要

一、什麼是電子貨幣

(一) 數位金融服務(Digital Financial Service, DFS)包括：

1. 行動銀行(Mobile Banking)。
2. 無分行之銀行業務(Branchless Banking)。
3. 電子支付(Electronic Payments)。
4. 電子貨幣(Mobile Money 或 e-money)。

(二) 電子貨幣必須同時符合下列要件：

1. 可透過行動裝置進行交易。
2. 可使用於發行者以外之第三人，作為支付方式。
3. 發行電子貨幣之價值須與貨幣相同(即幣值為 1：1)。
4. 以電子方式記錄交易。
5. 電子貨幣之價金必須儲存在銀行帳戶(該帳戶必須為信託帳戶以保障消費者)。
6. 可贖回現金。

(三) 現金存入(Cash-In)與存款(deposit)之差異：

1. 存款必須在銀行完成，而且必須存入銀行帳戶。
2. 存款可以用現金或支票存入。
3. 銀行吸收存款後可用來放款或投資，不必存入信託帳戶。
4. 現金存入(Cash-In)專指電子貨幣之取得。
5. 電子貨幣與現金之比率為 1：1。

(四) 由於筆者及部分參訓學員對於講師所講述內容仍有疑問，爰就教於講師，謹就相關內容說明如下：

1. 泰國之 BTS 捷運卡與我國之悠遊卡等具有儲值及消費功能之電子票證是否即為電子貨幣？

   講師在瞭解該等商品之運作方式後，表示因為該等商品如不可隨時且部分贖回現金，故不符合電子貨幣之要件，不能稱為電子貨幣。

2. 電子貨幣所吸收之款項可否進行投資？

講師表示電子貨幣所吸收之款項必須存入銀行之信託帳戶，而且該等款項不得進行投資，以保障消費者權益(此節與我國對於電子票證之管理不同：我國係要求此等吸收之款項必須交付信託或取得銀行履約保證；交付信託之款項可從事低風險之投資，包括銀行存款、購買政府債券或金融債券、購買國庫券或銀行可轉讓定期存單、購買經主管機關核准之其他金融商品)。

3. 存入信託帳戶之款項可否收取利息？

講師表示電子貨幣所吸收之款項雖然存入銀行之信託帳戶，通常業者會與銀行約定不給利息，因為如果收取利息，將會使整個營運模式複雜化。

二、 電子銀行與行動金融服務之發展趨勢

(一) 非銀行體系所發展之新金融服務：

1. 電子貨幣。
2. 行動金融服務。
3. 匯兌。
4. P2P 借貸。
5. 虛擬貨幣。

(二) 新產品：

1. 銀行主導模式：

(1)ATM 與 POS。

(2)電話、網路及行動裝置。

(3)即時支付結算機制(RTGS)。

(4)快速付款機制。

2. 非銀行主導模式：

(1)電子貨幣與電子票證。

(2)行動貨幣。

(3) P2P 借貸。

(4)比特幣(Bitcoin)及分佈式分類帳技術(Distributed Ledger)。

(三) 新合作對象：

1. 銀行經紀商。

2. 經許可之服務供應商(行動、電腦服務、雲端運算)。

3. 電信業者。

4. 小額信貸機構。

5. 未受監管之虛擬貨幣，P2P 借貸。

(四) 新傳遞機制：

1. 卡片、ATM 與 POS。

2. 個人電腦。

3. 銀行核心系統。

4. 行動電話。

5. 行動 ATM。

6. 雲端運算。

(五) 監理人員該如何因應：

1. 運用政策工具：

(1)政府直接經營。

(2)社會福利規範。

(3)經濟措施。

(4)私法自治+法院。

(5)核發執照。

(6)保險。

(7)政府保證。

(8)政府補貼。

(9)收取費用或罰款。

(10) 訂定技術規格。

(11) 產業自律規範。

2. 監理措施：

(1)道德勸說。

(2)警告函。

(3)民事處罰。

(4)刑事處罰。

(5)暫停業務。

(6)吊銷營業執照。

3. 風險應對矩陣：

衝擊 / 發生機率	高	低
高	避免	降低風險
低	移轉	承擔

(六) 金融服務之創新：

	漸進式創新	激進式創新
既有市場	中國銀聯卡 印度 RuPay 快速付款機制 支票清結算機制	行動銀行 行動 ATM 開放式介面之銀行業務
創新市場	電信業者主導之行動支付 第三方支付服務	肯亞行動支付服務(M-Pesa) 分佈式分類帳技術(區塊鏈)

(七) 本課堂中講師分享因應科技發展創新潮流之成功與失敗案例，如：

1. 數位相機之出現使得傳統底片膠卷沒落。

2. 智慧型手機之出現讓傳統手機業者失去舞台：

(1)Apple 成功關鍵在於破壞式創新+品質+品味=創新市場，首先進入市場獲得利益。

(2)Android 成功關鍵在於採取開放平台策略，降低成本，擴大市占率。

(3)Blackberry 失敗之原因在於僅對發展成熟之商品採漸進式之改變，無法面

對破壞式創新及滿足民眾需求。

3. 通訊軟體出現改變通訊方式。

4. 結語：如果你不是壓路機，你注定是馬路(等著被壓路機輾過)。

三、 數位金融服務之模式及成功因素

(一) 先進國家金融服務創新：

	漸進式創新	激進式創新
既有市場 (銀行主導)	網路銀行及行動銀行 儲值卡 快速支付機制 支票清結算機制 可攜式帳號 行動錢包 NFC/HCE 行動支付	分佈式分類帳技術 (Distributed Ledger) 開放式介面之銀行業務
創新市場 (非銀行主導)	匯款 P2P 借貸	比特幣(Bitcoin)

(二) 一般國家金融服務創新：

	漸進式創新	激進式創新
既有市場 (銀行主導)	支付卡網路 RTGS 清結算機制 網路銀行及行動銀行 快速支付機制 支票清結算機制 行動錢包	開放式介面之銀行業務 無分行之銀行業務
創新市場 (非銀行主導)	匯款 P2P 借貸	行動貨幣

(三) 新興國家金融服務創新：

	漸進式創新	激進式創新
既有市場 (銀行主導)	支付卡網路 RTGS 清結算機制 快速支付機制	無分行之銀行業務
創新市場 (非銀行主導)	匯款	行動貨幣

(四) 成功的關鍵因素－銀行主導模式

1. 巴西－銀行與零售業合作：

(1)政治面：2003 年工黨領袖當選總統，為履行競選承諾，推動貧窮家庭補助計畫(Bolsa Familia)，允許民眾可在國營銀行之合作單位(如：彩券行、超市、麵包店、藥局、郵局、加油站、百貨公司等)開立簡易帳戶，以接受政府撥付補助款。

(2)資訊面：1960 年代政府要求銀行提供繳費服務，1980 年代銀行為應付惡性通貨膨脹強化資訊系統運算功能，奠定良好之基礎環境。

2. 印度－發展無分行之銀行業務：

(1)國營銀行在 1969 年推動社會銀行政策。1991 年雖然因為金融危機而取消社會銀行政策，但多數銀行仍為國營銀行。

(2)1998 年提供農村信貸服務、2000 年開立簡易帳戶、2014 年推動社會福利計畫。

(3)基礎設施：電子資金移轉、跨行行動支付系統已建置完成。

(五) 成功的關鍵因素－非銀行主導模式

1. 肯亞行動支付(M-Pesa)

(1)城鄉差距大，匯款方式為利用巴士運用現金。

(2)電信業務鬆綁，使得行動電話滲透率高。

(3)金融包容性低。

(4)電信業者(Safaricom)第一次推動失敗，有經驗可循。

(5)Safaricom 在全國手機市占率達 70%。

(6)獲得肯亞央行支持。

2. 印度行動貨幣

(1)電信業者(Bharti Airtel)在 2011 年被許可試辦行動貨幣，於 2012 年正式發行。

(2)尚未達到建置新平台。

四、 行動金融服務－個案研討

(一) 以顧客為中心之金融服務：

1. 可用的(合法的商品)。

2. 無障礙的(合理的 KYC，鄰近有服務商)。

3. 可信賴的(網路機制健全)。

4. 適當的(明確的契約條款)。

5. 吸引人的(解決消費者實際需要，操作便利)。

6. 經濟實惠的(價格大眾化)。

(二) DFS 市場發展週期：

1. 成立期(1-4 年)。

2. 啟動期(3-5 年)。

3. 擴張期(3-6 年)。

4. 合併期(時間不確定)。

(三) 合作模式：

架構	銀行業者主導	電信業者主導	銀行業與電信業合作
說明	電信業僅是服務中一種管道	銀行業接受儲值金	銀行業提供金融管理，電信業提供電訊網路
服務	存款、放款、轉帳、付款	存款、轉帳、付款	存款、放款、轉帳、付款

目標客戶	銀行既有客戶	非銀行客戶	非銀行客戶
案例	BSP(巴布亞紐幾內亞、所羅門群島)、FNB(南非)	M-PESA(肯亞)、GCASH(菲律賓)	Easypisa(巴基斯坦)、WAVE MONEY(緬甸)

五、 行動銀行支付與風險

(一) 認證與傳遞模式：

1. 密碼 。
2. 手機號碼+密碼 。
3. 手機+密碼+一次性密碼(One Time Password)。
4. 簡訊 SMS(Short Message Service)。
5. 簡碼 USSD2 (Unstructured Supplementary Service Data 2)。
6. 語音。
7. 智慧型手機 App。

(二) 數位金融服務之風險：

1. 消費者保護：

風險	因應方式
消費者將款項轉錯人	－交易時，行動裝置螢幕會顯示收款人姓名讓消費者確認
消費者不知道如何使用該服務	－提供消費者使用手冊 －所有特約商店及經紀商必須經過教育訓練，包括如何協助消費者使用該服務 －電話客服中心亦可提供消費者諮詢
消費者密碼外洩	消費者必須被告知保護密碼之重要性
消費爭議	－每筆交易均會提供簡訊通知，消費者可要求提供紙本交易證明

	－電話客服中心處理客戶所有問題，所有電話必須錄音
個人隱私及保密	－所有員工必須接受個人隱私保護之教育訓練 －與消費者簽訂之定型化契約中須有個人隱私保密條款

2. 偽冒風險：

風險	因應方式
消費者密碼遺失被竊或身分被盜用	－由專人調查研究 －如不可歸責於消費者，消費者無須承擔損失
特約商店及經紀商發生偽冒	－平常即對特約商店及經紀商予以監控
越權登入帳戶	登入帳戶必須要有密碼，如果沒有密碼就無法查詢帳戶餘額或進行提現、轉帳交易
冒用身分	－開戶時即須確認消費者 ID －電話客服中心必須透過消費者 ID 及歷史交易紀錄確認消費者身分，所有電話必須錄音
系統性或組織內之偽冒	每天進行偽冒或異常態樣之偵測，並出具報告
語音網絡釣魚/簡訊詐騙	提醒消費者注意安全，並定期更換密碼

3. 科技風險

風險	因應方式
交易資料被攔截	USSD2 訊息傳遞時採加密機制，銀行必須控制 USSD Gateway 以確保登入資料
駭客攻擊	系統管理員必須遵守資訊安全政策，包括防火牆、入侵檢測及系統監控

4. 持續營運風險

風險	因應方式
資訊系統或通訊連線中斷	建立異地備援中心及備援線路
重要特定人士無法取得聯繫	建置多功能團隊及人力資源

5. 洗錢防制

風險	因應方式
行動貨幣作為大額資金移轉	限制交易金額
認識客戶(KYC)	以風險基礎、考量交易金額大小以決定 KYC 之條件
洗錢防制名單	每一個消費者之姓名必須與洗錢防制名單比對
非約定轉帳交易	－限制交易金額以降低洗錢交易之發生 －國內匯款不得使用於跨國資金移轉

六、 數位金融服務產品比較(個案研討)

本課程介紹兩個數位金融服務商品，簡述如下

(一) 南太平洋銀行(Bank of South Pacific)之行動支付：

1. 該行為太平洋上最大零售銀行，也是最多分行、ATM 及 POS 台數。
2. 2009 年推出行動銀行。
3. 2010 年推動農村開戶，以平板電腦開戶及留存客戶影像檔，榮獲 2012 年最佳銀行獎。
4. 推動行動支付目標：解決農村現金交易(收受現金款項之風險)、整合 POS 及銀行網路、提高民眾與銀行往來之意願及便利性。

(二) WING(柬埔寨行動貨幣業者)之電子貨幣：

1. 前身為 ANZ 子公司，主要業務為使用手機提供金融服務。
2. 服務項目：現金存入及提出(包括柬埔寨幣及美金)、柬埔寨境內資金移轉、現金存款、購買行動電話通話時間、繳付帳單、ATM 提款及工資給付。

3. 技術運用：使用 USSD 進行交易，整合柬埔寨境內 5 家電信業者並自行建置交易平台。

4. 消費者可隨時隨地申請該服務。

七、 資訊科技治理和風險管理

(一) 資訊科技風險管理系統(IT Risk Management System, ITRMS)：

1. 以風險基礎之監理方式。

2. 風險管理程式應該包括確認風險、衡量風險、監控風險及控制風險。

(二) 資訊科技治理(IT Governance)包括：

1. 組織與監督資訊科技功能。

2. 資訊科技政策、流程及標準。

3. 資訊科技風險管理。

4. 資訊科技稽核。

5. 資訊科技人員之權限及教育訓練。

(三) 資訊科技風險確認及評估：

1. 資料收集。

2. 風險分析。

3. 優先等級。

4. 監控。

(四) 資訊科技控管機制：

1. 資訊安全：必須在董事會和高級管理層支持下推動。

2. 管理計畫：金融機構必須就資訊科技相關計畫建立管理架構。

3. 資訊科技營運：金融機構之管理必須確保資訊科技基礎設施足夠，且資訊科技系統可信賴、安全及可使用。

4. 資訊科技委外作業之管理：金融機構對於資訊科技委外必須有風險管理政策。

5. 電子產品與服務：金融機構對於電子銀行風險管理，必須採行有效地策略計

畫。

(五) 資訊科技風險衡量與監控：

1. 策略計畫之績效。

2. 服務水準之績效。

3. 品質保證及控制。

4. 政策遵循。

5. 外部評估計畫。

八、 對雲端運算供應商之管理

(一) 什麼是雲端運算：

1. 隨需應變之服務(On-demand)

消費者可依據使用需求狀況自行使用雲端服務。

2. 使用服務無所不在(Accessible)

網路使用無所不在，亦即雲端供應者服務可隨時在網路取用，且使用者端無論大小，均可透過標準機制使用網路。

3. 共享資源池(Resource Pooling)

所有的承租人可以共享資源，包括儲存、處理、記憶、網路頻寬和虛擬機等。

4. 快速佈署靈活度(Rapid Elasticity)

能因應承租人之需求且快速調整資源規模大小。

5. 多租戶模式(Multi-tenancy)

資源彙整讓雲端供應者透過多租戶模式(Multi-tenancy)服務消費者，依據消費者要求，來指派或重新指派實體及虛擬資源，在所在地獨立性的概念下，消費者通常不知道所有資源確切位置，只可能掌握國家、州或資料中心等大範圍區域地點

6. 服務可追蹤(Utilization Tracking)

雲端服務各層次均由雲端供應者掌控與監管，確保資源使用可被監測、被控制和被報告，為供應者和消費者雙方提供透明化服務使用資訊。

(二) 雲端運算服務模式：

1. 基礎架構即服務（Infrastructure as a Service, IaaS）：包括伺服器、磁碟空間、網路設備及記憶體。
2. 平台即服務（Platform as a Service, PaaS）：供程式設計人員使用。
3. 軟體即服務（Software as a Service, SaaS）：商業應用軟體或其他應用軟體，如：facebook, gmail, yahoo 等。

(三) 雲端運算所面臨之挑戰與風險：

1. 風險管理
2. 法令遵循
3. 雲端資料之所有權
4. 持續營運及可用性
5. 雲端資料保護

(四) 亞太區國家採行雲端運算之情形：

1. 澳洲：澳洲審慎監管局(Australian Prudential Regulation Authority)觀察委外(包括雲端運算)風險增加，於 2015 年 7 月發布報告提醒使用雲端運算服務應審慎考慮及必須考量之關鍵原則。
2. 印度：銀行科技發展與研究機構 (Institute for Development and Research in Banking Technology)在 2013 年 8 月發布雲端安全架構，包含雲端運算安全之相關項目。
3. 印尼：GR 82 (印尼政府第 82 號規定)要求提供公眾服務之電子系統營運商必須將資料中心及災害復原中心設在印尼境內。
4. 菲律賓：2013 年發布使用雲端運算服務之風險管理指導原則。菲律賓央行目前僅允許非核心業務使用公共雲端運算。
5. 新加坡：新加坡金融管理局(MAS)未禁止使用雲端運算，實際上 MAS 對於特定案例允許使用雲端運算服務。
6. 南韓：2015 年 6 月南韓金融監理局發布相關規範，使得金融機構更容易使用雲端運算服務。

(五) 講師就雲端運算服務發生之機率及對企業影響程度予以分類，並將前述雲端運算之風險逐一說明可能發生之機率及對企業影響程度。

九、 電子管道之風險－自動提款機(ATM)與刷卡設備(POS)

本課程主要探討 ATM 與 POS 所面臨之風險：

(一) ATM 現金管理：

1. 預估交易量決定裝填現鈔之金額。
2. 營業場所內或營業場所外之 ATM 均由最鄰近之分行維運。
3. 依風險基礎決定金融卡每日、每筆及每月可於 ATM 提領現金之限額。
4. 建立日常監控機制。

(二) ATM 留置卡：

1. 問題：消費者在 ATM 放入一張逾有效期之卡片或輸錯密碼，以致卡片遭留置。
2. 一般規定：密碼輸錯達 3 次，卡片將被 ATM 留置。部分銀行 ATM 對於逾有效期之卡片也會留置。
3. 解決方法：於操作畫面提醒消費者密碼輸錯達 3 次，卡片將被留置。

(三) 偽冒交易之管理：

1. 雙鏡頭以監視 ATM 提款交易(一個針對提款人的面孔，另一個則針對提款機插槽)。
2. 首次使用卡片強制變更密碼。
3. 教育消費者用卡安全，如保管密碼、注意提款環境等。

(四) 側錄卡片：

1. 如果卡片側錄機、藍芽相機或密碼鍵盤讀卡器容易且便宜就能取得，將成為歹徒犯罪目標。
2. 應該加強偽冒交易偵測機制。
3. 將磁條卡升級為晶片卡。

十、 數位金融服務之監理架構

本課程主要由講師以設定情境之方式，就某地區發展數位金融服務，在金融監理可能面臨之相關問題，交由學員分組進行討論。筆者之小組所討論之議題及結論如下：

(一) 情境：某地區央行參考印度規定，發布新增「payment bank」營業執照，以允許電信業者提供更多之金融服務，「payment bank」禁止辦理放款業務，但可以承作下列業務：

1. 辦理存款業務，但有金額上限。
2. 可發行金融卡/轉帳卡，但不可以發行信用卡。
3. 透過 payment bank 分行、ATM 及行動銀行進行付款或匯款。
4. 儲值卡或行動錢包。
5. 網路銀行。
6. 代理銀行。
7. 電子資金移轉。
8. 符合外匯規範下之跨境匯款。
9. 帳單繳費服務。

(二) 討論問題：

1. 該地區限制電信業者發行行動貨幣是否合理？理由為何？
2. 允許電信業者申請「payment bank」業務，對現行金融體系是否產生衝擊？該如何因應？

(三) 本小組討論之答案：

1. 基於保護消費者之立場，上開限制尚屬合理。
2. 對金融體系確實產生衝擊，可行之解決方案如下：
   (1)鼓勵電信業者與銀行合作，成立產業公會(此產業公會必須要由央行主導，以免雙方意見分歧，無法解決問題)。
   (2)善用雲端運算服務，並建構生態系統，兼顧各方業務發展。

十一、 常見之漏洞與威脅－電子銀行及行動金融服務

(一) 銀行業過去所面臨之威脅包括：實體分行之安全維護、綁架人質(如搶銀行)或內神通外鬼等，而目前所面臨之威脅為：偽冒信用卡、偽冒身分、駭客入侵及網路攻擊(cyber attack)。

(二) 據統計 2015 年全球資料遺失或被竊筆數達 707,509,815 筆，平均每天有 1,938,383 筆，每小時有 80,766 筆，每分鐘有 1,346 筆，每秒鐘有 22 筆。如果依產業別區分，以政府資料之 43%最多，其次為醫療資料占 19%，金融資料不到 1%。但值得注意的是金融資料遺失或被竊筆數雖不多，但金額損失不小。

(三) 電子銀行之漏洞：安全漏洞、身分確認漏洞、App 碼漏洞及使用軟體版本過時(無法提供更新防護漏洞服務)。

(四) 電子銀行之威脅與攻擊：

1. 偽冒身分(identify theft)。
2. 網絡釣魚(phishing)。
3. 網路轉接(pharming)。
4. 惡意軟體攻擊(malware base attack)。
5. 中間人攻擊(man in the middle)。
6. 瀏覽器攻擊(man in the browser)。
7. 分散式阻斷服務攻擊(distributed denial of service attack)。
8. 鍵盤動作側錄木馬程式(keylogger trojans)。

(五) 行動銀行威脅與漏洞包括：手機惡意軟體、第三方所提供之 App、不安全之 Wifi 及使用者行為。

(六) 主管機關之監理必須在創新發展及規範防止網路攻擊中追求平衡。

十二、 網路安全評估架構

(一) 網路安全之威脅種類：

1. 網路犯罪(Cybercrime)。
2. 進階持續性滲透(Advanced Persistent Threat, APT)攻擊。

3. 分散式阻斷服務(Distributed Denial of Service, DDoS)攻擊。

4. 內部人威脅(Insider Threat)。

5. 惡意軟體(Malware)。

6. 勒索軟體(Ransomware)。

7. 社交工程攻擊(Social Engineering)。

8. 未修補之系統(Unpatched System)。

(二) 近期網路安全事件：

1. 孟加拉央行於 2016 年 2 月疑似遭中國駭客攻擊，其於美國聯準會之帳戶遭盜轉 1 億美元，其中 8,100 萬美元被轉至菲律賓。

2. 2016 年 2 月駭客計畫對英國央行、紐約證券交易所及部分 BIS 會員銀行發動分散式阻斷服務(Distributed Denial of Service, DDoS)攻擊。

(三) 維持網路安全之因素：

1. 人員：銀行從員工、管理階層至董事會都需參與，以確保安全性及業務回復能力。

2. 網路安全政策：建立迅速之決策、因應及回饋機制，包括有效地學習、改進及採行新措施。

3. 設施及作業程序：相關設施維持安全性及回復能力，並對於新服務、新產品、資訊投資及組織架構訂定作業程序。

4. 公司治理：董事會重視網路安全議題，並認知到網路風險是企業整體風險之一部分。

(四) 網路安全風險評估架構：

1. 確認所有網路風險之因素。

2. 確認網路安全之預防措施。

3. 評估預防措施是否足以因應風險。

4. 訂定風險管理措施。

(五) 講師最後用 PIN 作為本課程之結尾，其代表意義如下：

1. P：主動而不是被動(Proactive not Reactive)。

2. I：資訊分享與合作(Information Sharing and Collaboration)。

3. N：網路安全不僅是技術問題(Not just a Technical Issue)。

十三、 業務持續運作及災害復原計畫

(一) 業務持續運作計畫(BCP)之角色、責任及及結構：

1. 董事會及高階管理階層：

(1)訂定政策及控制風險，安排 BCP 之人事及財務資源。

(2)規劃成立 BCP 委員會以進行業務持續運作之管理。

(3)每年檢視 BCP 並測試結果。

(4)確保每位員工知道在 BCP 所扮演之角色。

(5)確保 BCP 能配合營運環境隨時更新。

2. BCP 委員會：

(1)執行及維持 BCP。

(2)確保 BCP 符合法令要求。

(3)確保員工及相關團隊瞭解 BCP。

(4)決定啟動 BCP。

(二) BCP 方法論：

1. 階段 1：企業衝擊分析(Business Impact Analysis, BIA)

(1)確認可能受影響之企業單位。

(2)依據 BIA 計算復原時間目標(Recovery Time Objectives, RTO)。

(3)對災變須作最嚴格之情境假設，才能規劃因應方案。

(4)確認復原點目標(Recovery Point Objectives, RPO)以因應資料損失。

2. 階段 2：風險評估(Risk Assessment)

(1)風險評估必須考慮企業所有流程，非僅針對 IT 部門。

(2)採行適當策略以達到銀行可接受之 RTO 與 RPO。

(3)對重要業務之衝擊，包括提供客戶使用之系統、支付及清算系統、網路銀行、行動銀行、ATM、POS、客服中心等。

(4)使用外部資訊之倚賴度及風險。

3. 階段 3：決定選擇及企業持續運作策略(Determining Choices and Business Continuity Strategy)

(1)BCP 必須包括人、作業程序及基礎設施。

(2)對於不同風險或災變應有因應措施。

4. 階段 4：發展及實行 BCP(Developing and Implementing BCP)

(1)行動計畫。

(2)緊急發電措施。

(3)兼顧銀行及服務提供者。

(4)配合時空環境調整。

(三) 測試 BCP：

1. 銀行必須定期測試 BCP 以確保其能因應現況且有效。

2. 銀行必須對 BCP 進行內部稽核。

3. 銀行必須將重要之合作單位(委外機構)BCP 納入考量。

十四、 防制洗錢個案研討

本課程主要就數位金融服務發展可能衍生之洗錢防制相關議題，由講師先就下列議題說明後，再將其他議題交由學員分組進行討論：

(一) 講師說明：

1. 議題：透過儲值卡進行非法賭博及洗錢。

2. 情境：

(1)一群嫌犯被控進行非法賭博而遭起訴，整個犯罪組織涉及美國境內之經紀商負責招攬賭客、收取賭金及分配彩金，境外機構則負責架設網路提供線上賭博。

(2)進行非法賭博之資金移轉手法，是先開立儲值卡並儲值後，提供卡片資訊(包括卡號、卡片有效期及卡片驗證碼)給境外網站，進行網路交易(即線上賭博)，此一運作模式每個月可賺進 10 萬美元。

(3)6 名嫌犯因非法賭博認罪，被判緩刑 3 年；1 名嫌犯因非法賭博及洗錢認罪，被判緩刑 3 年，家居隔離 6 個月；1 名嫌犯因非法走私現金，被判刑 4 個月，緩刑 3 年。

3. 討論問題：

本案在金融監理上之癥結為何？如何防範？

4. 結論：

主要癥結是儲值卡可重複加值及可於海外或網路上使用。防範措施為禁止儲值卡使用於賭博網站。

(二) 本組討論：

1. 議題：透過網路支付服務帳戶洗錢。

2. 情境：

(1)一名罪犯利用電腦竊取民眾電子銀行之個人資料，並向網路支付服務業者開立網路支付服務帳戶，所留存之個資(聯絡電話、住址及生日)均非真實資料，電子郵件信箱亦無法辨識或確認使用者。

(2)該名罪犯再利用被竊民眾之電子銀行服務，將該民眾銀行帳戶之款項轉入上開網路支付服務帳戶，利用相同手法進行非法資金移轉。

(3)法令並未規範網路支付服務業者須追查資金流向或確認開戶人身分。

3. 討論問題：

本案在金融監理上之癥結為何？如何防範？

4. 結論：

(1)加強規範線上開戶之 KYC 作業。

(2)要求網路支付服務業者須追查資金流向。

(3)限制網路支付服務帳戶之交易金額。

十五、 消費者保護

(一) 資訊揭露：

1. 市場機制有效：完全競爭市場。

2. 市場機制失效：市場壟斷、不完全競爭。

3. 可否以資訊揭露方式改善市場機制失效？

(1)美國證券交易法：不保證投資獲利，但保證資訊正確揭露。

(2)金融交易明確揭露有利及不利之條款。

(3)監理機關提供標準揭露範本。

4. 對監理機關之啟示：

就金融消費者保護法而言，資訊揭露是最受歡迎之作法，因為它會讓市場機制運作更好。但是實證研究指出揭露消費者金融交易資訊，就保護消費者而言並非有效之作法。所以監理機關可能必須訂定定型化契約範本，以取代信賴資訊揭露、自由市場競爭。

(二) 個人隱私及資料保護：

1. 個人隱私及資料保護法在各國作法不同：

(1)有些國家沒有相關立法。

(2)有些國家採低度管理-美國。

(3)有些國家採動態立法-澳洲。

(4)有些國家採強制性保護-歐盟。

2. 主要方式：公平資訊慣例

(1)注意資料限制。

(2)同意資料搜集。

(3)資料安全。

(4)限制資料搜集範圍。

(5)未經同意不得傳送資料。

3. 對監理機關之啟示：

(1)過度強調個人資料保護並非好的市場發展策略。

(2)業者會尋求資料處理運用之最大可能性，以提供客戶最好之服務。

(3)在降低監理成本與提高有效性中，找到一個平衡點。

十六、 行動金融服務與消費者保護之監理作業

本課程是由泰國央行監理集團風險管理及資訊系統檢查部，就泰國金融市場發展現況說明，內容包括泰國數位生態系統、偽冒與詐騙案例、泰國央行監理功能及消費者保護等。謹摘述重點如下：

(一) 泰國數位生態系統：說明泰國電子支付(E-payment)現行架構、發展歷程、相關統計，如何將電子商務與電子支付整合。

(二) 泰國央行之組織架構、職掌；該行資訊檢查之功能與資訊風險管理之架構。

(三) 泰國央行在消費者保護所扮演之角色：

1. 直接角色：建立消費者保護單位直接接受消費者對金融服務之申訴。
2. 間接角色：金融檢查、持續監控、即時糾正、持續支持金融機構瞭解資訊風險管理。

十七、 透過雲端提供行動銀行服務－個案研討

本課程是由亞馬遜網路服務(Amazon Web Services)公司介紹該公司及其所提供金融機構之雲端運算服務，並以該公司為銀行規劃之行動裝置應用程式(App)，說明雲端運算服務之安全性，其內容多偏向技術層面之說明。由於本項服務涉及金融機構作業委外，爰筆者就該服務如發生資料外洩時，該公司之責任及是否可以接受金融主管機關進行查核請教講師，惟兩位講師為技術人員，僅表達會與合作金融機構討論如何遵守當地國之法令。

肆、心得及建議事項

本次研討課程之設計以電子銀行與數位服務金融為主軸，系統性地介紹 e-money、e-banking、mobile financial services 成功案例與成功要素、以及支援該等服務有關之 IT 基礎設施與雲端服務平臺之管理與風險控管、網路安全之評估、業務持續運作及災害復原計畫、洗錢防制與消費者保護等議題。除了講師於課堂上授課外，同時透過個案研討及小組討論之方式進行腦力激盪，及分享各國金融監理實務經驗，獲益良多。筆者亦藉由此次機會就授課內容向講師請益，亦與各國代表保持良好互動。以下為參與本次研討會之心得及建議事項：

一、對於國外發展數位金融服務之現況有更進一步之瞭解：

本次研討會內容主要為數位金融服務，介紹數個已發展或發展中之數位金融服務，讓所有參訓學員，瞭解亞太區發展趨勢。

二、未來金融服務發展以消費者體驗為成功關鍵：

由於每個國家之社會、文化、環境、風俗民情及金融服務滲透度不同，各自發展出不同之數位金融服務，但是共通點就是利用行動裝置之便利性，提供金融服務。而筆者認為數位金融服務發展成功之主因在於消費者體驗，正如同 Bank3.0 作者 Brett King 所說：「You can't regulate consumers' behavior.（你無法規範消費者的行為)」，因此未來金融服務之發展，必須兼顧消費者使用便利，才會成功。

三、他山之石可以為錯：

本次課程中所提各項數位金融服務中，多數之金融服務我國已有，且有相關監理規範，惟尚無電子貨幣或行動貨幣，如同前面所述，我國電子票證因不能隨時提領現金，因此不具備電子貨幣之要件，惟隨著時空環境改變，我國未來如允許由非銀行發行電子貨幣，本次課程中就監理上建議作法，可作為本會未來採取相關監理作為之依據與參考。

另有關資訊安全、雲端服務及消費者保護等議題，我國已有相關因應規範，包括銀行公會訂定「金融機構辦理電子銀行業務安全控管作業基準」、「金融機構提供行動裝置應用程式注意事項」、「運用新興科技應注意事項」及「金融機構辦理電腦系統資訊安全評估辦法」等以強化資訊系統安全與使用雲端服務或行動裝置應用程式，本會已訂定網路銀行定型化契約範本、應記載及不得記載事項等。

四、參與此類研討會有助於金融監理：

金融業務之發展已朝多元化及國際化邁進，為因應此一變遷，瞭解國際發展趨勢，吸取國外經驗，是金融監理進步之不二法則，因此對於此類研討會，建議應積極參與，除學習新知外，亦可與其他國家監理機關建立聯繫關係、交換意見與交流金融監理經驗，提高我監理人員之視野，增進我金融監理水平。

筆者小組之成員(由左至右)

Macao：Mr. Chong Wa Ho

Korea：Mr. Kyoung-Rok NOH

Thailand：Ms. Boriporn URAIWATTANA

Nepal：Mr. Deepak SHARMA

Thailand：Ms. Dolraporn PRASONGSUTTIPORN

Thailand：Mr. Napadol KHUNANUGUL

筆者