出國報告（出國類別：出席國際研討會議）

參加 APEC 監理人員訓練倡議-「科技運作及風險管理研討會」 出國報告

服務機關：金融監督管理委員會銀行局

姓名職稱：周正山　專門委員

派赴國家：菲律賓

出國期間：108 年 5 月 13 日至 18 日

報告日期：108 年 6 月 4 日

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 Regional Seminar on Technology Operations and Risk Management）
會議時間	108年5月14日至17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	周正山、金融監督管理委員會銀行局、專門委員
聯絡電話、e-mail	(02)8968-9752、jschou@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監理人員，旨在對金融機構的IT監理提供訓練，介紹IT風險，風險管理和綜合監理的基本概念。 二、 課程主題:主要係介紹金融機構之資訊科技(IT)風險概念、IT風險主題包括雲端計算、網絡安全、行動銀行、FinTech以及支付系統和運營等。此外，還討論IT風險管理對資訊安全、數據治理、供應商管理、業務連續性和IT稽核。最後，就IT和業務風險之間的聯繫如何制定並納入綜合監理方法提供指導。 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。
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、 強化金融業對資訊安全管理之制度，提升董事會的重視與責任。 二、 落實金融市場資訊安全之資訊分享機制。 三、 透過對金融機構資訊安全進行完整的金融檢查，督促金融業落實相關風險之內控內稽 四、 金融機構引進資訊科技應用，於善用科技優勢之同時，應兼顧金融監理原則與要求。 五、 金融科技的創新發展空間與金融環境的安全穩定並重。

壹、前言

APEC 監理人員訓練倡議之「科技運作及風險管理研討會」於 108 年 5 月 14 日至 17 日在位於菲律賓馬尼拉之亞洲開發銀行舉行，計有柬埔寨、斐濟、澳門、韓國、尼泊爾、菲律賓、薩摩亞、泰國及我國等 9 個 APEC 國家及地區的中央銀行、存款保險公司及金融監理機關派員參加，共計 44 人。該研討會旨在對金融機構的 IT 監理提供訓練，介紹 IT 風險，風險管理和綜合監理的基本概念。 IT 風險主題包括雲端計算、網絡安全、行動銀行、FinTech 以及支付系統和運營等。此外，還討論 IT 風險管理對資訊安全、數據治理、供應商管理、業務連續性和 IT 稽核。最後，就 IT 和業務風險之間的聯繫如何制定並納入綜合監理方法提供指導。

此一研討會係亞洲開發銀行、菲律賓中央銀行及存款保險公司共同主辦，邀請到任職舊金山聯邦儲備銀行 Patrick Prickett 及任職芝加哥聯邦儲備銀行 Steve Galperin 擔任講師。

貳、會議內容紀要

本次研討會係由 2 位講師講授方式進行，共分 14 場次，涵蓋涉及 IT 風險及監理之議題，內容相當廣泛，以下茲就重要研討會議內容摘要介紹：

一、IT 風險監理

IT 風險的特殊性，來自於其隨自動化和科技進步，也來自於 IT 與金融機構業務的關聯性，造成其風險不斷擴張的特性。也因金融機構持續引入新技術以及新的 IT 策略，造成風險的動態變化。因此，IT 風險難以用一成不變的政策加以管理，對其監理必須保持靈活性，這對金融機構及監理機關均是挑戰。

對金融機構 IT 進行以風險為本的檢查就

業務運營	風險管理	環境變化
● 取得路徑和身份認證管理 ● 網際網路和行動銀行 ● 分支機構和遠程遙控 ● 電匯 ● ATM 處理 ● ACH 源頭 ● 虛擬化/雲端 ● 模型	● 資訊安全 ● 網絡安全 ● 供應商風險管理 ● 業務連續性/災難恢復 ● 應用程序訪問控制 ● 變遷管理 ● 數據治理 ● IT 稽核的範圍	● 實施新系統 ● 運營方面的重大變化，包括合併或系統轉換 ● 關鍵業務的新的或修改的外包關係 ● 重要的行業趨勢/問題 ● 內部控製或風險管理嚴重依賴信息技術的業務線 ● 對內部稽核或上次稽核報告中提出的問題採取後續行動 ● 與使用網際網路和網絡安全相關問題

IT 檢查的流程包括：1.了解業務營運環境；2.確認所採之技術和業務風險；3.進行風險評估及得出結論；4 對金融機構予以評等。

1.了解業務營運環境

委外處理	內部自行處理	混合處理
資料於供應商處進行處理	資料於銀行內部以購入之資訊軟硬體進行處裡	以委外及內部混合處理模式進行資料處理
如 Fiserv 公司為銀行處理帳務項目並將交易過帳到金融機構的總分類帳。	如金融機構購買用於處理帳務項目和將交易過帳到總帳的軟硬體件。	如帳務項目處理由銀行職員在內部執行，總分類賬的交易過賬由 Fiserv 執行。

IT 風險等級取決於控制程度，就保留內部運營得事項而言，其保留所有責任權限和責任，控制程度 100%。就外包業務而言，係透通契約將一些權力委託給外部各方，但風險與責任無法外包，其控制程度為 0%。對供應商，由於其產品或服務並沒有銀行投入開發，銀行必須仔細評估風險， 其控制成度亦為 0%。

就識別技術和業務風險可由下列幾的方向分析說明包括「管理流程」、「結構組成」、「正確性」、「安全」、「可用性」等。就管理流程而言，無效管理流程可能導致資訊系統與組織的業務流程和任務無法充分或恰當地結合。而有效的管理流程包括計劃、投資評估、系統開發、執行及人員配置。而其需考慮的關鍵議題為如何達到機構競爭優勢的提升，特別是面對全球競爭的趨勢，因此將 IT 建構與機構整體策略規劃相結合，至關重要。並且 IT 管理必須將終端使用者納入決策，應該要促使所有終端使用者對系統的了解。此外，在面對機構合併的情形，系統的整合成敗往往是關鍵。

對於 IT 管理流程的控制功能則包括預防性、偵測性及導正性功能，各項功能之措施關鍵臚列如下表：

預防性：	偵測性：	導正性：
● 策略計劃	● 管理報告	● 教育

● 繼任計劃 ● 通訊 ● 人員配置 ● 政策/程序 ● 職責分離 ● 交叉培訓/工作輪換 ● 文檔	● 財務報告 ● 差異報告 ● 員工評估 ● 錯誤統計和日誌 ● 內部和外部審計	● 新計劃或程序 ● 外包 ● 更換管理層

「結構組成」即是要處理對於自動資訊系統的基礎設計和各個組件無法滿足當前和長期組織目標的風險。必須考量各系統兼容性、容量管理，並與業務目標保持一致。至於資訊技術系統的基礎設計及其物理性和邏輯組成部分包括網絡通信、硬體及軟體，軟體如操作系統，通信軟件，數據庫管理系統，編程語言和桌面軟件等。

對於 IT 結構組成的控制功能，依預防性、偵測性及導正性功能分別列如下表：

預防性：	偵測性：	導正性：
● 策略和戰術計劃 ● 可行性研究 ● 採購政策 ● 系統開發方法 ● 資本計劃和程序 ● 變革控制 ● 驗收測試	● 庫存系統 ● 自我評估 ● 內部和外部審計	● 改造 ● 重新設計 ● 翻譯/轉換

「正確性」對管理流程的意義係指防範系統、應用程式或電腦程式以及由此產生的資訊流動的風險，避免無法滿足終端使用者的業務要求和期望的情

形。因此，需要規劃稽核範圍，並透過政策、程序和執行來確保可靠性，準確性和完整性。此過程的關鍵即為「系統開發生命週期」－啟動、要求標準、設計、編程、測試、實施、評估、維護。誠信風險的控制關鍵如下：

預防性：	偵測性：	導正性：
● 堅持系統開發生命週期質量保證 ● 程序 ● 改變控制 ● 驗收測試 ● 容量規劃 ● 資源調度	● 自我評估 ● 內部和外部審計 ● 驗收測試 ● 績效監測 ● 機器診斷/日誌 ● 錯誤統計	● 重新設計應用程序 ● 文件輪換和保留 ● 恢復和重啟 ● 更換 ● 重新安排需求

「安全」係指為控制資訊資產洩露的可能性，在其創建、傳輸、處理、維護或存儲期間，是系統防護最為脆弱時期，將可能導致未授權取得資訊、修改，銷毀或洩露。必須透過採行資訊安全計劃、實體安全及合乎邏輯的資訊取得管理。為防範主要安全風險，利用預防和偵測性控制，包括實體隔離大型主機和伺服器，並透過合乎邏輯的措施如限制對系統的存取路徑和對系統的更改，建置稽核追蹤制度，定期審查存取路徑及加密關鍵資訊（特別是敏感的客戶資訊）。誠信風險的關鍵控制點如下：

預防性：	偵測性：	導正性：
● 實體隔離/邏輯性的存取權限控制	● 違規報告 ● 自我評估 ● 內部和外部稽核 ● 庫存控制 ● 驗證/配置回電 ● 批量控制	● 漏洞/威脅評估 ● 災難恢復計劃 ● 保險 ● 重發/重路由

	● 事件響應團隊 ● 容量建模 ● 專有網絡 ● 可切換性路由 ● 協議 ● 公共網絡 ● 加密/認證 ● 訪問代碼 ● 防火牆	

「可用性」面向所要考量的是確保機構能夠及時持續提供資訊以支持業務流程和決策。因此必須採行「災難恢復計劃」、「業務持續性程序」以及制定資料備份/恢復程續。對於危及可用性之主要風險，應先識別關鍵系統、建置依重要性區分等級的資料備援系統、建立應變計畫並定期測試，最後是提供足夠的系統容量。而對於可用性關鍵控制點如下：

預防性：	偵測性：	導正性：
● 軟硬體維護 ● 冗餘 ● 模型 ● 測試 ● 多樣的路由 ● 實體安全	● 病毒檢測 ● 外部來源 ● 自我評估 ● 內部和外部稽核	● 災難恢復計劃 ● 保險 ● 互惠協議

資訊技術統一評級系統（URSIT）

美國為評估機構之 IT 管理，形成技術統一評級系統（URSIT）。1999 年 1 月 13 日，聯邦金融機構檢查委員會（The Federal Financial Institutions Examination

Council, FFIEC）[1]通過了修訂後的資訊技術統一評級系統（URSIT）。 FFIEC 於 1999 年 1 月 20 日公佈了修訂後的評級系統。經修訂的 URSIT 於 1999 年 4 月 1 日生效，並將用於所有銀行和資料處理服務提供商的資訊技術檢查。

URSIT 係就 4 項評等因素進行評估得出一綜合評級，其等級區分 1-5 級，與 CAMELS 評等類似。其 4 項評等因素為「稽核」、「管理」、「發展和收購」、「支持和交付」。

1. 稽核評級主要係就內部稽核審查包括：稽核過程的整體有效性;稽核獨立性;風險評估方法的充分性;內部和外部審計報告的範圍、頻率、準確性和時間性;稽核對於申請、開發、採購和測試等的參與程度;IT 稽核人員和資格;內部和外部稽核的質量和有效性;對整體 IT 風險具有充分的相關計畫。
2. 管理評級的主要範圍為各階層管理職責與功能，包括下列幾項：

- 董事會層級的監督和支持：重點包括充分的策略規劃、政策的審查/批准，以及應變計劃。
- 高階管理人員：重點包括建立 IT 計劃、政策、程序和標準;風險管理/風險識別執行;供應商管理計劃對於稽核查核與關切事項的回應，以及即時導正措施。
- 第一線管理人員：業務了解的深度和繼任代理制度，以及資格條件。

管理評級的評審內涵包括：監督的水平/質量和 IT 流程的支持;風險監測系統的有效性，包括識別，測量，監測和控制風險;對新業務活動及繼任計劃的管理規劃;MIS 報告的充分性;法遵意識;對契約、委外及服務提供的管理與監督。

3. 開發與採購評級的範圍包括：識別和實施 IT 解決方案、專案項目管理、IT 解決方案符使用者需求、變革管理、獨立的品質保證及測試。

開發和採購評級的審查內涵包括：高級管理層和董事會對系統開發或收購活

[1]聯邦金融機構檢查委員會成立於 1979 年 3 月 10 日，是一個由各金融監理機構共同成立的正式機構，有權為美國聯邦準備理事會（FRB），聯邦存款保險公司（FDIC），國家信合社管理局（NCUA）、貨幣監理辦公室（OCC）和金融消費者保護局（CFPB）等聯邦金融監理機構制定統一的原則、標準和報告表格，並可就促進金融機構監理一致性的措施，提出建議。

動的監督和支持;系統開發的課責性;系統開發生命週期的和編程標準的充分性;計畫項目管理程序、系統文檔和軟件版本的質量;品質保證功能的獨立性;網絡、系統和應用程式軟體的完整性和安全性;客戶於採購過程得予參與。

4. 支持和交付評級的範圍包括下列三層次：

- 安全管理：正式的政策和認知計劃、密切監控邏輯和實體安全。
- 連續性計劃：全面的營運持續計畫(BCP)、計劃的現況和受測試的情形、預為定義的恢復時間架構。
- IT 運營：一致的表現、可靠的流程、可用流程、最終使用者/客戶的支持。

支持和交付評級的審查內涵包括：操作政策、程序和手冊;實體和邏輯安全性，包括數據隱私;所有單位和各級金融機構的安全政策、程序和做法;滿足業務需求的服務級別;在準備、輸入、處理和輸出過程中的資料控制;企業應變計劃和業務恢復;監控容量/性能的程序/流程;為使用者提供的協助質量;控制和監控;防火牆架構/公共網絡的安全性。

美國的金融監理機構於執行 IT 風險評估系統時，會針對不同大小性質種類的金融機構調整評估內容，但並不針對資訊長或風控長評估適任與否，而是評估機構 IT 風險控制如何，但金融機構資訊長必須完全了解機構本身擁有使用的資訊技術，以及可以執行的功能為何。

二、IT 風險-雲端運算

金融機構採用雲端運算服務主要是基於商業考量。首先，雲端服務使企業避免支付可能不需要或不需要的設備，技能和其他資源，專注於核心業務流程和專業知識，也能夠更關注商業價值、核心業務流程，透過減少技術成本並利用外部服務、基礎設施和專業知識，來協助解決遺留不必要投資問題。另外，雲端運算服務也為金融機構提供更為彈性與價格低廉的資訊處理解決方案。

但雲端運算也會為金融機構帶來一些風險，例如使得企業的資料變得廣泛分散，當雲端服務未達預期效果，則企業亦無相關資源自行處理。另一方面，相關資訊/數據可能會意外被更改，也可能發生被存儲在別處，而未收到通知，雲端服務提供商可能金融業務和監管要求欠缺了解。

對此，於進行金融檢查時必須注意的重點包括金融機構的「策略/治理」、「供應商/契約管理」、「韌性/服務表現」、「資訊安全」、「獨立評估」。

策略/治理

- 審核雲服務策略並確定其是否與公司次略和目標（短期和長期）保持一致。
- 評估整體治理計劃，以確保實施適當的計畫管理、資源和風險評估流程，以部署和支持雲服務。
- 確定已更新的政策和程序已獲核准，以便選擇和持續監控雲服務提供商。
- 確定審查委員會是否包括所有利害關係者以及適當層級。
- 審核公司管理資訊系統，以確定是否正確地獲得雲服務的表現和關鍵風險資料，並向高級管理層報告。
- 審查盡職調查計劃，確保提供商在成本、服務質量、遵守法規要求和風險管理方面滿足機構的要求。

供應商/契約管理

- 評估供應商管理程序，以便選擇和持續監控雲提供商。
- 查看服務級別協議，了解有關數據的所有權，位置和格式以及爭議解決的具體資訊。
- 查看契約以確定是否明確定義了要放置在雲中的數據類型的控制要求。
- 審查契約，確保明確界定各方的責任，並已納入妥善的規範條文。
- 確定是否已考慮退出策略和轉換計劃以防止被供應商鎖定的情形。
- 審查契約以確定是否將供應商可能發生重組、合併或收購等情形納入考量。
- 審查契約以確保其明確揭露雲服務提供商與第三方的任何分包，包括雲間關係。
- 查看契約中有關地理限制的，雲數據可以駐留的位置以及可以移動的位置，對資料儲存於不同國家或其他司法管轄區的法律要求。
- 查看與其他雲客戶端隔離資料的契約。
- 為執行檢查，要求現場訪視時間表。
- 確定機構是否及時收到有關數據，應用程序和服務狀態的訊息。
- 查看服務等級協議所同意的服務成效監控和報告的流程。

韌性/服務表現

- 確定雲服務如何影響整體的業務連續性計畫（Business Continuity Planning）

及災害恢復計畫（ disaster recovery)(BCP / DR)。

- 確定雲提供商和服務是否包含在 BCP / DR 中予以測試。
- 確定是否已評估雲供應商的業務連續性和災難恢復計劃。
- 確定雲供應商如何在正常和意外的業務波動和峰值期間，衡量和報告雙方商定的服務提供和成果。
- 審查金融機構如何正式檢測/解決不同類型的服務中斷。
- 審查突發事件回應流程，以確保能適當且及時通知安全事件或違規行為的責任。
- 供應商是否要求機構需提前通知擴大或限縮雲服務項目範圍？（應該不可有）
- 確定雲端服務變更管理流程的適用範圍，處理金融機構和提供商雙方對雲環境需進行變更（伺服器強化、補丁管理和變更控制）。
- 確定能夠獲取雲服務的可用性實況並報告給金融機構高階管理層的內容（例如，正常運行時間歷史報告）是否足夠。

資訊安全

- 要求取得數據資料清單，以及其分類和雲端服務的控制要求。
- 確定實施的加密類型和位置（靜止和運動中）。
- 評估雲端供應商和服務的風險評估和差距分析。
- 確定雲端環境是獨立的還是多租戶共用。
  - 合邏輯的數據資料隔離
  - 數據無法攻擊數據，但資料處理的方式會攻擊數據。
  - 重複使用 IP 地址
- 查看雲供應商用於保護和監控雲端服務的控制工具清單。
- 查看提供商的管理資訊系統，了解安全指標和事件報告。
- 評估機構的安全資源和專業知識水平，以監督雲端服務的安全管理。
- 評估正在進行的測試以驗證安全要求。
- 評估記錄並報告給金融機構的活動類型。
- 雲端服務供應商對資訊安全、法院取證調查和資安事件通知的責任限制是什麼？
- 評估對實施雲端服務的身份和存取管理計劃。

- 確定是否正在進行任何複委託，以及授予該受託組織或個人的存取權限。

獨立評估

- 金融機構內部
  - 根據需要參與內部稽核、外部稽核、監理檢查以及其他對雲端服務契約內容必要的審查。
  - 確定稽核人員的資格。
  - 確定審查的頻率和深度是否合適。
  - 請求金融機構各稽核類型和頻率，以及其他內部控制和運營報告可以從雲端服務供應商處獲得的資料。
- 雲服務提供商
  - 要求供應商提供相關文件，顯示其內部稽核、外部稽核、監理機關和第三方足以覆蓋對所有雲端服務相關環境進行測試。
  - 確定審查的頻率和深度是否合適。

三、IT 風險-網路安全

網路安全基本上並無地理國界的概念，網絡風險與我們監理的其他風險不同，它是一種動態風險，所以在監管方法方面要超越傳統思維。它也是一種普遍存在的商業風險，識別和解決資安漏洞對於任何機構來說是一場持續不斷的貓捉老鼠遊戲，就像彌補措施和新漏洞的發生一樣快。監控和應對網絡安全風險的主要挑戰之一是不斷變化的威脅形勢。

在整個產業中，人們意識到不可能單獨面對網絡安全議題，因此，分享網路安全威脅情報和漏洞，對於個別機構具備能夠跟上這一動態威脅防止發生代價高昂的資安事件的能力而言至為重要。

對於網路安全的監理應採取更廣泛的考慮，網路安全應該是機構必須持續具備的能力之一：以識別和管理顯著風險，維護運營和服務，保護其客戶資訊，維護安全性、穩健性以及聲譽以保持公眾信心，並在適用的情況下限制對其他行業的傳染風險。而這些能力應該要金融機構對於風險評估、監督計劃、檢查程序和持續性監督計畫投入資源。

網路安全及資訊重點監理方法：

- 規模較小，不太複雜的金融機構：
  - 將網絡安全風險管理、控制和相應的協議規範納入 IT 檢查工作的要素。
  - 強調風險管理計劃的運用，如業務連續性、供應商風險管理和資訊安全計劃，包括資安事件回應、培訓和問題升級。
- 更大，更複雜的金融機構：
  - 考慮針對特定主題或風險因素的針對性工作。
  - 融入其他 IT 和更廣泛的風險管理檢查。
  - 強調對業務連續性，事件回應，供應商風險管理和資訊安全計劃等風險管理計畫的影響，並納入此類計畫的審核中。
  - 了解網絡安全如何影響其他銀行業務，如企業風險管理、新產品/服務部署計劃、運營和法遵風險重點檢查，甚至公司治理。

網路安全在整合監理範圍內是非常重要的一環，對於網路安全的觀點可能各不相同，但在金融機構整體運作和各監理層面都有關鍵性的影響。就金融監理而言，網路安全是橫跨其他所有監理議題：

- 資本規劃
  - 確定風險概況是否需要將網路安全事件視為特殊風險或壓力情景。
- 法遵
  - 認識到網路事件對法律層面及企業聲譽的廣泛影響。
  - 了解消費者保護的法令中對信用卡的重放和恢復、身份盜竊監控和客戶通知協議的意涵。
  - 考慮供應商風險管理，尤其是客戶資訊儲存於第三方所在地的管理。
- 流動性管理
  - 認識到網絡安全事件有可能使清算和結算系統癱瘓、刪除或損壞客戶數據、或僅使網站當機。
  - 確定應急資金計劃是否適用於較大範圍和持續性的事件。
- 企業風險管理
  - 審視風險識別和整體實務面的運作，了解它們如何解釋網路和其他業

務風險之間可能的相互作用。

- 了解網絡事件和持續風險管理的升級規範和報告線。

- 稽核
  - 評估並了解稽核如何結合新的和新興的風險和技術。

四、IT 風險-行動銀行與支付

行動金融服務主要的項目包括銀行相關服務、支付、資金移轉及行銷等，就當前新興支付模式來看，有以網路運營商為中心（例如 Verizon），有以銀行為中心，亦有由受信任的第三方管理（Google、Paypal，Square 等）。而在行動支付市場的主要參與者類別越來越多元，包括行動通訊業者、手機/ SIM 晶片製造商、銀行、信用卡資組織、網路支付業、預付卡公司、商戶、網路搜尋和支付服務提供商、支付應用程式商。行動銀行即是以使用行動設備如智慧手機或平板電腦進行銀行業務，如帳戶查詢、帳戶提醒及等帳單繳費等。而造成相關業者投入行動金融業務的驅力，也就是加值因素：

- 於分散化的市場中提升潛在市場開發的規模。
- 專注於新市場的能力（包括無銀行賬戶客戶、欠缺銀行服務地區）。
- 繞過當前基礎設施限制的創新。
- 對提升支付服務效率及便利性產生重大助益。

對於行動支付業務發展的挑戰和風險主要在於對新興市場及技術應用的監理不易，造成潛在的風險（如詐欺、資安）提高，因此對於資料治理和供應商管理的要求必須提高;另外在許多創新技術的引進或新創業者推出新種服務失敗後，其對消費者的影響並不明確，尤其當監力/消費者保護的責任無法及時予以明確化時，可能會產生重大的爭議事件。

行動金融服務業者應建立行動服務的安全策略，其原則如下：

- 從威脅和控制角度來定義策略：
  - 利用現有的政策和標準作為指導
  - 符合公司各項政策、行業標準和適用法規

- 考慮安全策略對業務功能和用戶體驗的影響
- 使安全策略與管理解決方案的能力保持一致
  - 確定可以實施哪些策略，以及如何管理和推動策略
  - 考慮如何檢測和驗證所執行的策略
  - 考慮安全策略對安全管理和基礎設施的影響
- 即使根據差異化使用情境的需要必須採取多種策略，但仍須盡可能限制其差異。

至於監理行動金融服務應考慮的因素如下：

- 控制行動產品開發，包括在各種複雜行動支付系統之間的互通與連結操作
- 控制第三方，包括非銀行合作夥伴、網路供應商和服務提供商，透過包括客戶需求建議書（Request For Proposal，RFP）和服務級別協議（Service Level Agreement，SLA）等方式。
- 完整考量法律及法遵風險。
- 實施限制客戶資訊暴露的相關措施，包括詐欺偵測與反應計畫。
- 落實安全和客戶教育的要求。
- 完善交易認證和認證授權的設計與執行。

五、IT 風險-金融科技

銀行最初將 Fintech 視為競爭，但最近，銀行與 Fintech 合作的形態已經出現。Fintech 的優勢在於有創新想法、新技術、服務或產品具有靈活性及上市快速等，並且具備數據資料處理專業知識；至於傳統銀行優勢則在於客戶信任，能夠使用清結算系統，同樣也具備數據資料處理專業知識，並且已經受到金融監理。至於金融監理機關為何關心？主要在於銀行與 Fintech 可能以多種方式建立聯結：

- 銀行投資金融科技公司。
- 銀行建立新創計劃，以孵化金融科技公司。
- 銀行與金融科技公司合作：
  - 為金融科技公司提供貸款

- 零售業務平台供應商-共同品牌合作安排。
- 代工/自有品牌合作安排。
- 業務轉介收費關係。

- 銀行收購金融科技公司
- 銀行推出自己的金融科技解決方案

美國聯邦儲備系統理事會成立了一個跨領域的工作小組，對金融科技創新進行 360 度分析，其關注於以下金融科技領域：另類貸款、儲蓄、投資及財務規劃、數位支付、區塊鍊和虛擬貨幣。而這些金融服務系建構在資訊技術生態系統，包括應用程式編程介面（API）標準，大數據/數據分析和型動交付渠道。

Fintech 為銀行產品和服務創建非傳統平台，可能影響金融服務的交付方式，但每個金融科技領域都以不同的速度發展，並非所有金融科技都同樣具有破壞性。

金融科技的發展解構金融服務，但其是否須納入監管，須視其所涉及的金融活動的本質是否需要被監管。對於金融科技的思考重點：

- Fintech 涵蓋多種類型的金融產品和服務。
- 了解金融機構如何參與或計劃參與金融科技活動
- 應超越區分好或壞的思維來思考創新，許多產品可能是有益的，並解決未滿足的需求。
- 了解各金融監理機關對於金融科技的新觀點和公開聲明
- 監理機關如何解決風險和顧慮，同時仍然培養發展機會？美國目前並無由金融監理機關建置的金融科技監理沙盒。但舊金山聯邦儲備銀行由於位近矽谷，為彰顯對科技產業及金融科技的支持，可能於近6個月內啟動金融科技沙盒計畫。

六、IT 風險管理-第三方風險/供應商管理

金融機構業務委外可能增加或減少風險，也可能使風險維持不變，取決於如何執行即委外的內容委外的對象以及如何委外。委外的潛在好處如降低成

本、增強績效表現、獲得更好的人才、運用高階系統、獲得專業知識、加速提供服務，最著要的是讓銀行專注於核心業務。

凡事一體兩面，委外的潛在缺點諸如就使銀行受限於長期契約關係的束縛;為配合委外改變業務執行和流程;需對外提供對機密資料的存去路徑;需要管理服務供應商;如配合委外裁撤內部原有人力，造成對服務供應商的潛在依賴性;可能造成銀行本身聲譽風險，尤其在服務供應商與客戶有互動時，以及威脅員工關係。

對於銀行業務辦理委外，董事會和高階管理層的職責在於確保委外的執行以安全可靠的方式進行，並遵守適當的法規;對於全機構的委外管理及政策進行審批，以降低委外風險;對於委外的執行是否遵守有關政策，須定期向董事會報告。

銀行應對服務供應商訂定風險管理計劃，進行相關風險評估，確定委外活動是否與機構的策略方向和整體業務策略一致，確定相關風險，並進行成本效益分析，並確定合格且經驗豐富的服務供應商是否可以持續執行服務，最後要定期更新風險評估。

對於委外契約中至少應包括但不限於下列規定：服務範圍、成本和報酬、稽核權限、資訊的機密性和安全性、服務失敗和服務終止、服務供應商的業務恢復和應急計劃、轉包。此外，爭議解決機制很重要，透過司法曠日費時且結果不確定，但契約內容安排沒有最好的答案，應有定期檢視重新訂約的機制。
金融機構業務委外對於其業務連續性和緊急應變影響甚巨，因此金融機構的災難恢復和業務連續性計劃應包括關鍵的委外服務，評估服務提供商的災難恢復業務連續性計劃的有效性及其與金融機構計劃的一致性。

金融機構業務委外尚需考慮的其他因素：

- 可疑交易活動報告（SAR）功能：基於洗錢防制辦理可疑交易活動報告具有高度機密性，如委外業務涉及 SAR 相關功能，則應有更審慎的考量。
- 境外的委外服務供應商：以美國為例，金融機構委託境外服務供應商仍需要遵守美國法規和監理指南，因此要考慮金融機構稽核外國服務提供商的

能力及外國法規的規定。

美國 Fed 對於銀行業務委外的官方立場，原則上是銀行所有的業務皆可委外，但在監理實務上仍要看委外的合理性，例如銀行如將整個資訊部門委外，Fed 則認為不能將基礎的功能委外。

七、IT 風險管理-災害復原及業務延續

業務連續性計劃（Business Continuity Planning，BCP）：包括恢復和維護業務的正常運作，而不只是恢復技術組件，涉及對恢復至關重要的業務目標和業務運作關鍵因素等，決定其優先順序以發展出全企業為範圍的BCP，並且必須將機構在金融市場中的作用納入計畫。BCP必須以日常業務變化、稽核建議事項及測試發現等為基礎，進行定期檢討修正，亦即以循環式、流程導向的方法進行，包括商業影響分析（BIA）、風險評估、風險管理以及風險監控和測試等。

業務影響分析（Business Impact Analysis，BIA）：分析業務運營的關鍵，機構對於業務恢復的目標，以及機構對業務委外第三方和 IT 功能的可行分析。

災難恢復計劃（Disaster Recovery Plan，DRP）：分析 IT 系統恢復的期望和現實的差異，規劃災難/系統故障後 IT 系統恢復的方法，對於此過程中，第三方 IT 供應商的期望為何。

所謂業務韌性（Business Resiliency）就是指機構在災難發生後恢復運營的整體計劃，能夠快速、有效、無縫地回應和恢復業務運營，包括系統和操作人員。是以，企業級計劃的關鍵要素包括：

- 管理連續性：定義關鍵角色和承擔責任
- 操作的連續性：對關鍵操作、人員和地點的高階分析
- 具體細節：誰做什麼、何時、何地以及如何做

金融機構要制定有效的 BCP，應於設想之災難發生前即考慮的關鍵問題，例如：記錄存儲在何處以及如何存取;如何在備用站點維護資料安全性（即安全的場外撥入）;替代站點之位置、容量、營業使用情況;與第三方供應商簽訂必要的合約，如資料存儲和採購、備用設施（如果使用外部供應商）、現金/票據存儲、保險;對小型銀行而言須指定負責執行重新開放張的任務團隊。

對於建立業務線計劃的關鍵要素，首先每個部門都有一個業務延續性協調員，他根據業務影響分析制定計劃，計劃是基於已識別的風險，如就關鍵運營建立疏散計畫，詳細的備份計劃，並且每年或在業務發生重大變化時進行修訂。其計畫內容應包括：疏散和緊急應變程序、通知內部和外部聯繫人的程序、備用恢復站點啟動程序、業務恢復程序如各項細節和優先性、恢復時間表等、有關資源需求的詳細信息， 至少每年測試一次所有計劃。

董事會和管理層的職責在相關的計劃流程中扮演種藥的角色，因相關政策、實施監督、審核、人力資源（培訓和可用性）、評估 BCP 測試計劃和結果及評估 BCP 流程的任何更新等，應皆須經過董事會核准。

在執行 DR-BCP-BIA 下計畫流程中應將考慮下列因素：

- 服務水準協議（SLA）準確性，也就是在計畫執行的環節有涉及委外辦理的情形，SLA 定義了期望從供應商處獲得的服務的水準，列出了衡量服務的度量標準，以及應達成協議的服務級別無法實現的補救措施或處罰。它是任何技術供應商合同的重要組成部分。
- 關鍵人物無法有效執行 職務風險。
- 恢復能力。
- 員工流動和損失。
- 業務預期與 IT 能力的一致性。

發生中斷正常營運程序的事件，並導致一定程度的危機，不一定是惡意攻擊，實務面臨的問題，在於事件回應團隊由於缺乏對流程的熟悉而啟動太慢，或無法就少量證據做出決策、修復特定事件與根本原因，而且對大多數組織而言，內部調查非常困難，尤其是取證。由監理的角度必須考慮到只有計劃的存在是不夠的。監理官必須驗證：

- 計劃與組織的業務模型相匹配的程度。
- 董事會，管理層和員工了解自己角色和計劃中的責任。
- 定期進行測試。
- 計劃反映了當前的運營環境，並考慮所有新系統。

八、IT 風險管理- IT 治理

公司治理之意即公司如何自我運作，制度定義上，為董事會實施的流程和結構的組合，用於通知、指導、管理和監控組織的活動，以實現其目標。至於 IT 治理，則係由領導、組織結構和流程組成，確保企業的資訊技術能夠支援和推展組織的戰略和目標：

- 由董事會和高階管理層執行的一系列職責和實踐組成，目標是提供策略指導，確保實現目標，確定風險得到適當管理，並驗證資源是否負責任地使用。
- 從廣義上講，它指的是組織的 IT 結構和運營文化。其中文化意指公司透過董事會和高級管理層的態度和行為表達的核心價值觀和目標。

IT 治理中的關鍵人物包括董事會及其高階管理層：

- 董事會和委員會：IT 指導委員會和風險委員會。
- 高階管理人員：技術長、資安長、和 IT 管理有關之運營、專案管理、研發規劃、電信部門主管，以及營業單位管理層。

金融機構的董事會主要應負責監督，高階管理層應負責執行，其治理結構應包括：有效的 IT 治理;適當監督 IT 活動;全面的 IT 管理，包括管理層發揮的各種作用，和有效能的企業組織運作架構。

至於是否於董事會層級設置 IT 委員會並非法規要求，其實美國也不是大多數銀行都設有 IT 委員會，但若有設置董事會級別 IT 策略委員會，主席應是董事會成員，其餘成員應根據他們在資訊相關技術的業務影響方面的知識和專業知識進行選擇。此外，董事會可以選擇選擇 IT 專家作為外部顧問，向董事會和管理層就 IT 策略提供建議，特別是當董事會需就 IT 策略進行批准前，可由董事會委任專家提供意見，另一重點則在關注當前和未來的 IT 策略議題。

IT 委員會應執行以下功能：

- 核准政策，將重大資安事件升級並報告給董事會或指導委員會，並適當回報政府主管機關及執法機關。

- 讓管理層負責識別、衡量和降低 IT 風險，並為 IT 控制提供獨立、全面有效的稽核範圍。

就董事會和管理層應扮演積極性的角色功能而言，包括：

- 董事會成員可以在 IT 治理中發揮積極作用，或委託 IT 策略委員會（或其他類似委員會）。
- 執行長應設計適當的組織結構以支持 IT 戰略的實施。
- 資訊長必須以業務為導向，並在 IT 和業務之間架起橋樑。
- 業務主管應參與 IT 指導委員會或類似委員會。

另外，董事會應確保有效管理資源：

- 理解並應用 IT 系統和服務採購的職責。
- 具備適當的方法和足夠的技能來管理和支持 IT 計畫和系統。
- 改進人力規劃和投資，以確保招聘和留住熟練的 IT 員工。
- 促使所有員工充分識別風險並解決 IT 教育、培訓和發展需求。
- 提供適當的設施，並有時間讓員工發展他們所需的技能。
- 任何服務採購帶來的好處都是實際可行的。

最後談到 IT 風險評估和計劃，有效的 IT 風險管理計劃取決於：協調 IT 和業務目標的規劃流程;持續的風險評估過程，評估環境和潛在的變化;適當控制的技術實施程序; 和有效識別風險暴露管理方法的測量和監控工作。

參、心得及建議

本次參加 APEC 監理人員訓練倡議之「科技運作及風險管理研討會」，雖以研討會為名，實則以訓練課程方式進行，分別來自舊金山聯邦儲備銀行的 Patrick Prickett 及芝加哥聯邦儲備銀行的 Steve Galperin 的兩位講師，主要係依據聯邦金融機構檢查委員會(FFIEC)資訊安全 IT 檢查手冊重要內容講述，並分享其對銀行監理經驗，內容幾乎涵蓋金融機構資訊科技風險及管理的所有議題。於餐敘交流時，Patrick Pricket 君表示其目前負責轄區內多家我國銀行分子行之監理業務，對臺灣銀行業發展及相關政策相當孰悉，並表達希望能有機會來臺訪問。

本次研討會共有 9 個 APEC 國家及地區的中央銀行、存款保險公司及金融監理機關派員參加，共計 44 人，其中來自地主國菲律賓中央銀行及存款保險公司者即占 20 人，於交流時了解到菲律賓近三年經濟成長率維持在 6%~7%的水準，為促進金融包容性，金融業亦積極引入資訊技術之發展與應用，中央銀行並設有資訊科技專責部門負責相關監理及政策事項。

以下謹就本次會議探討之相關重要議題內容，研提心得與建議如下：

一、強化金融業對資訊安全管理之制度，提升董事會的重視與責任。

貫穿研討會各場次主題之一項基本觀念，即是由於資訊科技應用於金融業務之滲透性高，金融機構於面對此類風險管理時，強調董事會及高階管理層的應有充分的認知並承擔責任，透過制定明確的政策、制度與計畫，由上而下貫徹執行，各部門應協調一致，不能將資訊安全視為資訊部門專屬事項，各業務部門於執行日常業務或推展新業務時，均應完整考量資安風險，更重要的是相關的政策、制度與計畫必須定期檢討更新。

我國為提升銀行業對資訊安全之重視，金管會於 107 年 3 月 31 日修正發布「金融控股公司及銀行業內部控制及稽核制度實施辦法」，要求銀行業應設置資訊安全專責單位及主管，專門負責資訊安全相關工作或職務，並要求銀行業資訊安全專責單位應將資訊安全整體執行情形提報董(理)事會，並由資訊安全專責單位主管與董(理)事長(主席)、總經理、總稽核聯名出具資訊安全聲明書。前揭資訊安全整體執行情形之內容，至少應包括依據資訊安全防護機制與緊急應變計畫等執行情形，此外，在人員訓練及定期檢

討銀行公會訂定之資訊安全自律規範等方面，亦有明確要求。

二、落實金融市場資訊安全之資訊分享機制。

由於資安風險具動態變化快速的特性，尚未有任何有效方法可預為防範風險事件的發生，就降低及控制整體金融市場資安風險而言，建立金融資安資訊分享機制為較具可行性的方式。有鑒於此，金管會於 106 年 12 月 22 日成立「金融資安資訊分享與分析中心（F-ISAC）」，委請財金資訊公司營運，服務對象包含銀行、保險、證券期貨、投信投顧等各業別金融機構，提供通報、情資研判分析、資安資訊分享、協處資安諮詢與評估、研討會教育訓練及國際交流、協助資安事件應變處理、金融機構資安演練、協助資安規範評估與建議等 9 大服務功能。由於尚處於起步發展階段，仍須適時檢視執行成效。

三、透過對金融機構資訊安全進行完整的金融檢查，督促金融業落實相關風險之內控內稽

由於美國金融監理主管機關管轄體系多元，爰成立聯邦金融機構檢查委員會並訂定資訊安全 IT 檢查手冊[2]，以統一各監理機關進行金融檢查之原則與標準，也作為金融機構就資安建立風險管理、內控內稽及法遵等制度之依據，其內容甚具參考價值。

查金管會檢查局歷年檢查重點[3]，均包括資安風險相關項目，近年來其重要性及涵蓋面均有顯著提高之趨勢，以 108 年對銀行檢查重點為例，即包括：

- 數位金融業務之辦理情形：如提供網路銀行、線上申辦及行動支付等金融服務，對使用者個資或交易安全機制、身分確認、異常交易監控機制、行動應用程式(APP)開發及發布(含定期安全檢測)之管理機制。
- 資通安全管理：如資安專責單位與專責主管之設置及指派情形、資安整體執行情形之掌握及提報、ATM 及 SWIFT 等支付系統安全防護措施、總行對海外分行資安防護之監督管理、使用物聯網設備安全控管、

[2] https://ithandbook.ffiec.gov/

[3] https://www.feb.gov.tw/ch/home.jsp?id=65&parentpath=0,4

網路安全措施(如：防火牆、入侵偵測防禦、弱點掃描及滲透測試等資安防禦措施暨相關缺失之追蹤改善、網路攻擊事件監控、通報及應變機制、模擬駭客攻擊情境演練作業)、數位證據之蒐集、保留程序與機制、資訊系統備援機制與演練之有效性。

四、金融機構引進資訊科技應用，於善用科技優勢之同時，應兼顧金融監理原則與要求。

由於資通訊技術的進步與市場專業分工的發展，許多金融機構希望透過委外的方式引進新的資訊服務，一方面降低成本，一方面提升效率與服務品質。而基於金融主管機關的立場，必然鼓勵金融業善用科技，但也必須同時要求金融業相應地提升風險評估與管理。由於許多資訊技術的應用與服務範圍理論上是超越國界的，這便與金融監理管轄權的觀念有所不同，雲端運算即是一例。以美國的監理原則觀之，主管機關須對金融機構透過委外獲得雲端運算服務進行廣泛詳盡的檢查與要求，不會因所謂「技術中立」對監理原則有所不同。

五、金融科技的創新發展空間與金融環境的安全穩定並重。

論者對於金融科技有所謂「破壞式創新」的看法，然所破壞者應為欠缺效率的傳統金融實務，而非指可以破壞金融秩序。美國金融主管機關對於金融科技的創新發展，持較中立的立場，認為仍須視其所涉及金融活動的本質來決定監理的原則，尤應檢視其引進之資安風險。本會政策上支持負責任的創新，兼顧創新、安全、效率及消費者保護。

美國目前並無由金融監理機關建置的金融科技監理沙盒，但近期可能由舊金山聯邦儲備銀行啟動金融科技沙盒計畫，以彰顯對金融科技的支持。我國「金融科技發展與創新實驗條例」自 107 年 4 月 30 日生效，據以執行金融科技監理沙盒迄今有 3 個申請案進入沙盒進行實驗，未來可與美方增加金融科技方面的交流，參考其相關作法。

附件：研討會議程及資料